महाराष्ट्र राज्य तंत्रशिक्षण मंडळ, मुंबई
(स्वायत्त) (ISO 21001:2018) (ISO/IEC 27001:2013)

अभियांत्रिकी आणि तंत्रज्ञान पदविका

शिक्षण पुस्तिका
(Learning Material)

नेटवर्क अँड इन्फॉर्मेशन सेक्युरिटी

NETWORK AND INFORMATION SECURITY

(316317)

K-Scheme

संगणक अभियांत्रिकी गट
(के-स्कीम)

मराठी-इंग्रजी (द्विभाषिक) माध्यम
(अभियांत्रिकी व तंत्रज्ञानातील सहावे सत्र पदविका)

शिक्षण पुस्तिका

(Learning Material)

नेटवर्क अँड इन्फॉरमेशन सेक्युरिटी

NETWORK AND INFORMATION SECURITY

(316317)

संगणक अभियांत्रिकी गट

(के-स्कीम)

K-Scheme

मराठी-इंग्रजी (द्विभाषिक) माध्यम

(अभियांत्रिकी व तंत्रज्ञानातील सहावे सत्र पदविका)

महाराष्ट्र राज्य तंत्रशिक्षण मंडळ, मुंबई
(स्वायत्त)(ISO 21001:2018) (ISO/IEC 27001:2013)

नेटवर्क अँड इन्फॉरमेशन सेक्युरिटी

Network and Information Security

(316317)

मार्गदर्शक

श्री. विजय नामदेवराव कुकरे

विभागप्रमुख, संगणक अभियांत्रिकी

प्रकल्प समन्वयक

श्री. विजय नामदेवराव कुकरे

विभागप्रमुख, संगणक अभियांत्रिकी

संकलक

श्री. संतोष यादवराव दिवेकर

अधिव्याख्याता संगणक अभियांत्रिकी

सौ. हेमलता अजयकुमार शिंदे

अधिव्याख्याता संगणक अभियांत्रिकी

महाराष्ट्र राज्य तंत्र शिक्षण मंडळ.

(स्वायत्त) (ISO: २१००१:२०१८) (ISO/IEC: २७००१-२०१३)

शासकीय तंत्रनिकेतन इमारत, चौथा मजला, ४९, खेरवाडी, बांद्रा (पूर्व), मुंबई - ४०० ०५१.

दूरध्वनी क्र.: ०२२-६२५४२१०० / १५३ / १७०

email : director@msbte.com web site : www.msbte.ac.in

प्रास्ताविक

महाराष्ट्र राज्यातील पदविका स्तरावरील तंत्रशिक्षणामध्ये विद्यार्थ्यांचे रोजगार कौशल्य विकसित करून विद्यार्थ्यांचा सर्वांगीण विकास घडवून आणण्याकरिता महाराष्ट्र राज्य तंत्रशिक्षण मंडळ कटिबद्ध आहे. उद्योगधंद्यातील बदलत्या तंत्रज्ञानाशी संबंधित गरजा लक्षात घेऊन महाराष्ट्र राज्य तंत्र शिक्षण मंडळाकडून पदविका अभ्यासक्रम वेळोवेळी अद्यावत करण्यात येतो. अभियांत्रिकी पदविका अभ्यासक्रम शिकत असताना संकल्पनात्मक ज्ञान, सुसंगत संदर्भ, प्रश्न विचारणे, विश्वसनीय पुरावे, कारणमीमांसा आणि सुस्पष्ट निकष यांचा वापर करून अर्थाची उकल करण्याची, विश्लेषण व मूल्यमापन करण्याची तसेच तर्काने अनुमान काढण्याची क्षमता म्हणजेच चिकित्सक विचार विद्यार्थ्यांमध्ये अधिक दृढ होतील असा मला विश्वास आहे. जेव्हा विद्यार्थी ज्ञान मिळवण्याच्या माध्यमाशी पूर्णपणे परिचित आणि सोयीस्कर असतात, तेव्हा त्यांच्यासाठी वर्गातील चर्चेत भाग घेणे सोपे होते, संकल्पनात्मक व सैद्धांतिक बाबींचे आकलन परिपूर्ण होते, संज्ञानात्मक क्षमता सुधारते आणि त्यांचा आत्मविश्वास देखील वाढतो. या सर्व गोष्टींचा विचार करून मंडळाकडून शैक्षणिक सामुग्रीची निर्मिती करण्यात आलेली आहे. भारत देश हा खेड्यापाडयातून विकसित झालेला देश असून ग्रामीण भागातील विद्यार्थ्यांना तांत्रिक शिक्षण घेताना भाषेचा अडसर न येता तांत्रिक बाबींचा आशय समजून घेणे शक्य होईल या दृष्टिकोनातून महाराष्ट्र राज्य तंत्र शिक्षण मंडळाने पदविका स्तरावरील तांत्रिक शिक्षणाकरीता विद्यार्थ्यांना मराठी-इंग्रजी द्विभाषिक माध्यमाचा पर्याय उपलब्ध करुन दिलेला आहे.

राष्ट्रीय शैक्षणिक धोरण-२०२० प्रादेशिक भाषेतील शिक्षणास प्रोत्साहन देते, ज्यामुळे विद्यार्थ्यांना तांत्रिक अभ्यासक्रमांसाठी प्रादेशिक भाषेतुन शिक्षणाचे माध्यम निवडता येते. त्या अनुषंगाने प्रादेशिक भाषांमध्ये तांत्रिक सामग्री आणि अभ्यास सामग्रीचा विकास आणि भाषांतर करण्याची आवश्यकता आहे. या धोरणास अनुसरुन मंडळाने भागधारकांसाठी शैक्षणिक वर्ष २०२१-२२ पासून I-Scheme तसेच शैक्षणिक वर्ष २०२३-२४ पासून K-Scheme मध्ये व्दिभाषिक माध्यमाचा पर्याय प्रथम ते तृतीय वर्षाकरिता उपलब्ध करून दिलेला आहे. या पर्यायास अनुसरून मंडळाने मराठी-इंग्रजी द्विभाषिक शैक्षणिक सामग्रीही संबंधीत विद्यार्थी व अधिव्याख्यातांकरिता उपलब्ध करून दिली आहे.

पदविका स्तरावरील तंत्रशिक्षण अधिक दर्जेदार करण्यासाठी महाराष्ट्रातील अनुभवी व तज्ञ अध्यापकांनी व्यवहारिक मराठी भाषा व इंग्रजी भाषेतील तांत्रिक शब्दावली यांचा वापर करून मराठी इंग्रजी भाषेचा सुवर्णमध्य साधण्याचा प्रयत्न केलेला आहे. मंडळाच्या स्तरावर गठीत सुकाणू समितीमार्फत सदर शैक्षणिक सामुग्रीचा दर्जा, तसेच इतर बाबींची तपासणी करण्यात आलेली आहे. त्यामुळे सदर शैक्षणिक सामुग्री अधिक संपन्न झालेली असून,विद्यार्थी त्यांच्या व्यक्तिमत्त्वाचा सुसंवादी आणि सर्वांगीण विकास साधतील. परिणामतः विश्वस्तरीय मनुष्यबळाच्या गरजा पूर्ण करण्यात महाराष्ट्र राज्य अग्रेसर राहील व पर्यायाने राष्ट्रनिर्मिती करीता निश्चितच हातभार लागेल, असा मला विश्वास आहे.

अभियांत्रिकी पदविका अभ्यासक्रमातील विषयांची मराठी-इंग्रजी (द्विभाषिक) शैक्षणिक सामुग्री बनविण्यासाठी अध्यापक व सुकाणू समितीचे सदस्य यांनी दर्शविलेले समर्पण व वचनबद्धता कौतुकास पात्र आहे, या सर्वांचे मी मनःपूर्वक अभिनंदन करतो!

(डॉ. प्रमोद नाईक)
संचालक
म. रा. तंत्र शिक्षण मंडळ, मुंबई

अनुक्रमणिका

युनिट-1
इंट्रोडक्शन टू कॉम्प्युटर अँड इन्फॉरमेशन सेक्युरिटी
(Introduction to Computer and Information Security)

विषय निष्पत्ती (Course Outcome):

CO1: सायबर-हल्ल्यांचे व धोके (Cyber-attacks and Threats) यांचे प्रकार ओळखा.

घटक निष्पत्ती (Theory Learning Outcome):

1. इन्फॉरमेशन सेक्युरिटी ची गरज स्पष्ट करा.
2. इन्फॉरमेशन क्लासिफिकेशन साठी निकष लिहा.
3. विविध प्रकारचे अटॅक्स ओळखा.
4. मालवेअर चे प्रकार लिहा.
5. ऑपरेटिंग सिस्टिम अपडेट्स चे महत्त्व स्पष्ट करा.
6. थ्रेट, व्हल्नरेबिलिटी आणि रिस्क यांतील संबंध योग्य उदाहरणासह स्पष्ट करा.

1.1 कम्प्युटर सेक्युरिटी ची पायाभूत तत्त्वे (Foundations of computer security)

1.1.1 कम्प्युटर सेक्युरिटी ची डेफिनिशन आणि गरज (Definition and Need of Computer Security)

कम्प्युटर सेक्युरिटी म्हणजे कम्प्युटर सिस्टिम्स, नेटवर्क्स आणि डेटा यांना अनऑथराइज्ड ॲक्सेस, मॉडिफिकेशन, डिस्रप्शन किंवा डीस्ट्रक्शन पासून संरक्षित करण्यासाठी वापरल्या जाणाऱ्या टेक्निक्स आणि मेकॅनिझम्स. सोप्या भाषेत सांगायचे तर, कम्प्युटर सेक्युरिटी डिजिटल ॲसेट्सना हॅकिंग, मालवेअर किंवा मिसयुज सारख्या सायबर थ्रेट्स पासून सुरक्षित ठेवते. कम्प्युटर सेक्युरिटीचा मुख्य उद्देश म्हणजे इन्फॉरमेशन ॲसेट्सचे संरक्षण करणे. हे त्यांच्या कॉन्फिडेन्शियलिटी, इंटेग्रिटी आणि अव्हेलेबिलिटी कायम ठेवून साध्य केले जाते. यासाठी योग्य सेक्युरिटी पॉलिसीज आणि टेक्नॉलॉजीजचा वापर केला जातो.

कम्प्युटर सेक्युरिटी ची गरज (Need of Computer Security)

इंटरनेटचा वेगाने वाढणारा वापर, ई-कॉमर्स, ऑनलाइन बँकिंग, क्लाऊड सर्व्हिसेस आणि सोशल नेटवर्किंग यामुळे कम्प्युटर सिस्टिम्सवर हॅकिंग, मालवेअर, फिशिंग आणि डिनायल-ऑफ-सर्व्हिस सारखे अनेक रिस्क्स वाढत आहेत. म्हणूनच कम्प्युटर सेक्युरिटीची गरज व्यक्ती, व्यवसाय आणि सरकारी संस्थांसाठी अत्यंत महत्त्वाची बनली आहे.

1. **सेंसेटिव्ह डेटा चे प्रोटेक्शन (Protection of Sensitive Data):** कम्प्युटर सेक्युरिटी संवेदनशील वैयक्तिक, आर्थिक आणि संस्थात्मक डेटाला चोरी किंवा मिसयुज पासून सुरक्षित ठेवते.
   उदाहरण: आधार (Aadhaar) किंवा क्रेडिट कार्ड माहिती सायबर क्रिमिनल्स पासून सुरक्षित ठेवणे.
2. **कॉन्फिडेन्शियलिटी (Confidentiality):** महत्त्वाच्या माहितीला फक्त ऑथराइज्ड युजर्सलाच ॲक्सेस मिळेल याची खात्री करते.
   उदाहरण: हॉस्पिटलमध्ये पेशंटच्या मेडिकल रिपोर्ट्सचे संरक्षण.
3. **इंटेग्रिटी (Integrity):** अनऑथराइज्ड मॉडिफिकेशन रोखून डेटाची अचूकता आणि सातत्य कायम ठेवते.
   उदाहरण: हॅकर्सना बँक अकाउंट बॅलन्स बदलण्यापासून रोखणे.
4. **अव्हेलेबिलिटी (Availability):** सिस्टिम्स, ॲप्लिकेशन्स आणि सर्व्हिसेस अधिकृत युजर्ससाठी नेहमी उपलब्ध राहतील याची खात्री करते.
   उदाहरण: ई-कॉमर्स वेबसाइट्सनी जास्त ट्रॅफिकमध्येही 24/7 उपलब्ध राहिले पाहिजे.
5. **अथेन्टिकेशन (Authentication):** ॲक्सेस देण्यापूर्वी युजरची ओळख (Identity) स्थापित करते.
   उदाहरण: ऑनलाइन बँकिंगमध्ये टू-फॅक्टर ऑथेन्टिकेशन (पासवर्ड + OTP).
6. **अकाउंटेबिलिटी (Accountability):** युजरच्या सर्व क्रियांची नोंद ठेवते जेणेकरून कृती ट्रेस करता येतील.
   उदाहरण: कंपनी नेटवर्कमध्ये फेल्ड लॉगिन अटेम्प्ट्सचे लॉग्स ठेवणे.
7. **नॉन-रिप्युडिएशन (Non-repudiation):** युजरने केलेली कृती नंतर नाकारता येऊ नये याची खात्री करते.
   उदाहरण: फंड ट्रान्स्फरमध्ये डिजिटल सिग्नेचरमुळे सेंडर ट्रान्सॅक्शन नाकारू शकत नाही.

8. **सायबर लॉज आणि स्टँडर्ड्सचे पालन (Compliance with Cyber Laws and Standards):** संस्थांनी राष्ट्रीय आणि आंतरराष्ट्रीय सेक्युरिटी स्टँडर्ड्सचे पालन करणे आवश्यक असते, जसे IT Act 2000, PCI DSS, HIPAA इत्यादी.
   उदाहरण: भारतातील बँकांनी RBI च्या सायबर सेक्युरिटी मार्गदर्शक तत्त्वांचे पालन करणे आवश्यक आहे.
9. **बिझनेस कॉन्टीन्युइटी (Business Continuity):** सेक्युरिटीमुळे सायबर हल्ले किंवा सिस्टिम फेल्युअर झाल्यासही बिझनेस ऑपरेशन्स व्यवस्थित सुरू राहतात.
   उदाहरण: क्लाऊड सर्व्हिस प्रोव्हायडर्स बॅकअप आणि रेडंडन्सी वापरतात ज्यामुळे सेवा खंडित होत नाही.
10. **प्रतिष्ठा आणि विश्वास (Reputation and Trust):** मजबूत सेक्युरिटीमुळे ग्राहक, कर्मचारी आणि बिझनेस पार्टनर्समध्ये विश्वास निर्माण होतो.
    उदाहरण: सुरक्षित पेमेंट गेटवे मुळे ऑनलाइन शॉपिंग साइट्सवरील ग्राहकांचा विश्वास वाढतो.

1.1.2 सेक्युरिटी बेसिक्स / प्रिन्सिपल्स ऑफ सेक्युरिटी (Security Basics /Principles of Security):

कम्प्युटर सेक्युरिटी ही सेक्युरिटी बेसिक्स किंवा गोल्स ऑफ सेक्युरिटी म्हणून ओळखल्या जाणाऱ्या काही प्रिन्सिपल्सवर आधारित असते. या प्रिन्सिपल्समुळे माहिती आणि सिस्टिम्स ऑथराइज्ड युजर्ससाठी सुरक्षित, अचूक आणि रिलायबल राहतात. यामधील सर्वात महत्त्वाचे प्रिन्सिपल्स म्हणजे: कॉन्फिडेन्शियलिटी, इंटेग्रिटी, अव्हेलेबिलिटी, अकाउंटेबिलिटी, अथेन्टिकेशन, नॉन-रिप्युडिएशन आणि रिलायबिलिटी.

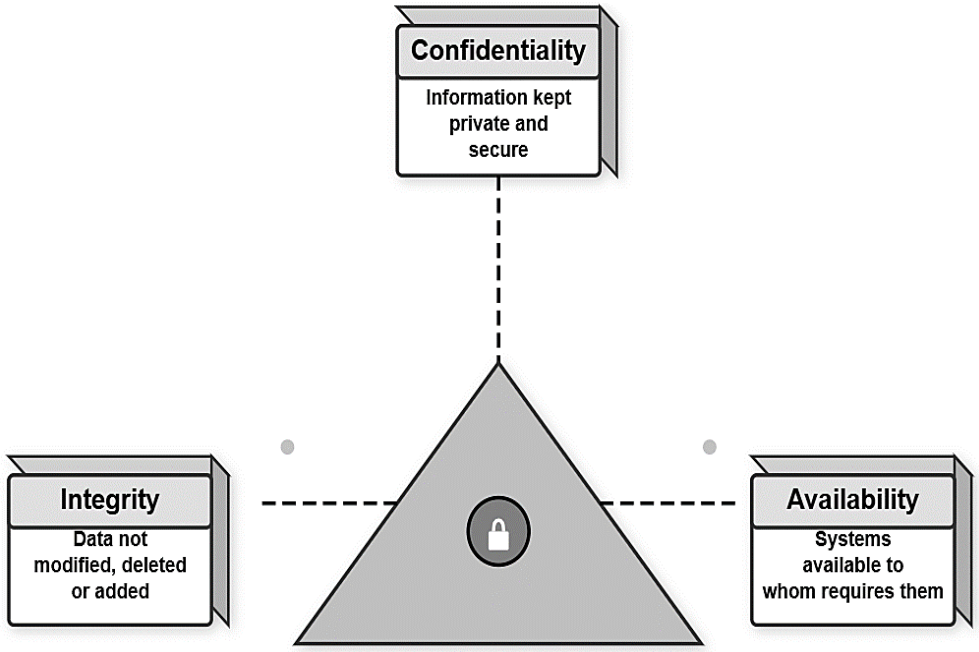


Fig 1.1: CIA ट्रायड इन्फॉरमेशन सेक्युरिटी मॉडेल (CIA Triad Information Security Model)

वरील CIA ट्रायड दर्शवतो, जो इन्फॉरमेशन सेक्युरिटीचा कोअर मॉडेल आहे. यात तीन मुख्य प्रिन्सिपल्स दाखवले आहेत: कॉन्फिडेन्शियलिटी, इंटेग्रिटी आणि अव्हेलेबिलिटी. कॉन्फिडेन्शियलिटी म्हणजे माहिती प्रायव्हेट आणि अनऑथराइज्ड ॲक्सेसपासून सुरक्षित ठेवणे. इंटेग्रिटी म्हणजे डेटा अनऑथराइज्ड पद्धतीने बदलला, डिलीट केला किंवा ॲड केला जाऊ नये, म्हणजेच डेटा अचूक आणि ट्रस्टवर्धी राहावा. अव्हेलेबिलिटी म्हणजे सिस्टिम्स आणि माहिती ऑथराइज्ड युजर्सना आवश्यक वेळी उपलब्ध राहावी. ही तीनही एलिमेंट्स मिळून इन्फॉरमेशन सेक्युरिटीची पायाभरणी करतात, ज्यामुळे प्रोटेक्शन, रिलायबिलिटी आणि ॲक्सेसिबिलिटी यांचा समतोल राखला जातो.

1. कॉन्फिडेन्शियलिटी (Confidentiality)

"कॉन्फिडेन्शियलिटी हे सुनिश्चित करते की माहिती अनधिकृत व्यक्ती, प्रक्रिया किंवा उपकरणांना उघड केली जाणार नाही."

कॉन्फिडेन्शियलिटी म्हणजे सेंसेटिव्ह डेटाची सिक्रीसी जपणे आणि ॲक्सेस फक्त ऑथराइज्ड युजर्सपुरता मर्यादित ठेवणे. हे एनक्रिप्शन, स्ट्राँग ॲक्सेस कंट्रोल्स आणि सिक्युर कम्युनिकेशन प्रोटोकॉल्सद्वारे साध्य केले जाते. मॉडर्न सिस्टिम्समध्ये,

विशेषतः बँकिंग, हेल्थकेअर आणि क्लाऊड एन्व्हायर्नमेंट्समध्ये कॉन्फिडेन्शियलिटी प्रायव्हसीसाठी अत्यंत महत्त्वाची आहे. याचे उल्लंघन झाल्यास आयडेंटिटी थेफ्ट, फायनान्शियल फ्रॉड किंवा कॉर्पोरेट गुप्तहेरी होऊ शकते.

उदाहरण: ई-बँकिंगमध्ये कस्टमरचे PINs आणि लॉगिन क्रेडेन्शियल्स हे एनक्रिप्ट केलेले असतात, ज्यामुळे हॅकर्सना ते ॲक्सेस करता येत नाहीत.

कॉन्फिडेन्शियलिटी हरवणे (Loss of Confidentiality):

Fig 1.2: कॉन्फिडेन्शियलिटी हरवणे (Loss of Confidentiality)

दोन वैध (legitimate) युजर्स एकमेकांमध्ये गोपनीय माहितीची देवाणघेवाण करत आहेत. एक अटॅकर स्निफिंगद्वारे ही कम्युनिकेशन गुपचूप इंटरसेप्ट करतो आणि डेटाला अनधिकृत ॲक्सेस मिळवतो. कारण अटॅकर आता प्रायव्हेट माहिती वाचू किंवा चोरू शकतो, त्यामुळे सिस्टिममध्ये कॉन्फिडेन्शियलिटीचा तोटा (Loss of Confidentiality) होतो.

2. इंटेग्रिटी (Integrity)

"इंटेग्रिटी म्हणजे माहितीमध्ये अयोग्य बदल किंवा नाश होऊ नये याची काळजी घेणे आणि माहितीची प्रामाणिकता (authenticity) सुनिश्चित करणे."

इंटेग्रिटी याची खात्री करते की डेटा अचूक, पूर्ण आणि विश्वासार्ह राहतो. डेटा मध्ये बदल करण्याची परवानगी फक्त ऑथराइज्ड युजर्सनाच असते. डेटा टॅम्परिंग ओळखण्यासाठी हॅशिंग (hashing), चेकसम्स (checksums) आणि डिजिटल सिग्नेचर्स (digital signatures) सारख्या तंत्रांचा वापर केला जातो. इंटेग्रिटी आर्थिक व्यवहार, हेल्थकेअर रेकॉर्ड्स आणि लीगल डेटाबेसमध्ये अत्यंत महत्त्वाची आहे, कारण अगदी छोटासा बदलही गंभीर परिणाम करू शकतो.

उदाहरण: ₹500 चा ऑनलाइन पेमेंट अटॅकरने बदलून ₹5000 होऊ नये. हॅश फंक्शन्स (Hash functions) अशा बदलांना (tampering) रोखतात किंवा ओळखतात.

इंटेग्रिटीचा तोटा (Loss of Integrity):

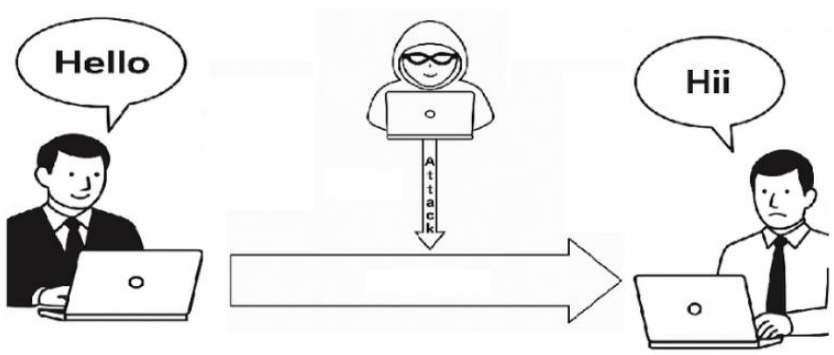


Fig 1.3: इंटेग्रिटीचा तोटा (Loss of Integrity)

सेंडर "Hello" हा मेसेज पाठवतो, परंतु एक अटॅकर कम्युनिकेशनमध्ये हस्तक्षेप (tamper) करतो. रिसिव्हरपर्यंत पोहोचेपर्यंत मेसेज बदलून "Hii" असा होतो. हे इंटेग्रिटीचा तोटा (Loss of Integrity) दर्शवते, कारण मूळ मेसेज ट्रान्झिटमध्ये बदलला गेला असून तो सेंडरच्या खऱ्या हेतूचे प्रतिनिधित्व करत नाही.

3. अव्हेलेबिलिटी (Availability)

"अव्हेलेबिलिटी हे सुनिश्चित करते की अधिकृत वापरकर्त्यांना माहिती आणि संसाधने योग्य वेळी आणि विश्वासार्हपणे उपलब्ध राहतील."

अव्हेलेबिलिटी याची खात्री करते की माहिती आणि सेवा आवश्यक वेळी नेहमी उपलब्ध राहतील. डिनायल-ऑफ-सर्व्हिस (Denial-of-Service (DoS)) अटॅक्स (attacks), पॉवर फेल्युअर्स किंवा नैसर्गिक आपत्तींसारखे थ्रेट्स ॲक्सेस ब्लॉक करू शकतात. अव्हेलेबिलिटी साध्य करण्यासाठी बॅकअप सर्व्हर्स (backup servers), रेडंडन्सी (redundancy), फॉल्ट-टोलरंट सिस्टिम्स (fault-tolerant systems) आणि लोड बॅलन्सिंग (load balancing) वापरले जाते. बँकिंग, हेल्थकेअर आणि ई-कॉमर्स सारख्या अत्यावश्यक सेवांसाठी downtime मोठे आर्थिक नुकसान करू शकतो.

उदाहरण: Amazon अनेक डेटा सेंटर्सचा वापर करते, ज्यामुळे त्याच्या सेवा जागतिक स्तरावर निरंतरपणे उपलब्ध राहतात.

अव्हेलेबिलिटीचा तोटा (Loss of Availability):

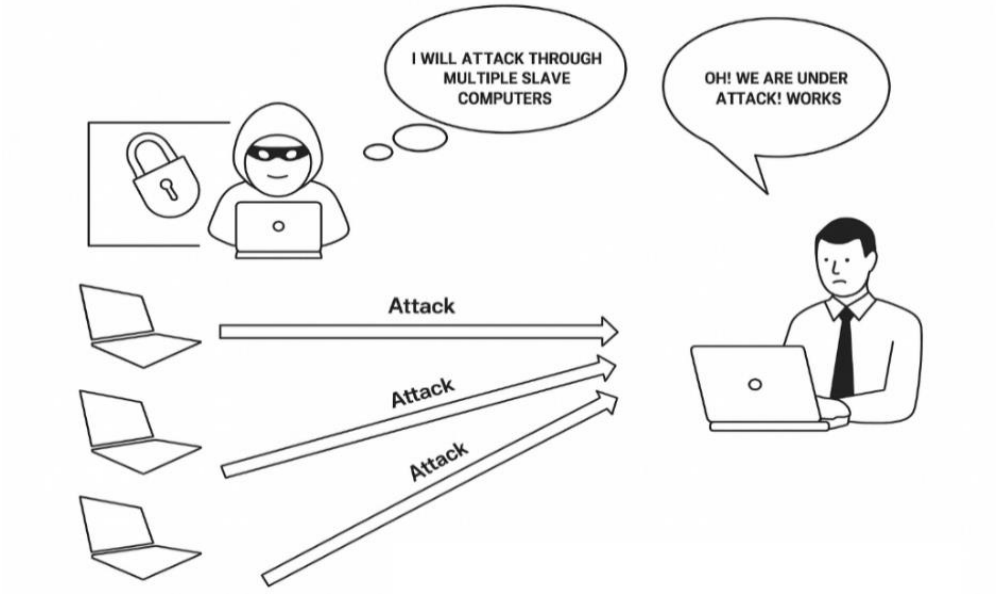


Fig 1.4: अव्हेलेबिलिटीचा तोटा (Loss of Availability)

जिथे अटॅकर अनेक कम्प्रमाइज्ड मशिन्स वापरून नॉर्मल सर्व्हिसमध्ये व्यत्यय आणतो, ज्यामुळे वैध (legitimate) युजर्सना आवश्यक संसाधनांना ॲक्सेस करता येत नाही.

4. अकाउंटेबिलिटी (Accountability)

"अकाउंटेबिलिटी म्हणजे एखाद्या घटकाने (entity) केलेली कृती त्या घटकापर्यंत स्पष्टपणे ट्रेस करता येण्याची क्षमता."

अकाउंटेबिलिटीमुळे सिस्टिममध्ये पारदर्शकता (transparency) आणि जबाबदारी (responsibility) सुनिश्चित होते. प्रत्येक कृती कोणत्या व्यक्तीने केली हे लिंक केले जाते. ऑडिट लॉग्स (Audit logs), मॉनिटरिंग सिस्टिम्स (monitoring systems) आणि इंट्रूजन डिटेक्शन टूल्स (intrusion detection tools) च्या मदतीने अकाउंटेबिलिटी लागू केली जाते.

अकाउंटेबिलिटीमुळे केवळ मालिशियस ॲक्टिव्हिटी शोधता येते असे नाही, तर पॉलिसीज आणि रेग्युलेशन्स चे पालन देखील सुनिश्चित होते. संस्थांमध्ये शिस्त, सुरक्षा-जागरूकता आणि जबाबदारी निर्माण करण्यासाठी हे अत्यंत महत्त्वाचे आहे.

उदाहरण: फेल्ड लॉगिन अटेम्प्ट्स सिस्टिम लॉग्समध्ये timestamps आणि IP addresses सह साठवले जातात, ज्यामुळे पुढील इन्व्हेस्टिगेशनसाठी उपयोग होतो.

अकाउंटेबिलिटीचा तोटा (Loss of Accountability):

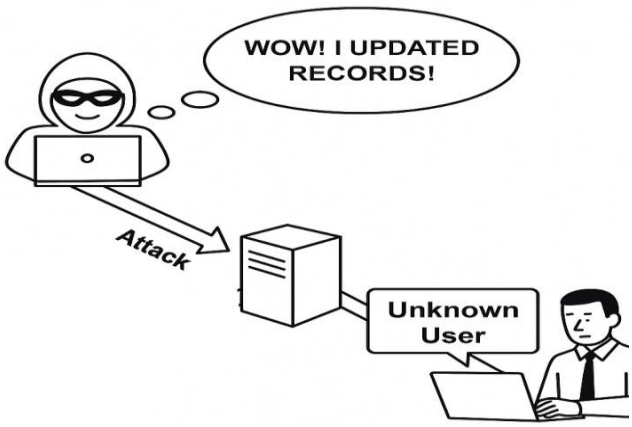


Fig 1.5: अकाउंटेबिलिटीचा तोटा (Loss of Accountability)

जिथे अटॅकर सर्व्हरवरील रेकॉर्ड्स अपडेट करतो, परंतु सिस्टिम त्या कृतीला खऱ्या युजरपर्यंत ट्रेस करू शकत नाही. त्याऐवजी वैध (legitimate) युजर्सना "Unknown User" असे दिसते. हे दाखवते की योग्य किंवा मजबूत लॉगिंग/ऑडिट मेकॅनिझम नसल्यामुळे जबाबदार घटक (responsible entity) ओळखणे अशक्य होते.

5. अथेन्टिकेशन (Authentication)

"अथेन्टिकेशन म्हणजे युजर, प्रोसेस किंवा डिव्हाइसची ओळख (identity) सत्यापित करण्याची प्रक्रिया."

अथेन्टिकेशन याची खात्री करते की फक्त वैध (legitimate) युजर्सनाच संसाधनांना (resources) ॲक्सेस मिळेल. हे पुढील तीन घटकांवर आधारित असते:

• तुम्हाला माहिती असलेली गोष्ट (Something you know) – उदा. पासवर्ड, PIN

• तुमच्याकडे असलेली गोष्ट (Something you have) – उदा. स्मार्ट कार्ड, OTP टोकन

• तुम्ही स्वतः आहात ती ओळख (Something you are) – उदा. बायोमेट्रिक्स (फिंगरप्रिंट (fingerprint), आयरिस (iris), फेस स्कॅन (face scan).

मल्टी-फॅक्टर ऑथेंटिकेशन (Multi-factor Authentication (MFA)) मध्ये दोन किंवा अधिक पद्धती एकत्र वापरल्या जातात, ज्यामुळे सेक्युरिटी अधिक मजबूत होते.

उदाहरण: ATM मध्ये डेबिट कार्ड (something you have) आणि PIN (something you know) दोन्ही आवश्यक असतात.

अथेन्टिकेशनचा तोटा (Loss of Authentication):

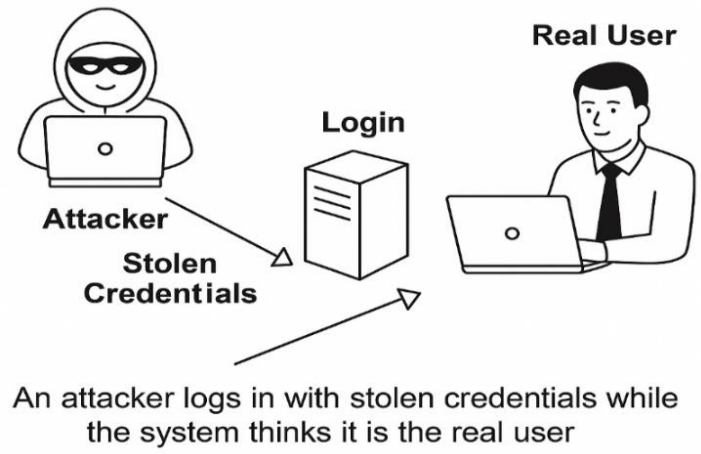


Fig 1.6: अथेन्टिकेशनचा तोटा (Loss of Authentication)

जिथे अटॅकर चोरी केलेली क्रेडेन्शियल्स वापरून सिस्टिममध्ये लॉगिन करतो. सिस्टिम अटॅकर आणि खरा युजर यांच्यातील फरक ओळखण्यात अपयशी ठरते आणि अटॅकरला वैध युजर असल्याप्रमाणे ॲक्सेस देते. हे दर्शवते की कमकुवत अथेन्टिकेशन किंवा कम्प्रमाइज्ड क्रेडेन्शियल्समुळे अनऑथराइज्ड ॲक्सेस होऊ शकतो.

6. नॉन-रिप्युडिएशन (Non-repudiation)

"नॉन-रिप्युडिएशन हे सुनिश्चित करते की डेटा पाठवणारा किंवा प्राप्त करणारा व्यक्ती डेटा पाठवला किंवा मिळवला याचा इन्कार करू शकत नाही."

नॉन-रिप्युडिएशन कम्युनिकेशन किंवा ट्रान्झॅक्शनचा इन्कार होऊ नये याची खात्री करते. हे डिजिटल सिग्नेचर्स, PKI सर्टिफिकेट्स आणि सिक्युर लॉग्सच्या मदतीने ओरिजिन (origin), डिलिव्हरी (delivery) आणि इंटेग्रिटी (integrity) चे पुरावे प्रदान करते. लीगल, बँकिंग आणि ई-कॉमर्स ॲप्लिकेशन्स सारख्या मध्ये हे प्रिन्सिपल अत्यंत महत्त्वाचे आहे, कारण ऑनलाइन केलेल्या कृतींवर वाद निर्माण होऊ शकतात.

उदाहरण: ऑनलाइन बँकिंगमध्ये, एखादे ट्रान्झॅक्शन डिजिटल सिग्नेचरद्वारे प्रमाणित (sign) झाल्यानंतर, सेंडर त्याने ते केले नाही असा दावा करू शकत नाही.

नॉन-रिप्युडिएशनचा तोटा (Loss of Non-repudiation):

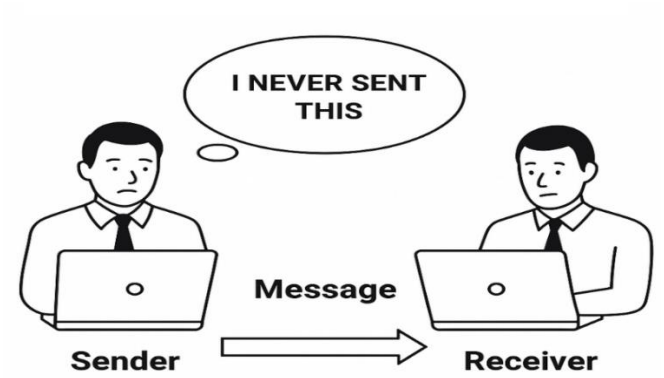


Fig 1.7: नॉन-रिप्युडिएशनचा तोटा (Loss of Non-repudiation)

जिथे सेंडर रिसिव्हरला मेसेज पाठवतो, परंतु नंतर "मी हा मेसेज पाठवलेलाच नाही" असा दावा करतो. डिजिटल पुरावे (उदा. सिग्नेचर्स किंवा लॉग्स) नसल्यामुळे रिसिव्हर सेंडरची जबाबदारी सिद्ध करू शकत नाही, ज्यामुळे कृतीचा इन्कार होतो आणि जबाबदारी निश्चित करता येत नाही.

7. रिलायबिलिटी (Reliability)

"रिलायबिलिटी म्हणजे सिस्टिमने दिलेल्या स्थितींमध्ये सातत्याने आणि योग्यरित्या आपली अपेक्षित कार्ये पार पाडण्याची क्षमता."

रिलायबिलिटी याची खात्री करते की सिस्टिम योग्य, सातत्यपूर्ण आणि प्रेडिक्टेबल पद्धतीने कार्य करते. सिस्टिमवर ताण (stress), फेल्युअर्स किंवा सायबर अटॅक्स आले तरीही एक रिलायबल सिस्टिम अनपेक्षित चुका न करता कार्यरत राहते. रिलायबिलिटी फॉल्ट-टोलरंट डिझाइन, रेडंडन्सी, सिस्टम अपडेट्स आणि मजबूत मॉनिटरिंगद्वारे साध्य केली जाते. टेलिकॉम, एअरोस्पेस आणि हेल्थकेअर सारख्या मिशन-क्रिटिकल ॲप्लिकेशन्स मध्ये रिलायबिलिटी अत्यंत महत्त्वाची असते.

उदाहरण: टेलिकॉम नेटवर्क्स पीक तासांमध्ये किंवा आपत्कालीन परिस्थितीतही सातत्यपूर्ण आणि विश्वासार्ह सेवा प्रदान करतात.

रिलायबिलिटीचा तोटा (Loss of Reliability):

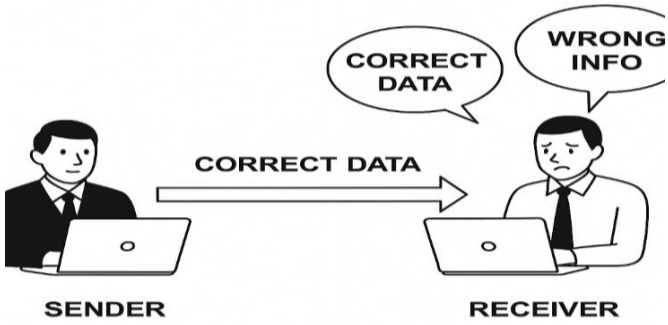


Fig 1.8: रिलायबिलिटीचा तोटा (Loss of Reliability)

जिथे सेंडर बरोबर डेटा पाठवतो, पण रिसिव्हरला कधीकधी योग्य माहिती मिळते आणि कधीकधी चुकीची. ही असंगतता (inconsistency) सिस्टिमला अविश्वासू बनवते, कारण सिस्टिमवर प्रत्येक वेळी अचूक परिणाम देण्यासाठी विसंबून राहता येत नाही.

1.2 इन्फॉर्मेशन सिक्युरिटीची ओळख (Information Security Overview)

1.2.1 इन्फॉर्मेशनची ओळख (Introduction to information)

माहिती (Information) म्हणजे प्रक्रियित (processed) आणि अर्थपूर्ण डेटा, जो संस्थेमध्ये निर्णय घेणे, संवाद साधणे आणि नियंत्रण ठेवणे यासाठी उपयोगी ठरतो. कच्चा डेटा (Raw Data) हा फक्त तथ्ये किंवा आकडे (figures) यांचा अव्यवस्थित संच असू शकतो, ज्यामध्ये परस्पर संबंध नसतो. परंतु माहिती ही व्यवस्थितपणे मांडलेली, संरचित (structured) आणि संदर्भासहित (contextualized) असल्यामुळे ती वापरकर्त्यांसाठी उपयुक्त ठरते.

माहिती प्रणाली (Information Systems) आणि माहिती सुरक्षा (Information Security) यांच्या संदर्भात, माहिती ही पैशाप्रमाणे किंवा यंत्रसामग्रीप्रमाणे एक मौल्यवान संसाधन मानली जाते. कारण:

1. निर्णय घेण्यात मदत: संस्थेच्या सर्व स्तरांवर योग्य आणि वेळेवर निर्णय घेण्यासाठी माहिती अत्यंत महत्वाची असते.
2. प्रभावी संवाद सुनिश्चित करते: कर्मचारी, व्यवस्थापन, ग्राहक आणि इतर हितधारकांमध्ये स्पष्ट आणि प्रभावी संवाद साधण्यासाठी माहिती आवश्यक असते.
3. व्यवसाय सातत्य आणि वाढ सुनिश्चित करते: व्यवसाय सुरळीत चालू राहण्यासाठी आणि वाढीसाठी माहिती आवश्यक असते.
4. माहितीचा जीवनचक्र (Life Cycle) असतो: माहिती निर्माण → साठवण → वापर → शेअरिंग → नष्ट करणे या सर्व टप्प्यांमध्ये माहितीची काळजी घेणे आवश्यक असते.

माहिती अत्यंत मौल्यवान असल्यामुळे तिला अनधिकृत प्रवेश, बदल किंवा नष्ट होण्यापासून सुरक्षित ठेवणे आवश्यक आहे. या संरक्षण प्रक्रियेची पायाभरणी म्हणजेच माहिती सुरक्षा (Information Security).

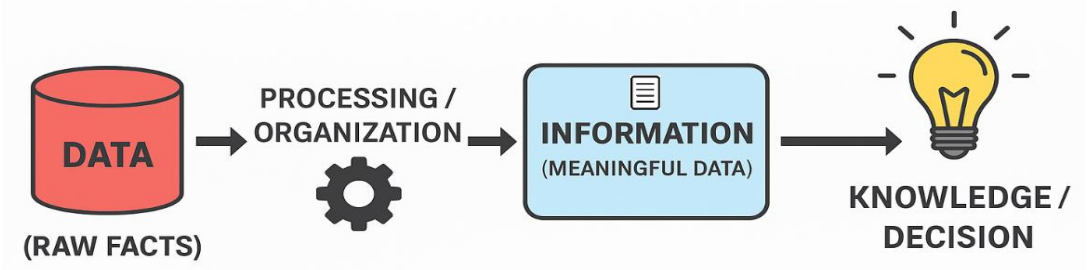


Fig 1.9: डेटाचे माहितीमध्ये / ज्ञानामध्ये रूपांतर (Transformation of Data into Information / Knowledge)

डेटाचे ज्ञानामध्ये रूपांतर कसे होते हे दाखवले आहे. सुरुवात कच्च्या डेटापासून (फॅक्ट्स) होते. हा डेटा प्रक्रिया करून आणि व्यवस्थित मांडून माहिती (अर्थपूर्ण डेटा) तयार केली जाते. पुढे या माहितीचे विश्लेषण करून आणि प्रत्यक्षात वापरून ज्ञान (Knowledge) किंवा निर्णय तयार होतात. अशाप्रकारे डेटा हळूहळू विकसित होत जाऊन उपयोगी आणि कृतीयोग्य (actionable) माहितीमध्ये रूपांतरित होतो.

1.2.2 इन्फॉरमेशन सेक्युरिटीची गरज आणि महत्त्व (Need and importance of information security)

माहिती सुरक्षेची गरज (Need for Information Security):

1. कॉन्फिडेन्शियलिटी / गोपनीयता (Confidentiality)- संवेदनशील माहिती अनधिकृत वापरकर्त्यांपासून लपवून ठेवण्यासाठी (उदा. वैयक्तिक माहिती, पासवर्ड).
2. इंटेग्रिटी / अखंडता (Integrity) – डेटामध्ये अनधिकृत बदल होऊ नयेत आणि माहिती अचूक राहावी यासाठी.
3. अव्हेलेबिलिटी / उपलब्धता (Availability) – अधिकृत वापरकर्त्यांना आवश्यक वेळी डेटा आणि सेवा उपलब्ध राहण्यासाठी.
4. ऑथेंटिकेशन / ओळखपट्टी (Authentication) – माहितीमध्ये प्रवेश करणाऱ्या वापरकर्त्यांची ओळख तपासण्यासाठी.
5. रेग्युलेटरी कॉम्प्लायन्स / नियमांचे पालन (Regulatory Compliance) – PCI DSS, ISO 27001, GDPR यांसारख्या कायदेशीर आणि औद्योगिक मानकांचे पालन करण्यासाठी.

6. बिझनेस कंटिन्युइटी / व्यवसाय सातत्य (Business Continuity) – हल्ले किंवा सिस्टिम बिघाडाच्या वेळीही कामकाज सुरळीत सुरू ठेवण्यासाठी.

माहिती सुरक्षेचे महत्त्व (Importance of Information Security):

1. संवेदनशील माहितीचे संरक्षण – वैयक्तिक, आर्थिक किंवा व्यवसायासाठी महत्त्वपूर्ण माहिती अनधिकृत उघड होण्यापासून वाचते.
2. विश्वास टिकवणे – ग्राहक, कर्मचारी आणि व्यावसायिक भागीदारांमध्ये विश्वास निर्माण करण्यास मदत होते.
3. व्यवसाय सातत्य सुनिश्चित करणे – सायबरहल्ले किंवा नैसर्गिक आपत्तींच्या वेळीही सिस्टिम चालू ठेवते.
4. कायदेशीर आणि औद्योगिक नियमांचे पालन – PCI DSS, ISO 27001, GDPR सारख्या मानकांचे पालन करण्यात मदत होते.
5. आर्थिक नुकसान कमी करणे – फसवणूक, डेटा चोरी आणि सिस्टिम डाउनटाइममुळे होणारे नुकसान टाळते.
6. स्पर्धात्मक फायदा – बौद्धिक संपदा (intellectual property) आणि व्यापार रहस्ये सुरक्षित ठेवून संस्थेला प्रतिस्पर्ध्यांपासून संरक्षण मिळते.
7. जबाबदारी आणि ओळख पटविणे – सर्व क्रिया अधिकृत वापरकर्त्यांशी स्पष्टपणे जोडल्या जातात.

1.2.3 इन्फॉर्मेशन क्लासिफिकेशन (Information classification)

माहिती वर्गीकरण (Information Classification) म्हणजे माहितीचे तिच्या संवेदनशीलता (sensitivity), मूल्य (value), वय (age), उपयुक्त आयुष्य (useful life) आणि वैयक्तिक संबंध (personal association) यांच्या आधारावर विविध गटांमध्ये वर्गीकरण करणे. यामुळे प्रत्येक प्रकारच्या माहितीवर तिच्या महत्त्वानुसार योग्य सुरक्षा नियंत्रण (security controls) लागू करता येतात. माहिती वर्गीकरणामुळे माहितीला कॉन्फिडेन्शियलिटी (Confidentiality), इंटेग्रिटी (Integrity), अव्हेलेबिलिटी (Availability) आणि ऑथेंटिकेशन (Authentication) (CIAA) या चारही सुरक्षा तत्त्वांनुसार आवश्यक संरक्षण मिळते.

माहिती वर्गीकरणाचे स्तर (Levels of Information Classification)

1. **सार्वजनिक माहिती (Public)**
   सार्वजनिक माहिती सगळ्यांसाठी उपलब्ध असते आणि तिच्या उघडकीमुळे संस्थेला काहीही हानी होत नाही. यावर विशेष सुरक्षा आवश्यक नसते.
   उदाहरण: विद्यापीठाची माहितीपत्रके, प्रेस रिलीज, कंपनी वेबसाइट्स.
2. **आंतरवली / खाजगी माहिती (Internal / Private)**
   ही माहिती फक्त संस्थेच्या आत वापरण्यासाठी असते.अनधिकृत उघडकीमुळे किरकोळ कामकाजात अडथळा येऊ शकतो.
   उदाहरण: आंतरिक नोटीस, कर्मचाऱ्यांच्या कामाच्या वेळापत्रका, HR धोरणे.
3. **गोपनीय माहिती (Confidential)**
   गोपनीय माहिती संवेदनशील असते आणि तिचा ॲक्सेस फक्त अधिकृत व्यक्तींनाच दिला जातो. अनधिकृत उघडकीमुळे आर्थिक, प्रतिष्ठात्मक किंवा कायदेशीर नुकसान होऊ शकते.
   उदाहरण: आर्थिक अहवाल, ग्राहक डेटाबेस, संशोधन आणि विकासातील माहिती.
4. **प्रतिबंधित / गुप्त माहिती (Restricted / Secret)**
   ही माहिती अत्यंत संवेदनशील असते आणि संस्थेच्या किंवा राष्ट्राच्या सुरक्षेसाठी अत्यंत महत्त्वाची असते. अनधिकृत उघडकीमुळे गंभीर नुकसान होऊ शकते.
   उदाहरण: लष्करी धोरणे, एन्क्रिप्शन कीज, सरकारी गुप्तचर नोंदी.

1.2.4 इन्फॉर्मेशन क्लासिफिकेशनसाठी निकष (Criteria for information classification)

1. **मूल्य (Value):** माहितीचे संस्थेसाठी किंवा व्यक्तीसाठी असलेले महत्त्व तिचे वर्गीकरण ठरवते. उच्च-मूल्य असलेला डेटा कठोरपणे संरक्षित केला पाहिजे.
   उदाहरण: बँक खात्याची माहिती आणि व्यापार रहस्ये (trade secrets) अत्यंत मौल्यवान असल्यामुळे गोपनीय (Confidential) ठेवली जातात.

2. **वय (Age):** माहितीची संवेदनशीलता काळानुसार कमी होत जाते. आज जी माहिती अत्यंत गोपनीय आहे, ती काही काळानंतर सार्वजनिक होऊ शकते.
   उदाहरण: परीक्षा होण्यापूर्वी प्रश्नपत्रिका गोपनीय असते, परंतु परीक्षा झाल्यानंतर ती सार्वजनिक केली जाऊ शकते.
3. **उपयुक्त आयुष्य (Useful Life):** माहिती किती काळ उपयोगी किंवा संबंधित राहते यावर तिचे वर्गीकरण अवलंबून असते. उपयुक्त आयुष्य संपल्यानंतर ती संग्रहित (archive) केली जाते किंवा नष्ट केली जाते.
   उदाहरण: प्रकल्पाच्या अंमलबजावणीदरम्यान प्रकल्प आराखडा अत्यंत महत्त्वाचा असतो, परंतु प्रकल्प पूर्ण झाल्यावर त्याचे महत्त्व कमी होते.
4. **वैयक्तिक संबंध (Personal Association):** व्यक्तींशी थेट संबंधित माहितीला गोपनीयतेच्या (privacy) आणि कायदेशीर कारणांमुळे विशेष संरक्षण आवश्यक असते.
   उदाहरण: कर्मचाऱ्यांचे वैद्यकीय रेकॉर्ड किंवा पगाराची माहिती गोपनीय ठेवणे आवश्यक आहे.

1.3 टाईप ऑफ अटॅक्स (Type of Attacks)

1.3.1 अटॅक्स (Attacks)

इन्फॉरमेशन सेक्युरिटीमध्ये अटॅक म्हणजे कोणतीही अशी कृती जी माहिती किंवा माहिती प्रणालींची गोपनीयता / कॉन्फिडेन्शियलिटी (Confidentiality), अखंडता/इंटेग्रिटी (Integrity), उपलब्धता/अव्हेलेबिलिटी (Availability) किंवा प्रामाणिकता/ऑथेंटिकेशन (Authenticity) — म्हणजेच CIAA यांना हानी पोहोचवते. अटॅक बाहेरील व्यक्तींकडून (जसे हॅकर्स, सायबर गुन्हेगार) किंवा आंतरिक व्यक्तींकडून (उदा. कर्मचारी, कंत्राटदार) तांत्रिक, भौतिक किंवा सामाजिक पद्धतींनी (social engineering) केला जाऊ शकतो. माहिती प्रणाली (Information Systems) हे अटॅकर्स साठी मौल्यवान लक्ष्य असतात, कारण त्यामध्ये वैयक्तिक माहिती, आर्थिक डेटा, बौद्धिक संपदा (intellectual property), सरकारी नोंदी अशा अत्यावश्यक मालमत्तेची साठवण आणि प्रक्रिया केली जाते. अटॅकर्स हार्डवेअर, सॉफ्टवेअर, नेटवर्क किंवा मानवी वर्तनातील त्रुटी (vulnerabilities) चा फायदा घेऊन त्यांच्या दुष्ट हेतू (malicious objectives) साध्य करतात.

टाईप ऑफ अटॅक्स (Types of Attacks)

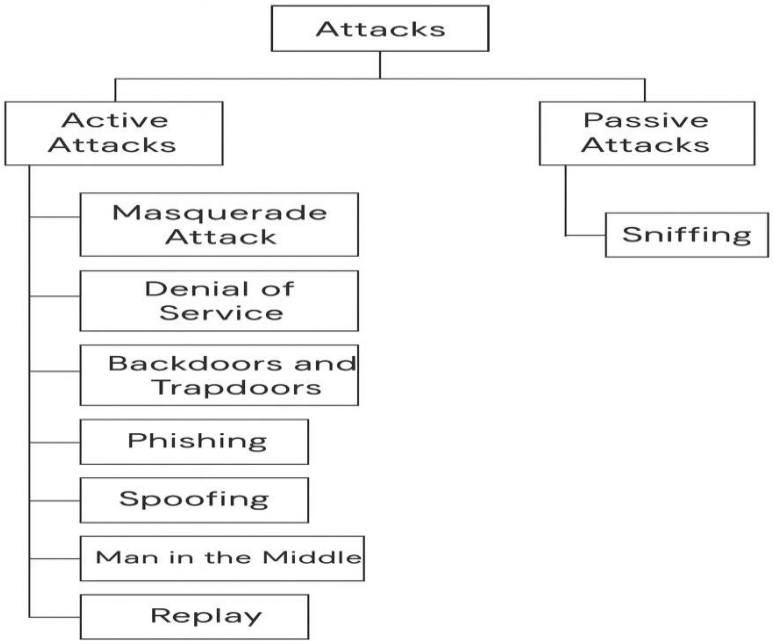


Fig 1.10: टाईप ऑफ अटॅक्स (Types of Attacks)

1. ॲक्टिव्ह अटॅक (Active Attacks)

ॲक्टिव्ह अटॅक (Active Attack) हा सुरक्षा हल्ल्याचा असा प्रकार आहे ज्यामध्ये अटॅकर डेटा किंवा सिस्टम संसाधने बदलण्याचा (modify), व्यत्यय आणण्याचा (disrupt) किंवा नष्ट करण्याचा (destroy) प्रयत्न करतो. पॅसिव्ह अटॅकमध्ये अटॅकर फक्त निरीक्षण (monitoring) करतो, पण ॲक्टिव्ह अटॅकमध्ये अटॅकर प्रत्यक्ष हस्तक्षेप करून कम्युनिकेशन

किंवा सेवांमध्ये अडथळा निर्माण करतो. अशा हल्ल्यांमुळे माहिती प्रणालींची अखंडता (Integrity) आणि उपलब्धता (Availability) यांना थेट धोका निर्माण होतो.

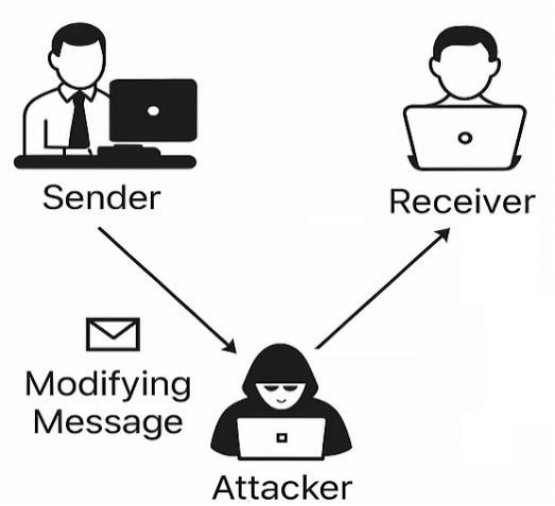


Fig 1.11: ॲक्टिव्ह अटॅक (Active Attacks)

अटॅकर सेंडर आणि रिसिव्हर यांच्यातील मेसेज इंटरसेप्ट करतो, त्यामध्ये बदल (modify) करतो आणि बदललेला मेसेज पुढे पाठवतो. ॲक्टिव्ह अटॅक्स अधिक धोकादायक असतात कारण ते थेट सिस्टिमच्या कार्यप्रणालीत हस्तक्षेप करतात आणि हानी पोहोचवतात. अशा हल्ल्यांमध्ये मालिशियस डेटा इंजेक्ट करणे, सेवांमध्ये व्यत्यय आणणे, किंवा अधिकृत युजरचे रूप धारण करणे (impersonation) यांचा समावेश होतो. हे हल्ले सामान्यतः लक्षात येण्याजोगे (noticeable) असतात, त्यामुळे संस्थांनी फायरवॉल, इंट्रूजन डिटेक्शन सिस्टिम्स (IDS) आणि मजबूत ऑथेन्टिकेशनचा वापर करणे आवश्यक असते.

2. पॅसिव्ह अटॅक्स (Passive Attacks)

पॅसिव्ह अटॅक हा सुरक्षा हल्ल्याचा प्रकार आहे ज्यामध्ये अटॅकर फक्त कम्युनिकेशन ऐकतो (monitor), इंटरसेप्ट करतो किंवा विश्लेषण (analyze) करतो, पण डेटा किंवा सिस्टिम ऑपरेशन्समध्ये कोणताही बदल करत नाही. पॅसिव्ह अटॅकचा मुख्य उद्देश म्हणजे माहिती चोरी करणे आणि गोपनीयता (कॉन्फिडेन्शियलिटी) भंग करणे, तेही लक्षात न येण्यासारखे. पॅसिव्ह अटॅक्स शोधणे कठीण असते कारण ते कम्युनिकेशनच्या सामान्य प्रवाहावर परिणाम करत नाहीत. सेंडर आणि रिसिव्हर यांना त्यांचा डेटा मॉनिटर केला जात आहे हे कळतही नाही. अटॅकर फक्त नेटवर्क ट्रॅफिक ऐकतो किंवा साठवलेला डेटा वाचतो यासाठी पॅकेट स्निफर्स (packet sniffers) सारखी साधने किंवा असुरक्षित कम्युनिकेशन चॅनेल्सचा वापर केला जातो. डेटामध्ये बदल केला जात नसल्यामुळे पॅसिव्ह अटॅक्स गोपनीयतेला (कॉन्फिडेन्शियलिटी) धोका पोहोचवतात; ते इंटेग्रिटी किंवा अव्हेलेबिलिटी ला हानी करत नाहीत.

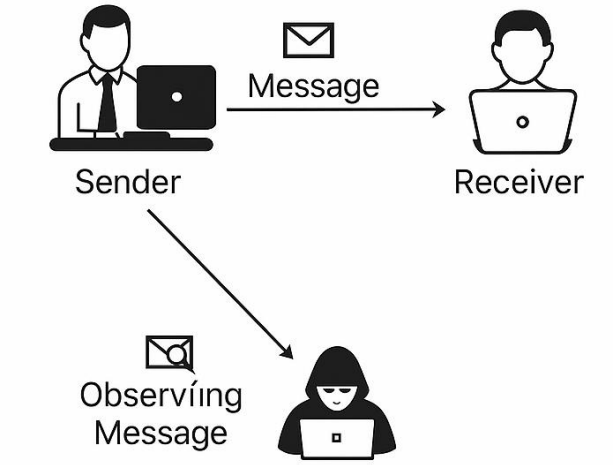


Fig 1.12: पॅसिव्ह अटॅक्स (Passive Attacks)

अटॅकर सेंडर आणि रिसिव्हर यांच्यातील कम्युनिकेशन गुपचूप निरीक्षण करतो. अटॅकर मेसेजमध्ये कोणताही बदल करत नाही; तो फक्त माहिती वाचतो किंवा मॉनिटर करतो. त्यामुळे माहितीची गोपनीयता (कॉन्फिडेन्शियलिटी) भंग होते.

Table 1.1: ॲक्टिव्ह आणि पॅसिव्ह अटॅक मधील तुलना (Comparison between Active and Passive Attack)

पहलू (Aspect)	ॲक्टिव्ह अटॅक (Active Attack)	पॅसिव्ह अटॅक (Passive Attack)
व्याख्या (Definition)	अटॅकर ट्रान्समिशनदरम्यान डेटा बदलतो, व्यत्यय आणतो किंवा इंजेक्ट करतो.	अटॅकर डेटा फक्त मॉनिटर किंवा इंटरसेप्ट करतो; डेटा बदलत नाही.
स्वरूप (Nature)	हस्तक्षेप करणारा (Intrusive) आणि सिस्टिमच्या कार्यात थेट परिणाम करणारा.	हस्तक्षेप न करणारा (Non-intrusive) आणि शांत; पीडितांना कळतही नाही.
परिणाम (Impact)	माहितीची इंटेग्रिटी आणि अव्हेलेबिलिटी धोक्यात येते.	माहितीची कॉन्फिडेन्शियलिटी धोक्यात येते.
शोधण्याची क्षमता (Detectability)	शोधणे सोपे, कारण डेटा बदलला जातो किंवा सेवा खंडित होतात.	शोधणे खूप कठीण, कारण डेटा बदल होत नाही.
उदाहरणे (Examples)	मॅस्करेड, डिनायल-ऑफ-सर्व्हिस (DoS), स्पूफिंग, रिप्ले, मॅन-इन-द-मिडल.	स्निफिंग, संदेशातील माहिती उघड होणे (Release of Message Contents), ट्रॅफिक ॲनालिसिस
अटॅकरचे उद्दिष्ट (Attacker's Goal)	हानी करणे, सेवा बिघडवणे, किंवा सिस्टिमवर अनधिकृत नियंत्रण मिळवणे.	कोणालाही न कळता गुप्त माहिती गोळा करणे.
प्रतिबंधक उपाय (Countermeasures)	फायरवॉल्स, IDS/IPS, एन्क्रिप्शन, ऑथेंटिकेशन, रेट लिमिटिंग.	मजबूत एनक्रिप्शन (HTTPS, VPNs), सिक्युअर प्रोटोकॉल्स, IDS, यूजर अवेअरनेस.

3. मस्करेड अटॅक (Masquerade Attack)

मस्करेड अटॅक हा एक ॲक्टिव्ह अटॅक आहे, ज्यामध्ये अनधिकृत वापरकर्ता अधिकृत वापरकर्ता असल्याचे भासवून (pretend) सिस्टम किंवा नेटवर्कमध्ये प्रवेश मिळवण्याचा प्रयत्न करतो. हे प्रामुख्याने क्रेडेन्शियल्स चोरी करून, बनावट ओळख तयार करून किंवा सेशन टोकन्सचा गैरवापर करून केले जाते. मस्करेड हल्ल्यामध्ये, अटॅकर वैध (legitimate) वापरकर्त्याचे रूप धारण करतो, ज्यामुळे तो ऑथेन्टिकेशन मेकॅनिझमला चकवत (bypass) सिस्टममध्ये प्रवेश मिळवतो. अशा प्रकारचे हल्ले प्रामुख्याने फिशिंग, पासवर्ड चोरी, स्पूफिंग इत्यादी तंत्रांसोबत केले जातात.

- **लक्ष्य (Target):**
  ऑथेंटिकेशन (Authentication) आणि ॲक्सेस कंट्रोल (Access Control)
- **परिणाम (Impact):**
  Confidentiality आणि Integrity यांचे उल्लंघन
- **प्रतिबंध (Prevention):**
  - मजबूत ऑथेन्टिकेशन (मल्टी-फॅक्टर ऑथेंटिकेशन, बायोमेट्रिक्स)
  - इंट्रूजन डिटेक्शन सिस्टिम्स (Intrusion Detection Systems (IDS))
  - सेशन मॉनिटरिंग

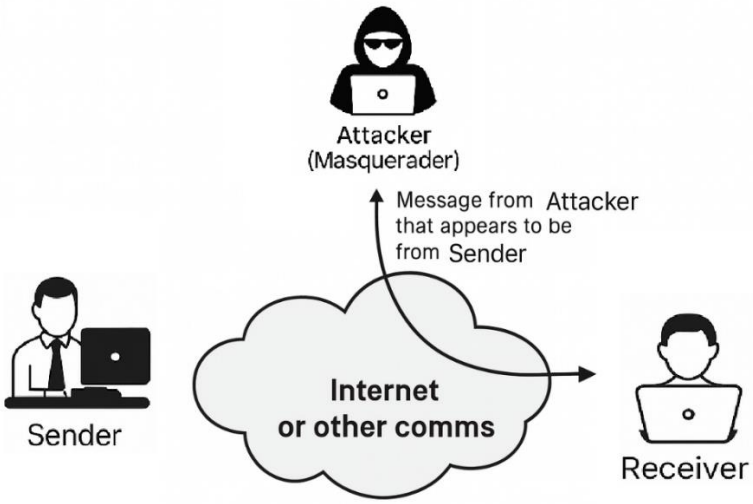


Fig 1.13: मस्करेड अटॅक (Masquerade Attack)

अटॅकर सेंडरची क्रेडेन्शियल्स चोरी करतो किंवा त्याची ओळख स्पूफ करतो आणि नंतर असा बनावट मेसेज पाठवतो जो सेंडरकडून आल्यासारखा दिसतो. रिसिव्हर हा मेसेज खरा आहे असे समजतो आणि त्यानुसार कृती करतो (उदा. पेमेंट मंजूर करणे), पण प्रत्यक्षात त्या कम्युनिकेशनच्या मागे अटॅकर असतो, सेंडर नाही.

4. डिनायल ऑफ सर्विस अटॅक Denial of Service (DoS)

डिनायल ऑफ सर्विस (DoS) हा एक ॲक्टिव्ह अटॅक आहे ज्यामध्ये अटॅकर सिस्टम, नेटवर्क किंवा सेवा वैध वापरकर्त्यांसाठी अनुपलब्ध (Unavailable) करण्याचा प्रयत्न करतो. हे साधण्यासाठी अटॅकर सिस्टमवर अनधिकृत आणि अतिप्रमाणात रिक्वेस्ट्स पाठवतो किंवा त्यातील कमकुवतपणांचा (vulnerabilities) फायदा घेतो. DoS हल्ल्याचा उद्देश डेटा चोरी करणे नसून, सिस्टमची कार्यक्षमता बिघडवणे आणि अधिकृत युजर्सना सेवा नाकारणे (deny access) हा असतो.

अटॅकर्स सहसा DoS हल्ला पुढील पद्धतींनी करतात:

- टार्गेटवर अतिरिक्त नेटवर्क ट्रॅफिकचा पूर (Flooding) आणून नेटवर्क ओव्हरलोड करणे
- मॅलफॉर्म्ड रिक्वेस्ट्स पाठवून ॲप्लिकेशन्स क्रॅश करणे
- ऑपरेटिंग सिस्टिम्स किंवा सर्व्हिसेस मधील असुरक्षिततेचा फायदा घेणे

डिस्ट्रिब्युटेड डिनायल ऑफ सर्विस (Distributed Denial of Service DDoS)

DoS चा अधिक शक्तिशाली प्रकार म्हणजे DDoS, ज्यामध्ये अटॅकर अनेक कम्प्रमाइज्ड मशिन्स (botnets) चा वापर करून एकाच टार्गेटवर एकाच वेळी हल्ला करतो. यामुळे हल्ला थांबवणे किंवा नियंत्रणात आणणे खूप कठीण होते.

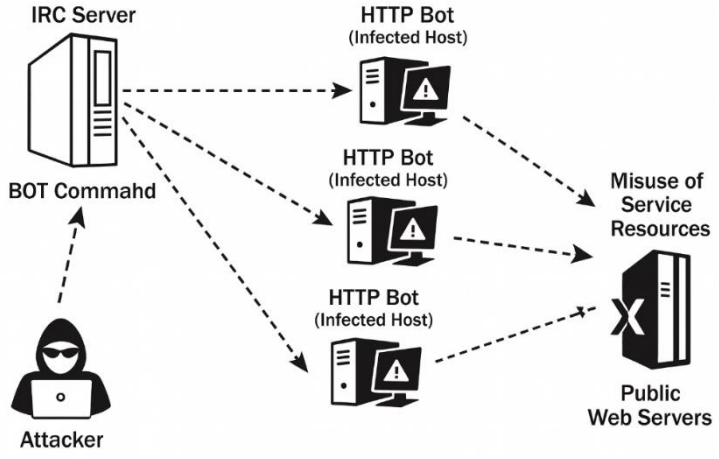


Fig 1.14: डिस्ट्रिब्युटेड डिनायल ऑफ सर्विस (Distributed Denial of Service (DDoS))

जिथे अटॅकर अनेक संक्रमित मशिन्स (bots) वर नियंत्रण ठेवतो, आणि हे नियंत्रण कमांड सर्व्हर (IRC Server) द्वारे केले जाते. हे बॉट्स एकाच वेळी टार्गेट सार्वजनिक वेब सर्व्हरवर मोठ्या प्रमाणात रिक्वेस्ट्स पाठवतात, ज्यामुळे सर्व्हरची संसाधने

ओव्हरलोड होतात. परिणामी, वैध (legitimate) वापरकर्त्यांना सेवा ॲक्सेस करता येत नाही आणि सिस्टिममध्ये व्यत्यय येतो तसेच संसाधनांचा दुरुपयोग होतो.

परिणाम (Impact):

- सेवा बंद पडणे (Service downtime)
- आर्थिक आणि प्रतिष्ठेचे नुकसान
- ग्राहकांचा विश्वास कमी होणे

प्रतिबंध (Prevention):

- फायरवॉल्स आणि इंट्रूजन डिटेक्शन सिस्टिम्स (IDS)
- रेट-लिमिटिंग आणि लोड बॅलेन्सिंग
- क्लाऊड-बेस्ड अँटी-DDoS सोल्यूशन्स

उदाहरणे (Examples):

1. **पिंग फ्लड अटॅक (Ping Flood Attack):** अटॅकर मोठ्या प्रमाणात ICMP "ping" रिक्वेस्ट्स पाठवतो, ज्यामुळे नेटवर्क बँडविड्थ संपते.
2. **सिन फ्लड अटॅक (SYN Flood Attack):** अटॅकर सतत अनेक कनेक्शन रिक्वेस्ट्स पाठवतो, पण हँडशेक पूर्ण करत नाही. यामुळे सर्व्हरची संसाधने व्यापली जातात.
3. **डीडॉस ऑन वेबसाईट्स (DDoS on Websites):** बॉटनेट एखाद्या ई-कॉमर्स साइटवर सेल सीझनमध्ये अचानक प्रचंड ट्रॅफिक पाठवतो, ज्यामुळे साइट ग्राहकांसाठी अनुपलब्ध होते.

5. गुप्त प्रवेशद्वार / बॅकडोअर (Backdoor)

बॅकडोअर म्हणजे संगणक प्रणाली, अनुप्रयोग किंवा जाळ्यातील असे गुप्त प्रवेशद्वार, जे नियमित ओळख पडताळणी (प्रमाणीकरण) आणि सुरक्षा तपासण्या वगळून थेट प्रवेश देते. कधी-कधी विकसित करणारे (विकसक) दुरुस्ती किंवा देखभालीसाठी असे प्रवेशद्वार जाणूनबुजून ठेवतात; तर अनेकदा हल्लेखोर दुर्भावनापूर्ण सॉफ्टवेअर वापरून हे गुप्त मार्ग लपूनछपून स्थापित करतात. अशा बॅकडोअरमुळे अनधिकृत व्यक्तीला प्रवेश, तसेच सिस्टमवर दूरस्थ नियंत्रण मिळू शकते, म्हणून ते अत्यंत गंभीर सुरक्षा धोका मानले जातात. बॅकडोअर हा माहिती सुरक्षेतील अत्यंत गंभीर सक्रिय हल्ला प्रकार आहे. काही वेळा प्रोग्राम तयार करणारे चाचणीसाठी देखभाल-द्वार (मेन्टेनन्स हुक) म्हणून बॅकडोअर तयार करतात. परंतु प्रणाली प्रत्यक्ष वापरात आणण्यापूर्वी हे काढून टाकले नाही तर ते अत्यंत धोकादायक सुरक्षा उणिवांमध्ये रूपांतरित होतात. बहुतेक वेळा हल्लेखोर दुर्भावनापूर्ण कार्यक्रम, कृमी-प्रोग्राम किंवा गुप्त संच यांच्या मदतीने बॅकडोअर प्रणालीमध्ये बसवतात, ज्यामुळे त्यांना दीर्घकाळ गुप्तपणे प्रवेश मिळू शकतो.

बॅकडोअर स्थापित झाल्यानंतर हल्लेखोर पुढील कृती करू शकतो: ओळख पडताळणी टाळून प्रमुख व्यवस्थापक पातळीचा अधिकार मिळवणे, प्रवेश-संकेत, आर्थिक नोंदी, संशोधन माहिती यांसारखा संवेदनशील डेटा चोरणे, अतिरिक्त हानिकारक कार्यक्रम बसवणे किंवा सेवा नाकारणारे व्यापक हल्ले सुरू करणे, ताब्यात घेतलेल्या संगणकांना गुप्त जाळ्याचा (बॉटजाळा) भाग बनवून दूरस्थपणे नियंत्रित करणे.

बॅकडोअर ओळखणे कठीण का असते?

बॅकडोअर बहुतेक वेळा अत्यंत शांतपणे, लपूनछपून कार्य करतात. त्यामुळे त्यांचा शोध लावणे अत्यंत कठीण ठरते.

त्यांना शोधण्यासाठी आणि रोखण्यासाठी पुढील आधुनिक सुरक्षा उपाय आवश्यक असतात: घुसखोरी शोधणारी प्रणाली, प्रवेश चाचणी (पेनिट्रेशन टेस्टिंग), सुरक्षित प्रोग्राम तयार करण्याच्या पद्धती, हानिकारक सॉफ्टवेअर ओळखून काढणारी साधने

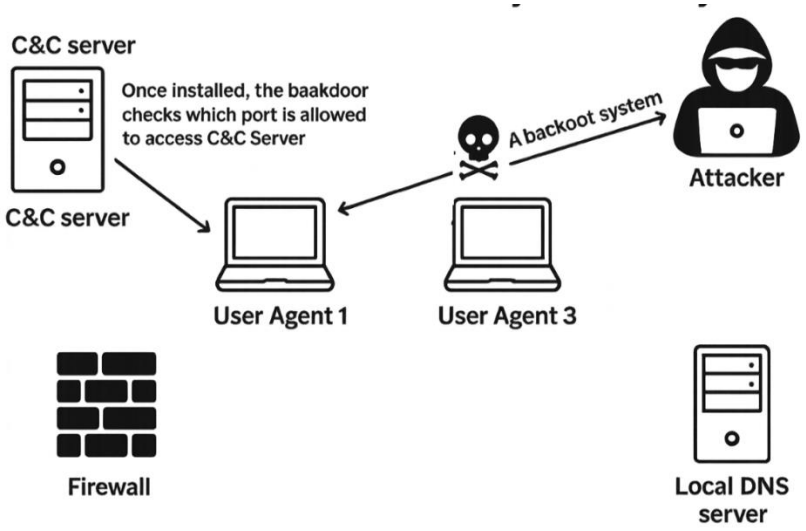


Fig 1.15: बॅकडोअर (Backdoor) अटॅक

1. हल्लेखोर वापरकर्ता प्रणालीमध्ये (उदा., वापरकर्ता घटक ३) गुप्त प्रवेशद्वार बसवतो, ज्यामुळे एक लपलेला प्रवेशमार्ग तयार होतो.
2. संक्रमण झालेली प्रणाली नियंत्रण आणि आदेश (C&C) सर्व्हरशी संपर्क साधते, जे सर्व दुर्भावनायुक्त क्रिया नियंत्रित करते.
3. एकदा बॅकडोअर स्थापित झाल्यानंतर ते उपलब्ध ओपन पोर्ट्स शोधते आणि त्यांचा वापर करून C&C सर्व्हरशी संपर्क साधते, त्यामुळे फायरवॉल बायपास केली जाते.
4. स्थानिक लोकल डीएनएस सर्व्हर देखील ही गुप्त देवाणघेवाण सुलभ करण्यासाठी वापरला जाऊ शकतो.
5. इतर वापरकर्ता प्रणाली (उदा., वापरकर्ता घटक 1) देखील या गुप्त मार्गाचा वापर करून संक्रमित होऊ शकतात.

उदाहरण: एका ट्रोजन हॉर्स बळीच्या संगणकात लपलेला बॅकडोअर बसवला. त्यानंतर हल्लेखोर कधीही दूरस्थपणे संगणकात प्रवेश करू शकतो, आणि त्यासाठी वापरकर्त्याच्या संकेतशब्दाची गरजही नसते.

प्रत्यक्ष उदाहरण: "बॅक ऑरिफिस" (1999) या दुष्ट कार्यक्रमाने विंडोज संगणकांमध्ये दूरस्थ बॅकडोअर्स तयार केले, ज्यामुळे हल्लेखोरांना वापरकर्त्याच्या नकळत संगणकांवर पूर्ण नियंत्रण मिळू शकत होते.

6. ट्रॅपडोअर (Trapdoors)

ट्रॅपडोअर म्हणजे एखाद्या प्रोग्राममध्ये विकसकांनी जाणूनबुजून तयार केलेले गुप्त प्रवेशद्वार, ज्याचा उपयोग चाचणी, दुरुस्ती किंवा देखभालीसाठी नियमित ऑथेन्टिकेशन प्रक्रियेविना करण्यासाठी केला जातो. जर हे नंतर काढून टाकले गेले नाही, तर हल्लेखोर हे शोधून त्याचा गैरवापर करून अनधिकृत प्रवेश मिळवू शकतात.

ट्रॅपडोअर बहुतांश वेळा विकासाच्या टप्प्यात (development phase) मुद्दाम घातले जातात. प्रोग्रामर चाचणी सुलभ करण्यासाठी किंवा समस्या शोधण्यासाठी सामान्य लॉगिन आणि सुरक्षा प्रक्रियेच्या बाहेर जाण्यासाठी हे मार्ग वापरतात. त्यांच्या हेतूमध्ये दुष्टता नसली तरी, असे ट्रॅपडोअर योग्यरित्या सुरक्षित न ठेवले तर संपूर्ण प्रणालीची सुरक्षा कमजोर होते. एकदा ट्रॅपडोअर शोधल्यावर हल्लेखोर त्याचा वापर करून:

- प्रमाणीकरण नियंत्रण (authentication controls) टाळू शकतात
- संवेदनशील प्रणाली कार्यांमध्ये थेट प्रवेश मिळवू शकतात
- हानिकारक सॉफ्टवेअर बसवू शकतात किंवा प्रणालीचे संरचना-मूल्य (configuration) बदलू शकतात

ट्रॅपडोअर्सचे मुख्य धोके म्हणजे: ते वापरकर्त्यांना आणि प्रशासकांना दिसत नाहीत, त्यांची कोठेही नोंद नसते (undocumented), अनेकदा ते चुकीने सिस्टममध्ये राहून जातात

यामुळे प्रणालीवर गंभीर सुरक्षा जोखीम निर्माण होते. जोखीम कमी करण्यासाठी आवश्यक उपाय सुरक्षित प्रोग्रामिंग पद्धती, कोडची तपासणी (code review), सुरक्षा उणिवांचे स्कॅनिंग (vulnerability scanning), प्रवेश-चाचणी (penetration testing)

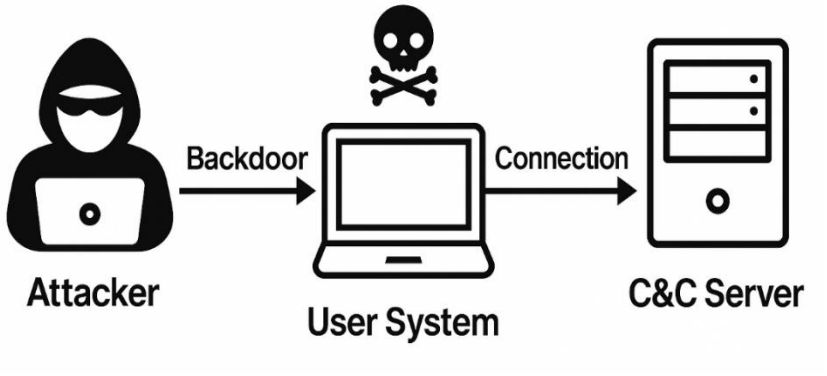


Fig 1.16: ट्रॅपडोअर (Trapdoors) अटॅक

हल्लेखोर बळीच्या संगणकावर एक लपलेला बॅकडोअर स्थापित करतो, आणि नंतर ती प्रणाली गुप्तपणे नियंत्रण-आणि-आदेश (C&C) सर्व्हरशी संपर्क साधते.

उदाहरण: एखादा प्रोग्रामर विकासाच्या काळात प्रणालीला सहज प्रवेश मिळावा म्हणून स्रोत-कोडमध्ये एक "मुख्य संकेतशब्द" (master password) हार्ड-कोड करून ठेवतो. जर हा ट्रॅपडोअर प्रणाली बाजारात आणण्यापूर्वी काढून टाकला नाही, तर तो शोधणारा हल्लेखोर सहजप्रवेश नियंत्रण टाळून (authentication bypass) अनधिकृत प्रवेश मिळवू शकतो.

प्रत्यक्ष उदाहरण: सुरुवातीच्या काही ऑपरेटिंग सिस्टीममध्ये विकसकांसाठी लपवलेली "देखभाल खात्ये" (maintenance accounts) ठेवली जात. नंतर हॅकर्सनी याचाच वापर करून ट्रॅपडोअरच्या माध्यमातून अनेक प्रणालींमध्ये अनधिकृत प्रवेश मिळवला.

Table 1.2: कम्पॅरिझन: बॅकडोर (Backdoor) वि. ट्रॅपडोर (Trapdoor)

पहलू (Aspect)	**बॅकडोअर (Backdoor)**	**ट्रॅपडोअर (Trapdoor)**
व्याख्या (Definition)	प्रणाली, प्रोग्राम किंवा जाळ्यातील लपलेले प्रवेशद्वार, जे नियमित प्रमाणीकरण टाळते. हे प्रामुख्याने हल्लेखोर दुर्भावनापूर्ण सॉफ्टवेअरद्वारे बसवतात किंवा काही वेळा विकसक जाणूनबुजून ठेवतात.	सॉफ्टवेअरमध्ये विकसकांनी चाचणी, दुरुस्ती किंवा देखभाल सुलभ करण्यासाठी तयार केलेला गुप्त शॉर्टकट किंवा प्रवेशबिंदू, जो प्रमाणीकरण टाळतो.
उगम (Origin)	बहुतांश वेळा हल्लेखोर ट्रोजन प्रोग्राम (Trojan), रूटकिट (Rootkit), वर्म (Worm) वापरून तयार करतात; काही वेळा निष्काळजी विकसकांमुळे राहतो.	पूर्णपणे विकसकांनी जाणूनबुजून कोड लिहिताना तयार केलेला, सहसा सोयीसाठी.
हेतू (Intent)	साधारणतः दुर्भावनायुक्त हल्लेखोरांना दीर्घकालीन अनधिकृत प्रवेश मिळवून देण्यासाठी.	हेतू दुर्भावनायुक्त नसतो चाचणीसाठी वापरतात, पण न काढल्यास सुरक्षा धोक्यात येते.
शोधण्याची क्षमता (Detection)	शोधणे कठीण ते दुर्भावनायुक्त प्रोग्राममध्ये लपलेले असते किंवा वैध सेवेप्रमाणे दिसते.	शोधणे तुलनेने सोपे स्रोत-कोड तपासणी किंवा कोड पुनरावलोकनात आढळू शकते, परंतु अनेकदा ती नोंदवलेली नसते.
सुरक्षेवरील परिणाम (Security Impact)	हल्लेखोर डेटा चोरी करू शकतात, हानिकारक सॉफ्टवेअर बसवू शकतात, किंवा प्रणाली दूरस्थपणे नियंत्रित करू शकतात.	प्रमाणीकरण व प्रणाली तपासण्या टाळण्याचा मार्ग उपलब्ध करून देते, ज्याचा शोध लागल्यास हल्लेखोर गैरवापर करू शकतात.
उदाहरण (Example)	बॅक ऑरिफिस (1999) विंडोज संगणकांवर दूरस्थ नियंत्रण मिळवण्यासाठी वापरले गेले.	विकसकांनी चाचणीसाठी हार्ड-कोड केलेला मुख्य संकेतशब्द (master password) प्रोग्राममध्ये ठेवणे.

7. फिशिंग (Phishing)

फिशिंग हा एक सामाजिक अभियांत्रिकीवर आधारित (Social Engineering) आणि सक्रिय हल्ला (Active Attack) आहे, ज्यामध्ये हल्लेखोर बँक, ई-कॉमर्स साइट, कंपनी अशा विश्वासार्ह संस्थेचे रूप धारण करून बनावट ईमेल, वेबसाइट किंवा संदेश तयार करतो आणि वापरकर्त्यांना फसवून त्यांच्याकडून वापरकर्ता-नाव, संकेतशब्द, क्रेडिट कार्ड क्रमांक, वैयक्तिक माहिती मिळवतो. फिशिंगमध्ये हल्लेखोर तांत्रिक उणिवांचा नाही तर मानवी मानसशास्त्राचा फायदा घेतो. हल्लेखोर विश्वासार्ह दिसणारे खोटे पण अतिशय पटणारे संदेश तयार करतो. बळी व्यक्ती ते खरे समजून संवेदनशील माहिती देते, ज्याचा वापर हल्लेखोर ओळख चोरी, फसवणूक किंवा अनधिकृत प्रवेश मिळवण्यासाठी करतात.

फिशिंगचे सामान्य प्रकार (Common Variants):

- **ईमेल फिशिंग (Email Phishing):** बनावट ईमेल ज्यामध्ये हानिकारक दुवे (links) किंवा जोडण्या (attachments) असतात.
- **स्पिअर फिशिंग (Spear Phishing):** विशिष्ट व्यक्ती किंवा संस्थेला लक्ष्य करून केलेले फिशिंग.
- **व्हेलिंग (Whaling):** उच्च पदस्थ अधिकारी, वरिष्ठ व्यवस्थापक किंवा प्रमुख व्यक्तींना लक्ष्य करणारे फिशिंग.
- **स्मिशिंग / विशिंग (Smishing / Vishing):** SMS चा वापर करून फिशिंग (Smishing) किंवा फोन कॉलद्वारे फिशिंग (Vishing).

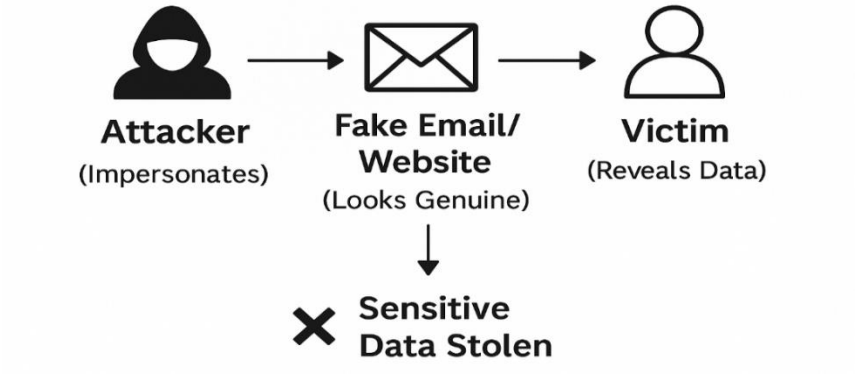


Fig 1.17: फिशिंग अटॅक (Phishing)

हल्लेखोर स्वतःला विश्वासार्ह संस्थेचे प्रतिनिधी असल्याचे भासवतो आणि अतिशय पटणारा बनावट ईमेल किंवा वेबसाइट तयार करतो. हा संदेश बळीपर्यंत पोहोचवला जातो. बळी व्यक्ती तो संदेश खरा आहे असे समजून संवेदनशील माहिती (उदा., वापरकर्ता-नाव, संकेतशब्द, बँक तपशील) टाकते आणि हल्लेखोर ती माहिती चोरून घेतो.

परिणाम (Impact):

- गोपनीयतेचा भंग (Confidentiality).
- माहितीची अखंडता धोक्यात येणे (Integrity)
- आर्थिक नुकसान
- ओळख चोरी (Identity Theft)
- प्रतिमेचे नुकसान (Reputation)

प्रतिबंध (Prevention):

- वापरकर्त्यांमध्ये जागरुकता (User Awareness)
- अँटी-फिशिंग तपासणी प्रणाली व फिल्टर्स
- दोन-घटक ओळख पडताळणी (Two-Factor Authentication)
- संवेदनशील माहिती टाकण्यापूर्वी URL तपासणे आणि खात्री करणे

उदाहरण (Example): हल्लेखोर बँकेकडून आल्यासारखा दिसणारा ईमेल पाठवतो, ज्याचा विषय असतो: "महत्वाचे: आपले खाते तात्काळ तपासा."

त्या ईमेलमध्ये एका बनावट लॉगिन पृष्ठाचा दुवा असतो, जो अगदी बँकेच्या अधिकृत वेबसाइटसारखा दिसतो. बळी व्यक्ती त्या पृष्ठावर आपले वापरकर्ता-नाव आणि संकेतशब्द टाकते. हल्लेखोर हे तपशील पकडतो आणि नंतर खऱ्या बँक खात्यात लॉगिन करून पैसे चोरी करतो किंवा वैयक्तिक माहिती मिळवतो.

8. स्पूफिंग (Spoofing)

स्पूफिंग हा एक ॲक्टिव्ह अटॅक आहे ज्यामध्ये हल्लेखोर विश्वासार्ह घटकाचे रूप धारण करतो, आणि स्वतःची ओळख लपवण्यासाठी किंवा बदलण्यासाठी खोटे IP पत्ते, ईमेल शीर्षके, DNS माहिती किंवा कॉलर आयडी तयार करतो. याचा उद्देश अनधिकृत प्रवेश, डेटा चोरी किंवा हानिकारक सॉफ्टवेअर पसरवणे असा असतो. स्पूफिंग हे कम्युनिकेशन सिस्टीममधील विश्वास-संबंधाचा (trust relationship) गैरवापर करते. हल्लेखोर IP, ईमेल, DNS यांसारखे पहिचान दर्शवणारे घटक बनावट करतो, ज्यामुळे बळीला असे वाटते की तो विश्वासार्ह स्त्रोताशी संवाद साधत आहे. पॅसिव्ह स्निफिंगपेक्षा वेगळे, स्पूफिंगमध्ये हल्लेखोर खोटी माहिती सक्रियपणे कम्युनिकेशन चॅनेलमध्ये इंजेक्ट करतो.

स्पूफिंगचे प्रकार (Types of Spoofing):

- आयपी स्पूफिंग (IP Spoofing): खोटा IP पत्ता वापरून विश्वासार्ह प्रणालीचे रूप धारण करणे.
- ईमेल स्पूफिंग (Email Spoofing): ईमेल पाठवणाऱ्याचा पत्ता बनावट करून तो खरा असल्याचा भास निर्माण करणे.
- डीएनएस स्पूफिंग (DNS Spoofing): DNS नोंदी बदलून वापरकर्त्यांना हानिकारक वेबसाइट्सवर वळवणे.
- कॉलर आयडी स्पूफिंग (Caller ID Spoofing): फोन क्रमांक लपवून किंवा बनावट करून बळीला फसवणे.

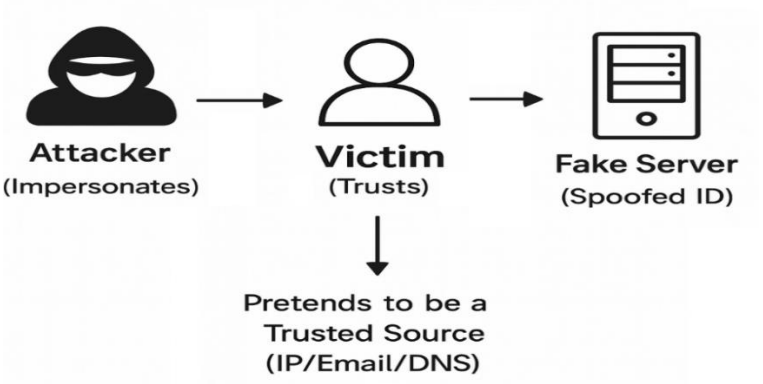


Fig 1.18: स्पूफिंग अटॅक (Spoofing)

हल्लेखोर विश्वासार्ह घटकाचे रूप धारण करतो आणि बळीला बनावट पण वैध दिसणाऱ्या सर्व्हरशी जोडण्यास प्रवृत्त करतो. IP पत्ता, ईमेल पत्ता किंवा DNS नोंदी बनावट करून (spoofing) हल्लेखोर बळीला फसवतो, ज्यामुळे बळी संकेतशब्द, प्रवेश-तपशील देतो किंवा हानिकारक सामग्री स्वीकारतो. यामुळे डेटा चोरी, खाते हानी (account compromise) किंवा पुढील हानिकारक सॉफ्टवेअरचा प्रसार होऊ शकतो. ही सोशिअल इंजिनिअरिंग आणि स्पूफिंग यांचे संयोजन असलेली पद्धत आहे, जी वापरकर्त्यांच्या विश्वासाचा गैरवापर करून सामान्य सुरक्षा तपासण्या चकवते.

परिणाम (Impact):

- डेटा चोरी
- हानिकारक सॉफ्टवेअर (malware) पसरवणे
- फिशिंग हल्ले
- सेशन हायजॅकिंग (Session Hijacking)
- डिनायल ऑफ सर्विस (Denial of Service)

प्रतिबंध (Prevention):

- पॅकेट फिल्टरिंग
- डिजिटल सिग्नेचर्स (Digital Signatures)
- ईमेल प्रमाणीकरण प्रोटोकॉल — SPF, DKIM, DMARC
- DNSSEC वापरणे (DNS सुरक्षा विस्तार)
- वापरकर्त्यांमध्ये जागरूकता वाढवणे

उदाहरण (Example): हल्लेखोर ईमेल स्पूफिंग चा वापर करून कंपनीच्या मानव संसाधन विभागाकडून (HR Department) आल्यासारखा दिसणारा संदेश पाठवतो: "पगार प्रक्रियेसाठी कृपया आपल्या बँक माहितीचे अद्ययावत तपशील भरा."

ईमेलचा पत्ता बनावट (उदा. hr@company.com) असतो, आणि त्यातील दुवा बनावट वेबसाइटवर नेतो. कर्मचारी त्या पृष्ठावर आपले तपशील भरतात आणि नकळत ते हल्लेखोराला सुपूर्द करतात.

9. मॅन-इन-द-मिडल (Man-in-the-Middle – MITM)

मॅन-इन-द-मिडल (MITM) हा एक ॲक्टिव्ह अटॅक आहे, ज्यामध्ये हल्लेखोर दोन व्यक्ती किंवा प्रणाली यांच्यातील संवाद गुप्तपणे अडवतो आणि त्यामध्ये बदल करतो किंवा हस्तक्षेप करतो, पण दोन्ही बाजूंस वाटते की ते थेट एकमेकांशी संवाद साधत आहेत. हल्लेखोर स्वतःला सेंडर आणि रिसिव्हर यांच्या मध्ये बसवतो आणि दोन्हीशी स्वतंत्रपणे कनेक्शन तयार करतो. यामुळे दोघांनाही वाटते की ते सुरक्षितपणे संवाद करत आहेत, परंतु प्रत्यक्षात हल्लेखोर: संदेश ऐकू शकतो (Eavesdrop), संदेश बदलू शकतो (Modify), खोटी माहिती टाकू शकतो (Inject), माहिती अडवून ठेवू शकतो (Block) यामुळे संवादाची गोपनीयता कॉन्फिडेन्शियलिटी (Confidentiality), इंटेग्रिटी (Integrity), आणि ऑथेन्टिसिटी (Authenticity) धोक्यात येते.

MITM मध्ये वापरल्या जाणाऱ्या तंत्रे:

- ARP स्पूफिंग: खोटे ARP संदेश पाठवून स्थानिक नेटवर्कवरील ट्रॅफिक स्वतःकडे वळवणे.
- DNS स्पूफिंग: DNS नोंदी बदलून बळी व्यक्तींना हानिकारक वेबसाइट्सवर वळवणे.
- HTTPS स्पूफिंग: सुरक्षित HTTPS प्रोटोकॉल हटवून संवाद असुरक्षित HTTP वर आणणे.
- Wi-Fi ऐकणी (Wi-Fi Eavesdropping): बनावट Wi-Fi हॉटस्पॉट तयार करून वापरकर्त्यांचा नेटवर्क ट्रॅफिक पकडणे.

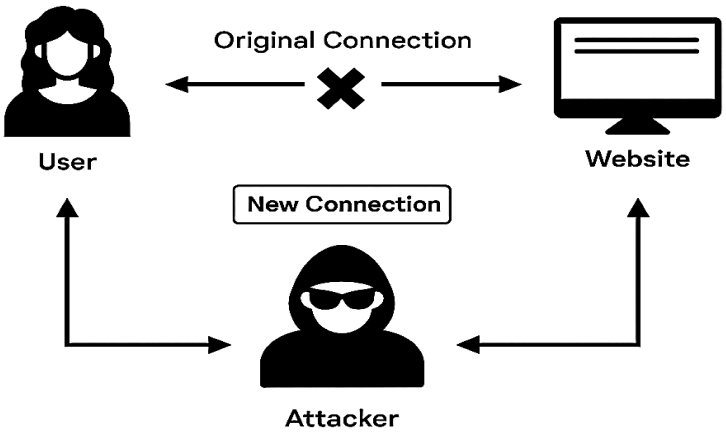


Fig 1.19: मॅन-इन-द-मिडल (Man-in-the-Middle – MITM)

हल्लेखोर वापरकर्ता आणि वेबसाइट यांच्यातील मूळ कनेक्शन अडवतो आणि बिघडवतो. वापरकर्ता आणि वेबसाइट दोघांनाही वाटते की ते एकमेकांशी थेट संवाद साधत आहेत, पण प्रत्यक्षात ते दोघेही हल्लेखोराशी स्वतंत्र नवीन कनेक्शन तयार करतात. हल्लेखोर त्यांच्यातील संवेदनशील माहिती पाहू शकतो, बदलू शकतो किंवा चोरू शकतो.

परिणाम (Impact):

- लॉगिन माहितीची चोरी
- आर्थिक फसवणूक
- ओळख चोरी
- सत्र हायजॅकिंग
- हानिकारक सामग्री इंजेक्ट करणे

प्रतिबंध (Prevention):

- एनक्रिप्शन (HTTPS, SSL/TLS)
- VPN चा वापर
- सुरक्षित DNS (DNSSEC)
- बहु-घटक प्रमाणीकरण (Multi-Factor Authentication)
- वापरकर्त्यांमध्ये जागरूकता

उदाहरण (Example):
तुम्ही एका कॅफेमध्ये फ्री Wi-Fi ला जोडता. तुम्हाला माहिती नसताना, तो हॉटस्पॉट हल्लेखोराने तयार केलेला असतो. तुम्ही ईमेलमध्ये लॉगिन करता तेव्हा हल्लेखोर तुमचे वापरकर्ता-नाव आणि संकेतशब्द अडवतो आणि नंतर ते वास्तविक ईमेल सर्व्हरकडे पाठवतो.

- तुम्हाला वाटते की तुम्ही थेट ईमेल सर्व्हरशी बोलत आहात.
- सर्व्हरला वाटते की तो थेट तुमच्याशी बोलतो आहे.
- प्रत्यक्षात हल्लेखोर मध्ये बसलेला असतो, शांतपणे मेसेज वाचतो आणि गरज असल्यास बदलतो.

10. रिप्ले अटॅक (Replay Attack)

रिप्ले अटॅक हा एक ॲक्टिव्ह अटॅक आहे, ज्यामध्ये हल्लेखोर एक वैध डेटा ट्रान्समिशन (उदा. प्रमाणीकरण विनंती, आर्थिक व्यवहार) पकडून ठेवतो आणि नंतर तेच संदेश पुन्हा पाठवतो, ज्यामुळे सिस्टम फसवली जाते आणि अनधिकृत प्रवेश किंवा नक्कल व्यवहाराला परवानगी देते. रिप्ले अटॅक हल्लेखोराला मूळ संदेशाचे अर्थ समजून घेण्याची किंवा तो बदलण्याची गरज नसते. तो फक्त वैध संदेश रेकॉर्ड करतो आणि योग्य वेळी पुन्हा पाठवतो. सिस्टमला तो संदेश खरा आणि मूळ असल्यासारखा वाटतो, त्यामुळे ती अनधिकृत कृतीला परवानगी देऊ शकते. रिप्ले अटॅक मुख्यतः प्रमाणीकरण प्रोटोकॉल्स किंवा आर्थिक प्रणालींवर केले जातात, जिथे संदेश पुन्हा पाठवून: अनधिकृत प्रवेश मिळवता येतो, नक्कल (duplicate) आर्थिक व्यवहार केले जाऊ शकतात.

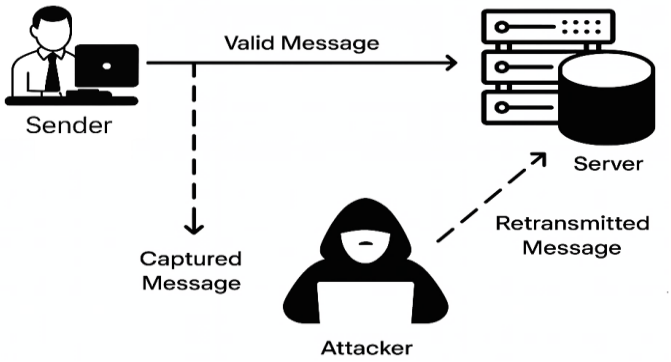


Fig 1.20: रिप्ले अटॅक (Replay Attack)

रिप्ले हल्ल्याचे परिणाम (Impact):

- अनधिकृतपणे प्रणालीमध्ये प्रवेश मिळणे
- बँकिंग किंवा ई-व्यवहारांमध्ये दुबार व्यवहार (Double Transactions) होणे
- सेशन हायजॅकिंग (Session Hijacking)

प्रतिबंध (Countermeasures):

- संदेश नवीन आहे की पुन्हा पाठवलेला हे तपासण्यासाठी टाइमस्टॅम्प्स आणि सत्र टोकनचा वापर
- प्रमाणीकरणामध्ये नॉन्स (Nonces) एकदाच वापरले जाणारे यादृच्छिक क्रमांक वापरणे
- रिप्ले संरक्षणासह मजबूत एनक्रिप्शन वापरणे

उदाहरण (Example): वापरकर्ता ऑनलाइन बँकिंगमध्ये लॉगिन करतो आणि लॉगिन विनंती बँक सर्व्हरकडे जाते. हल्लेखोर ही विनंती पकडून ठेवतो आणि नंतर पुन्हा पाठवतो (Replay). कारण संदेश वैध आहे, बँक सर्व्हर तो खरा समजतो आणि हल्लेखोराला वापरकर्त्याच्या खात्यात प्रवेश देतो, जरी वापरकर्त्याने दुसरी विनंती पाठवलेली नसते.

11. स्निफिंग (Sniffing)

स्निफिंग हा एक पॅसिव्ह अटॅक (Passive Attack) आहे, ज्यामध्ये हल्लेखोर नेटवर्कमधून जाणाऱ्या डेटा-पॅकेट्सना गुपचूप ऐकतो आणि पकडतो. याचा उद्देश वापरकर्ता-नाव, संकेतशब्द, क्रेडिट कार्ड तपशील, सत्र कुकीज यांसारखी संवेदनशील माहिती चोरणे हा असतो. हल्लेखोर स्निफिंगसाठी वायरशार्क, टीसीपीडम्प सारखी साधने वापरतात. स्निफिंग डेटामध्ये कोणताही बदल करत नाही फक्त ऐकते, त्यामुळे त्याचा शोध लागणे अत्यंत कठीण असते.
स्निफिंग कसे केले जाते?

- नेटवर्क इंटरफेस कार्ड (NIC) ला प्रॉमिस्क्युअस मोड मध्ये ठेवले जाते, ज्यामुळे ते सर्व पॅकेट्स पकडते, केवळ त्याच्यासाठी पाठवलेले नव्हे.
- ब्रॉडकास्ट नेटवर्क किंवा असुरक्षित Wi-Fi वर स्निफिंग करणे खूप सोपे असते.
- स्विच केलेल्या नेटवर्कमध्ये हल्लेखोर ARP स्पूफिंग किंवा DNS पॉयझनिंग वापरून ट्रॅफिक स्वतःकडे वळवतात.

स्निफिंग प्रामुख्याने गोपनीयतेस (Confidentiality) धोका निर्माण करते.

स्निफिंग प्रतिबंध (Prevention):

- एनक्रिप्शन वापरणे (HTTPS, VPNs, SSH)
- सुरक्षित Wi-Fi प्रोटोकॉल्स (WPA3)
- IDS/IPS चा वापर
- वापरकर्त्यांची जागरूकता वाढवणे

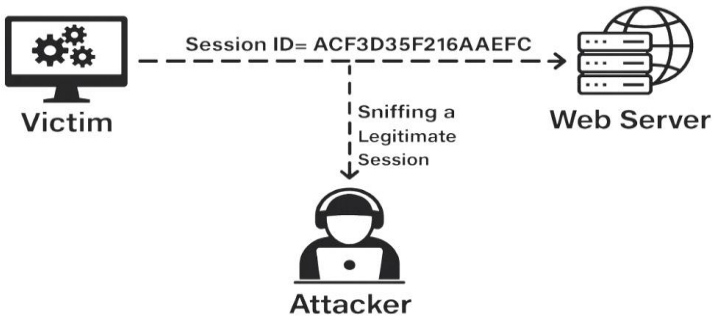


Fig 1.21: स्निफिंग अटॅक (Sniffing)

हल्लेखोर नेटवर्कवरील ट्रॅफिक गुपचूप स्निफ करून बळीच्या सक्रिय सत्राचा (Active Session) सत्र-ओळख क्रमांक (Session Identifier / Session Token) पकडतो. नंतर तोच चोरलेला सत्र-टोकन वापरून बळीचे रूप धारण करतो आणि वेब सर्व्हरशी स्वतःला वैध वापरकर्ता म्हणून दाखवतो. हल्लेखोर जेव्हा हा वैध सत्र-टोकन पुन्हा पाठवतो (Replay करतो), तेव्हा वेब सर्व्हर त्याला खरे सत्र समजून प्रवेश देतो, आणि हल्लेखोराला बळीच्या प्रमाणित सत्रात (Authenticated Session) अनधिकृत प्रवेश मिळतो तेही संकेतशब्द नसतानाच. या तंत्राला सत्र-हायजॅकिंग (Session Hijacking) म्हणतात. यामुळे डेटा चोरी, खाते ताब्यात घेणे किंवा इतर हानिकारक कृती होऊ शकतात, जोपर्यंत HTTPS, सुरक्षित कुकीज, सत्र-फेरबदल (Session Rotation) सारखी संरक्षणात्मक उपाययोजना वापरली जात नाही.

उदाहरण: वापरकर्ता एखाद्या वेबसाइटमध्ये HTTP (एनक्रिप्शन नसलेला) प्रोटोकॉल वापरून लॉगिन करतो. त्याच Wi-Fi वर असलेला हल्लेखोर स्निफर साधन वापरून लॉगिन विनंती पकडतो. कारण वापरकर्तानाव आणि संकेतशब्द सरळ मजकूरात (Plain Text) पाठवले जातात, हल्लेखोर ते सहज वाचतो आणि नंतर बळीच्या नावाने त्या वेबसाइटवर लॉगिन करतो.

1.3.2 टीसीपी/आयपी (TCP/IP) हॅकिंग

टीसीपी/आयपी (TCP/IP) हॅकिंग म्हणजे इंटरनेटवरील संवादासाठी वापरल्या जाणाऱ्या TCP/IP प्रोटोकॉल संचातील (protocol suite) कमकुवतपणांचा फायदा घेऊन केलेले हल्ले. या हल्ल्यांचा उद्देश नेटवर्क ट्रॅफिक अडवणे, रूप धारण करणे, बिघडवणे किंवा चुकीच्या दिशेने वळवणे असा असू शकतो. हे हल्ले प्रोटोकॉलच्या रचनेतील काही गृहितकांचा (assumptions), पूर्वानुमेय फील्ड्सचा (उदा., क्रमांक – sequence numbers) किंवा नेटवर्क उपकरणांमधील चुकीच्या संरचनेचा (misconfiguration) गैरवापर करतात.

TCP/IP प्रोटोकॉलमध्ये सुरक्षेची कमतरता का असते?

TCP/IP प्रोटोकॉलची रचना परस्पर-सुसंगतता (interoperability) आणि वेगासाठी खूप वर्षांपूर्वी केली गेली होती—तेव्हा आधुनिक सायबर हल्ल्यांचा विचार केला नव्हता.

म्हणून:

- IP स्रोत- पत्ता (source address)
- TCP क्रमांक (sequence numbers)
- ARP किंवा DNS नोंदी

हे घटक मजबूत प्रमाणीकरणाशिवाय तयार करण्यात आले.

हल्लेखोर या कमकुवतपणांचा वापर करून:

- बनावट पॅकेट्स तयार करतात (IP Spoofing)
- ऍड्रेस रिझोल्यूशनमध्ये फेरफार करतात (ARP Poisoning)
- सक्रिय सत्र हायजॅक करतात (TCP Session Hijacking)
- प्रोटोकॉल हाताळणारे घटक ओव्हरलोड करतात (SYN Flood**)**

TCP/IP हॅकिंगचे परिणाम:

- अनधिकृत प्रवेश
- डेटा अडवणे किंवा चोरी
- नेटवर्क ट्रॅफिक चुकीच्या मार्गाने वळवणे
- डिनायल ऑफ सर्विस (Denial of Service)

TCP/IP हॅकिंगविरुद्ध संरक्षण (Defence):

प्रोटोकॉल-स्तरावरील संरक्षण:

- अप्रत्याशित फील्ड्सचे यादृच्छिकीकरण (Randomization)
- सुरक्षित विस्तारांचा वापर (Secure Protocol Extensions)

संचालन-स्तरावरील नियंत्रण:

- ट्रॅफिक फिल्टरिंग
- नेटवर्क मॉनिटरिंग
- सुरक्षित संरचना (Secure Configuration)

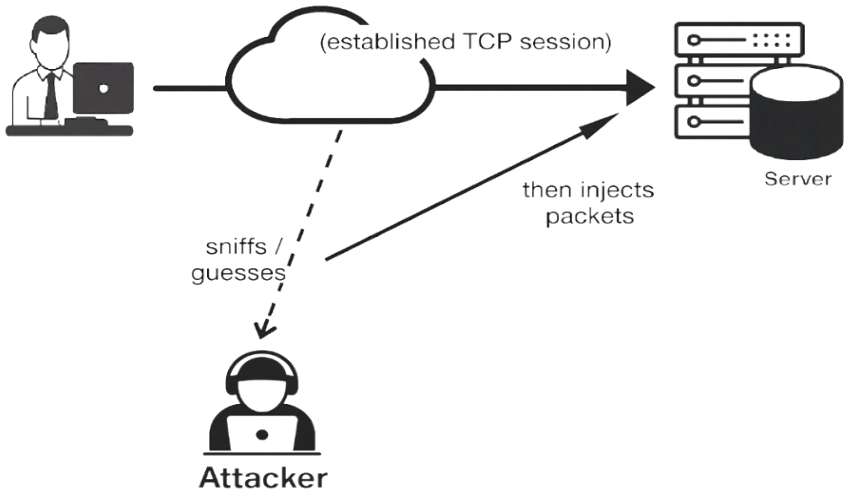


Fig 1.22: TCP/IP हॅकिंग अटॅक

हल्लेखोर नेटवर्कवरील ट्रॅफिक गुपचूप स्निफ करून बळीच्या सक्रिय सत्राशी संबंधित माहिती पकडतो. TCP/IP हॅकिंगमध्ये ही प्रक्रिया अनेक प्रकारच्या हल्ल्यांना कारणीभूत ठरते.

सामान्य TCP/IP हल्ले (Common Attacks):

- **आयपी स्पूफिंग (IP Spoofing):** पॅकेट्सचा स्रोत IP पत्ता बनावट करून त्यांना विश्वासार्ह होस्टकडून आलेले असल्यासारखे दाखवणे.
  उदाहरण: खोटा IP पत्ता वापरून साधे IP-आधारित प्रवेश-नियंत्रण (ACL) चकवणे किंवा हल्लेखोराचा खरा पत्ता लपवणे.
- **टीसीपी सत्र-हायजॅकिंग (TCP Session Hijacking):** TCP क्रमांक (Sequence Numbers) ओळखणे, अंदाज लावणे किंवा पकडणे आणि नंतर बनावट पॅकेट्स इंजेक्ट करून सक्रिय सत्रावर ताबा मिळवणे.
  उदाहरण: हल्लेखोर वापरकर्त्याच्या सक्रिय बँकिंग सत्रात बनावट "फंड ट्रान्सफर" विनंती इंजेक्ट करतो.

- **SYN फ्लड - टीसीपी डिनायल ऑफ सर्विस (SYN Flood – TCP DoS):** TCP 3-way handshake चा गैरवापर करून मोठ्या प्रमाणात SYN विनंत्या पाठवणे, त्या पूर्ण न करणे, आणि सर्व्हरचा कनेक्शन टेबल भरून टाकणे.
  उदाहरण: बँकेची वेबसाइट अनुपलब्ध होते कारण सर्व्हरचे बॅकलॉग अर्धवट (half-open) कनेक्शनने भरते.
- **ARP पॉयझनिंग / ARP स्पूफिंग:** लॅन (LAN) बनावट ARP संदेश पाठवून हल्लेखोराचा MAC पत्ता दुसऱ्या होस्टच्या IP शी जोडणे, ज्यामुळे संपूर्ण ट्रॅफिक हल्लेखोराकडे वळतो.
  उदाहरण:
  हल्लेखोर स्वतःला गेटवे म्हणून दर्शवतो आणि बळींच्या स्पष्ट-टेक्स्ट (plaintext) क्रेडेन्शियल्स पकडतो (Sniffing + MITM).
- **डीएनएस स्पूफिंग / कॅश पॉयझनिंग (DNS Spoofing / Cache Poisoning):** खोट्या DNS नोंदी टाकून वापरकर्त्यांना दुष्ट सर्व्हरकडे वळवणे (फिशिंग, मालवेअर प्रसार इत्यादीसाठी).
  उदाहरण: bank.example या बँकेच्या वेबसाइटवर जाण्याचा प्रयत्न करणारा वापरकर्ता हल्लेखोराच्या साइटवर पोहोचतो.
- **रूट मॅनिप्युलेशन / BGP हायजॅकिंग:** BGP मध्ये खोटे रूट जाहीर करून इंटरनेटवरील ट्रॅफिक वळवणे किंवा ब्लॅकहोल करणे.
  उदाहरण: अधिक विशिष्ट रूट जाहीर करून एका संपूर्ण आयपी श्रेणीचा मोठ्या प्रमाणात ट्रॅफिक अडवणे.

उदाहरण (TCP Session Hijack Scenario): एक कर्मचारी एनक्रिप्शन नसलेल्या नेटवर्कवर वेबमेलमध्ये लॉगिन करतो. हल्लेखोर स्निफर वापरून त्या सत्राचे TCP क्रमांक (Sequence Numbers) आणि सेशन-कुकी (Session Cookie) पकडतो. नंतर तोच क्रमांक आणि कुकी वापरून बनावट पॅकेट्स इंजेक्ट करतो.

परिणाम:

- हल्लेखोर सत्रावर पूर्ण ताबा मिळवतो
- बळीच्या नावाने ईमेल वाचतो
- ईमेल पाठवतो
- खाते पूर्णपणे काबीज करतो

1.3.3 सोशल इंजिनिअरिंग (Social Engineering)

सोशल इंजिनिअरिंग म्हणजे लोकांना फसवून त्यांच्याकडून गोपनीय माहिती उघड करवून घेणे किंवा विशिष्ट कृती करून घेणे, ज्यामुळे प्रणालीची सुरक्षा धोक्यात येऊ शकते. या हल्ल्यांमध्ये हल्लेखोर तांत्रिक उणिवांचा वापर न करता किंवा त्यासोबत मानवी मानसशास्त्राचा विश्वास, भीती, कुतूहल, मदत करण्याची वृत्ती गैरवापर करतो आणि सुरक्षा नियंत्रणांना चकवतो. सोशल इंजिनिअरिंग हल्ले मानवांना लक्ष्य करतात, प्रणालींना नव्हे.

हल्लेखोर विश्वासार्ह वाटणारी गोष्ट तयार करतो (Pretexting), तातडी निर्माण करतो (Urgency / Pressure), अधिकृततेचा भास निर्माण करतो (Authority Exploitation) आणि बळी व्यक्तीला संकेतशब्द देण्यासाठी, प्रवेश परवानगी देण्यासाठी, किंवा हानिकारक सॉफ्टवेअर इंस्टॉल करण्यासाठी फसवतो. कारण मानव हा सुरक्षा साखळीतील सर्वात कमकुवत दुवा असतो, म्हणूनच अत्यंत सुरक्षित प्रणाली देखील वापरकर्ते फसल्यास तोडल्या जाऊ शकतात.

प्रभावी संरक्षण कसे करावे?

सोशल इंजिनिअरिंगला तोंड देण्यासाठी केवळ तांत्रिक सुरक्षा पुरेशी नसते; त्यासोबत: वापरकर्ता शिक्षण (User Awareness Training), कडक सुरक्षा धोरणे (Strict Security Policies), ओळख पडताळणी प्रक्रिया (Verification Procedures) यांचा समावेश आवश्यक आहे. तांत्रिक नियंत्रणांमध्ये प्रमाणीकरण (Authentication), नोंदी ठेवणे आणि निरीक्षण (Logging & Monitoring) हे उपाय देखील महत्त्वाचे असतात.

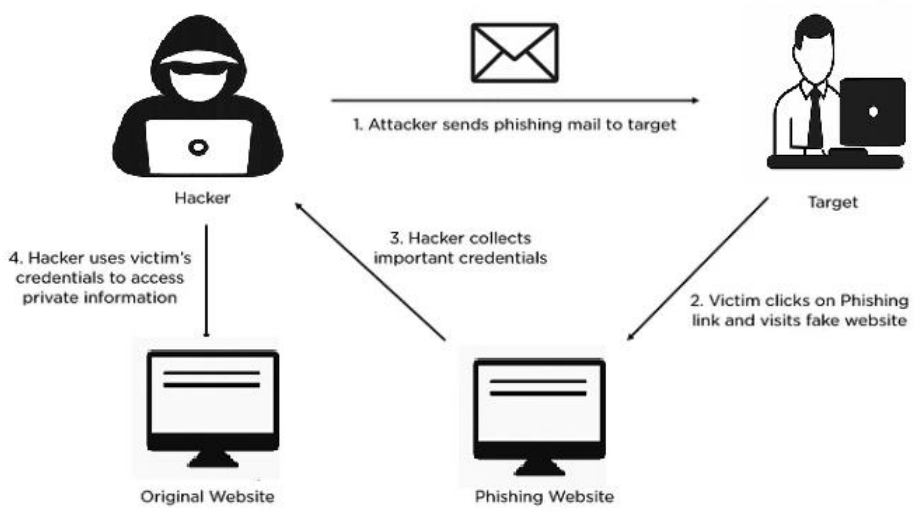


Fig 1.23: फिशिंग-बेस्ड सोशिअल इंजिनिअरिंग (Social Engineering)

हल्लेखोर लक्षित व्यक्तीला अविश्वसनीय / बनावट ईमेल पाठवतो. लक्षित व्यक्ती त्या ईमेलमधील हानिकारक दुव्यावर क्लिक करते आणि बनावट (फिशिंग) वेबसाइटवर जाते. तेथे ती स्वतःची ओळख माहिती / संकेतशब्द टाकते. हल्लेखोर ही सर्व माहिती संकलित करून नंतर ती वापरून बळीच्या खऱ्या खात्यात किंवा प्रणालींमध्ये प्रवेश मिळवतो.

उदाहरण: एक हल्लेखोर एखाद्या कर्मचाऱ्याला फोन करून स्वतःला IT विभागातील कर्मचारी असल्याचे सांगतो आणि म्हणतो: "आम्हाला तुमच्या खात्यात गंभीर सुरक्षा समस्या आढळली आहे. तुमचा पासवर्ड तात्काळ हवा आहे, जेणेकरून मी तुमचे खाते पुन्हा कॉन्फिगर करू शकेन." कर्मचारी, कॉल खरा असल्याचा समज करून आणि तातडीच्या दबावामुळे, पासवर्ड देतो. त्यानंतर हल्लेखोर त्या पासवर्डचा वापर करून कंपनीच्या प्रणालींमध्ये लॉगिन करतो आणि गोपनीय फाईल्स चोरी करतो.

1.4 मालवेअरचे प्रकार (Types of Malwares)

मालवेअर्स (Malwares): मालवेअर म्हणजे दुर्भावनायुक्त सॉफ्टवेअर, जे संगणक प्रणालींना, जाळ्यांना किंवा डेटाला हानी पोहोचवण्यासाठी, माहिती चोरी करण्यासाठी, किंवा अनधिकृत प्रवेश मिळवण्यासाठी जाणीवपूर्वक तयार केले जाते. मालवेअर हा एक विस्तृत प्रकार असून त्यामध्ये व्हायरस, वर्म, ट्रोजन, स्पायवेअर, रॅन्समवेअर, रूटकिट्स यांसारख्या अनेक हानिकारक प्रोग्राम्सचा समावेश होतो.

मालवेअरचे प्रकार (Types of Malware)

1. व्हायरस (Virus)

कंप्यूटर व्हायरस हा एक प्रकारचा हानिकारक प्रोग्राम आहे जो स्वतःला एखाद्या होस्ट फाईल किंवा अनुप्रयोगाला चिकटवून ठेवतो, आणि ती फाईल चालवल्यावर सक्रिय होतो. हा स्वतःची प्रतिमा तयार (Self-replication) करू शकतो आणि इतर फाईल्स, प्रोग्राम्स किंवा संगणकांवर पसरू शकतो. यामुळे डेटा खराब होणे, फाईल्स नष्ट होणे, किंवा प्रणालीची कार्यक्षमता कमी होणे असे नुकसान घडू शकते.

व्हायरसचे वैशिष्ट्ये: संगणकातील सामान्य कार्यप्रवाह बिघडवणे, प्रोग्राम्समध्ये बदल करणे, फाईल्स भ्रष्ट करणे, प्रणालीची साधने (resources) खर्च करणे, संक्रमित फाईल्स, ईमेल अटॅचमेंट्स, USB ड्राईव्ह, नेटवर्क शेअरिंगद्वारे पसरने.

महत्वाची गोष्ट: वर्मपेक्षा वेगळे, व्हायरस सक्रिय होण्यासाठी वापरकर्त्याची कृती आवश्यक असते, जसे की संक्रमित फाईल चालवणे. एकदा सक्रिय झाल्यावर, व्हायरस स्वतःची प्रती तयार करतो, डेटा बदलतो किंवा हटवतो, प्रणाली काम न करण्याजोगी बनवतो.

आधुनिक व्हायरसचे प्रकार:

- पॉलिमॉर्फिक व्हायरस (Polymorphic): स्वतःचा कोड बदलत राहतात, त्यामुळे अँटिव्हायरसना ओळखणे कठीण
- मेटामॉर्फिक व्हायरस (Metamorphic): प्रत्येक नव्या प्रतिमेत संपूर्ण रचना बदलतात

व्हायरसपासून संरक्षण: अद्ययावत अँटिव्हायरस सॉफ्टवेअर वापरणे, सुरक्षा पॅचेस इंस्टॉल करणे, सुरक्षित ब्राउजिंग करणे, अज्ञात ईमेल अटॅचमेंट्स न उघडणे.

व्हायरसचे जीवनचक्र (Lifecycle of a Virus)

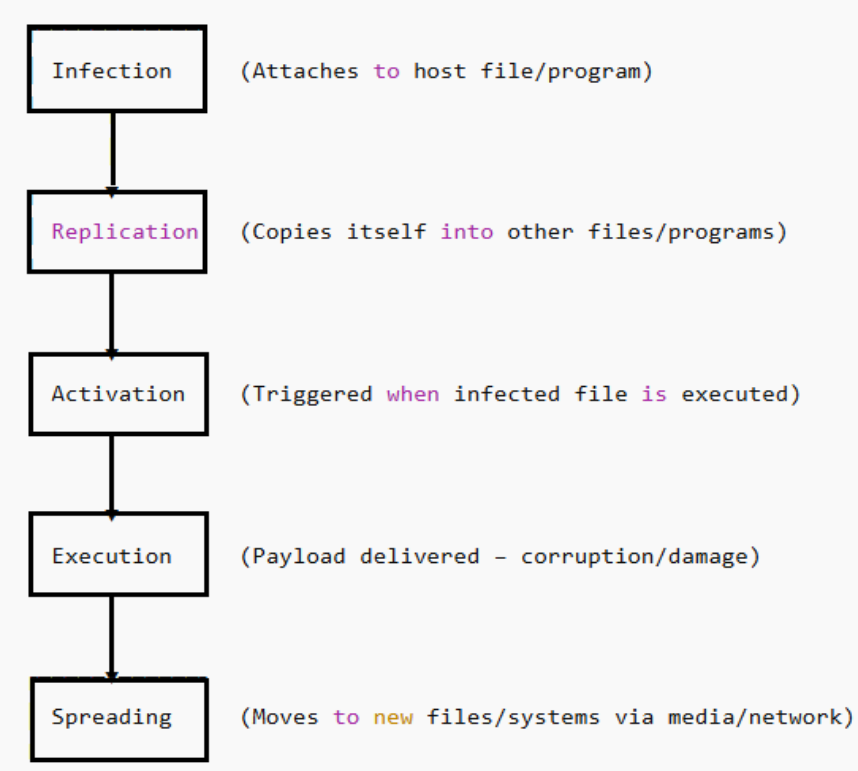


Fig 1.24: व्हायरसचा जीवनचक्र (Lifecycle of a Virus)

1. **संक्रमण (Infection):** व्हायरस स्वतःला होस्ट फाईल किंवा प्रोग्रामला चिकटवतो. यामुळे फाईल उघडल्यावर व्हायरस सक्रिय होण्याची शक्यता निर्माण होते.
2. **प्रतिकृती बनवणे (Replication):** व्हायरस स्वतःच्या प्रतिमा तयार करतो आणि त्या इतर फाईल्स किंवा प्रोग्राम्समध्ये कॉपी करतो. हा टप्पा व्हायरसच्या प्रसाराची सुरुवात करतो.
3. **सक्रियता (Activation):** संक्रमित फाईल चालवली गेली (executed) की व्हायरस सक्रिय होतो. वापरकर्ता नकळत फाईल उघडतो आणि व्हायरस कार्यरत होऊ लागतो.
4. **अंमलबजावणी (Execution):** या टप्प्यात व्हायरस त्याचे पेलोड (Payload) चालवतो, ज्यामध्ये: डेटा खराब करणे, फाईल्स हटवणे, प्रणाली ला नुकसान करणे यांसारख्या हानिकारक क्रिया असतात.
5. **प्रसार (Spreading):** व्हायरस नवीन फाईल्स किंवा संगणकांमध्ये पसरतो, हे माध्यम किंवा नेटवर्कद्वारे होते: USB, ईमेल अटॅचमेंट, नेटवर्क शेअरिंग यांद्वारे व्हायरस इतर प्रणालींमध्ये पोहोचतो.

उदाहरणे (Examples)

- मॅक्रो व्हायरस (Macro Virus): MS Word किंवा Excel सारख्या अनुप्रयोगांमधील मॅक्रो स्क्रिप्ट्सद्वारे दस्तऐवज संक्रमित करणारा व्हायरस.
  उदाहरण: मेलिसा व्हायरस (1999) संक्रमित ईमेल अटॅचमेंट्सद्वारे अतिशय वेगाने पसरला.
- बूट सेक्टर व्हायरस (Boot Sector Virus): स्टोरेज डिव्हाइसच्या मास्टर बूट रेकॉर्ड (MBR) मध्ये स्वतःला स्थापित करणारा व्हायरस. संगणक सुरू होताच (Boot होताच) सक्रिय होतो.
  उदाहरण: मायकेलएंजेलो व्हायरस (Michelangelo Virus)

प्रतिबंध आणि शोध (Prevention and Detection):

प्रतिबंध (Prevention):

1. अँटिव्हायरस सॉफ्टवेअरचा वापर
2. ऑपरेटिंग सिस्टीमचे नियमित अपडेट
3. अज्ञात / संशयास्पद फाईल्स डाउनलोड किंवा उघडू नये
4. फायरवॉल सक्षम ठेवणे

शोध (Detection):

1. अँटिव्हायरस स्कॅनिंग
2. फाईल अखंडता तपासणी (Integrity Checks)
3. फाईल्स वेगव्या पद्धतीने खराब होणे किंवा संशयास्पद वर्तन दिसणे

2. वर्म (Worms)

वर्म हा एक स्वतःहून प्रतिकृती तयार करणारा (Self-Replicating) आणि मानवी कृतीची आवश्यकता नसलेला हानिकारक प्रोग्राम आहे.तो साध्या व्हायरसपेक्षा वेगळा आहे कारण व्हायरस फाईल्स किंवा प्रोग्राम्सना चिकटतो पण वर्म हे स्वतंत्र प्रोग्राम असते.वर्म सिस्टम किंवा नेटवर्कमधील कमकुवतपणांचा (Vulnerabilities) फायदा घेऊन स्वतःला वेगाने नेटवर्कमध्ये पसरवतो. कंप्यूटर वर्म हा सर्वात धोकादायक मालवेअर प्रकारांपैकी एक आहे, कारण तो स्वतःची प्रतिकृती तयार करून (Self-Replicating) अतिशय वेगाने नेटवर्कमध्ये पसरू शकतो. व्हायरसपेक्षा वेगळे, वर्मला कोणत्याही होस्ट फाईलची आवश्यकता नसते; तो स्वतंत्र प्रोग्राम म्हणून अस्तित्वात असतो. वर्म ऑपरेटिंग सिस्टीममधील, ईमेल सेवा, किंवा कम्युनिकेशन प्रोटोकॉल्समधील कमकुवतपणांचा गैरवापर करून प्रणालींमध्ये प्रवेश करतो आणि पसरतो. वर्म प्रणालीला कसा त्रास देतो? एकदा वर्म संगणकात आला की तो: सिस्टम संसाधने खूप प्रमाणात वापरतो (मेमरी, बँडविड्थ), संगणकाचा वेग कमी करतो, प्रणाली हँग होणे किंवा क्रॅश होणे यांसारखे परिणाम घडवतो. काही वर्ममध्ये पेलोड (Payload) देखील असतो, ज्याद्वारे ते फाईल्स नष्ट करू शकतात बॅकडोअर बसवू शकतात हल्लेखोरांना दूरस्थ नियंत्रण देऊ शकतात. वर्मचे सर्वात मोठे धोके वर्मचा सर्वात गंभीर धोका म्हणजे तो अत्यंत अल्प वेळात मोठ्या प्रमाणात नेटवर्कमध्ये पसरून प्रचंड व्यत्यय आणि नुकसान घडवू शकतो.

इतिहासातील मोठ्या हल्ल्यांमध्ये: कोड रेड वर्म (Code Red Worm) कॉन्फिकर वर्म (Conficker Worm) हे वर्म अतिशय वेगाने हजारो–लाखो संगणकांमध्ये पसरले.

वर्मपासून संरक्षण (Prevention)

- ऑपरेटिंग सिस्टीम आणि सॉफ्टवेअरचे नियमित पॅचिंग
- मजबूत फायरवॉल वापरणे
- घुसखोरी शोध प्रणाली (IDS)
- नेटवर्क मॉनिटरिंग

वर्मचे जीवनचक्र (Lifecycle of a Worm):

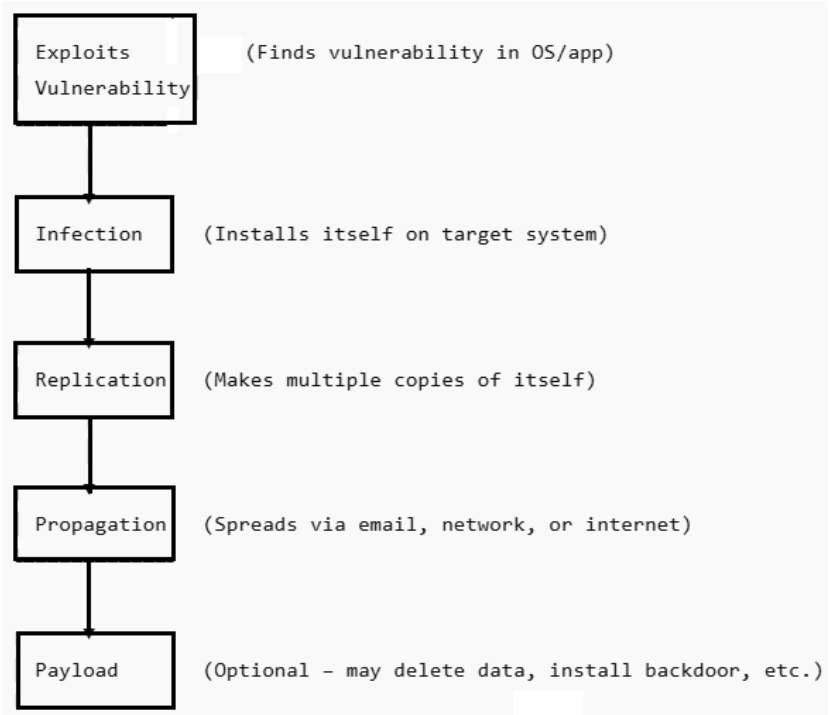


Fig 1.25: वर्मचे जीवनचक्र (Lifecycle of a Worm)

1. **कमकुवतपणा शोधणे आणि त्याचा गैरवापर करणे (Exploits Vulnerability):** वर्म ऑपरेटिंग सिस्टीम किंवा अनुप्रयोगातील कमकुवतपणा (Vulnerability) शोधतो आणि त्याचा उपयोग करून प्रणालीमध्ये शिरतो.
2. **संक्रमण (Infection):** वर्म स्वतःला लक्ष्य प्रणालीवर इंस्टॉल करतो.
3. **प्रतिकृती बनवणे (Replication):** वर्म स्वतःच्या अनेक प्रतिमा तयार करतो (Self-Replication).
4. **प्रसार (Propagation):** वर्म ईमेल, नेटवर्क किंवा इंटरनेटद्वारे नवीन प्रणालींमध्ये वेगाने पसरतो.
5. **पेलोड (Payload):** या टप्प्यात वर्म डेटा हटवू शकतो, बॅकडोअर इंस्टॉल करू शकतो, प्रणालीचे नियंत्रण हल्लेखोराकडे पाठवू शकतो किंवा इतर हानिकारक क्रिया करू शकतो.

उदाहरणे (Examples)

1. कोड रेड वर्म (Code Red Worm, 2001): Microsoft IIS वेब सर्व्हरमधील कमकुवतपणाचा (vulnerability) गैरवापर करून शेकडो हजारो प्रणाली संक्रमित केल्या आणि मोठ्या प्रमाणावर डिनायल-ऑफ-सर्व्हिस (Denial-of-Service (DoS)) अटॅक केले.
2. वॉन्नाक्राय (WannaCry, 2017): EternalBlue exploit चा वापर करून अतिशय वेगाने पसरलेला वर्म-आधारित रॅन्समवेअर. यामुळे जगभरात 200000 हून अधिक प्रणाली प्रभावित झाल्या.

प्रतिबंध आणि शोध (Prevention and Detection):

प्रतिबंध (Prevention):

- प्रणाली नियमितपणे पॅच करणे
- IDS/IPS वापरणे
- अनावश्यक सेवा बंद / मर्यादित करणे
- मजबूत फायरवॉल संरक्षण सक्षम ठेवणे

शोध (Detection):

- नेटवर्क ट्रॅफिकचे निरीक्षण करणे
- बँडविड्थ वापरातील असामान्य वाढ तपासणे
- IDS अलर्ट्स वर लक्ष ठेवणे

Table 1.3: कम्पॅरिझन: व्हायरस (Virus) वि. वर्म (Worm)

वैशिष्ट्य (Feature)	व्हायरस (Virus)	वर्म (Worm)
व्याख्या (Definition)	होस्ट फाईल किंवा प्रोग्रामला चिकटून राहणारा हानिकारक प्रोग्राम, जो ती होस्ट फाईल चालवल्यावर सक्रिय होतो.	एक स्वतंत्र, स्वतंत्रपणे चालणारा (Standalone) हानिकारक प्रोग्राम जो नेटवर्कमध्ये आपोआप पसरतो, आणि होस्टची गरज नसते.
अवलंबन (Dependency)	पसरायला होस्ट फाईल/प्रोग्रामची गरज असते.	कोणत्याही होस्टची गरज नाही; तो स्वतः पूर्ण (Self-contained) असतो.
प्रसार (Propagation)	संक्रमित फाईल्स शेअर केल्या गेल्यानंतर (USB, ईमेल अटॅचमेंट्स इ.) पसरतो.	नेटवर्कद्वारे आपोआप पसरतो कमकुवतपणाचा गैरवापर करून किंवा स्वतःच्या प्रतिमा पाठवून.
अंमलबजावणी (Execution)	वापरकर्त्याची कृती आवश्यक (जसे की संक्रमित फाईल चालवणे).	सिस्टममध्ये शिरल्यावर आपोआप चालतो; वापरकर्त्याच्या कृतीची आवश्यकता नसते.
प्रसाराचा वेग (Speed of Spread)	तुलनेने मंद, कारण वापरकर्त्याच्या क्रियेवर अवलंबून.	अत्यंत वेगवान, कारण नेटवर्कद्वारे सतत पसरतो.

नुकसान (Damage)	फाईल्स भ्रष्ट करणे किंवा हटवणे, सिस्टमचा वेग कमी करणे, डेटा चोरी करणे.	नेटवर्क बँडविड्थ वापरून नेटवर्क क्रॅश करणे, बॅकडोअर बसवणे, किंवा पेलोड चालवणे.
उदाहरणे (Examples)	मेलिसा व्हायरस, ILOVEYOU व्हायरस.	SQL Slammer वर्म, WannaCry वर्म.

3. ट्रोजन हॉर्स (Trojan horse)

ट्रोजन हॉर्स हा असा दुर्भावनायुक्त सॉफ्टवेअर प्रकार आहे जो स्वतःला वैध किंवा उपयुक्त प्रोग्रामचे रूप देतो, जेणेकरून वापरकर्ते ते विश्वासाने इंस्टॉल करतील.व्हायरस किंवा वर्मपेक्षा वेगळे, ट्रोजन स्वतःची प्रतिकृती तयार करत नाही; तो फसवणुकीवर (Deception) अवलंबून असतो.एकदा इंस्टॉल झाल्यावर ट्रोजन बॅकडोअर तयार करतो, डेटा चोरी करतो, किंवा अतिरिक्त मालवेअर इंस्टॉल करतो.ट्रोजन हॉर्स नावाची उत्पत्ती"ट्रोजन हॉर्स" हा शब्द ग्रीक पुराणकथेतून आलेला आहे, जिथे ग्रीकांनी मोठ्या लाकडी घोड्यात सैनिक लपवून ट्रॉय शहरात गुपचूप प्रवेश मिळवला. त्याचप्रमाणे, संगणक सुरक्षेतील ट्रोजन स्वतःला निरुपद्रवी / उपयुक्त सॉफ्टवेअर असल्याचे भासवतो, पण त्यामध्ये लपलेले हानिकारक कार्य असते.

ट्रोजन कसा पसरतो? वापरकर्ते ट्रोजन डाउनलोड करतात कारण तो: खरा अनुप्रयोग असल्यासारखा दिसतो. मोफत गेम किंवा मोफत साधन असल्यासारखा भासवतो. सिस्टम अपडेटसारखा दिसतो. वापरकर्ते फसवले गेले की ट्रोजन सिस्टममध्ये स्थापित होतो. इंस्टॉल झाल्यावर ट्रोजन काय करू शकतो? संकेतशब्द, बँक माहिती, वैयक्तिक फाईल्स चोरी करणे. दूरस्थ प्रवेश देऊन हल्लेखोराला सिस्टम नियंत्रित करण्याची परवानगी देणे. सिस्टमला बॉटनेट चा भाग बनवणे. अतिरिक्त मालवेअर डाउनलोड / इंस्टॉल करणे. व्हायरस किंवा वर्मपेक्षा फरक: ट्रोजन आपोआप पसरत नाही. सामाजिक अभियांत्रिकी (Social Engineering) वापरून बळीला फसवून इंस्टॉल करवावे लागते.

प्रतिबंध (Prevention):

- वापरकर्त्यांची जागरूकता आणि सतर्कता.
- अद्ययावत अँटिव्हायरस सोल्यूशन.
- फक्त विश्वसनीय स्रोतांमधून डाउनलोड.
- अज्ञात ईमेल अटॅचमेंट्स / दुवे न उघडणे.

ट्रोजन हॉर्सची कार्यपद्धती (Working of a Trojan horse):

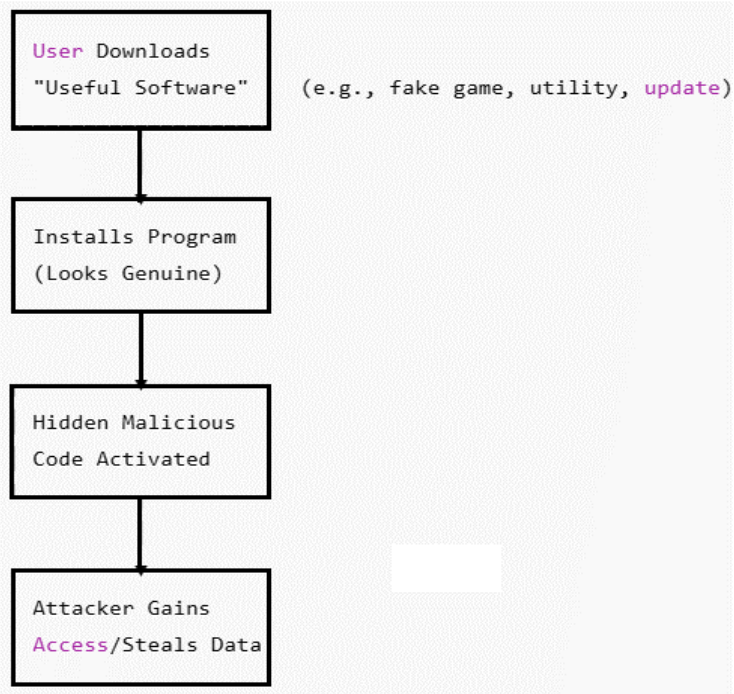


Fig 1.26 : ट्रोजन हॉर्सची कार्यपद्धती (Working of a Trojan Horse)

1. **वापरकर्ता "उपयुक्त सॉफ्टवेअर" डाउनलोड करतो:** (उदा., बनावट गेम, Utility, अपडेट इ.) ट्रोजन स्वतःला Genuine / उपयुक्त प्रोग्राम असल्याचे भासवतो.
2. **प्रोग्राम इंस्टॉल केला जातो (खरा असल्यासारखा दिसतो):** वापरकर्त्याला यात काहीही संशय येत नाही.
3. **लपलेला दुष्ट कोड (Malicious Code) सक्रिय होतो:** इंस्टॉल झाल्यानंतर ट्रोजनचे खरे हानिकारक कार्य सुरू होते.
4. **हल्लेखोराला प्रवेश मिळतो / डेटा चोरी होतो:** हल्लेखोर आता सिस्टमवर: अनधिकृत प्रवेश मिळवतो, संवेदनशील डेटा चोरी करतो, प्रणालीवर नियंत्रण मिळवतो.

उदाहरणे (Examples)

- झ्यूस ट्रोजन (Zeus Trojan / Zbot): सर्वात कुप्रसिद्ध बँकिंग ट्रोजन पैकी एक. हा ट्रोजन की-स्ट्रोक लॉगिंग (Keystroke Logging) करून बँकिंग माहिती, संकेतशब्द, आणि आर्थिक तपशील चोरी करतो.
- रिमोट ॲक्सेस ट्रोजन्स (RATs): उदा., DarkComet, Poison Ivy. हे ट्रोजन्स हल्लेखोराला बळीच्या संगणकावर पूर्ण नियंत्रण देतात- फाईल्स पाहणे, डेटा चोरी, वेबकॅम/मायक्रोफोनवर नियंत्रण, आणि संपूर्ण सिस्टीम रिमोटली ऑपरेट करणे.

प्रतिबंध आणि शोध (Prevention and Detection):

प्रतिबंध (Prevention):

- फक्त विश्वसनीय स्रोतांमधून सॉफ्टवेअर डाउनलोड करणे
- वापरकर्त्यांची जागरूकता आणि सुरक्षित सवयी
- मजबूत फायरवॉल संरक्षण

शोध (Detection):

- वर्तन-आधारित निरीक्षण (Behavior-based Monitoring)
- प्रणालीमध्ये दिसणाऱ्या असामान्य प्रक्रिया (Unusual Processes)
- संशयास्पद नेटवर्क ट्रॅफिक वर लक्ष ठेवणे

4. स्पायवेअर (Spyware):

स्पायवेअर हा एक प्रकारचा मालवेअर आहे जो वापरकर्त्याच्या माहितीशिवाय किंवा संमतीशिवाय त्याच्या क्रियाकलापांवर गुप्तपणे लक्ष ठेवतो आणि की-स्ट्रोक्स, ब्राउझिंग सवयी, तसेच वैयक्तिक माहिती गोळा करतो. तो अनेकदा फ्री सॉफ्टवेअरसोबत जोडलेला (bundled) असतो किंवा वैध अनुप्रयोग असल्यासारखा भासवला जातो. स्पायवेअरची रचना प्रणालीमध्ये गुपचूप प्रवेश करण्यासाठी आणि वापरकर्त्याच्या क्रियाकलापांचा मागोवा घेण्यासाठी केली जाते. याचा उद्देश प्रामुख्याने संवेदनशील माहिती चोरी करणे हा असतो, जसे की लॉगिन क्रेडेन्शियल्स, आर्थिक तपशील, किंवा वैयक्तिक माहिती. व्हायरस किंवा वर्मपेक्षा वेगळे, स्पायवेअर सहसा फाईल्सचे नुकसान करत नाही, परंतु गोपनीयता आणि सुरक्षा धोक्यात आणतो. स्पायवेअर खालील क्रिया करू शकतो: की-स्ट्रोक्स कॅप्चर करणे, ब्राउझिंग इतिहास नोंदवणे, ऑनलाइन खरेदीवर लक्ष ठेवणे, वापरकर्त्याचा वेबकॅम किंवा मायक्रोफोन हायजॅक करणे. स्पायवेअर अनेकदा फ्रीवेअर, पायरेटेड सॉफ्टवेअर, किंवा दुष्ट ईमेल अटॅचमेंट्स सोबत येतो. स्पायवेअरचे काही प्रकार लक्ष्यित जाहिरातींसाठी (Adware) वापरले जातात, तर काही सायबर गुन्हेगारांकडून की-लॉगर्स म्हणून वापरले जातात. स्पायवेअर संसर्ग टाळण्यासाठी, वापरकर्त्यांनी अविश्वसनीय स्रोतांमधून डाउनलोड टाळणे, ऑपरेटिंग सिस्टीम अद्ययावत ठेवणे, तसेच मजबूत अँटी-स्पायवेअर आणि फायरवॉल संरक्षण वापरणे आवश्यक आहे.

स्पायवेअरची कार्यपद्धती (Working of Spyware):

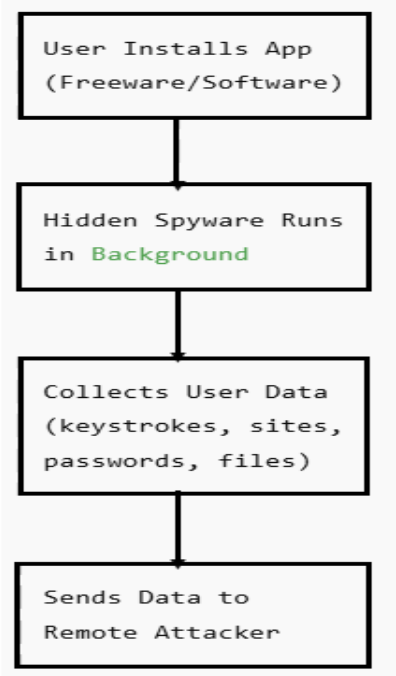


Fig 1.27: स्पायवेअरची कार्यपद्धती (Working of a Spyware)

1. **वापरकर्ता ॲप इंस्टॉल करतो (User Installs App)** – स्पायवेअर अनेकदा फ्रीवेअर, पायरेटेड सॉफ्टवेअर किंवा बनावट ॲप्लिकेशनसोबत जोडलेले असते.
2. **लपलेले स्पायवेअर बॅकग्राऊंडमध्ये चालू होते (Hidden Spyware Runs in Background)** – वापरकर्त्याच्या लक्षात न येता स्पायवेअर शांतपणे सक्रिय होते.
3. **वापरकर्ता डेटा संकलन (Collects User Data)** – स्पायवेअर, की-स्ट्रोक्स, ब्राउझिंग ॲक्टिव्हिटी, संकेतशब्द, फाईल्स यांची नोंद ठेवते.
4. **डेटा दूरस्थ हल्लेखोराकडे पाठवणे (Sends Data to Remote Attacker)** – चोरी केलेली माहिती सायबर गुन्हेगारांकडे पाठवली जाते आणि तिचा गैरवापर केला जातो.

उदाहरण (Example):

- की-लॉगर (Keyloggers): वापरकर्ता टाइप करत असलेले सर्व काही संकेतशब्द आणि वैयक्तिक माहिती नोंदवतात.
- कूलवेबसर्च (CoolWebSearch): वेब ब्राउझर हायजॅक करून माहिती चोरी करणारा स्पायवेअर प्रोग्राम.
- डार्कहॉटेल स्पायवेअर (DarkHotel Spyware): हॉटेल Wi-Fi वापरकर्त्यांवर लक्ष्यित सायबर गुप्तहेरगिरीसाठी वापरले जाणारे स्पायवेअर.

5. ॲडवेअर (Adware):

ॲडवेअर हा एक प्रकारचा सॉफ्टवेअर आहे जो वापरकर्त्याच्या संमतीशिवाय संगणक किंवा मोबाइल डिव्हाइसवर आपोआप जाहिराती दाखवतो, डाउनलोड करतो किंवा इंजेक्ट करतो. काही ॲडवेअर कायदेशीर असून ते फ्रीवेअरसोबत जोडलेले असते, परंतु दुर्भावनायुक्त ॲडवेअर वापरकर्त्याच्या क्रियाकलापांवर लक्ष ठेवून गोपनीयतेला धोका निर्माण करू शकते. ॲडवेअर साधारणपणे फ्री सॉफ्टवेअर किंवा शेअरवेअरसोबत इंस्टॉल होते, ज्यामुळे सॉफ्टवेअर विकसकांना उत्पन्न मिळते. जरी सर्व ॲडवेअर हानिकारक नसले, तरी अनेक ॲडवेअर प्रोग्राम्स ब्राउझिंग वर्तनावर नजर ठेवतात आणि पॉप-अप्स, बॅनर्स किंवा रिडायरेक्ट्स स्वरूपात त्रासदायक जाहिराती दाखवतात. काही दुर्भावनायुक्त ॲडवेअर स्पायवेअरप्रमाणे वागते, वापरकर्त्याचा डेटा गोळा करते आणि तो जाहिरातदार किंवा हल्लेखोरांकडे पाठवते. ॲडवेअर सिस्टम संसाधने वापरते, संगणकाची कार्यक्षमता कमी करते आणि ब्राउझिंगचा अनुभव त्रासदायक बनवते. काही गंभीर परिस्थितींमध्ये, ते इतर मालवेअर संसर्गासाठी बॅकडोअर उघडते. ॲडवेअर पासून संरक्षणासाठी वापरकर्त्यांनी: अविश्वसनीय स्रोतांमधून डाउनलोड टाळावे, ॲडवेअर -ब्लॉकर वापरावा, अद्ययावत अँटी-मालवेअर साधनांनी प्रणालीचे नियमित स्कॅन करावे.

अॅडवेअरची कार्यपद्धती (Working of Adware):

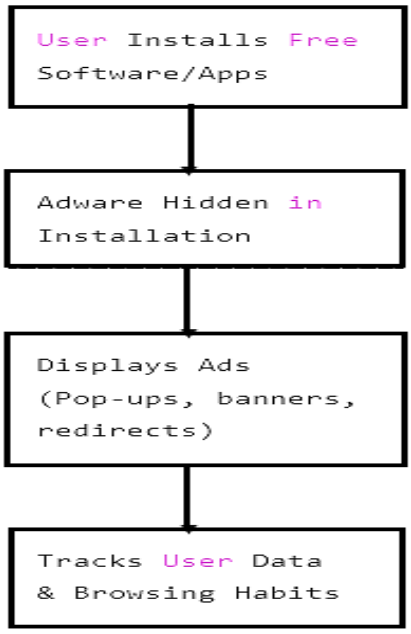


Fig 1.28: अॅडवेअरची कार्यपद्धती (Working of Adware)

1. **वापरकर्ता फ्री सॉफ्टवेअर / अॅप्स इंस्टॉल करतो (User Installs Free Software/Apps)** – अॅडवेअर अनेकदा फ्रीवेअर किंवा बनावट अॅप्लिकेशनसोबत जोडलेले असते.
2. **इंस्टॉलेशनमध्ये लपलेले अॅडवेअर (Adware Hidden in Installation)** – अॅडवेअर वापरकर्त्याच्या लक्षात न येता बॅकग्राऊंडमध्ये शांतपणे इंस्टॉल होते.
3. **जाहिराती दाखवतो (Displays Ads)** – पॉप-अप्स, बॅनर्स, रिडायरेक्ट्स यांसारख्या त्रासदायक जाहिराती दिसू लागतात.
4. **वापरकर्ता डेटा आणि ब्राउझिंग सवयी ट्रॅक करतो (Tracks User Data & Browsing Habits)** – अॅडवेअर वापरकर्त्याच्या क्रियाकलापांवर नजर ठेवते आणि माहिती जाहिरातदार किंवा हल्लेखोरांकडे पाठवते.

उदाहरण (Example)

- Fireball: ब्राउझर हायजॅक करून दुष्ट प्लग-इन्स इंस्टॉल करणारा अॅडवेअर.
- Gator (GAIN): 2000 च्या सुरुवातीच्या काळातील अॅडवेअर, जो पॉप-अप जाहिराती दाखवत असे आणि ऑनलाइन क्रियाकलाप ट्रॅक करत असे.
- Clippy-शैलीचे बनावट टूलबार्स: फ्रीवेअरसोबत येणारे अनेक बनावट टूलबार्समध्ये अॅडवेअर घटक असत.

प्रतिबंध आणि शोध (Prevention and Detection):

प्रतिबंध (Prevention):

- अविश्वसनीय स्रोतांमधून फ्रीवेअर डाउनलोड टाळणे
- अॅडवेअर-ब्लॉकर वापरणे

शोध (Detection):

- अती प्रमाणात जाहिराती दिसणे
- ब्राउझर सेटिंग्स बदललेली आढळणे
- अँटी-अॅडवेअर साधनांचा वापर

6. रॅन्समवेअर (Ransomware):

रॅन्समवेअर हा एक प्रकारचा मालिशस सॉफ्टवेअर आहे जो बळीच्या फाईल्स किंवा संपूर्ण सिस्टीम लॉक किंवा एनक्रिप्ट करतो आणि पुन्हा प्रवेश मिळवण्यासाठी खंडणी (Ransom) मागतो (सहसा क्रिप्टोकरन्सीमध्ये). हा मालवेअरचा सर्वात धोकादायक प्रकारांपैकी एक असून तो व्यक्ती, व्यवसाय आणि सरकारी संस्था यांना लक्ष्य करतो. रॅन्समवेअर हा वेगाने

वाढणारा सायबर धोका आहे जो मालवेअर आणि खंडणीखोरी यांचे संयोजन आहे. एकदा सिस्टीममध्ये इंस्टॉल झाल्यानंतर तो फाईल्स एनक्रिप्ट करतो किंवा ऑपरेटिंग सिस्टीम लॉक करतो आणि डिक्रिप्शन की देण्याच्या बदल्यात खंडणी मागणारी नोट दाखवतो. रॅन्समवेअर प्रामुख्याने फिशिंग ईमेल्स, मालिशस अटॅचमेंट्स, ड्राइव्ह-बाय डाउनलोड्स, किंवा सॉफ्टवेअरमधील कमकुवतपणांचा गैरवापर करून पसरतो. आधुनिक रॅन्समवेअर हल्ल्यांमध्ये क्रिप्टोग्राफी वापरली जाते, ज्यामुळे हल्लेखोराच्या कीशिवाय फाईल्स डिक्रिप्ट करणे जवळजवळ अशक्य होते. काही प्रकारचे रॅन्समवेअर पैसे न दिल्यास संवेदनशील डेटा लीक करण्याची धमकी देखील देतात. WannaCry आणि Petya यांसारख्या प्रसिद्ध हल्ल्यांनी जागतिक स्तरावर मोठा व्यत्यय निर्माण केला आहे. रॅन्समवेअरपासून संरक्षणासाठी सर्वोत्तम उपाय म्हणजे प्रतिबंध, ज्यामध्ये नियमित सिस्टीम अपडेट्स, ऑफलाइन बॅकअप्स, मजबूत ईमेल सुरक्षा, आणि अद्ययावत अँटिव्हायरस साधनांचा वापर यांचा समावेश होतो.

रॅन्समवेअरची कार्यपद्धती (Working of Ransomware):

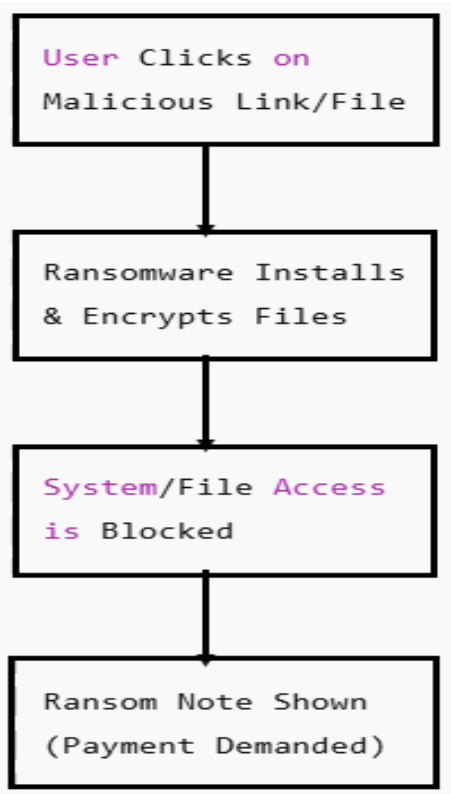


Fig 1.29: रॅन्समवेअरची कार्यपद्धती (Working of Ransomware)

1. **वापरकर्ता दुष्ट लिंक/फाईलवर क्लिक करतो (User Clicks on Malicious Link/File) –** फिशिंग ईमेल किंवा बनावट डाउनलोडद्वारे संसर्ग सुरू होतो.
2. **रॅन्समवेअर इंस्टॉल होतो आणि फाईल्स एनक्रिप्ट करतो (Ransomware Installs & Encrypts Files) –** फाईल्स किंवा संपूर्ण सिस्टीम एनक्रिप्ट केली जाते.
3. **सिस्टीम/फाईल ॲक्सेस ब्लॉक होतो (System/File Access is Blocked) –** बळी व्यक्ती महत्त्वाची डॉक्युमेंट्स उघडू शकत नाही.
4. **खंडणी संदेश दाखवला जातो (Ransom Note Shown) –** प्रवेश पुन्हा मिळवण्यासाठी हल्लेखोर पैसे मागतात.

उदाहरणे (Example)

- WannaCry (2017): Windows मधील EternalBlue vulnerability चा गैरवापर करून 150 हून अधिक देशांमध्ये डेटा एनक्रिप्ट केला.
- Petya / NotPetya (2016–17): Master Boot Record (MBR) एनक्रिप्ट करून सिस्टीम बूट होण्यापासून रोखली.
- CryptoLocker (2013): मजबूत RSA एनक्रिप्शन वापरणारा सुरुवातीच्या काळातील व्यापक रॅन्समवेअर.

प्रतिबंध आणि शोध (Prevention and Detection):

प्रतिबंध (Prevention):

- ऑफलाइन बॅकअप्स ठेवणे
- ऑपरेटिंग सिस्टीम पॅच करणे
- मॅक्रोज डिसेबल करणे
- फिशिंगबाबत जागरूकता

शोध (Detection):

- खंडणी संदेश दिसणे
- फाईल्सना प्रवेश न मिळणे
- असामान्य एनक्रिप्शन ॲक्टिव्हिटी दिसणे.

7. लॉजिक बॉम्ब्स (Logic Bombs):

लॉजिक बॉम्ब हा एक प्रकारचा दुर्भावनायुक्त कोड आहे, जो जाणीवपूर्वक एखाद्या प्रोग्राममध्ये घातला जातो आणि तो विशिष्ट अट किंवा ट्रिगर पूर्ण होईपर्यंत निष्क्रिय (Dormant) राहतो. ही अट एखादी ठराविक तारीख, युजर अकाउंट डिलीट होणे, किंवा विशिष्ट की-स्ट्रोक असू शकते. जेव्हा ही अट पूर्ण होते, तेव्हा लॉजिक बॉम्ब सक्रिय होतो आणि फाईल्स हटवणे, डेटा खराब करणे, किंवा सिस्टीम बंद पाडणे यांसारखी हानिकारक कृती करतो. लॉजिक बॉम्ब हा एक गुप्त (Covert) हल्ला तंत्र आहे, जो प्रामुख्याने इनसाइडर्स (कर्मचारी) किंवा मालवेअर लेखकांकडून वापरला जातो. व्हायरस किंवा वर्मपेक्षा वेगळे, लॉजिक बॉम्ब स्वतःची प्रतिकृती तयार करत नाही. तो सहसा वैध सॉफ्टवेअर किंवा स्क्रिप्टमध्ये लपवलेला असतो आणि शोध टाळण्यासाठी बराच काळ निष्क्रिय राहतो. लॉजिक बॉम्बचे ट्रिगर प्रकार: वेळ-आधारित (Time-based): ठराविक तारीख किंवा वेळ, घटना-आधारित (Event-based): एखादी फाईल किंवा युजर अस्तित्वात नसणे / असणे, कृती-आधारित (Action-based): सलग चुकीचे लॉगिन प्रयत्न इ. लॉजिक बॉम्ब सक्रिय झाल्यावर होणारे नुकसान: लक्षित डेटा हटवणे, सिस्टीम तोडफोड (System Sabotage) महत्त्वाच्या सेवा निष्क्रिय करणे. यामुळे लॉजिक बॉम्ब सूडकाम, तोडफोड किंवा खंडणी यासाठी प्रभावी साधन ठरतो. लॉजिक बॉम्ब शोधणे कठीण असते कारण तो ट्रिगर होईपर्यंत सामान्य कोडप्रमाणेच वागतो. म्हणून संरक्षणासाठी पुढील उपाय आवश्यक आहेत: मजबूत चेंज-कंट्रोल प्रक्रिया, कोड रिव्ह्यू, इनसाइडर थ्रेट मॉनिटरिंग, सुरक्षित सॉफ्टवेअर तैनाती (Secure Deployment Practices)

लॉजिक बॉम्बची कार्यपद्धती (Working of a Logic Bomb):

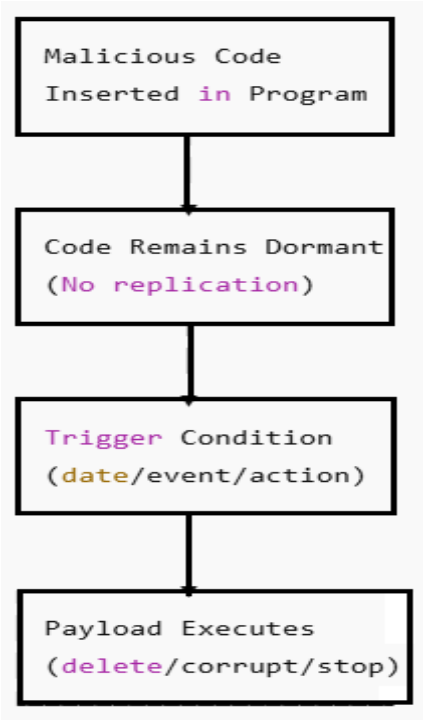


Fig 1.30: लॉजिक बॉम्बची कार्यपद्धती (Working of Logic Bomb)

1. **प्रोग्राममध्ये दुर्भावनायुक्त कोड घातला जातो (Malicious Code Inserted in Program) –** विकास किंवा देखभाल दरम्यान वैध कोडमध्ये लपवून घातला जातो.
2. **कोड निष्क्रिय अवस्थेत राहतो (Code Remains Dormant – No replication) –** ठराविक अटी पूर्ण होईपर्यंत तो कोणतीही ठळक कृती करत नाही आणि स्वतःची प्रतिकृती बनवत नाही.
3. **ट्रिगर अट (Trigger Condition – date/event/action) –** ठराविक तारीख, घटना किंवा सिस्टीम स्थिती पूर्ण झाल्यावर लॉजिक बॉम्ब सक्रिय होतो.
4. **पेलोड अंमलात येतो (Payload Executes – delete/corrupt/stop) –** डेटा हटवणे, डेटा खराब करणे किंवा सेवा बंद करणे यांसारखी हानिकारक कृती केली जाते.

उदाहरण (Example)

- वेळ-आधारित लॉजिक बॉम्ब (Time-triggered logic bomb): ठराविक तारखेला बॅकअप्स नष्ट करणारा कोड (उदा. आर्थिक वर्षाच्या शेवटी पेलोड चालेल अशी रचना).
- इनसाइडर तोडफोड (Insider Sabotage): नाराज कर्मचारी स्वतःचे खाते निष्क्रिय केल्यास रेकॉर्ड्स हटवणारी स्क्रिप्ट प्रणालीमध्ये लपवून ठेवतो.

प्रतिबंध आणि शोध (Prevention and Detection):

प्रतिबंध (Prevention):

- कोड रिव्ह्यू
- चेंज मॅनेजमेंट
- इनसाइडर ॲक्टिव्हिटीचे निरीक्षण

शोध (Detection):

- लॉग विश्लेषण (Log Analysis)
- फाईल अखंडता तपासणी (File Integrity Checks)
- अनपेक्षित कोड अंमलबजावणी

8. रूटकिट्स (Rootkits):

रूटकिट म्हणजे दुर्भावनायुक्त साधनांचा किंवा सॉफ्टवेअरचा संग्रह, जो संगणक प्रणालीमध्ये अनधिकृत root किंवा administrative प्रवेश मिळवण्यासाठी तयार केला जातो आणि त्याचवेळी स्वतःचे अस्तित्व लपवून ठेवतो. रूटकिट्स प्रामुख्याने की-लॉगर, स्पायवेअर किंवा ट्रोजन यांसारख्या इतर मालवेअरला लपवण्यासाठी वापरले जातात, त्यामुळे त्यांचा शोध घेणे आणि काढून टाकणे अत्यंत कठीण होते. रूटकिट्स हे अत्यंत गुप्तपणे कार्य करणारे (Stealthy) मालवेअर प्रोग्राम्स आहेत, जे हल्लेखोरांना संक्रमित सिस्टीमवर उच्चस्तरीय नियंत्रण आणि प्रवेश देतात. "Rootkit" हे नाव Unix/Linux सिस्टीममधील सर्वात उच्च प्रवेश पातळी "root" आणि वापरल्या जाणाऱ्या साधनांच्या संचाला दर्शवणाऱ्या "kit" या शब्दांपासून आले आहे. एकदा रूटकिट सिस्टीममध्ये इंस्टॉल झाले की, ते आपले फाईल्स, प्रोसेसेस, रजिस्ट्री एंट्रीज, लपवते, ज्यामुळे सामान्य ॲंटिव्हायरस प्रोग्राम्स त्याचा शोध घेऊ शकत नाहीत.

रूटकिट्सचे कार्यस्तर (Levels of Operation):

- यूजर-मोड (User-mode): अनुप्रयोग स्तरावर कार्य करतात
- कर्नल-मोड (Kernel-mode): ऑपरेटिंग सिस्टीमच्या कोअरमध्ये कार्य करतात
- फर्मवेअर-लेव्हल (Firmware-level): डिव्हाइस किंवा BIOS मध्ये लपलेले असतात
- हायपरवायझर-लेव्हल (Hypervisor-level): व्हर्च्युअलायझेशन लेयरवर कार्य करतात

रूटकिट्सचा वापर प्रामुख्याने सायबर गुन्हेगारांकडून दीर्घकालीन प्रवेश राखण्यासाठी, डेटा चोरी करण्यासाठी, अतिरिक्त मालवेअर इंस्टॉल करण्यासाठी किंवा वापरकर्त्याच्या क्रियाकलापांवर लक्ष ठेवण्यासाठी केला जातो. त्यांच्या गुप्त कार्यपद्धतीमुळे, रूटकिट्स हे सर्वात कठीण ओळखता येणारे मालवेअर प्रकारांपैकी एक आहेत.

प्रतिबंध (Prevention):

- सुरक्षित आणि नियमित सिस्टीम अपडेट्स
- फक्त विश्वसनीय सॉफ्टवेअरची इंस्टॉलेशन

- इंट्रूजन डिटेक्शन सिस्टिम्स (Intrusion Detection Systems (IDS))
- इंटेग्रिटी मॉनिटरिंग (Integrity Monitoring) (फाईल/सिस्टीम अखंडता तपासणी)

रूटकिटची कार्यपद्धती (Working of a Rootkit):

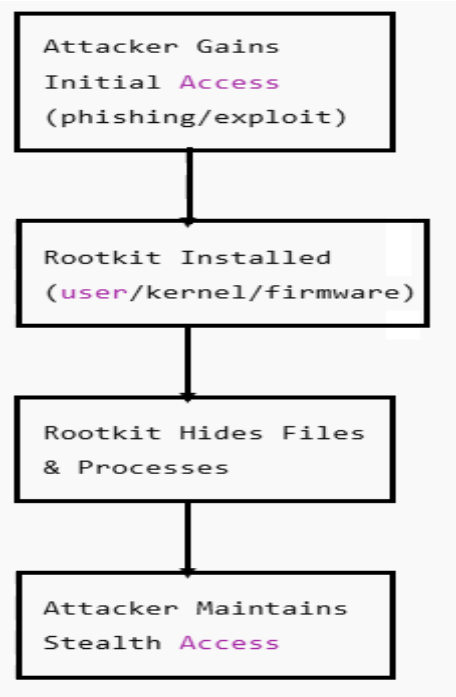


Fig 1.31: रूटकिटची कार्यपद्धती (Working of Rootkit)

1. हल्लेखोर प्रारंभिक प्रवेश मिळवतो (Attacker Gains Initial Access): फिशिंग, सॉफ्टवेअर एक्सप्लॉइट किंवा संक्रमित मीडिया यांच्या माध्यमातून.
2. रूटकिट इंस्टॉल केला जातो (Rootkit Installed – user/kernel/firmware): प्रणालीच्या वेगवेगळ्या स्तरांवर (युजर, कर्नल, फर्मवेअर) दुर्भावनायुक्त कोड बसवला जातो.
3. रूटकिट फाईल्स आणि प्रोसेसेस लपवतो (Rootkit Hides Files & Processes): स्वतःचे अस्तित्व आणि इतर मालवेअर सुरक्षा साधनांपासून लपवतो.
4. हल्लेखोर गुप्त प्रवेश कायम ठेवतो (Attacker Maintains Stealth Access): डेटा चोरी करणे किंवा सिस्टीम नियंत्रित करण्यासाठी हॅकर्स रूटकिटचा वापर करतात.

उदाहरण (Example)

- Sony BMG Rootkit (2005): DRM लागू करण्यासाठी म्युझिक CDs द्वारे इंस्टॉल केला गेला, नंतर मालवेअरने त्याचा गैरवापर केला.
- TDSS / Alureon Rootkit: मोठ्या प्रमाणावर पसरलेला रूटकिट, ज्याने वेब ट्रॅफिक हायजॅक केले आणि सुरक्षा साधने निष्क्रिय केली.
- ZeroAccess Rootkit: क्लिक फ्रॉड आणि क्रिप्टो-मायनिंगसाठी बॉटनेट तयार करण्यासाठी वापरलेला रूटकिट.

प्रतिबंध आणि शोध (Prevention and Detection):

प्रतिबंध (Prevention):

- सुरक्षित बूट (Secure Boot)
- OS / फर्मवेअर अपडेट्स
- किमान अधिकार तत्त्व (Least Privilege Access)

शोध (Detection):

- विशेष रूटकिट स्कॅनर्स
- सिस्टीम वर्तनातील असामान्यता

9. की-लॉगर (Keyloggers)

की-लॉगर (Keystroke Logger) हा एक प्रकारचा निगराणी सॉफ्टवेअर किंवा हार्डवेअर आहे, जो संगणक किंवा मोबाइल डिव्हाइसवर टाइप केलेली प्रत्येक की-स्ट्रोक नोंदवतो. सायबर गुन्हेगार की-लॉगरचा वापर वापरकर्त्याच्या माहितीशिवाय वापरकर्तानाव, संकेतशब्द, PIN, आणि क्रेडिट कार्ड तपशील यांसारखी संवेदनशील माहिती मिळवण्यासाठी करतात. की-लॉगर सायबर हल्ल्यांमध्ये मोठ्या प्रमाणावर वापरले जातात कारण ते वापरकर्त्याच्या इनपुटवर थेट लक्ष ठेवतात. ते सॉफ्टवेअर-आधारित प्रोग्राम किंवा हार्डवेअर-आधारित उपकरणे (कीबोर्ड किंवा USB पोर्टला जोडलेली) अशा स्वरूपात असू शकतात. एकदा इंस्टॉल झाल्यानंतर, की-लॉगर बॅकग्राऊंडमध्ये शांतपणे चालतो, की-स्ट्रोक्स रेकॉर्ड करतो आणि ही माहिती ईमेल, लॉग फाईल्स किंवा रिमोट सर्व्हर मार्फत हल्लेखोराकडे पाठवतो. काही प्रगत की-लॉगर स्क्रीनशॉट्स घेतात, क्लिपबोर्डमधील मजकूर ट्रॅक करतात, किंवा ऑनलाइन ॲक्टिव्हिटीवर लक्ष ठेवतात. जरी की-लॉगरचे काही वैध उपयोग (उदा. पालक नियंत्रण, कर्मचारी निरीक्षण, कायदा अंमलबजावणी) असले, तरी त्यांचा मोठ्या प्रमाणावर ओळख चोरी आणि आर्थिक फसवणूक यासाठी गैरवापर होतो.

प्रतिबंध (Prevention):

- अद्ययावत अँटिव्हायरस सॉफ्टवेअर
- फायरवॉल्स
- इंट्रूजन डिटेक्शन सिस्टिम्स (IDS)
- मल्टी-फॅक्टर ऑथेन्टिकेशन (MFA)

यांचा वापर करून चोरी झालेल्या क्रेडेन्शियल्सचा परिणाम कमी करता येतो.

की-लॉगरची कार्यपद्धती (Working of a Keylogger):

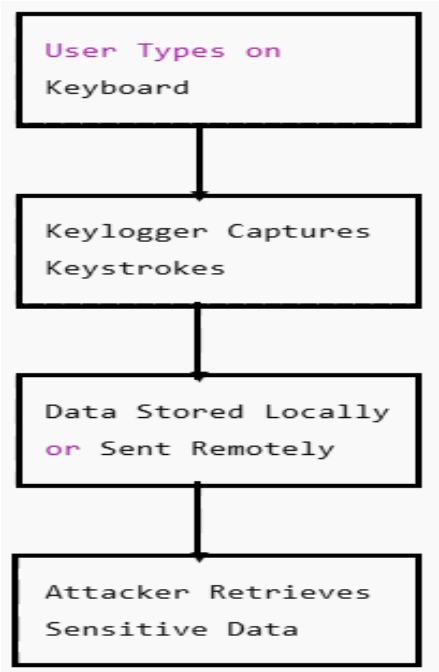


Fig 1.32: की-लॉगरची कार्यपद्धती (Working of Keylogger)

1. **वापरकर्ता कीबोर्डवर टाइप करतो (User Types on Keyboard):** बळी व्यक्ती आपली क्रेडेन्शियल्स किंवा वैयक्तिक माहिती टाइप करते.
2. **की-लॉगर की-स्ट्रोक्स कॅप्चर करतो (Keylogger Captures Keystrokes):** दुर्भावनायुक्त सॉफ्टवेअर किंवा हार्डवेअर वापरकर्त्याचा इनपुट नोंदवते.
3. **डेटा स्थानिकरित्या साठवला जातो किंवा दूरस्थपणे पाठवला जातो (Data Stored Locally or Sent Remotely):** नोंदी लपवलेल्या फाईल्समध्ये साठवल्या जातात किंवा इंटरनेटद्वारे पाठवल्या जातात.
4. **हल्लेखोर संवेदनशील डेटा मिळवतो (Attacker Retrieves Sensitive Data):** हॅकर्स वापरकर्तानाव, संकेतशब्द किंवा बँकिंग तपशीलांचा गैरवापरासाठी प्रवेश मिळवतात.

उदाहरणे (Example)

- झ्यूस ट्रोजन (Zeus Trojan / Zbot): बँकिंग क्रेडेन्शियल्स चोरी करण्यासाठी की-लॉगिंग मॉड्यूलचा समावेश होता.
- हार्डवेअर की-लॉगर्स (Hardware Keyloggers): कीबोर्ड आणि PC दरम्यान जोडलेली उपकरणे जी गुपचूप इनपुट कॅप्चर करतात.
- स्पायरिक्स कीलॉगर (Spyrix Keylogger): निरीक्षण तसेच दुर्भावनायुक्त उद्देशांसाठी वापरले जाणारे आधुनिक स्पायवेअर साधन.

प्रतिबंध आणि शोध (Prevention and Detection)

प्रतिबंध (Prevention):

- अँटिव्हायरस सॉफ्टवेअर
- बहु-घटक प्रमाणीकरण (MFA)
- अज्ञात ॲप्स टाळणे
- हार्डवेअर तपासणी करणे

शोध (Detection):

- अँटी की-लॉगर साधने
- संशयास्पद प्रोसेसेस
- बाहेर जाणाऱ्या लॉग ॲक्टिव्हिटीवर लक्ष ठेवणे

1.5 ऑपरेटिंग सिस्टीम अपडेट्स (Operating System Updates)

ऑपरेटिंग सिस्टीम अपडेट्स म्हणजे विक्रेत्यांकडून (vendors) प्रसिद्ध केलेले दुरुस्ती किंवा प्रतिबंधात्मक सॉफ्टवेअर बदल, जे सुरक्षा कमकुवतपणा (vulnerabilities), बग्स दुरुस्त करण्यासाठी किंवा कार्यक्षमता वाढवण्यासाठी वापरले जातात. ही अपडेट्स वेगवेगळ्या स्वरूपात असतात, जसे की हॉटफिक्स (Hotfix), पॅच (Patch), आणि सर्व्हिस पॅक (Service Pack).

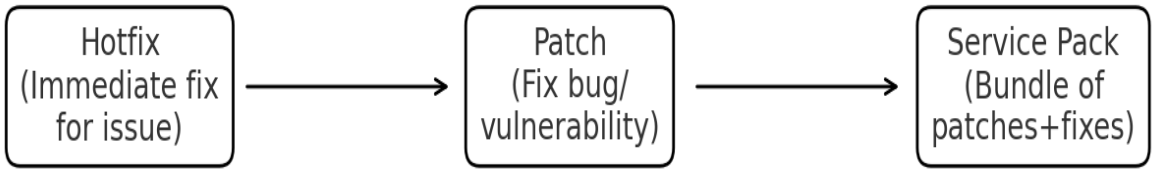


Fig 1.33: ऑपरेटिंग सिस्टीम अपडेट्स (Operating System Updates)

1. हॉटफिक्स (HotFix)

हॉटफिक्स म्हणजे ऑपरेटिंग सिस्टीम विक्रेत्याने (vendor) प्रसिद्ध केलेले लहान आणि तातडीचे सॉफ्टवेअर अपडेट, जे पुढील नियमित पॅच सायकलची वाट न पाहता विशिष्ट गंभीर समस्या—जसे की सुरक्षा कमकुवतपणा (security vulnerability) किंवा गंभीर बग दुरुस्त करण्यासाठी दिले जाते. हॉटफिक्स हे ऑपरेटिंग सिस्टीमच्या सुरक्षा किंवा स्थिरतेला धोका पोहोचवू शकणाऱ्या एका ठराविक समस्येवर उपाय करण्यासाठी तयार केले जाते. कमकुवतपणा आढळल्यानंतर साधारणपणे अतिशय लवकर विकसित करून प्रसिद्ध केले जाते, अनेकदा ती समस्या मोठ्या प्रमाणावर वापरली जाण्यापूर्वीच. हॉटफिक्स हे पॅचपेक्षा वेगळे असते कारण ते तात्काळ उपाय असतात आणि त्यावर पॅचइतकी सखोल चाचणी (testing) झालेली नसते. ते सहसा विक्रेत्याच्या ऑनलाइन अपडेट सेवेद्वारे किंवा सपोर्ट पोर्टलद्वारे वितरित केले जातात. झिरो-डे कमकुवतपणाच्या (Zero-day vulnerability) प्रतिसादामध्ये हॉटफिक्सची भूमिका अत्यंत महत्त्वाची असते, कारण मोठ्या अपडेट्स जसे की पॅच किंवा सर्व्हिस पॅक येईपर्यंत प्रणाली सुरक्षित ठेवण्यास ते मदत करतात. तथापि, हॉटफिक्स अतिशय घाईने लागू केले जात असल्यामुळे, जर त्यांची सखोल चाचणी झाली नसेल तर कधी कधी सुसंगततेच्या (Compatibility) समस्या उद्भवू शकतात.

हॉटफिक्स प्रक्रिया (HotFix Process):

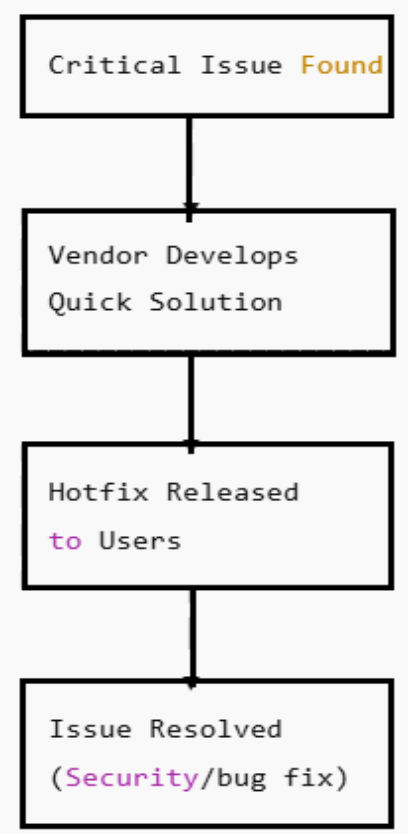


Fig 1.34: हॉटफिक्स प्रक्रिया (Hotfix Process)

1. **गंभीर समस्या आढळते (Critical Issue Found) –** एखादा गंभीर बग किंवा सुरक्षा कमकुवतपणा सापडतो.
2. **विक्रेता जलद उपाय विकसित करतो (Vendor Develops Quick Solution)** – डेव्हलपर्स त्या समस्येसाठी लक्ष्यित उपाय तयार करतात.
3. **हॉटफिक्स वापरकर्त्यांना प्रसिद्ध केला जातो (Hotfix Released to Users)** – ऑनलाइन अपडेट्सद्वारे त्वरित वितरित केला जातो.
4. **समस्या सोडवली जाते (Issue Resolved)** – सुरक्षा कमकुवतपणा किंवा बग तात्पुरता किंवा कायमस्वरूपी दुरुस्त केला जातो.

उदाहरणे (Example)

- Microsoft Security Hotfix: Windows मधील रिमोट कोड एक्झिक्युशन कमकुवतपणा दुरुस्त करण्यासाठी तातडीने प्रसिद्ध केलेला हॉटफिक्स.
- Linux Kernel Hotfix: अचानक उद्भवलेल्या प्रिव्हिलेज एस्कलेशन कमकुवतपणावर उपाय करणारा हॉटफिक्स.

प्रतिबंध आणि शोध (Prevention and Detection)

प्रतिबंध (Prevention):

- हॉटफिक्स त्वरित मिळण्यासाठी ऑटोमॅटिक अपडेट्स सक्षम ठेवणे.
- गंभीर अपडेट्ससाठी विक्रेत्यांच्या सुरक्षा बुलेटिन्स / अलर्ट्स ला सबस्क्राईब करणे.
- मोठ्या प्रमाणावर तैनात करण्यापूर्वी नॉन-प्रॉडक्शन / टेस्ट एन्व्हायर्नमेंटमध्ये हॉटफिक्स त्वरित लागू करणे.
- हॉटफिक्स लागू होईपर्यंत तात्पुरत्या संरक्षणासाठी नेटवर्क फायरवॉल्स / IDS वापरणे.

शोध (Detection):

- सिस्टीम ऑडिट्स करून हॉटफिक्स मिसिंग आहेत का ते तपासणे.
- व्हल्नरेबिलिटी स्कॅनिंग टूल्स (उदा. Nessus, OpenVAS) वापरून पॅच न केलेल्या सिस्टीम्स शोधणे.
- हॉटफिक्स इंस्टॉलेशन पडताळण्यासाठी सिस्टीम लॉग्स आणि विक्रेत्यांच्या सूचना (advisories) तपासणे.
- हॉटफिक्सने दुरुस्त करावयाच्या कमकुवतपणांवर होणाऱ्या हल्ल्यांच्या प्रयत्नांचे निरीक्षण करणे.

2. पॅच (Patch)

पॅच म्हणजे विक्रेत्याने प्रसिद्ध केलेले सॉफ्टवेअर अपडेट, जे ऑपरेटिंग सिस्टीम किंवा ॲप्लिकेशनमधील ओळखलेले बग्स, सुरक्षा कमकुवतपणा किंवा कार्यक्षमता समस्या दुरुस्त करण्यासाठी दिले जाते. हॉटफिक्सच्या तुलनेत, पॅचवर योग्य चाचणी (testing) केली जाते आणि तो नियमित अपडेट सायकलचा भाग म्हणून प्रसिद्ध केला जातो. पॅच हे सॉफ्टवेअर मेंटेनन्सचे सर्वात सामान्य स्वरूप आहे. ते सुरक्षा कमकुवतपणा, सॉफ्टवेअर बग्स, किंवा सुसंगततेच्या समस्या दुरुस्त करण्यासाठी डिझाइन केलेले असते. विक्रेते पॅच प्रसिद्ध करण्यापूर्वी त्याची चाचणी करतात, जेणेकरून सिस्टीम स्थिर राहील आणि नवीन समस्या निर्माण होणार नाहीत. हॉटफिक्सपेक्षा वेगळे, पॅच हे अधिक व्यापक असते आणि अनेक समस्या एकाच वेळी सोडवते. पॅच सहसा ऑटोमॅटिक अपडेट सेवा, विक्रेत्यांच्या वेबसाइट्सवरील डाउनलोड्स, किंवा एंटरप्राइज नेटवर्कमधील सिस्टीम ॲडमिनिस्ट्रेटर्स मार्फत वितरित केले जातात. नियमित पॅचिंग सिस्टीम सुरक्षेसाठी अत्यंत महत्त्वाचे आहे, कारण पॅच न केलेल्या सिस्टीम्स या हॅकर्सचे मुख्य लक्ष्य असतात. दीर्घकालीन सिस्टीम विश्वसनीयतेसाठी, पॅचेस पुढे जाऊन सर्व्हिस पॅक (Service Pack) मध्ये समाविष्ट केले जातात.

पॅच प्रक्रिया (Patch Process):

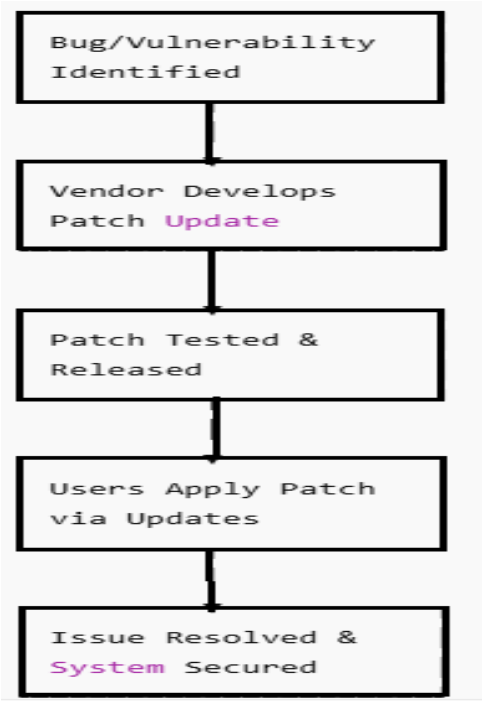


Fig 1.35: पॅच प्रक्रिया (Patch Process)

1. **बग / कमकुवतपणा ओळखला जातो (Bug/Vulnerability Identified):** वापरकर्ते किंवा संशोधकांकडून समस्या नोंदवली जाते.
2. **विक्रेता पॅच अपडेट विकसित करतो (Vendor Develops Patch Update):** त्या समस्येसाठी दुरुस्ती तयार केली जाते.
3. **पॅचची चाचणी करून प्रसिद्ध केला जातो (Patch Tested & Released):** स्थिरतेसाठी तपासणी केली जाते आणि नंतर वितरित केला जातो.
4. **वापरकर्ते अपडेट्सद्वारे पॅच लागू करतात (Users Apply Patch via Updates):** ऑटोमॅटिक किंवा मॅन्युअल अपडेट्सद्वारे इंस्टॉल केला जातो.
5. **समस्या सोडवली जाते व सिस्टीम सुरक्षित होते (Issue Resolved & System Secured):** सिस्टीम स्थिर आणि सुरक्षित बनते.

उदाहरणे (Example)

- मायक्रोसॉफ्ट पॅच ट्यूसडे (Microsoft Patch Tuesday): Windows OS साठी दरमहा प्रसिद्ध होणारे सुरक्षा पॅचेस.
- लिनक्स कर्नल पॅच (Linux Kernel Patch): मेमरी लीक कमकुवतपणा दुरुस्त करणारे पॅचेस.
- जावा सिक्युरिटी पॅच (Java Security Patch): Zero-day त्रुटी दुरुस्त करण्यासाठी Oracle कडून प्रसिद्ध केलेले पॅचेस.

प्रतिबंध आणि शोध (Prevention and Detection)

प्रतिबंध (Prevention):

- ओळखलेल्या कमकुवतपणांचा गैरवापर टाळण्यासाठी नियमितपणे पॅचेस लागू करणे.
- ऑपरेटिंग सिस्टीम आणि ॲप्लिकेशन्ससाठी ऑटोमॅटिक अपडेट्स सक्षम ठेवणे.
- एंटरप्राइज वातावरणात पॅच मॅनेजमेंट टूल्स वापरणे.
- क्रिटिकल सिस्टीम्सवर तैनात करण्यापूर्वी नियंत्रित वातावरणात पॅचची चाचणी करणे.

शोध (Detection):

- पॅचेस गायब आहेत का हे तपासण्यासाठी Vulnerability Scanning करणे.
- कॉन्फिगरेशन मॅनेजमेंट टूल्स (Configuration Management Tools) (उदा. SCCM, WSUS) वापरून पॅच स्थिती ट्रॅक करणे.
- पॅच न केलेल्या सिस्टीम्सवर होणाऱ्या हल्ल्यांच्या प्रयत्नांचे निरीक्षण करणे.
- पॅच अनुपालन सुनिश्चित करण्यासाठी सिस्टीम ऑडिट्स करणे.

3. सर्व्हिस पॅक (Service Pack)

सर्व्हिस पॅक (SP) म्हणजे ऑपरेटिंग सिस्टीम विक्रेत्याने प्रसिद्ध केलेले संचयी (Cumulative) सॉफ्टवेअर अपडेट, ज्यामध्ये अनेक पॅचेस, हॉटफिक्सेस आणि सुधारणा एकत्र केल्या जातात, ज्यामुळे सिस्टीमची स्थिरता, सुरक्षा आणि कार्यक्षमता वाढते. सर्व्हिस पॅक हे अपडेट्सचे मोठे रिलीज असते, ज्यामध्ये आधी प्रसिद्ध केलेले पॅचेस, हॉटफिक्सेस आणि लहान फीचर अपडेट्स एका इंस्टॉल करण्यायोग्य पॅकेजमध्ये एकत्र केलेले असतात. प्रत्येक अपडेट स्वतंत्रपणे इंस्टॉल करण्याऐवजी, वापरकर्ते एकाच सर्व्हिस पॅकद्वारे संपूर्ण सिस्टीम अपडेट करू शकतात. सर्व्हिस पॅक सहसा बऱ्याच अपडेट्स जमा झाल्यानंतर प्रसिद्ध केला जातो, ज्यामुळे सिस्टीम स्थिर राहते आणि सुसंगततेच्या समस्या कमी होतात. यामध्ये कधी कधी नवीन फीचर्स, ड्रायव्हर अपडेट्स किंवा कार्यक्षमता सुधारणा देखील असतात, त्यामुळे त्याचा आकार पॅच किंवा हॉटफिक्सपेक्षा मोठा असतो. संस्थांसाठी (Organizations), सर्व्हिस पॅक सिस्टीम मेंटेनन्स सुलभ करतो, कारण तो अनेक मशीनवर सुसंगतता (Consistency) सुनिश्चित करतो.

उदाहरण: Windows XP Service Pack 2 (SP2) – ज्यामध्ये फायरवॉल आणि सिक्युरिटी सेंटरसारखी महत्त्वाची सुरक्षा फीचर्स समाविष्ट करण्यात आली होती.

सर्व्हिस पॅक प्रक्रिया (Service Pack Process):

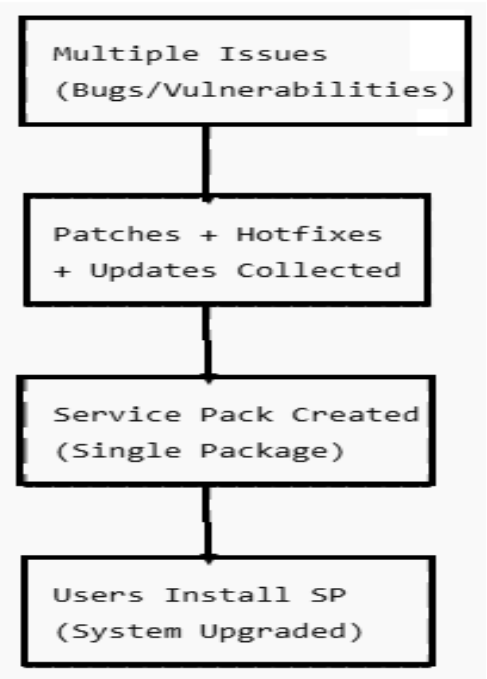


Fig 1.36: सर्व्हिस पॅक प्रक्रिया (Service Pack Process)

1. **अनेक समस्या (बग्स / कमकुवतपणा) (Multiple Issues – Bugs/Vulnerabilities):** कालांतराने ऑपरेटिंग सिस्टीममध्ये ओळखल्या जातात.

2. **पॅचेस + हॉटफिक्सेस + अपडेट्स एकत्र केले जातात (Patches + Hotfixes + Updates Collected):** सर्व अपडेट्स एकत्र बंडल केली जातात.
3. **सर्व्हिस पॅक तयार केला जातो (Service Pack Created – Single Package):** विक्रेता एकच संकलित पॅकेज प्रसिद्ध करतो.
4. **वापरकर्ते SP इंस्टॉल करतात (Users Install SP – System Upgraded):** सिस्टीम अधिक सुरक्षित, स्थिर आणि फीचर-एन्हान्स्ड होते.

उदाहरणे (Example)

- Windows XP Service Pack 2 (SP2): Windows Firewall, Security Center आणि वायरलेस सपोर्ट यांचा समावेश केला.
- Windows 7 Service Pack 1 (SP1): सुरक्षा अपडेट्स आणि स्थिरता सुधारणा एकत्र केल्या.
- SQL Server 2016 SP2: संचयी दुरुस्त्या आणि कार्यक्षमता सुधारणा प्रदान केल्या.

प्रतिबंध आणि शोध (Prevention and Detection)

प्रतिबंध (Prevention):

- जुन्या कमकुवतपणांपासून सिस्टीम सुरक्षित ठेवण्यासाठी नवीनतम सर्व्हिस पॅक इंस्टॉल करणे.
- एंटरप्राइज वातावरणात केंद्रीकृत अपडेट मॅनेजमेंट टूल्स वापरणे.
- मोठ्या प्रमाणावर तैनातीपूर्वी स्टेजिंग एन्व्हायर्नमेंटमध्ये सर्व्हिस पॅकची चाचणी करणे.
- सर्व्हिस पॅक इंस्टॉल करण्यापूर्वी बॅकअप इमेजेस नियमितपणे ठेवणे.

शोध (Detection):

- सिस्टीम माहिती तपासणे (उदा. Windows मध्ये winver) आणि इंस्टॉल केलेला SP व्हर्जन पडताळणे.
- इन्व्हेंटरी आणि कम्प्लायन्स टूल्स वापरून गहाळ सर्व्हिस पॅक्स शोधणे.
- व्हल्नरेबिलिटी स्कॅन्स (Vulnerability Scans) करून पॅच न केलेल्या सिस्टीम्स ओळखणे.
- सर्व्हिस पॅक इंस्टॉलेशननंतर सिस्टीम स्थिरता आणि परफॉर्मन्स लॉग्सचे निरीक्षण करणे.

1.6 सुरक्षेला असलेला धोका (Threat to Security)

1.6.1 ॲसेट्स, व्हल्नरेबिलिटी, थ्रेट्स आणि रिस्क्स यांची ओळख (Introduction to assets, vulnerability, threats, risks)

सुरक्षेला असलेला धोका म्हणजे कोणताही संभाव्य धोका किंवा हानिकारक घटना जी संगणक प्रणाली, नेटवर्क किंवा माहिती संसाधनातील vulnerabilty (कमकुवतपणा) चा गैरवापर करून माहितीची कॉन्फिडेन्शियलिटी / गोपनीयता (Confidentiality), इंटेग्रिटी / अखंडता (Integrity) किंवा अव्हेलेबिलिटी / उपलब्धता (Availability) म्हणजेच CIA Triad यांचे नुकसान करू शकते. इन्फॉरमेशन सेक्युरिटीमध्ये मौल्यवान संसाधनांचे नुकसान होण्यापासून संरक्षण करणे हे मुख्य उद्दिष्ट असते. सुरक्षा म्हणजे Assets (मूल्यवान गोष्टी), कमकुवतपणा (Vulnerabilities), थ्रेटस / धोके (Threats) आणि रीस्क्स/ जोखीम (Risks) यांच्यातील संबंध समजून घेणे. हे सर्व संकल्पना एकत्रितपणे संस्थांना योग्य संरक्षण उपाययोजना आखण्यास आणि सुरक्षा प्राधान्यक्रम निश्चित करण्यास मदत करतात.

1. ॲसेट्स / मालमत्ता (Assets)

ॲसेट्स (Asset) (मालमत्ता) म्हणजे एखाद्या व्यक्ती किंवा संस्थेसाठी मूल्य असलेली कोणतीही गोष्ट, जिला सुरक्षा धोक्यांपासून संरक्षित करणे आवश्यक असते. ॲसेट्स या Physical (हार्डवेअर), Logical (सॉफ्टवेअर, डेटा), Human (लोक) किंवा Intangible (प्रतिष्ठा, बौद्धिक संपदा) स्वरूपाच्या असू शकतात. ॲसेट्स या इन्फॉरमेशन सेक्युरिटीचा पाया आहेत. प्रत्येक संस्थेकडे अशी संसाधने असतात जी तिच्या कारभार, वाढ आणि विश्वासार्हतेसाठी अत्यावश्यक असतात. यामध्ये सर्व्हर आणि राऊटर्ससारखे हार्डवेअर, ऑपरेटिंग सिस्टीम्स आणि ॲप्लिकेशन्ससारखे सॉफ्टवेअर, तसेच ग्राहक नोंदी किंवा आर्थिक माहिती यांसारखा डेटा यांचा समावेश होतो. लोक, प्रक्रिया आणि संस्थेची प्रतिष्ठा देखील महत्त्वाची मालमत्ता मानली जाते. या मालमत्तांचे संरक्षण केल्याने माहितीची कॉन्फिडेन्शियलिटी / गोपनीयता (Confidentiality), इंटेग्रिटी / अखंडता (Integrity) किंवा अव्हेलेबिलिटी / उपलब्धता (Availability) (CIA Triad) सुनिश्चित होते. Security Policies, Risk Assessments आणि Protective Controls हे सर्व प्रामुख्याने मालमत्तांना धोके व कमकुवतपणांपासून सुरक्षित ठेवण्यासाठी डिझाइन केले जातात.

अॅसेट्स चे प्रकार (Types of Assets):

1. हार्डवेअर मालमत्ता (Hardware Assets)

संस्थेच्या IT Infrastructure चा कणा असलेली भौतिक उपकरणे.

- सर्व्हर्स (अनुप्रयोग सर्व्हर, डेटाबेस सर्व्हर, मेल सर्व्हर)
- नेटवर्किंग उपकरणे (राऊटर्स, स्विचेस, फायरवॉल्स, प्रवेश बिंदू)
- संचयन उपकरणे (हार्ड डिस्क्स, बॅकअप ड्राइव्हस्)
- अंतिम-वापरकर्ता उपकरणे (डेस्कटॉप्स, लॅपटॉप्स, टॅब्लेट्स, स्मार्टफोन)
- परिधीय उपकरणे (प्रिंटर्स, स्कॅनर्स, जैवमेट्रिक उपकरणे)

उदाहरण: अंतर्गत नेटवर्कचे संरक्षण करणारे Firewall डिव्हाइस.

2. सॉफ्टवेअर मालमत्ता (Software Assets)

संस्थेच्या कार्यासाठी आवश्यक असलेले प्रोग्राम्स, ॲप्लिकेशन्स आणि सिस्टीम्स.

- ऑपरेटिंग सिस्टिम्स (Windows, Linux, macOS, Android)
- ॲप्लिकेशन सॉफ्टवेअर (ERP Systems, Banking Applications, Office Suites)
- डेटाबेसेस (Oracle, MySQL, PostgreSQL)
- सिक्युरिटी सॉफ्टवेअर (Antivirus, Intrusion Detection Systems, Firewalls)
- क्लाऊड-बेस्ड ॲप्लिकेशन्स **(**SaaS Platforms, Virtual Machines**)**

उदाहरण: ई-कॉमर्स वेबसाइटवर ग्राहकांची माहिती साठवणारे Database Software.

3. **डेटा मालमत्ता (Data Assets)**

संस्थेद्वारे साठवलेली, प्रक्रिया केलेली किंवा प्रसारित केलेली माहिती.

- ग्राहक माहिती (वैयक्तिक, आर्थिक, वैद्यकीय नोंदी)
- व्यावसायिक माहिती (व्यवहार नोंदी, वेतनपत्रक, आर्थिक विवरणपत्रे)
- बौद्धिक संपदा (संशोधन माहिती, पेटंट्स, व्यापार गुपिते)
- संप्रेषण माहिती (ई-मेल्स, चॅट नोंदी, व्हिडिओ रेकॉर्डिंग्स)
- मेटाडेटा (ऑडिट नोंदी, प्रणाली निरीक्षण नोंदी)

उदाहरण: आर्थिक डेटाबेसमध्ये साठवलेली ग्राहकांची बँकिंग नोंदी.

4. मानवी मालमत्ता (People Assets)

माहिती प्रणाली वापरणारे, व्यवस्थापित करणारे आणि संरक्षित करणारे मानवी संसाधन.

1. आंतरिक कर्मचारी (इंटरनल स्टाफ)
   - आयटी प्रशासक (सिस्टीम कॉन्फिगर व निरीक्षण करतात)
   - विकसक (सुरक्षित अनुप्रयोगांची रचना करतात)
   - कर्मचारी (नियमित सिस्टीम वापरकर्ते)
2. बाह्य वापरकर्ते (एक्सटर्नल युजर्स)
   - सेवा वापरणारे ग्राहक व क्लायंट्स
   - तृतीय-पक्ष विक्रेते / कंत्राटदार
3. व्यवस्थापन (मॅनेजमेंट)
   - कार्यकारी अधिकारी व धोरणनिर्माते जे सुरक्षा धोरणे निश्चित करतात

उदाहरण: वापरकर्ता प्रमाणीकरण व प्रवेश नियंत्रण व्यवस्थापित करणारा प्रणाली प्रशासक

2. कमकुवतपणा / व्हल्नरेबिलिटी (Vulnerability)

कमकुवतपणा (Vulnerability) म्हणजे प्रणाली, प्रक्रिया किंवा कॉन्फिगरेशनमधील अशी दुर्बलता किंवा त्रुटी, जिचा वापर करून धोका (Threat) मालमत्तेची सुरक्षा भंग करू शकतो. कमकुवतपणा हार्डवेअर, सॉफ्टवेअर, नेटवर्क्स, प्रोटोकॉल्स किंवा मानवी वर्तनामध्ये अस्तित्वात असू शकतो आणि त्यामुळे सुरक्षा नियंत्रणांची प्रभावीता कमी होते. कमकुवतपणा हे रिस्क मॅनेजमेंट चे केंद्रबिंदू आहेत, कारण धोके फक्त तेव्हाच हानी पोहोचवू शकतात जेव्हा त्यांना शोषण करता येईल असा कमकुवतपणा सापडतो. कमकुवतपणा सहसा अयोग्य डिझाइन, कोडिंगमधील चुका, चुकीची कॉन्फिगरेशन किंवा योग्य सुरक्षा धोरणांचा अभाव यामुळे निर्माण होतात. सामान्य उदाहरणांमध्ये क्रिप्टोग्राफिक कमकुवतपणा (उदा. अयोग्य की व्यवस्थापन किंवा कालबाह्य अल्गोरिदम), तसेच चुकीने कॉन्फिगर केलेले फायरवॉल्स किंवा पॅच न केलेले सॉफ्टवेअर

यांचा समावेश होतो. मजबूत अल्गोरिदम्स आणि सुरक्षित उपकरणे देखील निरुपयोगी ठरतात, जर त्यांच्या अंमलबजावणी किंवा कार्यपद्धतीत कमकुवतपणा अस्तित्वात असेल.

कमकुवतपणाचे वर्गीकरण (Classification of Vulnerabilities)

- तांत्रिक कमकुवतपणा (Technical Vulnerabilities): सॉफ्टवेअर बग्स, प्रोटोकॉल त्रुटी, पॅच न केलेल्या सिस्टीम्स
- भौतिक कमकुवतपणा (Physical Vulnerabilities): असुरक्षित हार्डवेअर, उपकरणांची चोरी, पर्यावरणीय संरक्षणाचा अभाव
- मानवी कमकुवतपणा (Human Vulnerabilities): सोशल इंजिनिअरिंग, फिशिंग, इनसाइडर धोके कमकुवतपणा हे ॲसेट्स (Assets), थ्रेट्स (Threats) आणि रिस्क्स(Risks) यांच्यातील दुवा म्हणून कार्य करतात. मालमत्तेला मूल्य असते, धोका संभाव्य हानी असतो, आणि कमकुवतपणा त्या धोक्याला यशस्वी होण्याची संधी प्रदान करतो.

कमकुवतपणाचे प्रकार (Types of Vulnerabilities)

1. हार्डवेअर कमकुवतपणा: असुरक्षित डिव्हाइस कॉन्फिगरेशन, कालबाह्य फर्मवेअर
2. सॉफ्टवेअर कमकुवतपणा: कोडिंगमधील त्रुटी, बफर ओव्हरफ्लो
3. नेटवर्क कमकुवतपणा: उघडे पोर्ट्स, कमकुवत फायरवॉल नियम
4. मानवी कमकुवतपणा: कमकुवत पासवर्ड पद्धती, प्रशिक्षणाचा अभाव
5. प्रक्रियात्मक कमकुवतपणा: दुर्बल सुरक्षा धोरणे, अयोग्य प्रवेश नियंत्रण

उदाहरण (Example): एखाद्या बँकिंग वेब ॲप्लिकेशनमध्ये वापरकर्त्याच्या इनपुटची योग्य पडताळणी केली जात नाही, तर ही एक कमकुवतता (Vulnerability) आहे. हॅकर SQL Injection Attack चा वापर करून ग्राहकांचे आर्थिक रेकॉर्ड्स मिळवू किंवा बदलू शकतो. येथे ॲसेट्स म्हणजे ग्राहकांचा डेटा, थ्रेट्स म्हणजे हल्लेखोर, आणि निर्माण होणारी रिस्क्स म्हणजे संस्थेला होणारे आर्थिक नुकसान आणि प्रतिष्ठेला झालेली हानी.

3. धोके / थ्रेट्स (Threats)

धोका (Threat) म्हणजे कोणतीही संभाव्य कारणे किंवा परिस्थिती जी कमकुवतपणा (Vulnerability) चा वापर करून एखाद्या मालमत्ता (Asset) ला हानी पोहोचवू शकते. धोके जाणीवपूर्वक (Intentional) असू शकतात (उदा. हॅकिंग, मालवेअर हल्ले) किंवा अनवधानाने (Unintentional) असू शकतात (उदा. मानवी चुका, उपकरण बिघाड, नैसर्गिक आपत्ती). धोके सुरक्षा मॉडेलमध्ये मध्यवर्ती भूमिका बजावतात, कारण तेच हल्ल्यांमागील प्रेरक शक्ती असतात. जिथे व्हल्नरेबिलिटीज (Vulnerabilities) म्हणजे प्रणालीतील कमकुवतपणा असतो, तिथे थ्रेट्स (Threats) हे बाह्य किंवा आंतरिक घटक असतात जे त्या कमकुवतपणाचा फायदा घेण्याचा प्रयत्न करतात.

धोके सुरक्षेच्या विविध बाबींना लक्ष्य करतात

- कॉन्फिडेन्शियलिटी / गोपनीयता (Confidentiality): संवेदनशील डेटा चोरी करणे किंवा उघड करणे.
- इंटेग्रिटी / अखंडता (Integrity): माहितीमध्ये अनधिकृत बदल करणे किंवा डेटा खराब करणे.
- अव्हेलेबिलिटी / उपलब्धता (Availability): संसाधनांवर अधिकृत प्रवेशात अडथळा आणणे किंवा सेवा नाकारणे.

धोक्यांची समज रिस्क असेसमेंट (Risk Assessment) साठी अत्यंत महत्त्वाची आहे, कारण एखादा धोका कमकुवतपणाचा यशस्वीपणे वापर करण्याची शक्यता जितकी जास्त, तितकी संस्थेला भेडसावणारी जोखीम (Risk) अधिक असते.

धोक्यांचे प्रकार (Types of Threats)

1. नैसर्गिक धोके (Natural Threats): भूकंप, पूर, आग, वीज कोसळणे, हार्डवेअर किंवा डेटा सेंटर्सचे भौतिक नुकसान करतात
2. तांत्रिक / हार्डवेअर धोके (Technical / Hardware Threats): सिस्टीम क्रॅश होणे, वीजपुरवठा खंडित होणे, हार्डवेअर बिघाड, सेवा खंडित होणे किंवा डेटा गमावण्यास कारणीभूत ठरतात.
3. मानवी / जाणीवपूर्वक धोके (Human / Intentional Threats): हॅकिंग, फिशिंग, मालवेअर हल्ले, SQL Injection, मुद्दाम नुकसान करणे किंवा मालमत्ता चोरी करण्यासाठी केले जातात
4. मानवी / अनवधानाने होणारे धोके (Human / Unintentional Threats): चुकून फाईल्स डिलीट करणे, कमकुवत पासवर्ड वापरणे, चुकीची कॉन्फिगरेशन, निष्काळजीपणा किंवा प्रशिक्षणाच्या अभावामुळे होतात

5. नेटवर्क धोके (Network Threats): डिनायल ऑफ सर्व्हिस (DoS), मॅन-इन-द-मिडल (MITM), पॅकेट स्निफिंग, प्रवासात असलेल्या डेटावर आणि कम्युनिकेशन सिस्टीम्सवर हल्ला करतात
6. संस्थात्मक धोके (Organizational Threats): इन्सायडर थ्रेट्स, इंडस्ट्रियल सर्व्हेलन्स, पॉलिसी व्हायोलेशन्स, कर्मचारी, कंत्राटदार किंवा स्पर्धकांकडून निर्माण होतात

उदाहरण (Example): एखाद्या ई-कॉमर्स प्लॅटफॉर्म मध्ये हॅकर डिस्ट्रिब्यूटेड डिनायल ऑफ सर्व्हिस (DDoS) अटॅक करतो. येथे धोका (Threat) म्हणजे दुष्ट ट्रॅफिकचा प्रचंड मारा, जो ऑनलाइन स्टोअरच्या उपलब्धता (Availability) ला लक्ष्य करतो. हल्ला यशस्वी झाल्यास सिस्टीम क्रॅश होऊ शकते, ज्यामुळे आर्थिक नुकसान आणि ग्राहक असमाधान निर्माण होते.

4. जोखीम / रिस्क (Risks)

जोखीम (Risk) म्हणजे एखादा धोका (Threat) जेव्हा कमकुवतपणा (Vulnerability) चा यशस्वीपणे गैरवापर करतो, तेव्हा मालमत्ता (Asset) ला होणारे संभाव्य नुकसान, हानी किंवा नाश. जोखीम सहसा घटना घडण्याची शक्यता (Likelihood) आणि त्याचा संस्थेवर होणारा परिणाम (Impact) यांच्या संयोगाने व्यक्त केली जाते. जोखीम ही थ्रेट्स आणि व्हल्नरेबिलिटीज यांच्या परस्पर क्रियेचा परिणाम दर्शवते. धोके म्हणजे संभाव्य धोकादायक घटक आणि कमकुवतपणा म्हणजे दुर्बलता; परंतु जोखीम म्हणजे धोका यशस्वी झाल्यास निर्माण होणारा प्रत्यक्ष परिणाम.

इन्फॉरमेशन सेक्युरिटीमधील जोखीम व्यवस्थापन (Risk Management)

1. ओळख (Identification): मालमत्ता, धोके आणि कमकुवतपणा ओळखणे.
2. मूल्यांकन (Assessment): जोखीम घडण्याची शक्यता आणि संभाव्य परिणामांचे विश्लेषण करणे.
3. जोखीम कमी करणे (Mitigation): तांत्रिक, प्रशासकीय आणि भौतिक नियंत्रण उपाय लागू करणे.
4. निरीक्षण (Monitoring): नवीन किंवा बदलत्या जोखमींचे सतत निरीक्षण करणे.

जोखीमचे प्रकार (Types of Risks)

1. तांत्रिक जोखीम (Technical Risks): हार्डवेअर किंवा सॉफ्टवेअर बिघाड, पॅच न केलेल्या सिस्टीम्स, असुरक्षित प्रोटोकॉल्समुळे निर्माण होतात.
2. ऑपरेशनल जोखीम (Operational Risks): मानवी चुका, प्रक्रिया अपयश, इनसाइडर धोके किंवा कमकुवत प्रवेश नियंत्रणाशी संबंधित.
3. भौतिक जोखीम (Physical Risks): आग, पूर, चोरी किंवा नैसर्गिक आपत्ती ज्यांचा इन्फ्रास्ट्रक्चर आणि डेटा सेंटर्सवर परिणाम होतो.
4. कायदेशीर व अनुपालन जोखीम (Legal and Compliance Risks): सायबर कायदे, डेटा संरक्षण कायदे किंवा उद्योग मानकांचे पालन न केल्यामुळे उद्भवतात.
5. व्यवसायिक / आर्थिक जोखीम (Business / Financial Risks): सायबर घटनांमुळे महसुलातील तोटा, प्रतिष्ठेला हानी किंवा व्यवसाय सातत्य (Business Continuity) समस्या

उदाहरण (Example): एखाद्या बँकिंग सिस्टीममध्ये ग्राहकांची नोंद डेटाबेसमध्ये साठवली जाते. जर ॲप्लिकेशन SQL Injection ला बळी पडण्यासारखा कमकुवतपणा (Vulnerability) ठेवत असेल आणि हॅकर हल्ला करण्याचा प्रयत्न करत असेल (Threat), तर निर्माण होणारी जोखीम (Risk) म्हणजे संवेदनशील आर्थिक डेटाची चोरी किंवा बदल. याचा परिणाम म्हणून आर्थिक नुकसान, नियामक दंड आणि ग्राहकांचा विश्वास गमावणे होऊ शकते.

1.6.2. थ्रेट, व्हल्नरेबिलिटी आणि रिस्क यांच्यातील संबंध (Relation between threats, vulnerability, risks): इन्फॉरमेशन सेक्युरिटीमध्ये थ्रेट, व्हल्नरेबिलिटी आणि रिस्क या संकल्पना परस्परांशी घट्ट जोडलेल्या असून रिस्क मॅनेजमेंट चा पाया बनतात.

- ॲसेट / मालमत्ता (Asset): संरक्षित करणे आवश्यक असलेली मूल्यवान गोष्ट
- व्हल्नरेबिलिटी / कमकुवतपणा (Vulnerability): मालमत्तेतील किंवा तिच्या वातावरणातील दुर्बलता
- थ्रेट / धोका (Threat): कमकुवतपणाचा वापर करून हानी पोहोचवू शकणारा संभाव्य घटक
- रिस्क / जोखीम (Risk): धोका यशस्वी झाल्यास होणारे नुकसान किंवा हानी

संबंधाचे सूत्र (Formula for Relation):

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset}$$

जोखीम गणना (Risk Calculation):

Risk = Threat × Vulnerability × Asset

Risk = 0.7 × 0.8 × 10 = 5.6

स्पष्टीकरण: या गणनेनुसार बँकेला लक्षणीय जोखीम (Significant Risk) आहे.

म्हणूनच मजबूत सुरक्षा नियंत्रण उपाय आवश्यक आहेत, जसे की:

- इनपुट पडताळणी
- फायरवॉल्स
- इंट्रूजन डिटेक्शन सिस्टिम्स (IDS)

हे उपाय राबविल्यास जोखीम कमी करता येते आणि मालमत्तेचे संरक्षण सुनिश्चित होते.

References:

1. Stallings, W., & Brown, L. (2014). *Computer security: Principles and practice* (3rd ed.). Pearson. ISBN: 978-0-13-377392-7.
2. Kahate, A. (2018). *Cryptography and network security* (3rd ed.; 4th ed.). McGraw-Hill. ISBN: 978-9353163303.
3. Merkow, M., & Breithaupt, J. (2006). *Information security: Principles and practices*. Pearson. ISBN: 978-81-317-1288-7.
4. Pachghare, V. K. (2012). *Cryptography and information security*. Prentice Hall India. ISBN: 978-81-203-5082-3.
5. Gollmann, D. (2011). *Computer security* (3rd ed.). Wiley. ISBN: 978-0-470-74115-3.
6. YouTube. (2019). Simulation of intrusion detection system in MANET using NetSim. Retrieved from https://www.youtube.com/watch?v=NlpnJE0m-NU
7. NPTEL. (2022). Introduction to Information Security. Retrieved from https://archive.nptel.ac.in/courses/106/106/106106129/
8. Swayam. (2022). Information Technology course. Retrieved from https://onlinecourses.swayam2.ac.in/cec22_cs15/preview
9. YouTube. (2020). Firewall configuration tutorial. Retrieved from https://www.youtube.com/watch?v=T9c5ZpT2FV0
10. Virtual Labs, IIIT Hyderabad. (n.d.). Virtual lab for cryptography experiments. Retrieved from https://cse29-iiith.vlabs.ac.in/List%20of%20experiments.html
11. GeeksforGeeks. (2021). Active and passive attacks in information security. Retrieved from https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/

युनिट-2
यूजर ऑथेन्टीकेशन अँड ॲक्सेस कंट्रोल
(User Authentication and Access Control)

विषय निष्पत्ती (Course Outcome):

CO2: मल्टी-फॅक्टर यूजर ऑथेन्टिकेशन आणि ॲक्सेस कंट्रोल लागू करा.

घटक निष्पत्ती (Theory Learning Outcome):

1. विविध प्रकारच्या ऑथेन्टिकेशन मेथड्स लागू करा.
2. पासवर्ड अटॅक पासून संरक्षण करण्यासाठी विविध पद्धती लागू करा.
3. दिलेल्या बायोमेट्रिक पॅटर्न्स स्पष्ट करा.
4. ऑथरायझेशनचा उद्देश स्पष्ट करा.
5. दिलेल्या पॅरामिटर्सच्या आधारे DAC, MAC, RBAC आणि ABAC यांची तुलना करा.

2.1 आयडेंटिफिकेशन आणि ऑथेन्टिकेशन पद्धती (Identification and Authentication methods)

वापरकर्ता ओळख आणि प्रमाणीकरण या दोन मूलभूत सुरक्षा यंत्रणा आहेत, ज्या केवळ वैध (Legitimate) वापरकर्त्यांनाच संगणक प्रणाली, नेटवर्क किंवा ऑनलाइन सेवांमध्ये प्रवेश मिळेल याची खात्री करतात.

a. **ओळख (Identification):** आयडेंटिफिकेशन ही ती प्रक्रिया आहे ज्यामध्ये वापरकर्ता आपली ओळख दर्शवतो. (उदा. यूजरनेम किंवा यूजर आयडी टाकणे).
b. **प्रमाणीकरण (Authentication**): ऑथेंटिकेशन ही ती प्रक्रिया आहे ज्यामध्ये वापरकर्ता खरोखरच तोच आहे का, याची पडताळणी केली जाते. यासाठी पासवर्डस, टोकन्स, बायोमेट्रिकस किंवा मल्टीपल फॅक्टर्स वापरले जातात. ही दोन्ही प्रक्रिया एकत्रितपणे वापरल्यास फक्त अधिकृत वापरकर्त्यांनाच प्रणालीमध्ये प्रवेश मिळतो.

कम्प्युटर सेक्युरिटी म्हणजे कम्प्युटर सिस्टिम्स, नेटवर्क्स आणि डेटा यांना अनऑथराइज्ड ॲक्सेस, मॉडिफिकेशन, डिस्रप्शन किंवा डीस्ट्रक्शन पासून संरक्षित करण्यासाठी वापरल्या जाणाऱ्या टेक्निक्स आणि मेकॅनिझम्स. सोप्या भाषेत सांगायचे तर, कम्प्युटर सेक्युरिटी डिजिटल ॲसेट्सना हॅकिंग, मालवेअर किंवा मिसयुज सारख्या सायबर थ्रेट्स पासून सुरक्षित ठेवते.

1. इलेक्ट्रॉनिक युजर ऑथेंटिकेशन (Electronic user authentication)

इलेक्ट्रॉनिक युजर ऑथेंटिकेशन ही एक सुरक्षा प्रक्रिया आहे, जी डिजिटल सिस्टिम, नेटवर्क, डिव्हाइस किंवा ऑनलाइन सेवेमध्ये प्रवेश करण्याचा प्रयत्न करणाऱ्या वापरकर्त्याची ओळख पडताळून पाहते. या प्रक्रियेमध्ये पासवर्ड्स, पिन्स, ओटीपीज, टोकन्स, स्मार्ट कार्ड्स किंवा बायोमेट्रिक डेटा यांसारख्या इलेक्ट्रॉनिक क्रेडेन्शियल्सचा वापर केला जातो, ज्यामुळे वापरकर्ता खरोखरच वैध आहे याची खात्री केली जाते. इलेक्ट्रॉनिक युजर ऑथेंटिकेशन मुळे फक्त ऑथराइज्ड युजर्स यांनाच संवेदनशील माहिती किंवा सिस्टिम रिसोर्सेसमध्ये प्रवेश मिळतो. ही प्रक्रिया तेव्हा सुरू होते जेव्हा वापरकर्ता युजरनेम किंवा आयडी देऊन आपली ओळख दर्शवतो. त्यानंतर सिस्टिम पासवर्ड्स, पिन्स, ओटीपीज, टोकन्स किंवा बायोमेट्रिक वैशिष्ट्ये यांसारख्या इलेक्ट्रॉनिक पद्धतींचा वापर करून त्या ओळखीचे प्रमाणीकरण करते. इलेक्ट्रॉनिक ऑथेंटिकेशनमुळे आधुनिक कम्प्युटिंग एन्व्हायर्नमेंटमध्ये कॉन्फिडेन्शियलिटी, इंटिग्रिटी, नॉन-रिप्युडिएशन आणि सिक्युअर ॲक्सेस सुनिश्चित केला जातो.

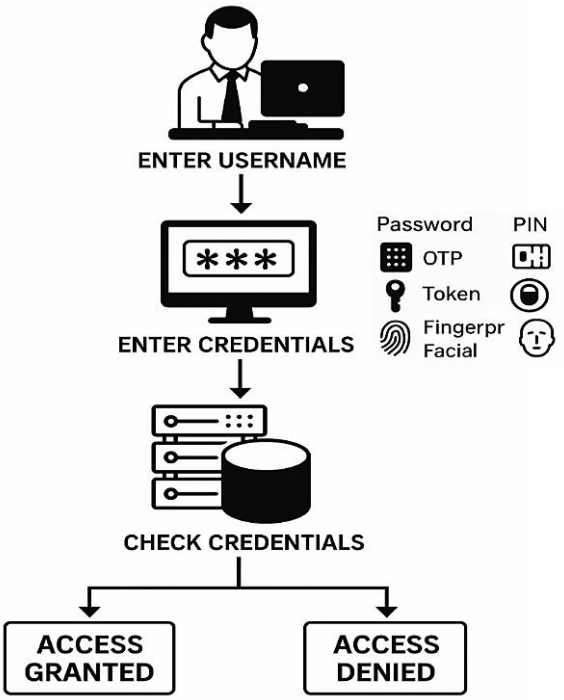


Fig 2.1: इलेक्ट्रॉनिक युजर ऑथेंटिकेशन प्रक्रिया (Electronic User Authentication Process)

इलेक्ट्रॉनिक युजर ऑथेंटिकेशन ही डिजिटल सिस्टिममध्ये प्रवेश देण्यापूर्वी वापरकर्त्याची ओळख पडताळून पाहण्याची प्रक्रिया आहे. सर्वप्रथम वापरकर्ता युजरनेम किंवा युजर आयडी टाकून स्वतःची ओळख दर्शवतो. त्यानंतर सिस्टिम इलेक्ट्रॉनिक ऑथेंटिकेशन करते, ज्यामध्ये वापरकर्त्याकडून एक किंवा अधिक क्रेडेन्शियल्स मागितली जातात, जसे की पासवर्ड, पिन, ओटीपी, टोकन, स्मार्ट कार्ड किंवा बायोमेट्रिक डेटा (उदा. फिंगरप्रिंट किंवा फेस रिकग्निशन). ही क्रेडेन्शियल्स सर्व्हर द्वारे सुरक्षितरीत्या तपासली जातात. यासाठी हॅश मॅचिंग किंवा टोकन व्हेरिफिकेशन यांसारख्या व्हॅलिडेशन टेक्निक्स वापरल्या जातात. जर दिलेली माहिती साठवलेल्या माहितीसोबत जुळली, तर प्रवेश दिला जातो; अन्यथा प्रवेश नाकारला जातो. ही प्रक्रिया सुनिश्चित करते की फक्त ऑथराइज्ड युजर्स यांनाच सिस्टिममध्ये प्रवेश मिळेल आणि संवेदनशील माहिती अनऑथराइज्ड ॲक्सेसपासून सुरक्षित राहील.

उदाहरणे (Examples):

1. पासवर्ड ऑथेंटिकेशन: वापरकर्ता युजरनेम आणि पासवर्ड टाकून कम्प्युटरमध्ये लॉगिन करतो. सिस्टिम साठवलेला हॅश तपासते आणि प्रवेश देते.
2. ओटीपी-बेस्ड ऑथेंटिकेशन: ऑनलाइन बँकिंगदरम्यान वापरकर्ता एसएमएस किंवा ई-मेलद्वारे मिळालेला ओटीपी टाकून आपली ओळख सिद्ध करतो.:
3. टोकन-बेस्ड ऑथेंटिकेशन: वेब ॲप्लिकेशन्स यशस्वी लॉगिननंतर युजर सेशन टिकवण्यासाठी सुरक्षित सेशन टोकन तयार करतात.
4. बायोमेट्रिक ऑथेंटिकेशन: स्मार्टफोन्स फिंगरप्रिंट किंवा फेस रिकग्निशन वापरून इलेक्ट्रॉनिक पद्धतीने युजरचे प्रमाणीकरण करतात.
5. मल्टी-फॅक्टर ऑथेंटिकेशन (एमएफए): लॉगिनसाठी खालील घटक आवश्यक असतात:
   c. पासवर्ड (नॉलेज फॅक्टर)
   d. ओटीपी (पझेशन फॅक्टर)
   e. फिंगरप्रिंट (इनहेरन्स फॅक्टर)

2. युजरनेम आणि पासवर्ड (User Name and Password)

युजरनेम हा संगणक सिस्टिममध्ये वापरकर्त्याचे प्रतिनिधित्व करण्यासाठी वापरला जाणारा एक युनिक आयडेंटिफायर असतो, तर पासवर्ड ही अक्षरे, अंक किंवा चिन्हांची गुप्त साखळी असते, जी वापरकर्त्याचे प्रमाणीकरण करून तो खरोखरच वैध आहे याची खात्री करते. युजरनेम आणि पासवर्ड ऑथेंटिकेशन ही इलेक्ट्रॉनिक युजर ऑथेंटिकेशनची सर्वात सामान्य

आणि मूलभूत पद्धत आहे. या पद्धतीमध्ये वापरकर्ता आपली ओळख युनिक युजरनेम टाकून दर्शवतो आणि सिस्टिम त्या वापरकर्त्याची ओळख फक्त त्यालाच माहीत असलेल्या पासवर्डद्वारे पडताळून पाहते. सुरक्षेच्या दृष्टीने पासवर्ड सहसा हॅश्ड किंवा एन्क्रिप्टेड स्वरूपात साठवले जातात आणि लॉगिन दरम्यान त्यांची तुलना केली जाते. सुरक्षा वाढवण्यासाठी मजबूत व क्लिष्ट पासवर्ड्स वापरणे आणि नियमित कालावधीनंतर पासवर्ड अपडेट करणे शिफारसीय आहे.

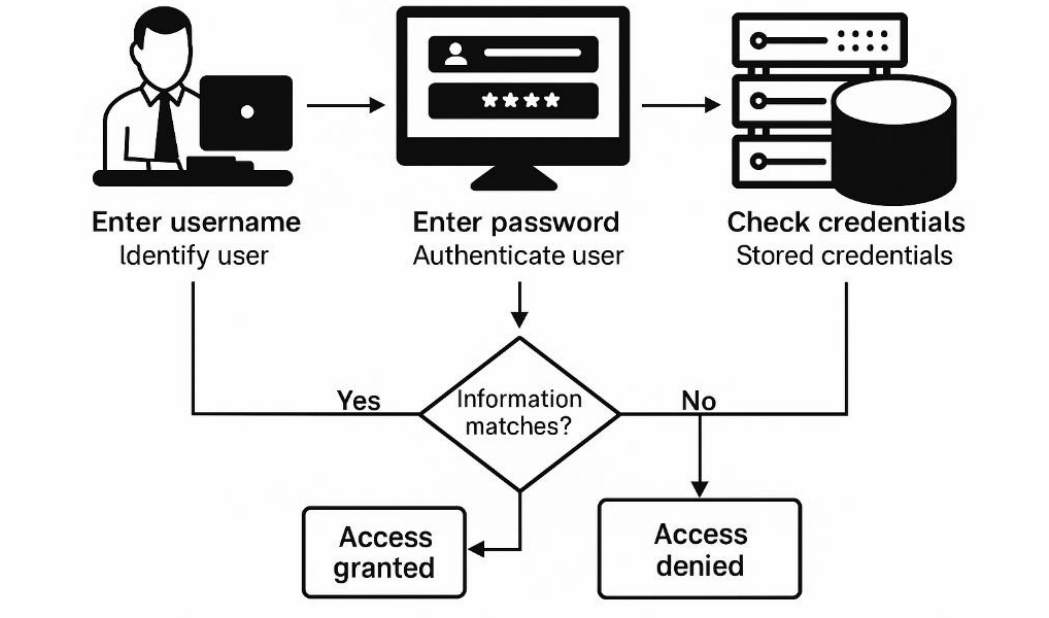


Fig 2.2: युजरनेम आणि पासवर्ड ऑथेंटिकेशन प्रक्रिया (User Name and Password)

ही आकृती युजरनेम आणि पासवर्ड वापरून लॉगिन करण्याची प्रक्रिया दर्शवते. सर्वप्रथम वापरकर्ता युजरनेम टाकतो, ज्याद्वारे त्याची ओळख निश्चित केली जाते. त्यानंतर वापरकर्ता पासवर्ड टाकतो, जो वापरकर्त्याची ओळख पडताळण्यासाठी वापरला जातो. यानंतर सिस्टिम वापरकर्त्याने टाकलेला पासवर्ड साठवलेल्या क्रेडेन्शियल्सशी तुलना करते. जर दिलेली माहिती जुळली, तर वापरकर्त्याला प्रवेश दिला जातो; अन्यथा प्रवेश नाकारला जातो. ही प्रक्रिया सुनिश्चित करते की फक्त योग्य आणि अधिकृत वापरकर्त्यालाच सिस्टिममध्ये प्रवेश मिळतो.

उदाहरण (Examples): ई-मेल आयडी (युजरनेम) आणि पासवर्ड वापरून जी-मेल मध्ये लॉगिन करणे.

3. मल्टी-फॅक्टर ऑथेंटिकेशन (Multi-Factor Authentication)

मल्टी-फॅक्टर ऑथेंटिकेशन (एमएफए) ही एक सुरक्षा तंत्रज्ञान पद्धत आहे, ज्यामध्ये वापरकर्त्याची ओळख सिद्ध करण्यासाठी दोन किंवा अधिक स्वतंत्र व्हेरिफिकेशन फॅक्टर्स द्यावे लागतात. या पद्धतीमध्ये पासवर्ड्स, ओटीपीज, स्मार्ट कार्ड्स आणि बायोमेट्रिक्स यांसारख्या विविध प्रकारच्या क्रेडेन्शियल्सचा एकत्रित वापर करून ॲक्सेस कंट्रोल अधिक मजबूत केला जातो. मल्टी-फॅक्टर ऑथेंटिकेशन सुरक्षेची पातळी वाढवते, कारण यात वापरकर्त्याला खालील तीन मुख्य फॅक्टर कॅटेगरीजमधून एकापेक्षा जास्त घटक वापरून ऑथेंटिकेशन करावे लागते:

- समथिंग यू नो (काहीतरी जे तुम्हाला माहीत आहे): पासवर्ड किंवा पिन
- समथिंग यू हॅव (काहीतरी जे तुमच्याकडे आहे): ओटीपी, टोकन, स्मार्ट कार्ड
- समथिंग यू आर (काहीतरी जे तुम्ही आहात): बायोमेट्रिक वैशिष्ट्ये जसे की फिंगरप्रिंट किंवा फेस रिकग्निशन

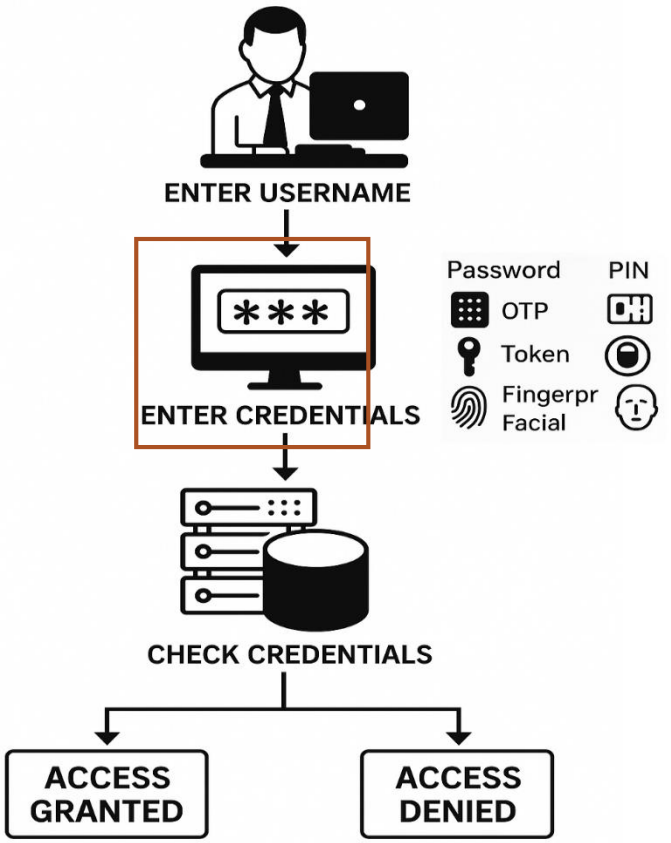


Fig 2.3: मल्टी-फॅक्टर ऑथेंटिकेशन प्रक्रिया (Multi-Factor Authentication Process)

ही आकृती मल्टी-फॅक्टर ऑथेंटिकेशन (एमएफए) वापरून लॉगिन करण्याची प्रक्रिया दर्शवते. सर्वप्रथम वापरकर्ता युजरनेम किंवा आयडी टाकून स्वतःची ओळख दर्शवतो. यानंतर फक्त पासवर्ड वापरण्याऐवजी, सिस्टिम दोन किंवा अधिक ऑथेंटिकेशन फॅक्टर्स मागते.

यामध्ये पुढील घटकांचा समावेश असतो:

- पासवर्ड – (समथिंग यू नो / काहीतरी जे तुम्हाला माहीत आहे)
- ओटीपी किंवा स्मार्ट कार्ड – (समथिंग यू हॅव / काहीतरी जे तुमच्याकडे आहे)
- बायोमेट्रिक्स जसे की फिंगरप्रिंट किंवा फेस स्कॅन – (समथिंग यू आर / काहीतरी जे तुम्ही आहात)

हे सर्व फॅक्टर्स सर्व्हरकडे व्हेरिफिकेशनसाठी पाठवले जातात. जर दिलेले सर्व घटक साठवलेल्या नोंदींशी जुळले, तर वापरकर्त्याला प्रवेश दिला जातो; अन्यथा प्रवेश नाकारला जातो. एमएफए अनेक स्वतंत्र तपासण्या एकत्र वापरत असल्यामुळे अधिक मजबूत सुरक्षा प्रदान करते.

उदाहरण: ऑनलाइन बँकिंग लॉगिन

- पासवर्ड – (नो / Know)
- मोबाइलवर पाठवलेला ओटीपी – (हॅव / Have)

4. टोकन-बेस्ड ऑथेंटिकेशन (Token-Based Authentic)

टोकन-बेस्ड ऑथेंटिकेशन ही अशी प्रमाणीकरण पद्धत आहे, ज्यामध्ये वापरकर्ता एकदाच लॉगिन करतो आणि त्यानंतर सर्व्हरकडून एक सुरक्षित व युनिक टोकन प्राप्त करतो. हे टोकन पुढील सर्व विनंत्यांसाठी वापरले जाते आणि प्रत्येक वेळी युजरनेम व पासवर्ड पुन्हा टाकण्याची गरज नसते. टोकन हे वापरकर्त्याच्या ओळखीचे डिजिटल पुरावे म्हणून कार्य करते. टोकन-बेस्ड ऑथेंटिकेशनमध्ये पारंपरिक पद्धतीप्रमाणे वारंवार पासवर्ड पाठवण्याऐवजी तात्पुरते आणि एन्क्रिप्टेड टोकन वापरले जाते, त्यामुळे सुरक्षा अधिक मजबूत होते. वापरकर्ता यशस्वीपणे लॉगिन केल्यानंतर सर्व्हर लांब, रँडम आणि सुरक्षित स्ट्रिंग स्वरूपाचे टोकन तयार करतो, जे छेडछाड टाळण्यासाठी साइन केलेले किंवा एन्क्रिप्ट केलेले असते. हे टोकन क्लायंट साइडवर (उदा. वेब ब्राउझर, मोबाईल ॲप किंवा एपीआय क्लायंट) साठवले जाते आणि प्रत्येक विनंतीसोबत ऑथेंटिकेशनसाठी सर्व्हरकडे पाठवले जाते. कारण पासवर्ड वारंवार पाठवला जात नाही, त्यामुळे नेटवर्क

अटॅक्स, स्निफिंग किंवा रिप्ले अटॅक्सद्वारे पासवर्ड चोरी होण्याचा धोका कमी होतो. टोकनमध्ये अनेकदा एक्सपायरी टाइम, युजर रोल्स आणि ॲक्सेस परमिशन्स यांची माहितीही समाविष्ट असते. ही पद्धत आधुनिक वेब ॲप्लिकेशन्स, एपीआय, मोबाईल ॲप्स आणि क्लाऊड सिस्टिम्समध्ये मोठ्या प्रमाणावर वापरली जाते.

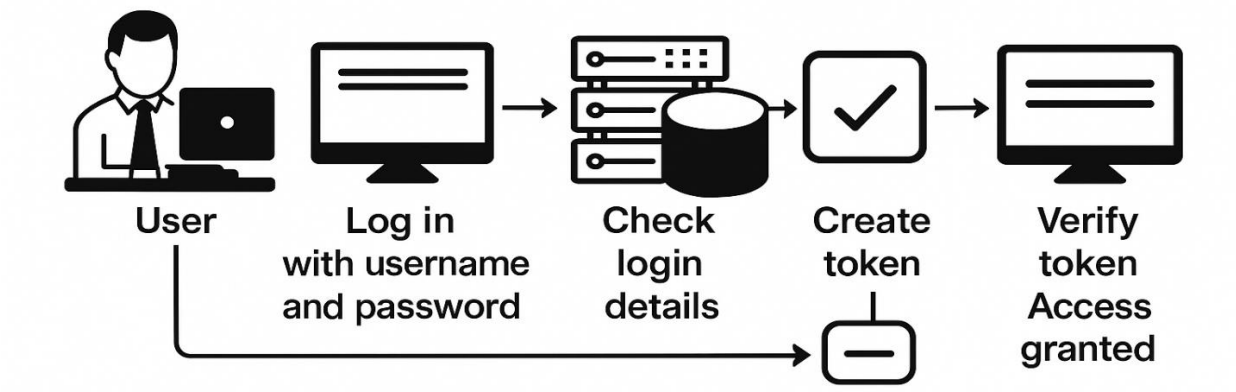


Fig 2.4: टोकन-बेस्ड ऑथेंटिकेशन प्रक्रिया (Token-Based Authentic)

ही आकृती टोकन-बेस्ड ऑथेंटिकेशन कसे कार्य करते हे दर्शवते. सर्वप्रथम वापरकर्ता युजरनेम आणि पासवर्ड वापरून लॉगिन करतो. सर्व्हर लॉगिन तपशील तपासतो आणि ते योग्य असल्यास एक सुरक्षित टोकन तयार करून वापरकर्त्याकडे पाठवतो. हे टोकन वापरकर्त्याच्या ओळखीचे पुरावे म्हणून कार्य करते. पुढील प्रत्येक विनंतीसाठी वापरकर्ता पासवर्ड पुन्हा न टाकता हेच टोकन सर्व्हरकडे पाठवतो. सर्व्हर टोकनची पडताळणी करतो आणि टोकन वैध असल्यास वापरकर्त्याला प्रवेश दिला जातो. या पद्धतीमुळे पासवर्ड वारंवार पाठवला जात नसल्याने लॉगिन प्रक्रिया अधिक सुरक्षित होते.

उदाहरण: मोबाईल ॲप ऑथेंटिकेशन: फेसबुक, इन्स्टाग्राम किंवा बँकिंग ॲप्स यांसारखी मोबाईल ॲप्स लॉगिननंतर टोकन साठवतात, त्यामुळे वापरकर्त्यांना पुन्हा पुन्हा पासवर्ड टाकण्याची गरज राहत नाही.

2.2 पासवर्ड अटॅक (Password Attacks)

पासवर्ड अटॅक म्हणजे संगणक सिस्टिम्स, युजर अकाउंट्स किंवा नेटवर्क्समध्ये अनऑथराइज्ड ॲक्सेस मिळवण्यासाठी हल्लेखोर वापरतात त्या पद्धती, ज्यामध्ये पासवर्ड चोरी करणे, ओळखणे किंवा फोडणे यांचा समावेश होतो. जेव्हा हल्लेखोर पासवर्ड-बेस्ड ऑथेंटिकेशन मोडण्याचा किंवा बायपास करण्याचा प्रयत्न करतो, तेव्हा पासवर्ड हल्ले घडतात. कमकुवत, अंदाज लावता येणारे किंवा पुन्हा पुन्हा वापरलेले पासवर्ड्स सिस्टिम्सना अत्यंत असुरक्षित बनवतात.

हल्लेखोर खालील तंत्रांचा वापर करू शकतात:

- साधे पासवर्ड ओळखण्याचा प्रयत्न करणे
- वापरकर्ता पासवर्ड टाकताना निरीक्षण करणे
- सुरक्षित ठिकाणी वापरकर्त्याच्या मागे मागे प्रवेश करणे
- फेकून दिलेल्या कागदांमधून लिहिलेले पासवर्ड शोधणे

सामान्य पासवर्ड अटॅकमध्ये पासवर्ड गेसिंग, शोल्डर सर्फिंग, पिगीबॅकिंग आणि डम्पस्टर डायव्हिंग यांचा समावेश होतो. हे हल्ले मानवी कमकुवतपणा, चुकीच्या पासवर्ड सवयी आणि सुरक्षा जागरूकतेचा अभाव यांचा गैरफायदा घेतात. अशा हल्ल्यांपासून संरक्षणासाठी मजबूत पासवर्ड निर्मिती, मल्टी-फॅक्टर ऑथेंटिकेशन (एमएफए), युजर अवेअरनेस आणि संवेदनशील माहितीची सुरक्षित विल्हेवाट अत्यावश्यक आहे. मजबूत संस्थात्मक सुरक्षा धोरणे देखील या जोखमी मर्यादित करतात.

1. पासवर्ड गेसिंग (Guessing Password)

पासवर्ड गेसिंग हा पासवर्ड हल्ल्याचा एक प्रकार आहे, ज्यामध्ये हल्लेखोर सामान्य शब्द, अंदाज लावता येणारे पॅटर्न्स किंवा वैयक्तिक माहिती वापरून वापरकर्त्याचा पासवर्ड ओळखण्याचा प्रयत्न करतो. पासवर्ड गेसिंग हा सर्वात सोपा आणि सर्वाधिक आढळणारा पासवर्ड हल्ला आहे. हल्लेखोर खालीलप्रमाणे सहज अंदाज लावता येणारे पासवर्ड वापरून प्रयत्न करतो: 123456, पासवर्ड, ॲडमिन नावे, जन्मतारीख, फोन नंबर जे वापरकर्ते कमकुवत किंवा साधे पासवर्ड्स निवडतात, ते या हल्ल्यास अत्यंत असुरक्षित असतात. मानक सुरक्षा मार्गदर्शक तत्त्वांनुसार, अंदाजे पासवर्ड्स कोणतीही प्रगत साधने

न वापरता सहज ओळखता येतात. या प्रकारचा हल्ला टाळण्यासाठी मजबूत, क्लिष्ट आणि युनिक पासवर्ड्स वापरणे अत्यंत आवश्यक आहे.

उदाहरण (Example): समजा कृष्णा नावाचा वापरकर्ता krishna123 असा कमकुवत पासवर्ड तयार करतो. हल्लेखोराला कृष्णाचे नाव माहीत असल्यामुळे तो खालीलप्रमाणे सोपे आणि सामान्य पासवर्ड कॉम्बिनेशन्स वापरून प्रयत्न करतो:

- Krishna
- krishna123
- krishna2024
- 123456
- password

krishna123 हा पासवर्ड सहज अंदाज लावता येणारा असल्यामुळे हल्लेखोर कृष्णाच्या अकाउंटमध्ये यशस्वीपणे लॉगिन करतो. वरील पासवर्ड अटॅक (Password Attacks) टाळण्यासाठी खालील पासवर्ड सिलेक्शन स्ट्रॅटेजीज वापराव्यात. सिक्युरिटी मजबूत करण्यासाठी वापरल्या जाणाऱ्या टेक्निक्स (Techniques for Strengthening Securities) पुढीलप्रमाणे आहेत:

1. **युजर एज्युकेशन (User Education):** युजर एज्युकेशन म्हणजे वापरकर्त्यांना मजबूत आणि ओळखणे कठीण असलेले पासवर्ड कसे निवडावेत याचे प्रशिक्षण देणे. "वापरकर्त्यांना ओळखणे कठीण असलेल्या पासवर्डचे महत्त्व सांगितले जाऊ शकते आणि मजबूत पासवर्ड निवडण्यासाठी मार्गदर्शक तत्त्वे दिली जाऊ शकतात." यामध्ये वापरकर्त्यांना सोपे पासवर्ड, वैयक्तिक माहिती आणि डिक्शनरी शब्द टाळण्याचा सल्ला दिला जातो तसेच लांब, क्लिष्ट कॉम्बिनेशन्स वापरण्यास प्रोत्साहन दिले जाते.
2. **कम्प्युटर-जनरेटेड पासवर्ड्स (Computer-Generated Passwords):** या पद्धतीमध्ये सिस्टिम स्वतःच वापरकर्त्यांसाठी रँडम पासवर्ड्स जनरेट करते. "सामान्यतः कम्प्युटर-जनरेटेड पासवर्ड स्कीम्स वापरकर्त्यांना पसंत पडत नाहीत." हे पासवर्ड रँडम आणि अंदाज न लावता येणारे असल्यामुळे अत्यंत सुरक्षित असतात.
3. **रिॲक्टिव पासवर्ड चेकिंग (Reactive Password Checking):** रिॲक्टिव पासवर्ड चेकिंग म्हणजे सिस्टिम ठराविक कालावधीनंतर स्वतःचा पासवर्ड-क्रॅकिंग प्रोग्राम चालवून आधीपासून वापरात असलेले कमकुवत किंवा सहज ओळखता येणारे पासवर्ड्स शोधते. सिस्टिम विद्यमान पासवर्ड्सची तुलना ज्ञात कमकुवत पॅटर्न्स आणि डिक्शनरी फाइल्स शी करते.
4. **प्रोॲक्टिव पासवर्ड चेकिंग (Proactive Password Checking):** प्रोॲक्टिव पासवर्ड चेकिंग ही पद्धत पासवर्ड तयार करतानाच त्याची मजबुती तपासते. सिस्टिम पासवर्ड सिलेक्शनच्या वेळीच त्याची ताकद तपासते आणि कमकुवत पासवर्ड लगेच नाकारते. या पद्धतीमुळे फक्त मजबूत, क्लिष्ट आणि सुरक्षित पासवर्ड्सच स्वीकारले जातात.

पासवर्ड सिलेक्शनसाठी मार्गदर्शक तत्त्वे (Guidelines for Password Selection):

1. लांब पासवर्ड वापरा: किमान 8-12 कॅरेक्टर्स; पासवर्ड जितका लांब तितका मजबूत.
2. वेगवेगळ्या प्रकारचे कॅरेक्टर्स वापरा

यामध्ये खालील गोष्टींचा समावेश करा:

- अपरकेस अक्षरे (A–Z)
- लोअरकेस अक्षरे (a–z)
- नंबर (0–9)
- स्पेशल कॅरेक्टर्स (!, @, #, $, %, इ.)

3. वैयक्तिक माहिती टाळा

खालील गोष्टी वापरू नका:

- नावे (उदा. Krishna123)
- जन्मतारीख
- मोबाईल नंबर

- पाळीव प्राण्यांची नावे
- सामान्य शब्द

4. डिक्शनरी शब्द आणि पॅटर्न्स टाळा उदा.: password, admin, qwerty, 123456, abcd1234
5. प्रत्येक अकाउंटसाठी वेगळा पासवर्ड वापरा: यामुळे क्रेडेन्शियल-स्टफिंग अटॅक्स टाळता येतात.
6. पासवर्ड नियमित बदलत रहा: विशेषतः हाय-सिक्युरिटी सिस्टिम्स साठी आवश्यक.
7. पासफ्रेसेस वापरा: उदाहरण: Blue$Tiger! Road2024 लक्षात ठेवायला सोपे पण फोडायला कठीण.
8. जुने पासवर्ड पुन्हा वापरू नका: पासवर्ड हिस्टरी नियम पाळा.
9. पासवर्ड कागदावर लिहू नका: स्टिकी नोट्स, डायरी किंवा प्लेन टेक्स्टमध्ये साठवणे टाळा.
10. मल्टी-फॅक्टर ऑथेंटिकेशन (एमएफए) सक्षम करा: पासवर्ड चोरीला गेला तरीही अतिरिक्त संरक्षण मिळते.

2. पिगीबॅकिंग (Piggybacking)

पिगीबॅकिंग हा एक सुरक्षा अटॅक आहे, ज्यामध्ये अनऑथराइज्ड व्यक्ती अधिकृत वापरकर्त्याच्या अगदी जवळून शारीरिक किंवा डिजिटल पद्धतीने पाठलाग करून सिस्टिम, नेटवर्क किंवा प्रतिबंधित क्षेत्रात प्रवेश मिळवते. या अटॅकमध्ये हल्लेखोर ऑथेंटिकेशन न करता अधिकृत वापरकर्त्याच्या प्रवेशाचा फायदा घेतो आणि त्याच्यासोबतच "राइड" करतो. पिगीबॅकिंग तेव्हा घडते जेव्हा हल्लेखोर अधिकृत वापरकर्त्याचा गैरफायदा घेऊन सुरक्षित क्षेत्रात प्रवेश करतो किंवा आधीच लॉगिन असलेली सिस्टिम वापरतो. भौतिक (Physical) वातावरणात, कर्मचारी सुरक्षित दरवाजा उघडत असताना हल्लेखोर मानवी शिष्टाचार किंवा दुर्लक्षाचा फायदा घेऊन त्याच्या मागून आत प्रवेश करतो. डिजिटल (Digital) वातावरणात, वापरकर्ता आपला कम्प्युटर, ॲप्लिकेशन किंवा सेशन अनलॉक आणि अनअटेंडेड ठेवतो, तेव्हा पिगीबॅकिंग घडते. त्यानंतर हल्लेखोर सक्रिय सेशनचा वापर करून संवेदनशील डेटावर प्रवेश करतो किंवा अनधिकृत कृती करतो. या अटॅकमध्ये पासवर्ड गेसिंग किंवा पासवर्ड क्रॅकिंगची गरज नसते; त्याऐवजी तो वापरकर्त्याचा निष्काळजीपणा, कमकुवत सेशन मॅनेजमेंट आणि दुर्बल भौतिक सुरक्षा यांचा गैरफायदा घेतो. पिगीबॅकिंग सहसा ऑफिसेस, लॅब्स, शेअर्ड कम्प्युटर्स आणि प्रतिबंधित वर्कस्पेसेस येथे आढळते.

प्रतिबंधात्मक उपाय (Preventive Measures)

- स्क्रीन लॉक ठेवणे
- ऑटो-लॉगआउट सक्षम करणे
- मजबूत ॲक्सेस कंट्रोल वापरणे
- युजर अवेअरनेस वाढवणे
- भौतिक प्रवेश बिंदूंचे निरीक्षण (मॉनिटरिंग) करणे

पिगीबॅकिंगचे प्रकार (Types of Piggybacking)

1. फिजिकल पिगीबॅकिंग (Physical Piggybacking)

"अनऑथराइज्ड व्यक्ती सुरक्षित दरवाज्यातून अधिकृत वापरकर्त्याच्या मागून प्रवेश करते."

फिजिकल पिगीबॅकिंग हा एक सुरक्षा अटॅक आहे, ज्यामध्ये अनऑथराइज्ड व्यक्ती स्वतःची ऑथेंटिकेशन पद्धत न वापरता अधिकृत वापरकर्त्याच्या अगदी मागे मागे जाऊन प्रतिबंधित किंवा सुरक्षित भौतिक क्षेत्रात प्रवेश मिळवते. या अटॅकमध्ये हल्लेखोर मानवी शिष्टाचार, घाई किंवा दुर्लक्ष यांचा फायदा घेतो आणि सुरक्षित दरवाज्यातून आत प्रवेश करतो.

Fig 2.5: फिजिकल पिगीबॅकिंग (Physical Piggybacking)

उदाहरण (Example): एक अधिकृत वापरकर्ता आपले आयडी कार्ड वापरून मुख्य ऑफिसचा दरवाजा उघडतो. तो आत प्रवेश करत असताना, हल्लेखोर लगेचच त्याच्या मागून दरवाजा बंद होण्यापूर्वी आत शिरतो. हल्लेखोर कोणतेही आयडी कार्ड न दाखवता सुरक्षित इमारतीत प्रवेश करतो. हा फिजिकल पिगीबॅकिंग चा प्रकार आहे.

2. डिजिटल पिगीबॅकिंग (Digital Piggybacking)

"हल्लेखोर दुसऱ्या वापरकर्त्याने लॉगिन करून ठेवलेला कम्प्युटर किंवा ॲप्लिकेशन वापरतो."

डिजिटल पिगीबॅकिंग हा एक सुरक्षा अटॅक आहे, ज्यामध्ये अनऑथराइज्ड वापरकर्ता अधिकृत वापरकर्त्याने लॉगिन करून ठेवलेली किंवा अनलॉक सोडलेली सेशन वापरून कम्प्युटर सिस्टिम, ऑनलाइन अकाउंट किंवा ॲप्लिकेशनमध्ये प्रवेश मिळवतो. या प्रकारात हल्लेखोर सक्रिय सेशनचा गैरवापर करून संवेदनशील माहिती मिळवतो किंवा अनधिकृत कृती करतो.

Fig 2.6: डिजिटल पिगीबॅकिंग (Digital Piggybacking)

उदाहरण (Example): एक अधिकृत वापरकर्ता कॉलेजच्या ईआरपी पोर्टलवर लॅबमधील कम्प्युटरवर लॉगिन करतो. तो लॉगआउट न करता कम्प्युटर सोडून जातो. नंतर दुसरा विद्यार्थी त्याच सिस्टिमवर बसतो आणि अधिकृत वापरकर्त्याचे उघडे सेशन वापरून गुण पाहतो, तपशील बदलतो किंवा फाईल्स डाउनलोड करतो. हा डिजिटल पिगीबॅकिंग चा प्रकार आहे, कारण हल्लेखोराने अधिकृत वापरकर्त्याच्या आधीच ऑथेंटिकेट केलेल्या सेशनचा वापर केला आहे.

प्रतिबंधात्मक उपाय (Preventions)

फिजिकल पिगीबॅकिंगसाठी प्रतिबंध (Physical Piggybacking Preventions)

1. कडक दरवाजा ॲक्सेस कंट्रोल लागू करा: दरवाज्यांमधून एका वेळी फक्त एकाच व्यक्तीला आयडी कार्ड्स, बायोमेट्रिक्स किंवा पिन्स वापरून प्रवेश मिळावा.
2. वापरकर्त्यांना इतरांना मागून येऊ न देण्याचे प्रशिक्षण द्या: कर्मचाऱ्यांनी अनोळखी व्यक्तींसाठी दरवाजे उघडे धरू नयेत.
3. सीसीटीव्ही कॅमेरे आणि सुरक्षा रक्षक बसवा: मॉनिटरिंगमुळे अनधिकृत प्रवेशाचे प्रयत्न ओळखता येतात.
4. ऑटोमॅटिक दरवाजा बंद होणारी प्रणाली वापरा: कोणतीही व्यक्ती आत गेल्यानंतर दरवाजा लगेच बंद झाला पाहिजे.
5. इशारा देणारी फलक लावा: कर्मचाऱ्यांना आठवण करून देणारे पोस्टर्स लावा: "टेलगेटिंग किंवा पिगीबॅकिंगला परवानगी देऊ नका."

डिजिटल पिगीबॅकिंगसाठी प्रतिबंध (Digital Piggybacking Preventions):

1. दूर जाताना नेहमी स्क्रीन लॉक करा: वापरकर्त्यांनी कम्प्युटरपासून दूर जाताना पीसी लॉक (विन + एल) करणे आवश्यक आहे.
2. ऑटोमॅटिक स्क्रीन लॉक / टाइमआउट सक्षम करा: काही वेळ निष्क्रियतेनंतर सिस्टिम आपोआप लॉक झाली पाहिजे.
3. ऑटोमॅटिक सेशन लॉगआउट सक्षम करा: वेब पोर्टल्स, ईआरपी, बँकिंग आणि ॲडमिन कन्सोल्समध्ये निष्क्रिय वापरकर्त्यांचे सेशन आपोआप लॉगआउट झाले पाहिजे.
4. पासवर्ड शेअर करू नका किंवा लिहून ठेवू नका: यामुळे इतरांनी सेशनचा गैरवापर करण्याची शक्यता कमी होते.
5. वापरल्यानंतर योग्य प्रकारे लॉगआउट करा: विशेषतः लॅब्स, सायबर कॅफे, शेअर्ड सिस्टिम्स आणि ऑफिसेस मध्ये हे अत्यंत महत्त्वाचे आहे.

3. शोल्डर सर्फिंग (Shoulder Surfing)

शोल्डर सर्फिंग हा असा अटॅक आहे ज्यामध्ये अनऑथराइज्ड व्यक्ती वापरकर्ता पासवर्ड्स, PINs किंवा लॉगिन क्रेडेन्शियल्स टाइप करत असताना त्याच्या खांद्यावरून किंवा जवळून गुपचूप निरीक्षण करून ही संवेदनशील माहिती मिळवते. शोल्डर सर्फिंग हा एक सामान्य ह्युमन-बेस्ड अटॅक आहे, ज्यामध्ये हल्लेखोर दृश्य निरीक्षणाद्वारे (visually) वापरकर्त्याची गोपनीय माहिती कॅप्चर करतो. स्टँडर्ड सिक्युरिटी प्रिन्सिपल्सनुसार, हा अटॅक मानवी वर्तन, अवेअरनेसचा अभाव आणि गर्दीची ठिकाणे यांचा गैरफायदा घेतो. हा अटॅक सहसा ATMs, कम्प्युटर लॅब्स, सायबर कॅफे, ऑफिसेस आणि सार्वजनिक ठिकाणी होतो, जिथे वापरकर्ते कीपॅड किंवा स्क्रीन झाकून न घेता पासवर्ड किंवा PIN एंटर करतात.
तांत्रिक स्रोतांनुसार, शोल्डर सर्फिंगसाठी हॅकिंग स्किल्सची गरज नसते, फक्त निरीक्षण किंवा मोबाईल कॅमेरे, प्रतिबिंब (reflections) किंवा दुर्बिणी (binoculars) यांसारखी सोपी साधने पुरेशी असतात. ट्रेनिंग मटेरियल्समध्ये नमूद केले आहे की हल्लेखोर पीडिताच्या मागे उभा राहू शकतो, जवळ बसू शकतो किंवा दूरून रेकॉर्डिंग करू शकतो. सिक्युरिटी अवेअरनेस डॉक्युमेंट्सनुसार, कमकुवत प्रायव्हसी पद्धती, अपुरी युजर एज्युकेशन आणि निष्काळजीपणा यामुळे हा अटॅक अत्यंत यशस्वी ठरतो. शोल्डर सर्फिंग टाळण्यासाठी, वापरकर्त्यांनी कीपॅड झाकणे, योग्य अंतर ठेवणे, प्रायव्हसी स्क्रीन वापरणे, सार्वजनिक ठिकाणी पासवर्ड एंटर टाळणे आणि आजूबाजूच्या परिस्थितीबद्दल सतर्क राहणे आवश्यक आहे.

Fig 2.7: शोल्डर सर्फिंग (Shoulder Surfing)

उदाहरण (Example): एक अधिकृत वापरकर्ता गर्दीच्या ठिकाणी असलेल्या ATM वर PIN एंटर करत आहे. एक हल्लेखोर अगदी जवळून मागे उभा राहून वापरकर्ता नंबर टाइप करताना कीपॅड थेट पाहतो. हल्लेखोर थोड्याच अंतरावरून सहज निरीक्षण करू शकत असल्यामुळे PIN कॅप्चर केला जातो. काही परिस्थितींमध्ये हल्लेखोर दूरून दुर्बिणी किंवा कॅमेरे वापरूनही निरीक्षण करू शकतो. हा शोल्डर सर्फिंग चा स्पष्ट उदाहरण आहे, ज्यामध्ये थेट निरीक्षणाद्वारे संवेदनशील माहिती चोरली जाते.

शोल्डर सर्फिंगसाठी प्रतिबंध (Preventions of Shoulder Surfing)

1. टाइप करताना कीपॅड / स्क्रीन झाका: पासवर्ड, PIN किंवा पॅटर्न एंटर करताना हात किंवा शरीराचा वापर करून कीपॅड / स्क्रीन झाका.
2. इतरांपासून योग्य अंतर ठेवा: विशेषतः ATMs, सार्वजनिक कम्प्युटर्स किंवा ऑफिसेसमध्ये पासवर्ड एंटर करताना कोणीही खूप जवळ उभे नाही याची खात्री करा.
3. प्रायव्हसी स्क्रीन वापरा: लॅपटॉप, डेस्कटॉप आणि मोबाईल स्क्रीनवर प्रायव्हसी फिल्टर्स लावा, ज्यामुळे स्क्रीन फक्त समोरूनच दिसेल.
4. सुरक्षित ATMs किंवा बंद जागा निवडा: बंद केबिन्स, CCTV मॉनिटरिंग असलेले किंवा कमी गर्दीचे ATMs वापरा, ज्यामुळे निरीक्षणाची शक्यता कमी होते.
5. आजूबाजूच्या परिस्थितीबद्दल सतर्क रहा: संवेदनशील माहिती एंटर करण्यापूर्वी आपल्या मागे किंवा बाजूला कोण आहे हे नेहमी तपासा.
6. गर्दीच्या ठिकाणी पासवर्ड टाइप करणे टाळा: फक्त निरीक्षणापासून सुरक्षित वाटत असेल तेव्हाच लॉगिन तपशील एंटर करा.
7. ऑटोमॅटिक स्क्रीन टाइमआउट आणि लॉक वापरा: जर कोणी तुमची स्क्रीन पाहण्याचा प्रयत्न केला, तर स्क्रीन लगेच लॉक केल्याने पुढील निरीक्षण टाळता येते.

4. डम्पस्टर डायव्हिंग (Dumpster Diving)

डम्पस्टर डायव्हिंग हा असा अटॅक आहे, ज्यामध्ये अनऑथराइज्ड व्यक्ती टाकून दिलेल्या साहित्यामधून (जसे की कागदपत्रे, नोट्स, प्रिंटआउट्स, स्टोरेज मीडिया किंवा कचरा) संवेदनशील माहिती शोधते. या माहितीत पासवर्ड्स, PINs, अकाउंट डिटेल्स किंवा गोपनीय डॉक्युमेंट्स यांचा समावेश असू शकतो. डम्पस्टर डायव्हिंग हा नॉन-टेक्निकल पण अत्यंत प्रभावी अटॅक आहे, ज्यामध्ये हल्लेखोर टाकून दिलेल्या वस्तूंचे परीक्षण करून माहिती मिळवतो. सिक्युरिटी लिटरेचरनुसार, हल्लेखोर अनेकदा फेकून दिलेली कागदपत्रे, स्टिकी नोट्स, ड्राफ्ट्स, ॲक्सेस कोड्स, कॉन्फिगरेशन फाइल्स आणि अगदी जुनी स्टोरेज डिव्हाइसेस देखील गोळा करतात. अनेक वापरकर्ते पासवर्ड लिहून ठेवतात किंवा संवेदनशील डेटा प्रिंट करून नंतर निष्काळजीपणे टाकून देतात, आणि हल्लेखोर या मानवी कमकुवतपणाचा गैरफायदा घेतो. ट्रेनिंग मटेरियल्सनुसार, अर्धवट फाटलेले किंवा चुरगळलेले कागदही हल्लेखोराला पासवर्ड किंवा अकाउंट माहिती पुन्हा तयार (reconstruct) करण्यास मदत करू शकतात. सायबर सिक्युरिटी कोर्सेसमध्ये नमूद केले आहे की हा अटॅक आयडेंटिटी थेफ्ट, अनधिकृत अकाउंट ॲक्सेस, सोशल इंजिनियरिंग आणि कॉर्पोरेट गुप्तहेरगिरी यांना कारणीभूत ठरू शकतो. या अटॅकसाठी तांत्रिक कौशल्यांची गरज नसते फक्त डस्टबिन्स, रिसायकल बिन्स, प्रिंटर्स किंवा कचरा टाकण्याच्या जागांपर्यंत पोहोच आवश्यक असते. म्हणूनच योग्य डिस्पोजल पद्धती, कागद फाडून टाकणे (shredding) आणि युजर अवेअरनेस प्रोग्राम्स हे डम्पस्टर डायव्हिंग टाळण्यासाठी अत्यंत आवश्यक आहेत.

Fig 2.8: डम्पस्टर डायव्हिंग (Dumpster Diving)

उदाहरण (Example): एक कर्मचारी युजरनेम्स आणि फोन नंबर असलेली प्रिंट केलेली ई-मेल्स आणि रफ नोट्स साध्या डस्टबिनमध्ये टाकून देतो. एक हल्लेखोर त्या डस्टबिनमध्ये शोध घेतो, ही कागदपत्रे मिळवतो आणि त्या माहितीचा वापर करून संस्थेला बनावट फिशिंग ई-मेल्स पाठवतो.

डम्पस्टर डायव्हिंगसाठी प्रतिबंध (Preventions of Dumpster Diving)

1. सर्व गोपनीय कागदपत्रे टाकण्यापूर्वी श्रेड करा: पासवर्ड्स, PINs, अकाउंट नंबर किंवा वैयक्तिक तपशील असलेले कागद क्रॉस-कट श्रेडर्स वापरून पूर्णपणे नष्ट करा.
2. सुरक्षित डिस्पोजल बिन्स वापरा: संवेदनशील कागदपत्रे लॉक केलेल्या किंवा मॉनिटर केलेल्या बिन्समध्येच टाका; उघड्या डस्टबिनमध्ये टाकू नका.
3. पासवर्ड कागदावर लिहिणे टाळा: पासवर्ड्स स्टिकी नोट्स, वही किंवा प्रिंट केलेल्या शीट्सवर लिहून ठेवू नका, कारण त्या कचऱ्यात जाऊ शकतात.
4. जुनी स्टोरेज मीडिया योग्य प्रकारे नष्ट करा: CDs, USB ड्राइव्ह्स, हार्ड डिस्क्स आणि मेमरी कार्ड्स टाकण्यापूर्वी वाइप करा, डीगॉस करा किंवा भौतिकरित्या नष्ट करा.
5. संस्थास्तरावर डिस्पोजल पॉलिसीज लागू करा: संस्थांनी सुरक्षित डॉक्युमेंट डिस्पोजल प्रक्रिया लागू कराव्यात आणि संरक्षित श्रेडिंग एरियाज निश्चित कराव्यात.
6. क्लीन डेस्क आणि क्लीन डिस्पोजल पद्धती पाळा: प्रिंट केलेली कागदपत्रे अनअटेंडेड ठेवू नका; वापरल्यानंतर सुरक्षितपणे डिस्पोज करा.
7. कर्मचाऱ्यांना माहिती हाताळणीबाबत प्रशिक्षण द्या: अवेअरनेस प्रोग्राम्समुळे वापरकर्त्यांना सामान्य कचऱ्यात संवेदनशील माहिती टाकण्याचे धोके समजतात.
8. कचरा टाकण्याच्या जागांचे नियमित मॉनिटरिंग करा: CCTV किंवा नियमित तपासणी वापरून अनधिकृत व्यक्तींना कचऱ्यापर्यंत प्रवेश होत नाही याची खात्री करा.
9. अनावश्यक संवेदनशील माहिती प्रिंट करणे टाळा: कचऱ्यामधून गळती होऊ शकणाऱ्या संवेदनशील डेटाचे प्रमाण कमी करा.

2.3 बायोमेट्रिक्स (Biometrics)

बायोमेट्रिक्स ही एक ऑथेंटिकेशन पद्धत आहे, ज्यामध्ये वापरकर्त्याची ओळख किंवा पडताळणी त्याच्या अद्वितीय जैविक (Biological) किंवा वर्तनात्मक (Behavioral) वैशिष्ट्यांवर आधारित केली जाते. यामध्ये फिंगरप्रिंट्स, फेस पॅटर्न्स, आयरिस टेक्सचर, व्हॉईस इत्यादींचा समावेश होतो. बायोमेट्रिक्स ही सर्वात सुरक्षित आणि विश्वसनीय ऑथेंटिकेशन पद्धतींपैकी एक मानली जाते, कारण ती अशा मानवी वैशिष्ट्यांवर आधारित असते जी सहज ओळखता, कॉपी करता किंवा विसरता येत नाहीत. पारंपरिक ऑथेंटिकेशन तंत्रे जसे की पासवर्ड्स, ही गेसिंग, शोल्डर सर्फिंग, डम्पस्टर डायव्हिंग आणि सोशल इंजिनियरिंग सारख्या अटॅक्सना बळी पडू शकतात. बायोमेट्रिक्स या समस्या दूर करते, कारण ती वेळेनुसार स्थिर (consistent) राहणाऱ्या आणि प्रत्येक व्यक्तीसाठी वेगळ्या असणाऱ्या वैशिष्ट्यांवर आधारित असते. त्यामुळे वापरकर्त्याची ओळख अधिक अचूक आणि सुरक्षित पद्धतीने निश्चित केली जाते.

बायोमेट्रिक सिस्टिम (Biometric System)

ही आकृती बायोमेट्रिक ऑथेंटिकेशन सिस्टिमचा संपूर्ण वर्कफ्लो दर्शवते. या प्रक्रियेत वापरकर्त्याचा बायोमेट्रिक डेटा कसा कॅप्चर केला जातो, प्रोसेस केला जातो, स्टोअर केला जातो आणि व्हेरिफिकेशन दरम्यान मॅच केला जातो, हे दाखवलेले आहे.

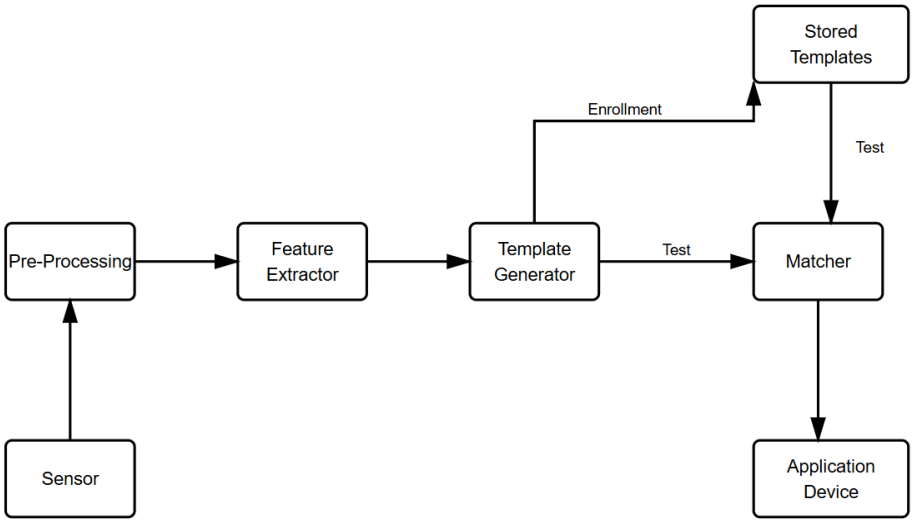


Fig 2.9: बायोमेट्रिक सिस्टिम (Biometric System)

1. **सेन्सर (Sensor):** सिस्टिमची सुरुवात सेन्सर पासून होते (फिंगरप्रिंट स्कॅनर, कॅमेरा, मायक्रोफोन). सेन्सर कच्चा बायोमेट्रिक डेटा कॅप्चर करतो, जसे की फिंगरप्रिंट इमेज, फेस इमेज, आयरिस स्कॅन किंवा व्हॉईस सॅम्पल.
2. **प्री-प्रोसेसिंग (Pre-Processing):** कच्च्या डेटामध्ये अनेकदा नॉईज, लाइटिंग प्रॉब्लेम्स, डिस्टॉर्शन इत्यादी असतात. प्री-प्रोसेसिंग प्रक्रियेत बायोमेट्रिक सॅम्पल स्वच्छ (clean) आणि एन्हान्स केला जातो, ज्यामुळे अचूक फीचर्स एक्स्ट्रॅक्ट करता येतात.
3. **फीचर एक्स्ट्रॅक्टर (Feature Extractor):** हा मॉड्यूल स्वच्छ केलेल्या बायोमेट्रिक डेटामधून अद्वितीय वैशिष्ट्ये (unique characteristics) काढतो.
   उदाहरणे: रिज पॅटर्न्स (फिंगरप्रिंट), आयरिस टेक्सचर, फेशियल जिओमेट्री, व्हॉईस फ्रिक्वेन्सी पॅटर्न
4. **टेम्पलेट जनरेटर (Template Generator):** एक्स्ट्रॅक्ट केलेल्या फीचर्सना डिजिटल बायोमेट्रिक टेम्पलेट मध्ये रूपांतरित करतो. टेम्पलेट हे प्रत्यक्ष इमेज नसून गणितीय प्रतिनिधित्व (mathematical representation) असते. येथून दोन प्रक्रिया होतात:
   a. एनरोलमेंट (Enrollment): टेम्पलेट डेटाबेसमध्ये रेफरन्स म्हणून स्टोअर केले जाते.
   b. टेस्ट (Test): व्हेरिफिकेशन दरम्यान मॅचिंगसाठी टेम्पलेट पाठवले जाते.
5. **स्टोअर्ड टेम्पलेट्स (Stored Templates – Database):** सर्व नोंदणीकृत वापरकर्त्यांचे बायोमेट्रिक टेम्पलेट्स येथे साठवलेले असतात. भविष्यातील तुलना (comparison) साठी टेम्पलेट्स सुरक्षितपणे स्टोअर केले जातात.

6. **मॅचर (Matcher):** टेस्ट टेम्पलेटची डेटाबेसमधील स्टोअर्ड टेम्पलेट्सशी तुलना करतो. मॅच स्कोअर कॅलक्युलेट करून ओळख योग्य आहे की नाही हे ठरवतो.
7. **ॲप्लिकेशन डिव्हाइस (Application Device):** मॅचरच्या निर्णयावर आधारित ॲप्लिकेशन डिव्हाइस पुढील कृती करते: ॲक्सेस देणे (Grant access), अक्सेस नाकारणे (Deny access), अलार्म ट्रिगर करणे, दरवाजा किंवा सिस्टिम अनलॉक करणे.

बायोमेट्रिक्सचे प्रकार (Types of Biometrics)

बायोमेट्रिक्सचे मुख्यत्वे दोन प्रकारांमध्ये वर्गीकरण केले जाते:

1. **फिजिओलॉजिकल बायोमेट्रिक्स (Physiological Biometrics):** बायोमेट्रिक्स हे मानवी शरीराच्या भौतिक आणि जैविक वैशिष्ट्यांवर आधारित असतात. ही वैशिष्ट्ये वेळेनुसार स्थिर (Stable) राहतात आणि ऑथेंटिकेशनसाठी उच्च अचूकता (High Accuracy) प्रदान करतात. यामध्ये खालील प्रकारांचा समावेश होतो: फिंगरप्रिंट्स (Fingerprints), हॅन्डप्रिंट्स (Handprints), रेटिना स्कॅन पॅटर्न्स (Retina Scan Patterns), फेस रिकग्निशन (Face Recognition)
2. **बिहेविअरल बायोमेट्रिक्स (Behavioral Biometrics):** बायोमेट्रिक्स हे व्यक्तीच्या कृती, सवयी आणि वर्तनात्मक पॅटर्न्सवर आधारित असतात. ही वैशिष्ट्ये वेळेनुसार बदलू शकतात, परंतु कॉन्टिन्युअस ऑथेंटिकेशन साठी उपयुक्त असतात. यामध्ये खालील प्रकारांचा समावेश होतो: व्हॉईस पॅटर्न्स (Voice Patterns), सिग्नेचर आणि रायटिंग पॅटर्न्स (Signature and Writing Patterns), कीस्ट्रोक्स (Keystrokes).

2.3.1 फिंगरप्रिंट्स (Finger Prints)

फिंगरप्रिंट रिकग्निशन ही एक फिजिओलॉजिकल बायोमेट्रिक तंत्रज्ञान आहे, ज्यामध्ये व्यक्तीची ओळख बोटांच्या टोकांवरील अद्वितीय रिज पॅटर्न्स, लूप्स, व्हॉर्ल्स आणि मिन्युशिया पॉइंट्स यांच्या आधारे केली जाते. फिंगरप्रिंट बायोमेट्रिक्स ही सर्वाधिक वापरली जाणारी आणि विश्वासार्ह ऑथेंटिकेशन पद्धतींपैकी एक आहे. या पद्धतीत प्रथम फिंगरप्रिंट इमेज कॅप्चर केली जाते, त्यानंतर ती एन्हान्स केली जाते, त्यामधील अद्वितीय पॉइंट्स एक्स्ट्रॅक्ट केले जातात आणि शेवटी ती आधी स्टोअर केलेल्या टेम्पलेट्सशी तुलना (matching) केली जाते. फिंगरप्रिंट पॅटर्न्स हे स्थिर (stable), अद्वितीय (unique) आणि बनावट करणे अत्यंत कठीण असतात. त्यामुळे पासवर्ड्सच्या तुलनेत फिंगरप्रिंट्स अधिक सुरक्षित ठरतात, कारण पासवर्ड्स गेसिंग, शोल्डर सर्फिंग किंवा डम्पस्टर डायव्हिंग यांसारख्या अटॅक्सद्वारे सहज मिळवता येऊ शकतात. फिंगरप्रिंट सिस्टिम्स एक संरचित आर्किटेक्चर अनुसरतात, ज्यामध्ये सेन्सर कॅप्चर, प्री-प्रोसेसिंग, फीचर एक्स्ट्रॅक्शन, टेम्पलेट जनरेशन आणि मॅचिंग या टप्प्यांचा समावेश असतो. या सिस्टिम्सचा वापर स्मार्टफोन्स, अटेंडन्स मशिन्स, आधार ऑथेंटिकेशन, बॉर्डर कंट्रोल, डिजिटल फॉरेन्सिक्स आणि सुरक्षित ॲक्सेस सिस्टिम्स मध्ये मोठ्या प्रमाणावर केला जातो.

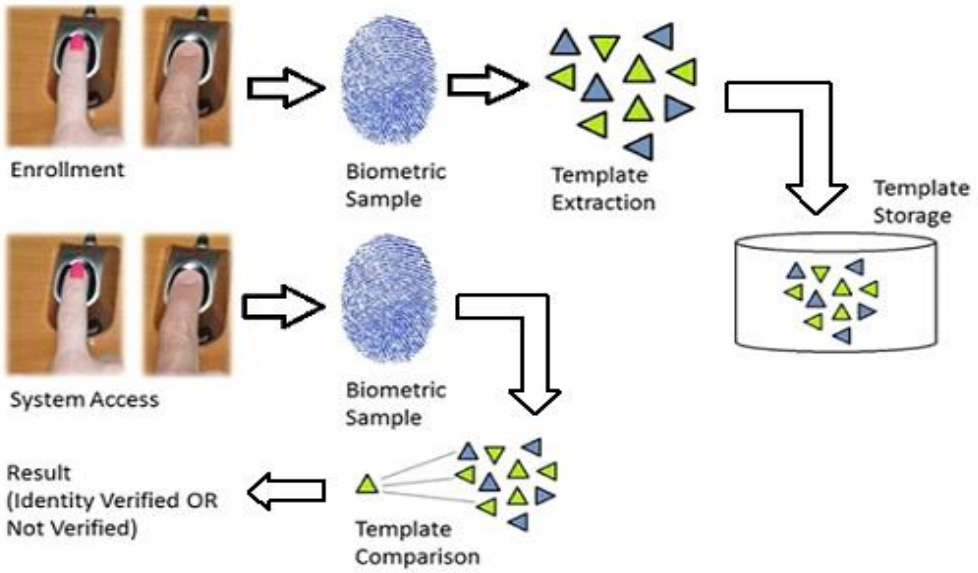


Fig 2.10: फिंगरप्रिंट रजिस्ट्रेशन आणि व्हेरिफिकेशन प्रक्रिया (Fingerprint Registration & Verification Process)

1. एनरोलमेंट (Enrollment / Registration Phase): एनरोलमेंट म्हणजे एखादी व्यक्ती पहिल्यांदा बायोमेट्रिक सिस्टिम वापरते ती प्रक्रिया. या टप्प्यात सिस्टिम वापरकर्त्याचा फिंगरप्रिंट कॅप्चर करते आणि त्याचा डिजिटल टेम्पलेट तयार करून स्टोअर करते.
2. व्हेरिफिकेशन फेज (Verification Phase): व्हेरिफिकेशन टप्प्यात नवीन फिंगरप्रिंट सॅम्पल कॅप्चर केला जातो आणि तो एनरोलमेंट दरम्यान स्टोअर केलेल्या टेम्पलेटशी तुलना करून वापरकर्त्याची ओळख निश्चित केली जाते.

स्टेप्स (Steps):

1. सेन्सर (Sensor – Data Capture): हा सिस्टिममधील पहिला ब्लॉक आहे. तो रिअल वर्ल्ड आणि बायोमेट्रिक सिस्टिम यांच्यातील इंटरफेस म्हणून काम करतो. स्कॅनर किंवा सेन्सरद्वारे सर्व आवश्यक फिंगरप्रिंट डेटा कॅप्चर करतो.
2. प्री-प्रोसेसिंग (Pre-Processing): कॅप्चर केलेल्या फिंगरप्रिंट इमेजमध्ये नॉईज, डिस्टॉर्शन किंवा लाइटिंग समस्या असू शकतात. प्री-प्रोसेसिंग टप्प्यात इमेज एन्हान्स केली जाते, जेणेकरून ती फीचर एक्स्ट्रॅक्शनसाठी योग्य बनेल. यामध्ये नॉईज रिमूव्हल, नॉर्मलायझेशन आणि सेगमेंटेशन यांचा समावेश असतो.
3. फीचर एक्स्ट्रॅक्शन (Feature Extraction): हा एक महत्त्वाचा टप्पा आहे, ज्यामध्ये अद्वितीय मिन्युशिया फीचर्स काढली जातात, जसे की: रिज एंडिंग्स, बायफर्केशन्स, रिज फ्लो आणि काउंट. फीचर एक्स्ट्रॅक्शन हे योग्य आणि ऑप्टिमाइझ्ड फीचर एक्स्ट्रॅक्शनमुळे मॅचिंगची अचूकता वाढते.
4. टेम्पलेट जनरेशन आणि मॅचिंग (Template Generation & Matching)
5. एनरोलमेंट दरम्यान: एक्स्ट्रॅक्ट केलेली फीचर्स बायोमेट्रिक टेम्पलेटमध्ये रूपांतरित केली जातात. व टेम्पलेट डेटाबेसमध्ये, कार्डवर किंवा सुरक्षित मॉड्यूलमध्ये स्टोअर केले जाते.
6. व्हेरिफिकेशन दरम्यान: नवीन टेस्ट टेम्पलेट तयार केले जाते. मॅचर हे टेस्ट टेम्पलेट स्टोअर्ड टेम्पलेट्सशी तुलना करतो. तो सिमिलॅरिटी / डिस्टन्स स्कोअर कॅलक्युलेट करतो. मॅचिंग स्कोअरच्या आधारे सिस्टिम ॲक्सेस मंजूर (Grant) किंवा नाकारते (Deny).

2.3.2 हॅन्डप्रिंट्स (Handprints)

हॅन्डप्रिंट किंवा हॅन्ड जिओमेट्री रिकग्निशन ही एक फिजिओलॉजिकल बायोमेट्रिक तंत्रज्ञान आहे, ज्यामध्ये व्यक्तीची ओळख हाताचा आकार, माप आणि भौतिक परिमाणे यांच्या आधारे केली जाते. यामध्ये बोटांची लांबी, तळहाताची रुंदी, नकल्सचा आकार आणि संपूर्ण हाताची जिओमेट्री यांचा समावेश होतो. हॅन्ड जिओमेट्री बायोमेट्रिक्स ही व्यक्तीच्या हाताच्या अद्वितीय भौतिक वैशिष्ट्यांवर आधारित असते. जिथे फिंगरप्रिंट्स आणि आयरिस पॅटर्न्स सूक्ष्म (micro-level) वैशिष्ट्यांवर आधारित असतात, तिथे हॅन्ड जिओमेट्री ही मोठ्या स्तरावरील (macro-level) मोजमापांवर आधारित असते, जसे की बोटांची लांबी व रुंदी, तळहाताचा आकार, नकल्सची स्थिती आणि हाताचा एकूण आकार. ही वैशिष्ट्ये प्रौढ व्यक्तींमध्ये वेळेनुसार स्थिर राहतात, त्यामुळे हॅन्ड-आधारित ऑथेंटिकेशन विश्वसनीय आणि वापरण्यास सोपी ठरते. हॅन्ड जिओमेट्री सिस्टिम मध्ये सुरुवातीला कॅमेरा किंवा हॅन्ड-स्कॅनर डिव्हाइस वापरून हाताची इमेज कॅप्चर केली जाते. कॅप्चर केलेली इमेज प्री-प्रोसेसिंग द्वारे स्वच्छ केली जाते, ज्यामध्ये नॉईज काढून टाकणे, आउटलाईन्स आणि महत्त्वाची मोजमापे एक्स्ट्रॅक्ट करणे यांचा समावेश असतो. यानंतर फीचर एक्स्ट्रॅक्शन प्रक्रियेत या मोजमापांचे न्युमेरिकल डेटामध्ये रूपांतर केले जाते आणि त्यावर आधारित बायोमेट्रिक टेम्पलेट तयार केले जाते. व्हेरिफिकेशन दरम्यान, वापरकर्त्याचे टेस्ट टेम्पलेट स्टोअर केलेल्या टेम्पलेट्सशी तुलना करून ओळख निश्चित केली जाते. हॅन्डप्रिंट रिकग्निशन चा मोठ्या प्रमाणावर वापर अटेंडन्स सिस्टिम्स, ॲक्सेस कंट्रोल, टाइम-ट्रॅकिंग सिस्टिम्स आणि जलद व संपर्क-आधारित व्हेरिफिकेशन आवश्यक असलेल्या वर्कप्लेसेस मध्ये केला जातो.

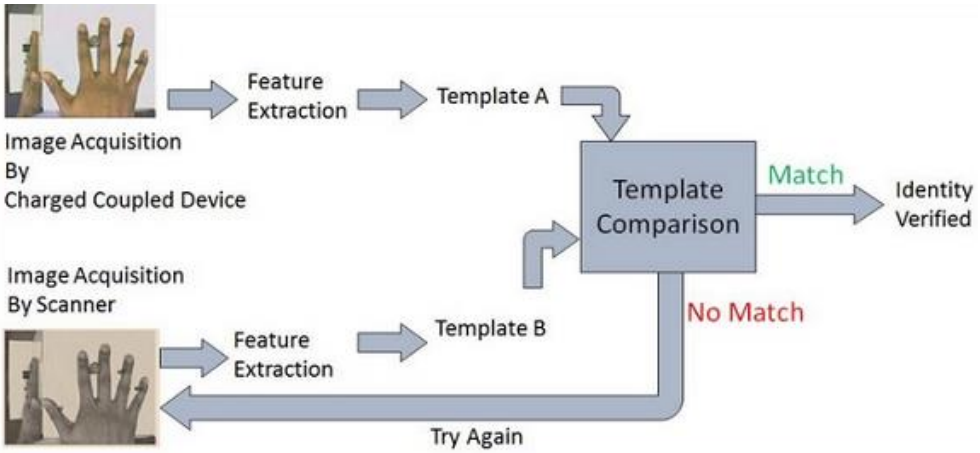


Fig 2.11: हॅन्डप्रिंट रजिस्ट्रेशन आणि व्हेरिफिकेशन प्रक्रिया (Handprint Registration & Verification Process)

1. सेन्सर (Sensor / Capture Module): कॅमेरा, ऑप्टिकल स्कॅनर किंवा इन्फ्रारेड डिव्हाइस वापरून हाताची इमेज कॅप्चर केली जाते.
2. प्री-प्रोसेसिंग (Pre-Processing): इमेज एन्हान्स केली जाते. नॉईज काढून टाकला जातो. हाताचा आउटलाईन (outline) निश्चित केला जातो.
3. फीचर एक्स्ट्रॅक्शन (Feature Extraction): खालील मोजमापे एक्स्ट्रॅक्ट केली जातात: बोटांची लांबी (Finger lengths), बोटांची रुंदी (Finger widths), तळहाताची रुंदी (Palm width), हाताचा एकूण आकार (Overall hand shape), नकल्सची स्थिती (Knuckle positions), परस्पर अंतर (Relative distances).
4. टेम्पलेट जनरेशन आणि स्टोरेज (Template Generation & Storage): एनरोलमेंट दरम्यान, एक्स्ट्रॅक्ट केलेली फीचर्स न्युमेरिकल टेम्पलेटमध्ये रूपांतरित करून स्टोअर केली जातात. व्हेरिफिकेशन दरम्यान, नवीन मोजमापे स्टोअर केलेल्या टेम्पलेट्सशी तुलना केली जातात.
5. मॅचिंग आणि निर्णय (Matching & Decision): मॅचर सिमिलॅरिटी स्कोअर्स कॅलक्युलेट करतो. मॅचिंगच्या आधारे सिस्टिम ॲक्सेस मंजूर (Grant) किंवा नाकारते (Deny).

2.3.3 रेटिना स्कॅन पॅटर्न्स (Retina Scan Patterns)

रेटिना स्कॅन ही एक फिजिओलॉजिकल बायोमेट्रिक तंत्रज्ञान आहे, ज्यामध्ये व्यक्तीची ओळख डोळ्याच्या मागील बाजूस असलेल्या (रेटिना) रक्तवाहिन्यांच्या अद्वितीय पॅटर्न्सच्या विश्लेषणावर आधारित केली जाते. हे पॅटर्न्स अत्यंत स्थिर, गुंतागुंतीचे आणि प्रत्येक व्यक्तीसाठी वेगळे असतात. रेटिना स्कॅनिंग ही सर्वात अचूक बायोमेट्रिक ओळख पद्धतींपैकी एक आहे. रेटिनामध्ये रक्तवाहिन्यांचे घनदाट जाळे असते, जे इतके अद्वितीय असते की एकसारख्या जुळ्या (identical twins) व्यक्तींमध्येही वेगळे असते. हा पॅटर्न आयुष्यभर अत्यंत स्थिर राहतो, त्यामुळे रेटिना बायोमेट्रिक्स अत्यंत विश्वासार्ह ठरते. रेटिना स्कॅनर डोळ्याच्या आत प्रकाश टाकण्यासाठी लो-इंटेन्सिटी इन्फ्रारेड लाईट वापरतो आणि रक्तवाहिन्यांची रचना कॅप्चर करतो. कॅप्चर केलेली इमेज प्री-प्रोसेसिंग करून कॉन्ट्रास्ट एन्हान्स केला जातो. त्यानंतर ब्रँचिंग पॉइंट्स आणि व्हेसल डिस्ट्रिब्युशन यांसारखी महत्त्वाची फीचर्स एक्स्ट्रॅक्ट केली जातात. ही फीचर्स बायोमेट्रिक टेम्पलेटमध्ये रूपांतरित करून एनरोलमेंट दरम्यान स्टोअर केली जातात. व्हेरिफिकेशन दरम्यान, नवीन रेटिनल पॅटर्न कॅप्चर केला जातो आणि तो स्टोअर केलेल्या टेम्पलेट्सशी मॅच करून ओळख निश्चित केली जाते. रेटिना स्कॅन्स चा मोठ्या प्रमाणावर वापर हाय-सिक्युरिटी एरियाज, मिलिटरी फॅसिलिटीज, ऑथेंटिकेशन टर्मिनल्स आणि अत्यंत महत्त्वाच्या सिस्टिम्समध्ये केला जातो, जिथे कमाल अचूकता आणि कमी फॉल्स-मॅच रेट्स आवश्यक असतात.

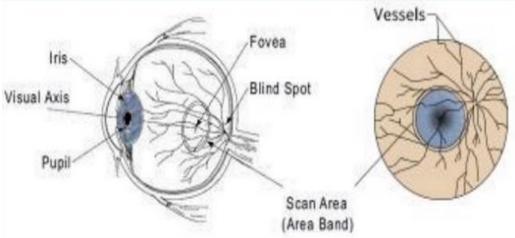


Fig 2.12: रेटिना स्कॅन पॅटर्न्स (Retina Scan Patterns)

रेटिना स्कॅन रजिस्ट्रेशन आणि व्हेरिफिकेशन प्रक्रिया (Retina Scan Registration & Verification Process)

1. सेन्सर (Sensor – Retina Scanner): इन्फ्रारेड लाईट वापरून डोळ्याच्या मागील बाजूस असलेल्या रक्तवाहिन्यांचा पॅटर्न कॅप्चर करतो.
2. प्री-प्रोसेसिंग (Pre-Processing): नॉईज काढून टाकतो, रक्तवाहिन्यांचा कॉन्ट्रास्ट एन्हान्स करतो, लाइटिंग आणि फोकस ॲडजस्ट करतो
3. फीचर एक्स्ट्रॅक्शन (Feature Extraction): पुढील प्रमाणे अद्वितीय फीचर्स एक्स्ट्रॅक्ट केली जातात: रक्तवाहिन्यांचे ब्रँचिंग पॅटर्न्स, व्हेसल थिकनेस, रक्तवाहिन्यांचे स्पेशियल डिस्ट्रिब्युशन, कर्व्हेचर आणि बायफर्केशन पॉइंट्स.
4. टेम्पलेट जनरेशन आणि स्टोरेज (Template Generation & Storage): एनरोलमेंट दरम्यान: रेटिनल टेम्पलेट तयार करून सुरक्षितपणे स्टोअर केले जाते. व्हेरिफिकेशन दरम्यान: नवीन स्कॅनचे टेस्ट टेम्पलेटमध्ये रूपांतर केले जाते.
5. मॅचिंग आणि निर्णय (Matching & Decision): मॅचर टेस्ट टेम्पलेटची स्टोअर केलेल्या टेम्पलेट्सशी तुलना करतो. सिमिलॅरिटी स्कोअरच्या आधारे सिस्टिम ॲक्सेस मंजूर (Grant) किंवा नाकारते (Deny).

2.3.4 व्हॉईस पॅटर्न रिकग्निशन (Voice Pattern Recognition)

व्हॉईस रिकग्निशन, ज्याला स्पीकर रिकग्निशन असेही म्हणतात, ही एक बिहेव्हियरल बायोमेट्रिक तंत्रज्ञान पद्धत आहे. या पद्धतीमध्ये व्यक्तीची ओळख किंवा पडताळणी आवाजाच्या अद्वितीय वैशिष्ट्यांवर आधारित केली जाते, जसे की पिच, टोन, फ्रिक्वेन्सी, ॲक्सेंट आणि स्पीच रिदम. व्हॉईस पॅटर्न बायोमेट्रिक्स मध्ये व्होकल ट्रॅक्टचे भौतिक गुणधर्म आणि बोलण्याशी संबंधित वर्तनात्मक वैशिष्ट्ये यांचा एकत्रित वापर केला जातो. एनरोलमेंट फेजमध्ये, वापरकर्ता मायक्रोफोनमध्ये एखादा शब्द किंवा वाक्य बोलतो. मायक्रोफोन साउंड वेव्ह्सना इलेक्ट्रिकल सिग्नल्समध्ये रूपांतरित करतो. हे सिग्नल्स पुढे ॲनालॉग-टू-डिजिटल कन्व्हर्टर (ADC) द्वारे डिजिटाइझ केले जातात आणि व्हॉईस टेम्पलेट म्हणून स्टोअर केले जातात. व्हेरिफिकेशन दरम्यान, वापरकर्त्याचा लाईव्ह आवाज पुन्हा कॅप्चर केला जातो, डिजिटाइझ केला जातो आणि स्टोअर केलेल्या व्हॉईस टेम्पलेट्सशी तुलना करून ओळख निश्चित केली जाते. फीचर एक्स्ट्रॅक्शन अल्गोरिदम्स पुढील गुणधर्मांचे विश्लेषण करतात: फ्रिक्वेन्सी स्पेक्ट्रम, पिच, टोन, मेल-फ्रिक्वेन्सी सेप्स्ट्रल कोएफिशंट्स (MFCCs). व्हॉईस रिकग्निशन चा मोठ्या प्रमाणावर वापर टेलिफोन बँकिंग, व्हर्च्युअल असिस्टंट्स, सिक्युअर ॲक्सेस कंट्रोल आणि ऑटोमेटेड कॉल सिस्टिम्स मध्ये केला जातो. ही पद्धत कॉन्टॅक्टलेस आणि सोयीस्कर असली तरी आवाजातील नॉईज, आजारपण किंवा खराब मायक्रोफोन क्वालिटी यामुळे तिच्या अचूकतेवर परिणाम होऊ शकतो.

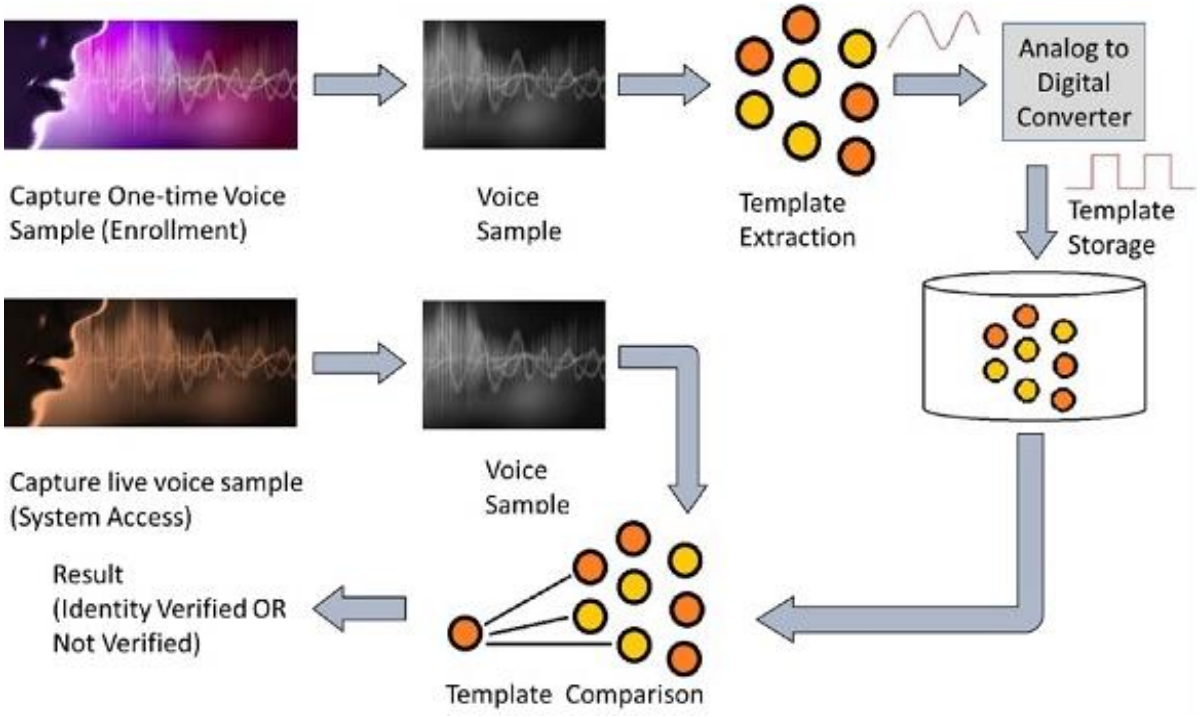


Fig 2.13: व्हॉईस पॅटर्न रिकग्निशन प्रक्रिया (Voice pattern recognition Process)

1. **स्पीकर डिपेंडंट (Speaker Dependent):** या प्रकारामध्ये वापरकर्त्याला आधी सिस्टिमला आपला आवाज शिकवावा लागतो (ट्रेनिंग आवश्यक असते).
   उदाहरणे: पर्सनल व्हॉईस असिस्टंट्स, सिंगल-यूजर ॲक्सेस कंट्रोल सिस्टिम्स.
2. **स्पीकर इंडिपेंडंट (Speaker Independent):** या प्रकारामध्ये कोणत्याही पूर्व ट्रेनिंगशिवाय अनेक वापरकर्त्यांचे आवाज ओळखले जातात.

उदाहरणे: ऑटोमेटेड टेलिफोन मेन्यू, IVR सिस्टिम्स, कस्टमर सर्व्हिस हेल्पलाइन्स.

यामुळे व्हॉईस बायोमेट्रिक्स ही पद्धत वैयक्तिक तसेच मल्टी-यूजर वातावरणासाठी लवचिक आणि उपयुक्त ठरते.

1. सेन्सर (मायक्रोफोन): वापरकर्त्याचा आवाज नमुना कॅप्चर करतो.
2. ॲनालॉग-टू-डिजिटल कन्व्हर्जन (ADC): इलेक्ट्रिकल ऑडिओ सिग्नलला डिजिटल डेटामध्ये रूपांतरित करतो.
3. प्री-प्रोसेसिंग: बॅकग्राऊंड नॉईज काढून टाकतो, अनावश्यक फ्रिक्वेन्सी फिल्टर करतो आणि व्हॉल्यूम नॉर्मलाइझ करतो
4. फीचर एक्स्ट्रॅक्शन: पुढील वैशिष्ट्ये काढली जातात: पिच, टोन, फ्रिक्वेन्सी कॉम्पोनंट्स, MFCCs (मेल-फ्रिक्वेन्सी सेप्स्ट्रल कोएफिशंट्स), बोलण्याचा वेग (स्पीकिंग रेट).
5. टेम्पलेट जनरेशन व स्टोरेज: एनरोलमेंट: व्हॉईस टेम्पलेट स्टोअर केले जाते, व्हेरिफिकेशन: नवीन सॅम्पलची तुलना केली जाते.
6. मॅचर आणि डिसिजन: टेस्ट टेम्पलेटची स्टोअर केलेल्या टेम्पलेटशी तुलना केली जाते आणि जुळणी योग्य असल्यास प्रवेश दिला जातो, अन्यथा नाकारला जातो.

2.3.5 फेस रिकग्निशन (Face Recognition)

फेस रिकग्निशन ही एक फिजिओलॉजिकल बायोमेट्रिक तंत्रज्ञान आहे, ज्यामध्ये व्यक्तीची ओळख किंवा पडताळणी चेहऱ्यावरील अद्वितीय वैशिष्ट्यांचे विश्लेषण करून केली जाते. यामध्ये डोळे, नाक, जबड्याची रचना (jawline), गालांच्या हाडांची रचना (cheekbone structure) आणि चेहऱ्यावरील विविध लँडमार्क्समधील परस्पर अंतर यांचा समावेश होतो.

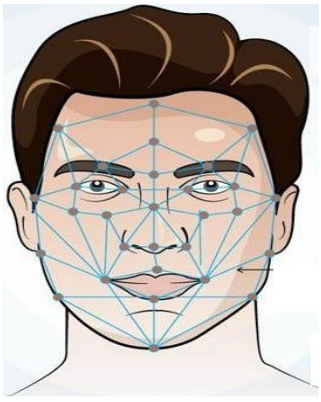


Fig 2.14: फेस रिकग्निशन (Face Recognition)

फेस रिकग्निशन हे कॉन्टॅक्टलेस, जलद आणि युजर-फ्रेंडली असल्यामुळे सर्वाधिक वापरल्या जाणाऱ्या बायोमेट्रिक तंत्रज्ञानांपैकी एक आहे. या तंत्रज्ञानामध्ये चेहऱ्याची डिजिटल इमेज कॅप्चर करून डोळ्यांमधील अंतर, नाकाचा आकार, हनुवटीचा कंटूर, चेहऱ्याची सिमेट्री आणि टेक्सचर पॅटर्न्स यांसारखी वेगळी वैशिष्ट्ये विश्लेषित केली जातात. प्रगत अल्गोरिदम्स या वैशिष्ट्यांना गणितीय प्रतिनिधित्वात (फेस टेम्पलेट) रूपांतरित करतात. फेस रिकग्निशन सिस्टिम इतर बायोमेट्रिक पद्धतींसारखीच बायोमेट्रिक आर्किटेक्चर अनुसरते. यामध्ये सेन्सर (कॅमेरा) चेहऱ्याची इमेज कॅप्चर करतो, प्री-प्रोसेसिंग द्वारे लाइटिंग आणि ओरिएंटेशन ॲडजस्ट केले जाते, फीचर एक्स्ट्रॅक्शन मध्ये महत्त्वाचे फेशियल पॉइंट्स ओळखले जातात आणि नंतर टेम्पलेट जनरेट करून स्टोअर केले जाते. व्हेरिफिकेशन दरम्यान, लाईव्ह फेशियल इमेज स्टोअर केलेल्या टेम्पलेट्सशी मॅच केली जाते, यासाठी पॅटर्न-मॅचिंग तंत्रे किंवा AI-आधारित मॉडेल्स वापरले जातात. फेस रिकग्निशन चा मोठ्या प्रमाणावर वापर मोबाईल अनलॉकिंग, सर्व्हेलन्स सिस्टिम्स, अटेंडन्स सिस्टिम्स, एअरपोर्ट्स, बँकिंग सिक्युरिटी, ऑनलाइन व्हेरिफिकेशन आणि ॲक्सेस कंट्रोल मध्ये केला जातो, कारण ते सोयीस्कर आणि उच्च अचूकता प्रदान करते.

फेस रिकग्निशन रजिस्ट्रेशन आणि व्हेरिफिकेशन प्रक्रिया (Face Recognition Registration & Verification Process)

1. सेन्सर (Sensor – Camera Capture): रिअल-टाइममध्ये वापरकर्त्याची चेहऱ्याची इमेज कॅप्चर करतो.
2. प्री-प्रोसेसिंग (Pre-Processing): लाइटिंग ॲडजस्ट करतो, चेहऱ्याची पोझिशन नॉर्मलाइझ करतो, बॅकग्राउंड नॉईज काढून टाकतो, फेस ओरिएंटेशन डिटेक्ट करतो
3. फीचर एक्स्ट्रॅक्शन (Feature Extraction): पुढीलप्रमाणे अद्वितीय फेशियल फीचर्स एक्स्ट्रॅक्ट केली जातात: डोळ्यांची स्थिती (Eye positions), नाकाचा आकार (Nose shape), जबड्याची आणि हनुवटीची रचना (Jawline and chin structure), चेहऱ्याचे प्रमाण (Facial proportions), टेक्सचर आणि स्किन पॅटर्न (Texture and skin pattern)
4. टेम्पलेट जनरेशन आणि स्टोरेज (Template Generation and Storage): एनरोलमेंट दरम्यान, एक्स्ट्रॅक्ट केलेली फीचर्स डिजिटल फेस टेम्पलेटमध्ये रूपांतरित करून स्टोअर केली जातात. व्हेरिफिकेशन दरम्यान, नवीन इमेजचे टेस्ट टेम्पलेटमध्ये रूपांतर केले जाते.
5. मॅचिंग आणि निर्णय (Matching and Decision): मॅचर टेस्ट टेम्पलेटची स्टोअर केलेल्या टेम्पलेट्सशी तुलना करतो. सिमिलॅरिटी जास्त असल्यास, सिस्टिम ॲक्सेस मंजूर (Grant) करते.

2.3.6 स्वाक्षरी व लेखन पॅटर्न्स (Signature and Writing Patterns)

स्वाक्षरी आणि लेखन पॅटर्न ओळख (Signature and Writing Pattern Recognition) ही एक वर्तणूक-आधारित बायोमेट्रिक (Behavioral Biometric) तंत्र आहे, ज्यामध्ये व्यक्तीची ओळख किंवा पडताळणी ही तिच्या स्वाक्षरी किंवा लेखन करण्याच्या वैशिष्ट्यपूर्ण पद्धतीवर आधारित असते. यामध्ये पुढील घटकांचा अभ्यास केला जातो: स्ट्रोक्सचा क्रम (Stroke Order), लेखनाचा वेग (Speed), पेनचा दाब (Pressure), पेनची हालचाल (Pen Movement), लेखनाची लय (Writing Rhythm). स्वाक्षरी व लेखन पॅटर्न बायोमेट्रिक्समध्ये एखादी व्यक्ती नैसर्गिकरित्या कशी लिहिते किंवा सही करते, यातील वर्तणूक वैशिष्ट्यांचे विश्लेषण केले जाते. पारंपरिक पद्धतींमध्ये फक्त स्वाक्षरीचा आकार (Static Signature) तुलना केला जातो; परंतु आधुनिक बायोमेट्रिक सिस्टिम्समध्ये डायनॅमिक वैशिष्ट्ये कॅप्चर केली जातात. या डायनॅमिक वैशिष्ट्यांमध्ये पुढील बाबी समाविष्ट असतात: स्ट्रोक्सचा वेग, पेन प्रेशर, दिशा बदल (Direction Changes), लेखनाची लय (Rhythm), ॲक्सेलरेशन (Acceleration) ही वैशिष्ट्ये फक्त दृश्य स्वरूपावर आधारित नसल्यामुळे, स्वाक्षरी बनावट करणे (Forgery) अत्यंत कठीण होते. त्यामुळे स्वाक्षरी आणि लेखन पॅटर्न आधारित बायोमेट्रिक प्रणाली सुरक्षित आणि विश्वासार्ह ऑथेंटिकेशन पद्धत मानली जाते.

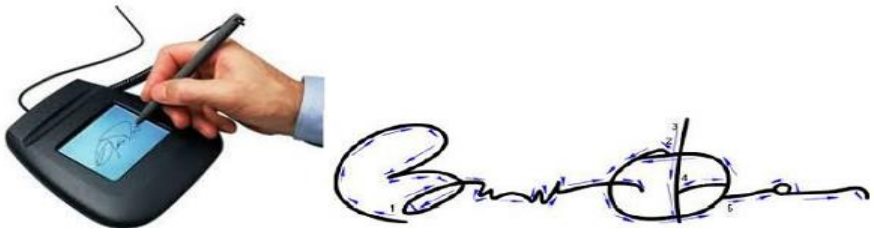


Fig 2.15: स्वाक्षरी व लेखन पॅटर्न ओळख आणि व्हेरिफिकेशन प्रक्रिया (Signature and Writing Patterns)

या सिस्टिममध्ये डिजिटल पेन, टॅब्लेट किंवा टच-सेंसिटिव्ह डिव्हाइस वापरून स्वाक्षरी किंवा लेखन प्रक्रिया रिअल-टाइममध्ये कॅप्चर केली जाते. एनरोलमेंट (Enrollment) दरम्यान, स्थिर आणि विश्वासार्ह स्वाक्षरी टेम्पलेट तयार करण्यासाठी अनेक नमुने (Samples) गोळा केले जातात. व्हेरिफिकेशन (Verification) दरम्यान, नवीन स्वाक्षरी ही साठवलेल्या टेम्पलेट्सशी पॅटर्न-रेकग्निशन अल्गोरिदम्स वापरून तुलना केली जाते.स्वाक्षरी डायनॅमिक्सचा वापर पुढील ठिकाणी मोठ्या प्रमाणावर केला जातो: बँकिंग, डॉक्युमेंट व्हेरिफिकेशन, सिक्युअर फॉर्म्स, ॲक्सेस कंट्रोल, कायदेशीर कागदपत्रे ही ऑथेंटिकेशन पद्धत वापरकर्त्यांना परिचित व सोपी असूनही सिक्युरिटी सुधारते. तथापि, स्वाक्षरी बायोमेट्रिक्सवर ताण (Stress), थकवा (Fatigue) किंवा लेखन पद्धतीतील शारीरिक बदल यांचा परिणाम होऊ शकतो.

स्वाक्षरी व लेखन पॅटर्न रजिस्ट्रेशन आणि व्हेरिफिकेशन प्रक्रिया

1. सेन्सर (Input Device): स्वाक्षरी/लेखन कॅप्चर करण्यासाठी पुढील उपकरणांचा वापर केला जातो: डिजिटल पेन, स्टायलस, टचपॅड, सिग्नेचर टॅब्लेट.

2. प्री-प्रोसेसिंग (Pre-Processing): नॉईज काढून टाकणे, वक्ररेषा स्मूथ करणे, आकार आणि ओरिएंटेशन नॉर्मलाइज करणे.
3. फीचर एक्स्ट्रॅक्शन (Feature Extraction): पुढील डायनॅमिक लेखन वैशिष्ट्ये काढली जातात: पेन प्रेशर, स्ट्रोक ऑर्डर, लेखनाचा वेग, दिशा आणि कोन (Angle), लय (Rhythm) आणि ॲक्सेलरेशन, प्रत्येक स्ट्रोकसाठी लागणारा वेळ.
4. टेम्पलेट जनरेशन आणि स्टोरेज:
   - एनरोलमेंट: अनेक नमुने गोळा करून टेम्पलेट्स म्हणून साठवले जातात.
   - व्हेरिफिकेशन: नवीन लेखन नमुना टेस्ट टेम्पलेटमध्ये रूपांतरित केला जातो
5. मॅचिंग आणि निर्णय (Matching & Decision): मॅचर टेस्ट सॅम्पलमधील डायनॅमिक फीचर्सची साठवलेल्या टेम्पलेट्सशी तुलना करतो आणि सिमिलॅरिटी स्कोअरनुसार सिस्टिम ॲक्सेस मंजूर किंवा नाकारते

2.3.7 कीस्ट्रोक्स (Keystrokes)

कीस्ट्रोक डायनॅमिक्स (Keystroke Dynamics) ही एक वर्तणूक-आधारित बायोमेट्रिक (Behavioral Biometric) तंत्र आहे, ज्यामध्ये वापरकर्त्याची ओळख किंवा पडताळणी ही त्याच्या टायपिंग पॅटर्न्स वर आधारित असते. यामध्ये पुढील घटकांचा विचार केला जातो: टायपिंगचा वेग, की प्रेस ड्युरेशन, की रिलीज टाइम, टायपिंग रिदम, टायपिंग सिक्वेन्स. कीस्ट्रोक डायनॅमिक्समध्ये एखादी व्यक्ती कीबोर्ड किंवा टचस्क्रीनवर कशी टाइप करते, याचे विश्लेषण केले जाते. प्रत्येक व्यक्तीचा टायपिंग रिदम हा बोटांची हालचाल, दाब, समन्वय आणि सवयीच्या टायपिंग शैलीमुळे वेगळा असतो. या सूक्ष्म फरकांमुळे एक युनिक टायपिंग सिग्नेचर तयार होते, जे ऑथेंटिकेशनसाठी वापरले जाऊ शकते.

Fig 2.16: कीस्ट्रोक डायनॅमिक्स (Keystroke Dynamics)

एनरोलमेंट (Enrollment) दरम्यान, सिस्टिम वापरकर्त्याचा टायपिंग पॅटर्न नोंदवते. यामध्ये पुढील डेटाचा समावेश असतो: की होल्ड टाइम (Key Hold Time), इंटर-की डिले (Inter-key Delay), टायपिंग फ्रिक्वेन्सी, टायपिंग प्रेशर (समर्थन असलेल्या डिव्हाइसवर). या माहितीवरून एक टायपिंग प्रोफाइल किंवा टेम्पलेट तयार करून साठवले जाते. व्हेरिफिकेशन (Verification) दरम्यान, वापरकर्ता पुन्हा टाइप करतो आणि नवीन टायपिंग पॅटर्नची तुलना साठवलेल्या टेम्पलेटशी मशीन लर्निंग किंवा स्टॅटिस्टिकल मॅचिंग टेक्निक्स वापरून केली जाते. कीस्ट्रोक डायनॅमिक्सचा वापर पुढील ठिकाणी मोठ्या प्रमाणावर केला जातो: कंटिन्युअस ऑथेंटिकेशन, ऑनलाईन बँकिंग, सिक्युअर लॉगिन सिस्टिम्स, फ्रॉड डिटेक्शन, सायबरसिक्युरिटी सिस्टिम्स. या पद्धतीसाठी कोणत्याही अतिरिक्त हार्डवेअरची आवश्यकता नसते आणि ती बॅकग्राऊंडमध्ये शांतपणे (Silently) कार्य करते.

कीस्ट्रोक डायनॅमिक्स रजिस्ट्रेशन आणि व्हेरिफिकेशन प्रक्रिया

1. सेन्सर (कीबोर्ड / टचस्क्रीन इनपुट): टायपिंगशी संबंधित सर्व डेटा कॅप्चर करतो.
2. प्री-प्रोसेसिंग (Pre-Processing): नॉईज काढून टाकणे, असामान्य डिले फिल्टर करणे, टायपिंग वेगातील चढ-उतार नॉर्मलाइज करणे.
3. फीचर एक्स्ट्रॅक्शन (Feature Extraction): खालील वर्तणूक-आधारित टायपिंग फीचर्स काढले जातात: ड्वेल टाइम (Dwell Time): एखादी की किती वेळ दाबलेली राहते.
4. फ्लाइट टाइम (Flight Time): एक की सोडल्यानंतर पुढील की दाबेपर्यंतचा वेळ: टायपिंग स्पीड आणि रिदम एरर पॅटर्न्स, की प्रेशर (समर्थन असल्यास), वारंवार टाइप होणारे पॅटर्न्स.
5. टेम्पलेट जनरेशन आणि स्टोरेज:
   a. एनरोलमेंट: टायपिंग डेटा कीस्ट्रोक टेम्पलेटमध्ये रूपांतरित करून साठवला जातो
   b. व्हेरिफिकेशन: नवीन टायपिंग सॅम्पलपासून टेस्ट टेम्पलेट तयार केले जाते

6. मॅचिंग आणि निर्णय (Matching & Decision): टेस्ट टेम्पलेटची साठवलेल्या टेम्पलेट्सशी तुलना केली जाते. सिमिलॅरिटी स्कोअरनुसार ॲक्सेस मंजूर किंवा नाकारला जातो.

2.4 ऑथरायझेशन (Authorization):

2.4.1 ऑथरायझेशनची ओळख (Introduction to Authorization)

ऑथरायझेशन (Authorization) ही अशी प्रक्रिया आहे ज्यामध्ये ओळख पटलेल्या (Authenticated) व्यक्तीला विशिष्ट क्रिया करण्याचा किंवा संसाधनांवर प्रवेश करण्याचा अधिकार आहे की नाही, हे तपासले जाते. ऑथरायझेशन ही प्रक्रिया ऑथेंटिकेशनशिवाय होऊ शकत नाही. सोप्या शब्दांत सांगायचे तर, ऑथरायझेशन म्हणजे वापरकर्त्यांना परवानग्या (Permissions) आणि हक्क (Rights) देणे, ज्यांच्या आधारे ते कम्प्युटर रिसोर्सेस किंवा माहितीचा वापर करू शकतात. ऑथरायझेशन हे सुनिश्चित करते की: फक्त परवानगी असलेले वापरकर्तेच विशिष्ट सिस्टिम रिसोर्सेस ॲक्सेस करू शकतात. आणि वापरकर्ते फक्त त्यांना अनुमती दिलेल्याच क्रिया (Actions) करू शकतात.

उदाहरणार्थ, एखादा वापरकर्ता लॉगिन (Authentication) केल्यानंतरही, त्याला फक्त त्याच्या रोलनुसार (Role) फाइल वाचण्याची, बदलण्याची किंवा डिलीट करण्याची परवानगी दिली जाते. ही प्रक्रिया म्हणजे ऑथरायझेशन.

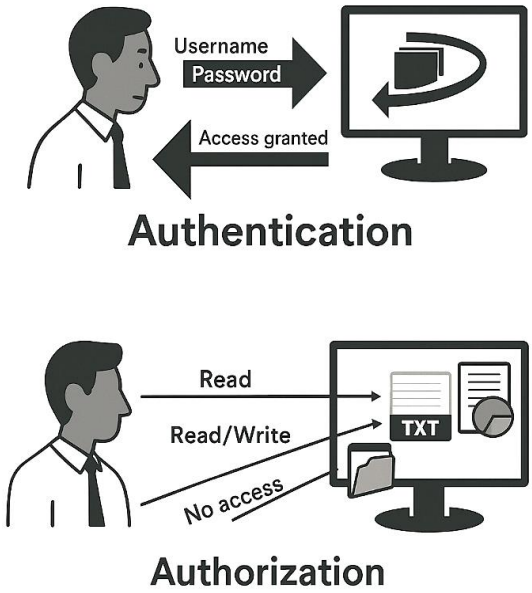


Fig 2.17: ऑथेंटिकेशन, ऑथरायझेशन (Authentication, Authorization)

ऑथरायझेशन (Authorization) हे इन्फॉरमेशन सेक्युरिटीचे एक अत्यंत महत्त्वाचे घटक आहे, जे एखाद्या ऑथेंटिकेटेड (Authenticated) वापरकर्त्याला सिस्टिममध्ये काय करण्याची परवानगी आहे, हे निश्चित करते. वापरकर्त्याची ओळख ऑथेंटिकेशनद्वारे पडताळल्यानंतर, सिस्टिम त्या वापरकर्त्यासाठी ठरवलेली पॉलिसीज, नियम (Rules) आणि ॲक्सेस राइट्स तपासते.ऑथरायझेशन ही प्रक्रिया रोल्स (Roles), परमिशन्स (Permissions) आणि ॲक्सेस कंट्रोल लिस्ट्स (ACLs) अशा यंत्रणांद्वारे कार्य करते. यामुळे वापरकर्ते फक्त आवश्यक माहिती आणि सिस्टिम फंक्शन्सच ॲक्सेस करतात याची खात्री होते. ऑथरायझेशनमुळे अनधिकृत क्रिया (Unauthorized Activities) रोखल्या जातात, सिक्युरिटी रिस्क्स कमी होतात आणि लीस्ट प्रिव्हिलेज (Least Privilege) हे तत्त्व प्रभावीपणे राबवले जाते. फाइल्स, डेटाबेसेस, सर्व्हिसेस आणि ॲप्लिकेशन्सवरील ॲक्सेस नियंत्रित करून, ऑथरायझेशन कॉन्फिडेन्शियलिटी, इंटेग्रिटी आणि सिक्युअर ऑपरेशन राखण्यास मदत करते.

उदाहरण (Example): एखाद्या कंपनीच्या इंटरनल सिस्टिममध्ये, कर्मचारी यूजरनेम आणि पासवर्ड वापरून लॉगिन करतो (ऑथेंटिकेशन). त्यानंतर, ऑथरायझेशन ठरवते की तो कर्मचारी काय ॲक्सेस करू शकतो.

- सामान्य कर्मचारी → फक्त स्वतःचा पेस्लिप आणि अटेंडन्स पाहू शकतो
- मॅनेजर → टीम मेंबर्सच्या लीव्ह रिक्वेस्ट्स मंजूर करू शकतो
- HR ॲडमिनिस्ट्रेटर → कर्मचारी रेकॉर्ड्स एडिट करू शकतो

हे सर्व वेगवेगळे ॲक्सेस राइट्स ऑथरायझेशनद्वारे दिले जातात.

2.4.2 ऑथरायझेशनची उद्दिष्टे (Goals of Authorization)

1. अनधिकृत ॲक्सेस रोखणे: फक्त परवानगी असलेल्या वापरकर्त्यांनाच विशिष्ट रिसोर्सेस ॲक्सेस करण्याची खात्री करणे.
2. लीस्ट प्रिव्हिलेज तत्त्व लागू करणे: वापरकर्त्याला त्याचे काम करण्यासाठी आवश्यक तेवढ्याच परवानग्या देणे.
3. प्रिव्हिलेज एस्कलेशन टाळणे: वापरकर्त्यांनी अनधिकृतरीत्या उच्च-स्तरीय ॲक्सेस मिळवू नये याची खात्री करणे.
4. सेन्सिटिव्ह डेटाचे संरक्षण: गोपनीय माहितीचा गैरवापर किंवा उघड होणे टाळणे.
5. सिस्टिम इंटेग्रिटी राखणे: अनधिकृत वापरकर्त्यांकडून डेटा किंवा ऑपरेशन्समध्ये बदल होऊ नयेत याची खात्री करणे.
6. अकाउंटेबिलिटी सुनिश्चित करणे: लॉग्स आणि ऑडिटिंग मेकॅनिझम्सद्वारे वापरकर्त्यांच्या क्रिया ट्रॅक करणे.
7. रोल-बेस्ड ॲक्सेस कंट्रोल (RBAC) ला समर्थन देणे: जॉब रोल्स किंवा जबाबदाऱ्यांनुसार परमिशन्स लागू करणे.
8. संपूर्ण सिस्टिम सिक्युरिटी वाढवणे: कडक आणि नियंत्रित ॲक्सेस पॉलिसीज लागू करून रिस्क्स कमी करणे.
9. रिसोर्सेसचा गैरवापर टाळणे: वापरकर्त्यांना फक्त त्यांच्या कामासाठी आवश्यक रिसोर्सेस वापरण्याची परवानगी देणे.
10. ऑर्गनायझेशनल पॉलिसीज आणि रेग्युलेशन्सचे पालन: सिक्युरिटी स्टँडर्ड्स आणि कायदेशीर गरजांचे समर्थन करणे.

Table 2.1 ऑथेन्टिकेशन आणि ऑथरायझेशन यांच्यातील तुलना (Comparison between Authentication and Authorization)

निकष (Criteria)	ऑथेंटिकेशन (Authentication)	ऑथरायझेशन (Authorization)
ॲक्सेस (Access)	ऑथेंटिकेशन हे युजर किंवा सर्व्हिस लेव्हलवर कार्य करते. युजर किंवा सर्व्हिसला पूर्ण ॲक्सेस मिळतो किंवा अजिबात मिळत नाही.	ऑथरायझेशन हे ऑब्जेक्ट लेव्हलवर कार्य करते. युजर किंवा सर्व्हिसला पूर्ण, मर्यादित किंवा शून्य ॲक्सेस मिळू शकतो.
कॉन्फिगरेशन (Configuration)	ऑथेंटिकेशन कॉन्फिगर करणे, इम्प्लिमेंट करणे आणि मॅनेज करणे तुलनेने सोपे असते.	ऑथरायझेशन कॉन्फिगर करणे, इम्प्लिमेंट करणे आणि मॅनेज करणे अधिक क्लिष्ट असते.
लेयर (Layer)	ऑथेंटिकेशन ही अनऑथराइज्ड ॲक्सेसविरुद्ध पहिली संरक्षण लेयर आहे.	ऑथरायझेशन ही दुसरी संरक्षण लेयर आहे आणि ती ऑथेंटिकेशननंतर कार्य करते.
सिक्युरिटी (Security)	ऑथेंटिकेशन अधिक सिक्युरिटी प्रदान करते.	ऑथरायझेशन अधिक फ्लेक्सिबल असते, पण ऑथेंटिकेशनपेक्षा कमी सिक्युअर मानले जाते.
कॉम्प्लेक्सिटी (Complexity)	ऑथेंटिकेशन तुलनेने सोपे असते.	ऑथरायझेशन अधिक क्लिष्ट असते.
उदाहरणे (Examples)	यूजरनेम आणि पासवर्ड, बायोमेट्रिक्स, स्मार्ट कार्ड, PAP आणि CHAP ही ऑथेंटिकेशनची उदाहरणे आहेत.	फाइल आणि फोल्डर परमिशन्स, सिस्टिम प्रॉपर्टीज बदलण्याचे अधिकार, एन्क्रिप्शन आणि ACLs ही ऑथरायझेशनची उदाहरणे आहेत.

2.5 ॲक्सेस कंट्रोल्स (Access Controls)

2.5.1 ॲक्सेस कंट्रोल्स व्याख्या (Access Controls Definition)

"ॲक्सेस कंट्रोल म्हणजे योग्य व्यक्तींनाच विशिष्ट माहिती, फाइल्स किंवा रिसोर्सेस वापरण्याची किंवा पाहण्याची परवानगी देणे आणि इतर सर्वांना अडवणे."

अक्सेस कंट्रोल ही एक सिक्युरिटी मेकॅनिझम आहे जी खालील गोष्टी नियंत्रित करते:

- कोण (Who) सिस्टिम रिसोर्सेस वापरू शकतो.
- कसे (How) वापरू शकतो.
- कोणत्या अटींवर (Under what conditions) वापरू शकतो

ॲक्सेस कंट्रोल हे सुनिश्चित करते की फक्त ऑथराइज्ड आणि ऑथेंटिकेटेड वापरकर्तेच पूर्वनियोजित नियम, परमिशन्स किंवा पॉलिसीजनुसार डेटा, सर्व्हिसेस आणि सिस्टिम कॉम्पोनंट्स ॲक्सेस करू शकतात. यामुळे माहितीची

कॉन्फिडेन्शियलिटी, इंटेग्रिटी आणि अव्हेलेबिलिटी सुरक्षित राहते. ॲक्सेस कंट्रोल हे इन्फॉरमेशन सेक्युरिटीचे मूलभूत घटक आहे. यामुळे केवळ वैध (Legitimate) वापरकर्त्यांनाच विशिष्ट सिस्टिम रिसोर्सेसचा ॲक्सेस मिळतो. ही प्रक्रिया मुख्यतः दोन टप्प्यांमध्ये कार्य करते:

1. ऑथेंटिकेशन (Authentication) – वापरकर्त्याची ओळख पडताळली जाते
2. ऑथरायझेशन (Authorization) – वापरकर्त्याला कोणत्या क्रिया करण्याची परवानगी आहे, हे ठरवले जाते

ॲक्सेस कंट्रोल्स हे पॉलिसीज, परमिशन्स, रोल्स आणि सिक्युरिटी नियमांद्वारे अंमलात आणले जातात, जे संस्था ठरवते. हे कंट्रोल्स अनधिकृत ॲक्सेस रोखतात, सेन्सिटिव्ह माहितीचे संरक्षण करतात आणि मिसयूज, डेटा ब्रीचेस व इनसाइडर अटॅक्सचा धोका कमी करतात.

प्रभावी ॲक्सेस कंट्रोल सिस्टिम्स: लीस्ट प्रिव्हिलेज तत्त्व लागू करतात, लॉग्सद्वारे अकाउंटेबिलिटी राखतात, सिक्युरिटी स्टँडर्ड्स आणि कॉम्प्लायन्स गरजा पूर्ण करण्यास मदत करतात.

2.5.2 ॲक्सेस कंट्रोल्स: ऑथेंटिकेशन मेकॅनिझम (Authentication mechanism)

ऑथेंटिकेशन मेकॅनिझम ही अशी पद्धत आहे ज्याद्वारे वापरकर्ता, डिव्हाइस किंवा सर्व्हिसची ओळख पडताळली जाते, त्यांना सिस्टिम रिसोर्सेसवर ॲक्सेस देण्यापूर्वी. ही प्रक्रिया हे सुनिश्चित करते की संबंधित व्यक्ती किंवा घटक खरोखरच तोच आहे, ज्याचा तो दावा करतो. ऑथेंटिकेशन ही ॲक्सेस कंट्रोलमधील पहिली पायरी आहे आणि ती ऑथरायझेशनपूर्वी अनिवार्यपणे केली जाते. ऑथेंटिकेशन यशस्वी झाल्याशिवाय वापरकर्त्याला कोणत्याही रिसोर्सवर ॲक्सेस दिला जात नाही.

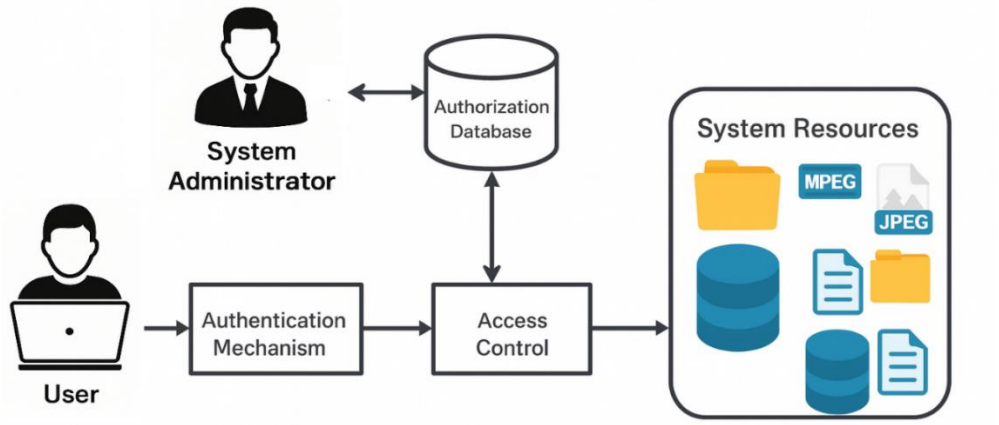


Fig 2.18: ऑथेंटिकेशन मेकॅनिझम (Authentication Mechanism)

ही आकृती ऑथेंटिकेशन, ऑथरायझेशन आणि ॲक्सेस कंट्रोल हे घटक एकत्रितपणे कसे कार्य करतात आणि सिस्टिम रिसोर्सेसचे संरक्षण कसे करतात, हे दर्शवते.

1. **यूजर (User):** ही प्रक्रिया त्या वापरकर्त्यापासून सुरू होते, ज्याला सिस्टिममधील काही फाइल्स, ॲप्लिकेशन्स किंवा डेटा ॲक्सेस करायचा असतो. वापरकर्ता लॉगिन क्रेडेन्शियल्स जसे की यूजरनेम आणि पासवर्ड सबमिट करतो.
2. **ऑथेंटिकेशन मेकॅनिझम (Authentication Mechanism):** वापरकर्ता लॉगिन करण्याचा प्रयत्न केल्यानंतर, ऑथेंटिकेशन मेकॅनिझम वापरकर्त्याची ओळख पडताळतो.
   हा टप्पा पुढील प्रश्नाचे उत्तर देतो: "तुम्ही कोण आहात?" (Who are you?)
   ऑथेंटिकेशनसाठी पुढील तंत्रांचा वापर केला जाऊ शकतो: पासवर्ड्स, बायोमेट्रिक्स (फिंगरप्रिंट, फेस स्कॅन), OTP, स्मार्ट कार्ड्स. जर ओळख योग्य आढळली, तर वापरकर्ता ऑथेंटिकेटेड ठरतो. जर ओळख चुकीची असेल, तर ताबडतोब ॲक्सेस नाकारला जातो.
3. **ॲक्सेस कंट्रोल (Access Control):** ऑथेंटिकेशन यशस्वी झाल्यानंतर, वापरकर्त्याची रिक्वेस्ट ॲक्सेस कंट्रोलकडे जाते. हा घटक पुढील बाबी ठरवतो: "तुम्ही काय करू शकता?", "तुम्हाला कोणते रिसोर्सेस ॲक्सेस करण्याची परवानगी आहे?"
   ॲक्सेस कंट्रोल स्वतः निर्णय घेत नाही; तो ऑथरायझेशन डेटाबेसचा सल्ला घेतो.
4. **ऑथरायझेशन डेटाबेस (Authorization Database):** ऑथरायझेशन डेटाबेसमध्ये पुढील माहिती असते: युजर रोल्स (Admin, Staff, Student), परमिशन्स (Read, Write, Delete), प्रत्येक फाइल, फोल्डर किंवा सिस्टिम

रिसोर्ससाठी ॲक्सेस राइट्स. ॲक्सेस कंट्रोल जेव्हा डेटाबेस तपासतो, तेव्हा त्याला पुढील प्रमाणे सूचना मिळतात: "फोल्डरला फक्त Read-Only ॲक्सेस द्या", "Confidential फाइल्सना ॲक्सेस नाकारावा", "Admin प्रिव्हिलेजेस द्या"

5. **सिस्टिम ॲडमिनिस्ट्रेटर (System Administrator):** सिस्टिम ॲडमिनिस्ट्रेटर पुढील जबाबदाऱ्या पार पाडतो: युजर अकाउंट्स तयार करणे आणि मॅनेज करणे, रोल्स आणि परमिशन्स सेट करणे, ऑथरायझेशन नियम अपडेट करणे, ऑथरायझेशन डेटाबेसची देखभाल करणे.
   ॲडमिनिस्ट्रेटर हे सुनिश्चित करतो की फक्त अधिकृत वापरकर्त्यांनाच आवश्यक त्या परवानग्या दिल्या जातात.
6. **सिस्टिम रिसोर्सेस (System Resources):** ऑथेंटिकेशन आणि ऑथरायझेशनच्या निकालावर आधारित, वापरकर्त्याला सिस्टिम रिसोर्सेसवर ॲक्सेस मंजूर किंवा नाकारला जातो.
   सिस्टिम रिसोर्सेसमध्ये पुढील घटक समाविष्ट असू शकतात: फोल्डर्स, डेटाबेसेस, डॉक्युमेंट्स, मीडिया फाइल्स (JPEG, MPEG), ॲप्लिकेशन्स. वापरकर्ता फक्त परवानगी दिलेल्याच ऑपरेशन्स (View, Read, Write, Delete) करू शकतो.

2.5.3 ॲक्सेस कंट्रोलची तत्त्वे (Access Control Principles)

ॲक्सेस कंट्रोल ही इन्फॉरमेशन सेक्युरिटीमधील एक महत्त्वाची संकल्पना आहे, जी वापरकर्ते, डिव्हाइसेस आणि प्रोसेसेस यांना सिस्टिम रिसोर्सेसवर ॲक्सेस द्यायचा की नाकारायचा, हे ठरवते. प्रभावी ॲक्सेस कंट्रोल खालील मूलभूत तत्त्वांवर आधारित असतो, जे माहितीची कॉन्फिडेन्शियलिटी, इंटेग्रिटी आणि अव्हेलेबिलिटी सुनिश्चित करतात.

1. आयडेंटिफिकेशन (Identification): आयडेंटिफिकेशन ही अशी प्रक्रिया आहे ज्याद्वारे वापरकर्ता किंवा सिस्टिम आपली ओळख घोषित करते, कोणत्याही रिसोर्सला ॲक्सेस करण्यापूर्वी.
   उदाहरणे: यूजरनेम, एम्प्लॉयी आयडी, डिव्हाइस आयडी
2. ऑथेंटिकेशन (Authentication): ऑथेंटिकेशन ही प्रक्रिया घोषित केलेली ओळख खरी आहे की नाही, याची पडताळणी करते.
   सामान्य ऑथेंटिकेशन पद्धती: पासवर्ड्स किंवा PIN, स्मार्ट कार्ड्स किंवा टोकन्स, बायोमेट्रिक व्हेरिफिकेशन, मल्टी-फॅक्टर ऑथेंटिकेशन (MFA)
3. ऑथरायझेशन (Authorization): ऑथरायझेशन ठरवते की ऑथेंटिकेटेड वापरकर्त्याला सिस्टिममध्ये काय करण्याची परवानगी आहे.
   यामध्ये समाविष्ट आहे: फाइल्स किंवा डेटाबेसेसचा ॲक्सेस, विशिष्ट टास्क्स करण्याची परवानगी, रोल-बेस्ड किंवा पॉलिसी-बेस्ड ॲक्सेस राइट्स.
4. लीस्ट प्रिव्हिलेज (Least Privilege): वापरकर्ते आणि प्रोसेसेस यांना फक्त त्यांचे काम करण्यासाठी आवश्यक तेवढाच ॲक्सेस दिला पाहिजे. यामुळे मिसयूज किंवा नुकसान होण्याचा धोका कमी होतो.
5. नीड-टू-नो (Need-to-Know): वापरकर्ता ऑथराइज्ड असला तरी, त्याने फक्त त्याच्या कामाशी संबंधित माहितीच ॲक्सेस करावी. यामुळे सेन्सिटिव्ह डेटाचा अनावश्यक प्रसार टाळला जातो.
6. सेपरेशन ऑफ ड्युटीज (Separation of Duties): महत्त्वाच्या क्रिया वेगवेगळ्या व्यक्ती किंवा रोल्समध्ये विभागल्या पाहिजेत, जेणेकरून एकाच व्यक्तीकडे पूर्ण नियंत्रण राहणार नाही. यामुळे फ्रॉड किंवा मिसयूजची शक्यता कमी होते.
7. अकाउंटेबिलिटी (Auditing & Logging): सर्व वापरकर्त्यांच्या क्रिया मॉनिटर आणि लॉग केल्या पाहिजेत. अकाउंटेबिलिटीमुळे पुढील गोष्टी सुनिश्चित होतात: ट्रेसेबिलिटी, पॉलिसी उल्लंघनांचे डिटेक्शन, तपास (Investigation) प्रक्रियेस मदत.
8. कॉन्फिडेन्शियलिटी (Confidentiality): ॲक्सेस कंट्रोल मेकॅनिझम्समुळे माहिती अनधिकृत वापरकर्त्यांना उघड होण्यापासून सुरक्षित राहते. यामुळे सेन्सिटिव्ह डेटा गोपनीय राहतो.
9. इंटेग्रिटी (Integrity): ॲक्सेस कंट्रोल हे सुनिश्चित करते की फक्त अधिकृत वापरकर्त्यांनाच डेटा बदलण्याची परवानगी असते. यामुळे अनधिकृत बदल किंवा टॅम्परिंग टाळली जाते.

10. अव्हेलेबिलिटी (Availability): अधिकृत वापरकर्त्यांना आवश्यक तेव्हा माहिती आणि रिसोर्सेस सहज उपलब्ध असले पाहिजेत. ॲक्सेस कंट्रोल्स अशा प्रकारे कॉन्फिगर केले पाहिजेत की वैध ॲक्सेस अनावश्यकपणे अडवला जाणार नाही.
11. नॉन-रिप्युडिएशन (Non-Repudiation): नॉन-रिप्युडिएशन हे सुनिश्चित करते की वापरकर्ते आपल्या केलेल्या क्रिया नाकारू शकत नाहीत. हे सिक्युअर लॉगिंग आणि डिजिटल व्हेरिफिकेशन पद्धतींनी साध्य केले जाते.

2.5.4 ॲक्सेस राइट्स आणि परवानग्या (Access Rights and Permissions)

ॲक्सेस राइट्स (ज्यांना परवानग्या असेही म्हणतात) म्हणजे एखाद्या वापरकर्ता, प्रक्रिया, किंवा प्रणालीला कोणत्या संसाधनावर (resource) कोणती क्रिया करता येईल, हे ठरवणारे नियम आहेत. या परवानग्या ॲक्सेस कंट्रोलचा मुख्य भाग आहेत आणि यामुळे फक्त अधिकृत वापरकर्त्यांनाच माहिती व प्रणाली घटक पाहणे, बदलणे, वापरणे किंवा व्यवस्थापित करणे शक्य होते. सोप्या शब्दांत सांगायचे तर, ऑथेंटिकेशननंतर वापरकर्ता काय करू शकतो, हे ॲक्सेस राइट्स ठरवतात.

ॲक्सेस राइट्सचे सामान्य प्रकार

a) वाचन (Read – R): वापरकर्त्याला डेटा पाहण्याची किंवा प्रत बनवण्याची परवानगी देते. उदाहरणे: फाईल उघडणे, डेटाबेसमधील नोंद पाहणे.
b) लेखन (Write – W): वापरकर्त्याला डेटा बदलण्याची किंवा अद्ययावत करण्याची परवानगी देते. उदाहरणे: दस्तऐवज संपादन करणे, रेकॉर्ड अपडेट करणे.
c) अंमलबजावणी (Execute – X): प्रोग्राम किंवा स्क्रिप्ट चालवण्याची परवानगी देते.
उदाहरणे: सॉफ्टवेअर ॲप्लिकेशन चालवणे, सर्व्हर-साइड स्क्रिप्ट चालवणे
d) हटवणे (Delete): फाईल्स किंवा डेटा नोंदी काढून टाकण्याची परवानगी देते.
e) तयार करणे / जोडणे (Create / Add): नवीन घटक तयार करण्याची परवानगी देते, जसे की: नवीन फाईल्स, नवीन फोल्डर्स, नवीन डेटाबेस रेकॉर्ड्स.
f) बदल (Modify): साध्या लेखनापेक्षा पुढे जाऊन संसाधनाची रचना किंवा मजकूर बदलण्याची परवानगी देते.
g) पूर्ण नियंत्रण / रूट ॲक्सेस (Full Control / Root Access): वापरकर्त्याला सर्व प्रकारच्या क्रिया करण्याची परवानगी देते, त्यामध्ये: वाचन, लेखन, हटवणे, परवानग्या बदलणे, मालकी हक्क (Ownership) घेणे. ही परवानगी सहसा फक्त प्रशासकांना (Administrators) दिली जाते.

2.5.5 ॲक्सेस कंट्रोल पॉलिसीज (Access Control Policies)

ॲक्सेस कंट्रोल पॉलिसीज म्हणजे माहिती प्रणालीमध्ये ॲक्सेस राइट्स कशा प्रकारे दिल्या जातील, व्यवस्थापित केल्या जातील आणि अंमलात आणल्या जातील, हे ठरवणारे औपचारिक नियम आहेत.

या पॉलिसीज स्पष्टपणे ठरवतात की:

- कोण (वापरकर्ता / प्रक्रिया)
- कशाला (फाईल, डेटाबेस, संसाधन)
- कोणत्या अटींमध्ये
- कोणती क्रिया (वाचन, लेखन, अंमलबजावणी इ.) करू शकतो

ॲक्सेस कंट्रोल पॉलिसीजमुळे सर्व वापरकर्ते आणि संसाधनांमध्ये सुसंगतता (Consistency), सुरक्षा (Security) आणि योग्य अधिकृतता (Proper Authorization) सुनिश्चित होते.

a) डिस्क्रेशनरी ॲक्सेस कंट्रोल (Discretionary Access Control – DAC)

डिस्क्रेशनरी ॲक्सेस कंट्रोल (DAC) ही एक ॲक्सेस कंट्रोल मॉडेल आहे, ज्यामध्ये सब्जेक्ट (वापरकर्ता) आणि तो ज्या ग्रुपचा सदस्य आहे, त्याच्या ओळखीवर आधारित ऑब्जेक्ट्सवर (फाईल्स, डेटा, संसाधने) प्रवेश मर्यादित केला जातो.

या मॉडेलमध्ये: संसाधनाचा मालक (Owner) ठरवतो की इतर कोणत्या वापरकर्त्यांना कोणत्या परवानग्या (Read, Write, Execute) द्यायच्या. म्हणजेच, ॲक्सेस देण्याचा अधिकार पूर्णपणे रिसोर्स ओनरच्या इच्छेवर (Discretion) अवलंबून असतो.

DAC ची वैशिष्ट्ये:

- ॲक्सेस लवचिक (Flexible) असतो.
- वापरकर्ते स्वतः परवानग्या बदलू शकतात.
- ॲक्सेस अटींवर आधारित (Conditional) असतो.
- लहान किंवा मध्यम प्रणालींसाठी उपयुक्त.

उदाहरण: UNIX / Linux आधारित प्रणालींमध्ये DAC मोठ्या प्रमाणावर वापरला जातो.
फाईलचा मालक खालील परवानग्या देऊ शकतो:

- वाचन (Read)
- लेखन (Write)
- अंमलबजावणी (Execute)

उदाहरणार्थ, एखाद्या फाईलचा मालक ठरवू शकतो की: तो स्वतः फाईल वाचू व बदलू शकतो, ग्रुप सदस्य फक्त वाचू शकतात.

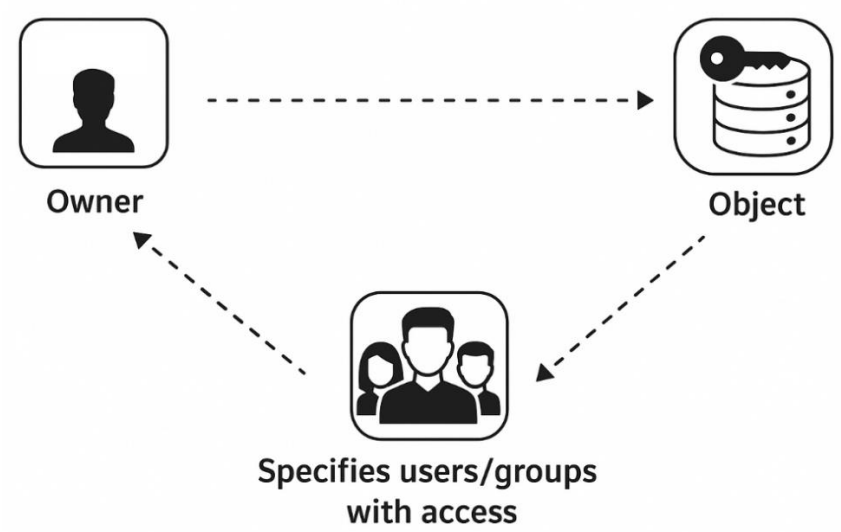


Fig 2.19: डिस्क्रेशनरी ॲक्सेस कंट्रोल (Discretionary Access Control – DAC)

1. **Owner (मालक):** डाव्या वरच्या बाजूला असलेला व्यक्तीचा चिन्ह (स्टार्ससह) मालक दर्शवतो. मालक हा संसाधन (Resource) तयार करतो आणि त्यावर नियंत्रण ठेवतो.
2. **Object (ऑब्जेक्ट / संसाधन):** उजव्या वरच्या बाजूला किलीसह असलेले डेटाबेसचे चिन्ह ऑब्जेक्ट दर्शवते. हे ऑब्जेक्ट म्हणजे फाईल, फोल्डर किंवा डेटा असू शकतो, ज्याचे संरक्षण आवश्यक असते.
3. **Users / Groups (वापरकर्ते / गट):**खालच्या बाजूला अनेक व्यक्तींचे चिन्ह वापरकर्ते किंवा गट दर्शवते. मालक या वापरकर्त्यांना किंवा गटांना ॲक्सेस देऊ शकतो किंवा नाकारू शकतो.

DAC मध्ये कोणाला कोणता ॲक्सेस द्यायचा हे पूर्णपणे मालकाच्या निर्णयावर अवलंबून असते.
उदाहरण: UNIX प्रणालीमध्ये एखादा वापरकर्ता report.txt नावाची फाईल तयार करतो. तो त्या फाईलचा मालक असल्यामुळे chmod सारख्या कमांड्स वापरून परवानग्या सेट करू शकतो.
उदा.: स्वतःसाठी पूर्ण ॲक्सेस (rwx), गटासाठी फक्त वाचन (r--), इतरांसाठी ॲक्सेस नाकारणे
या सर्व परवानग्या मालक स्वतः नियंत्रित करतो. हेच डिस्क्रेशनरी ॲक्सेस कंट्रोल (DAC) चे उत्तम उदाहरण आहे.

b) मॅन्डेटरी ॲक्सेस कंट्रोल (Mandatory Access Control – MAC)

मॅन्डेटरी ॲक्सेस कंट्रोल (MAC) ही एक कठोर (Strict) ॲक्सेस कंट्रोल मॉडेल आहे, ज्यामध्ये सिस्टम रिसोर्सेसवरचा ॲक्सेस पूर्णपणे केंद्रिय प्राधिकरणाद्वारे (Central Authority) नियंत्रित केला जातो.
MAC मध्ये: वापरकर्ते परवानग्या बदलू शकत नाहीत, कोणाला ॲक्सेस द्यायचा हे वापरकर्ता ठरवू शकत नाही, ॲक्सेस पूर्वनिश्चित सुरक्षा पॉलिसीजवर आधारित असतो. या मॉडेलमध्ये: वापरकर्त्यांना आणि संसाधनांना सुरक्षा लेबल्स दिली जातात.

उदाहरण: टॉप सिक्रेट (Top Secret), सिक्रेट(Secret), कॉन्फिडेन्शियल(Confidential).
ॲक्सेस फक्त तेव्हाच दिला जातो जेव्हा: वापरकर्त्याचा Clearance Level आणि ऑब्जेक्टच्या Classification Level इतका किंवा त्याहून जास्त असतो.
MAC ची वैशिष्ट्ये:

- अत्यंत उच्च सुरक्षा
- माहितीचा प्रवाह कठोरपणे नियंत्रित
- वापरकर्त्यांना कोणताही स्वातंत्र्यपूर्ण ॲक्सेस बदलण्याचा अधिकार नाही

वापर: MAC प्रामुख्याने खालील ठिकाणी वापरला जातो:

- लष्करी प्रणाली (Military Systems)
- सरकारी संस्था (Government Organizations)
- उच्च-सुरक्षा वातावरण (High-Security Environments)

जिथे गोपनीयता (Confidentiality) आणि माहितीवरील कठोर नियंत्रण अत्यंत महत्त्वाचे असते.

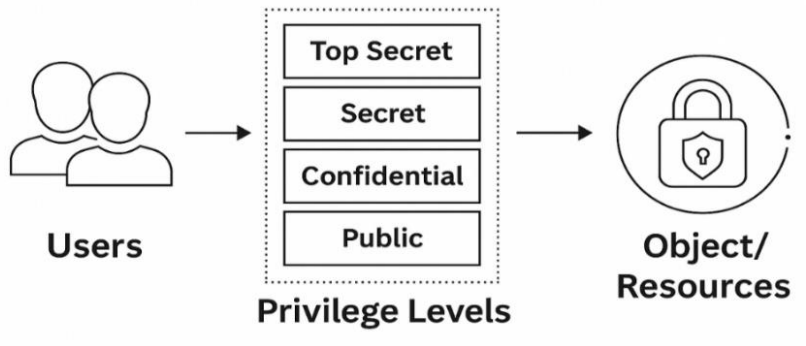


Fig 2.20: मॅन्डेटरी ॲक्सेस कंट्रोल (Mandatory Access Control – MAC)

1. **केंद्रिय प्राधिकरण (Central Authority):** डाव्या वरच्या बाजूला ढाल किंवा सरकारी इमारतीचे चिन्ह केंद्रिय प्राधिकरण दर्शवते.
   हे प्राधिकरण:
   - सुरक्षा धोरणे (Security Policies) ठरवते
   - वापरकर्ते आणि संसाधनांना सुरक्षा लेबल्स देते
   - ॲक्सेस कंट्रोलची अंमलबजावणी करते

   MAC मध्ये सर्व नियंत्रण सिस्टम/केंद्रिय प्राधिकरणाकडे असते, वापरकर्त्याकडे नाही.
2. **वर्गीकृत संसाधन (Classified Object)**
   उजव्या वरच्या बाजूला लॉक असलेल्या दस्तऐवजाचे किंवा सुरक्षित फोल्डरचे चिन्ह ऑब्जेक्ट / संसाधन दर्शवते. या ऑब्जेक्टला सुरक्षा वर्गीकरण दिलेले असते,
   उदाहरण: टॉप सिक्रेट (Top Secret), सिक्रेट(Secret), कॉन्फिडेन्शियल(Confidential).
3. **सुरक्षा क्लिअरन्स असलेले वापरकर्ते (Subjects with Security Labels)**
   खालच्या बाजूला असलेली व्यक्तींची चिन्हे वापरकर्ते (Subjects) दर्शवतात. प्रत्येक वापरकर्त्याला ठरावीक Security Clearance Level दिलेला असतो.
   ➞ॲक्सेस फक्त तेव्हाच दिला जातो जेव्हा वापरकर्त्याचा क्लिअरन्स लेव्हल हा ऑब्जेक्टच्या वर्गीकरणाइतका किंवा त्याहून जास्त असतो. यावरून MAC चे पूर्णपणे सिस्टम-नियंत्रित स्वरूप स्पष्ट होते.
   उदाहरण: लष्करी प्रणालीमध्ये दस्तऐवज पुढील प्रमाणे वर्गीकृत असतात: टॉप सिक्रेट (Top Secret), सिक्रेट(Secret), कॉन्फिडेन्शियल(Confidential),
   जर एखाद्या वापरकर्त्याकडे Secret क्लिअरन्स असेल तर: तो Secret आणि Confidential दस्तऐवज पाहू शकतो पण Top Secret दस्तऐवज पाहू शकत नाही, जरी वापरकर्त्याने स्वतः दस्तऐवज तयार केला असला तरी: तो त्याचे

वर्गीकरण बदलू शकत नाही, इतरांना ॲक्सेस देऊ शकत नाही. सर्व परवानग्या आणि नियम केंद्रिय सुरक्षा धोरणांद्वारे नियंत्रित होतात. हेच MAC चे कठोर (Strict) स्वरूप दर्शवते.

c) रोल-बेस्ड ॲक्सेस कंट्रोल (Role-Based Access Control – RBAC)

रोल-बेस्ड ॲक्सेस कंट्रोल (RBAC) ही एक ॲक्सेस कंट्रोल मॉडेल आहे ज्यामध्ये: परवानग्या थेट वापरकर्त्यांना न देता Roles (भूमिका) यांना दिल्या जातात आणि वापरकर्त्यांना त्यांच्या संस्थेतील भूमिकेनुसार ॲक्सेस मिळतो

उदाहरण: रोल्स (Roles): ॲडमिन, मॅनेजर, स्टाफ, स्टुडंट.

प्रत्येक रोल्स साठी ठरावीक परवानग्या (Permissions) असतात आणि वापरकर्ते त्या रोल्स मध्ये नियुक्त केल्यावर त्या परवानग्या स्वयंचलितपणे वारशाने (inherit) मिळतात.

RBAC चे फायदे (Advantages of RBAC (Role-Based Access Control)):

1. व्यवस्थापन सोपे होते
2. मोठ्या संस्थांसाठी अतिशय उपयुक्त
3. सुरक्षा वाढते
4. चुका कमी होतात

RBAC खालील तत्त्वांना समर्थन देते:

- Least Privilege – वापरकर्त्याला आवश्यक तेवढाच ॲक्सेस
- Separation of Duties – एकाच व्यक्तीकडे सर्व अधिकार नसणे

म्हणूनच, RBAC हे आधुनिक संस्थांमध्ये कार्यक्षम, सुरक्षित आणि व्यवस्थापनीय ॲक्सेस कंट्रोल मॉडेल मानले जाते.

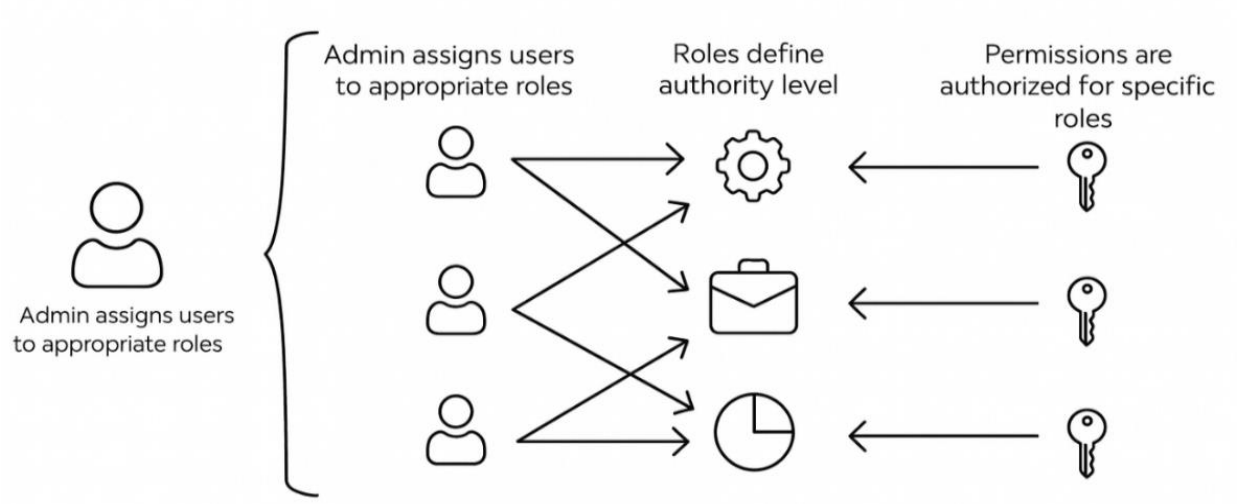


Fig 2.21: रोल-बेस्ड ॲक्सेस कंट्रोल (Role-Based Access Control – RBAC)

ही आकृती रोल-बेस्ड ॲक्सेस कंट्रोल (RBAC) या संकल्पनेचे स्पष्टीकरण तीन मुख्य घटकांच्या साहाय्याने करते: यूजर्स (Users), रोल्स (Roles) आणि परमिशन्स (Permissions). डाव्या बाजूला, यूजर आयकॉन्सचा समूह प्रणालीतील अशा व्यक्तींना दर्शवतो ज्यांना संसाधनांवर प्रवेश आवश्यक असतो. मधल्या भागात, गिअर, ब्रीफकेस आणि पाई चार्टसारखी आयकॉन्स संस्थेद्वारे निश्चित केलेले रोल्स दर्शवतात, जे विशिष्ट अधिकार पातळी किंवा नोकरीची भूमिका सूचित करतात. उजव्या बाजूला, की (Key) आयकॉन्स परमिशन्स दर्शवतात, ज्या त्या रोल्सना दिलेल्या असतात आणि प्रत्येक रोल कोणत्या क्रिया किंवा संसाधनांवर प्रवेश करू शकतो हे दाखवतात. प्रवेशाचा प्रवाह परमिशन्स → रोल्स → यूजर्स असा असतो, म्हणजेच यूजर्सना थेट परमिशन्स दिल्या जात नाहीत, तर त्यांना दिलेल्या रोल्सद्वारे त्या परमिशन्स मिळतात. ही रचना प्रणालीमध्ये सुसंगत, सुव्यवस्थित आणि सुरक्षित ॲक्सेस मॅनेजमेंट सुनिश्चित करते.

उदाहरण: कॉलेज मॅनेजमेंट सिस्टिममध्ये, टीचर रोलला गुण आणि उपस्थिती अपलोड करण्याची परमिशन असू शकते, स्टुडंट रोलला वैयक्तिक रेकॉर्ड्स पाहण्याची परमिशन असू शकते, आणि ॲडमिन रोल यूजर्स आणि सिस्टिम सेटिंग्ज व्यवस्थापित करू शकतो. जेव्हा नवीन शिक्षक रुजू होतो, तेव्हा त्याला "टीचर" रोल दिल्यास आवश्यक सर्व परमिशन्स आपोआप मिळतात—यामुळे RBAC ची कार्यक्षमता आणि सुरक्षा स्पष्ट होते.

d) ॲट्रिब्यूट-बेस्ड ॲक्सेस कंट्रोल (Attribute-based access control (ABAC))

ॲट्रिब्यूट-बेस्ड ॲक्सेस कंट्रोल (ABAC) हे एक प्रगत आणि अत्यंत लवचिक ॲक्सेस कंट्रोल मॉडेल आहे, ज्यामध्ये प्रवेशाचे निर्णय यूजर, संसाधन, क्रिया आणि पर्यावरण यांच्याशी संबंधित विविध ॲट्रिब्यूट्सच्या संयोजनावर आधारित असतात. फक्त ओळख (DAC), क्लिअरन्स (MAC) किंवा रोल्स (RBAC) वर अवलंबून न राहता, ABAC मध्ये अशा पॉलिसीजचे मूल्यांकन केले जाते ज्या अनेक ॲट्रिब्यूट्सचा विचार करतात, जसे की यूजरचा विभाग, नोकरीचे पद, संसाधनाची संवेदनशीलता, प्रवेशाचा वेळ, स्थान, डिव्हाइसचा प्रकार इत्यादी. ABAC सूक्ष्म (Fine-grained) आणि डायनॅमिक ॲक्सेस कंट्रोल सक्षम करते, त्यामुळे आधुनिक क्लाऊड सिस्टिम्स, एंटरप्रायझेस आणि मोठ्या प्रमाणातील संस्थांसाठी हे उपयुक्त ठरते, जिथे प्रवेशाच्या गरजा वारंवार बदलतात आणि संदर्भानुसार जुळवून घेणे आवश्यक असते.

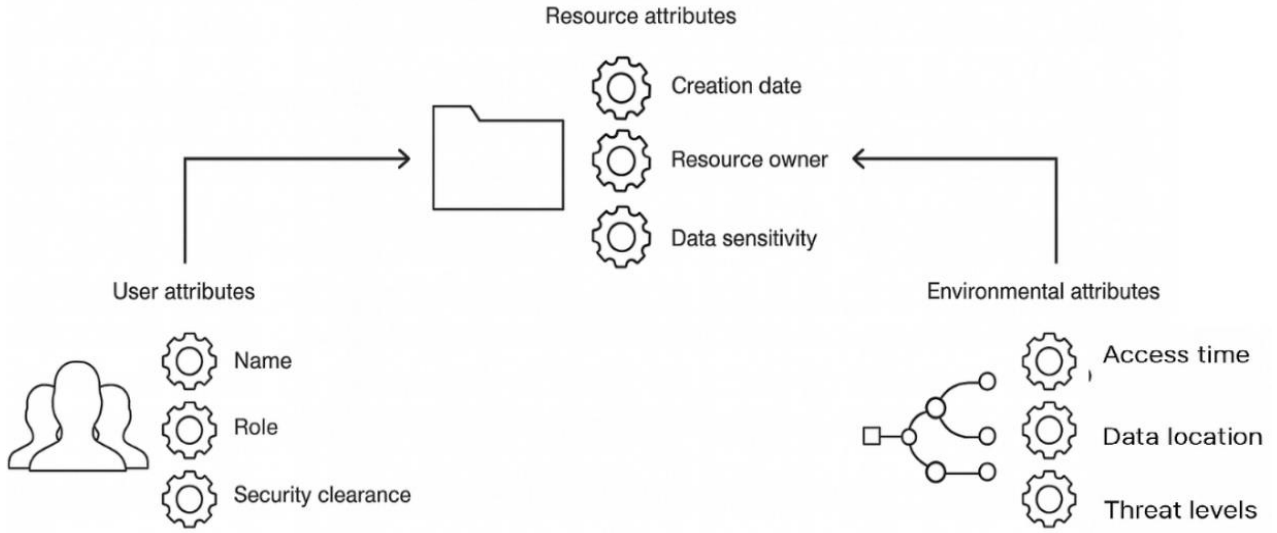


Fig 2.22: ॲट्रिब्यूट-बेस्ड ॲक्सेस कंट्रोल (Attribute-based access control (ABAC))

ही आकृती ॲट्रिब्यूट-बेस्ड ॲक्सेस कंट्रोल (ABAC) या संकल्पनेचे स्पष्टीकरण तीन मुख्य ॲट्रिब्यूट प्रकारांचा वापर करून करते: यूजर ॲट्रिब्यूट्स (User Attributes), रिसोर्स ॲट्रिब्यूट्स (Resource Attributes) आणि एन्व्हायर्नमेंटल ॲट्रिब्यूट्स (Environmental Attributes).डाव्या बाजूला, गिअर चिन्हांसह असलेली यूजर आयकॉन्स यूजर ॲट्रिब्यूट्स दर्शवतात, ज्यामध्ये यूजरचे नाव, रोल आणि सुरक्षा क्लिअरन्स यांसारखी माहिती समाविष्ट असते. मध्यभागी, फोल्डर आयकॉनभोवती असलेली गिअर चिन्हे रिसोर्स ॲट्रिब्यूट्स दर्शवतात, जसे की तयार करण्याची तारीख, रिसोर्सचा मालक आणि डेटाची संवेदनशीलता. उजव्या बाजूला, नेटवर्कसदृश आयकॉन्स आणि गिअर चिन्हे एन्व्हायर्नमेंटल ॲट्रिब्यूट्स दर्शवतात, ज्यामध्ये प्रवेशाचा वेळ, डेटाचे स्थान आणि सध्याची थ्रेट पातळी यांसारखे संदर्भात्मक घटक समाविष्ट असतात. या सर्व ॲट्रिब्यूट गटांमधून रिसोर्सकडे जाणारे बाण हे दर्शवतात की प्रणाली सर्व ॲट्रिब्यूट्सचा एकत्रितपणे विचार करते. प्रवेशाचे निर्णय पूर्वनिश्चित पॉलिसीजच्या आधारे यूजर, रिसोर्स आणि एन्व्हायर्नमेंटल ॲट्रिब्यूट्सची तुलना करून घेतले जातात, आणि सर्व अटी पूर्ण झाल्यावरच प्रवेश मंजूर केला जातो.

उदाहरण: रुग्णालयीन प्रणालीमध्ये, एखादा डॉक्टर फक्त तेव्हाच रुग्णाचा वैद्यकीय अहवाल पाहू शकतो जेव्हा डॉक्टर ड्युटीवर असतो, रुग्ण त्याच विभागातील असतो आणि प्रवेशाची विनंती रुग्णालयाने मान्य केलेल्या डिव्हाइसवरून येते. डॉक्टरचे ऑथेन्टिकेशन झालेले असले तरीही, जर विनंती रुग्णालयाबाहेरून किंवा कामकाजाच्या वेळेबाहेर करण्यात आली असेल तर प्रवेश नाकारला जाईल. या अटी—ज्या अनेक ॲट्रिब्यूट्सवर आधारित आहेत—ABAC चे डायनॅमिक आणि कॉन्टेक्स्ट-अवेयर स्वरूप स्पष्ट करतात.

Table 2.2: DAC, MAC, RBAC आणि ABAC ॲक्सेस कंट्रोल मॉडेल्सची तुलना (Comparison of DAC, MAC, RBAC, and ABAC Access Control Models)

निकष (Criteria)	DAC (डिस्क्रेशनरी ॲक्सेस कंट्रोल)	MAC (मॅन्डेटरी ॲक्सेस कंट्रोल)	RBAC (रोल-बेस्ड ॲक्सेस कंट्रोल)	ABAC (ॲट्रिब्युट-बेस्ड ॲक्सेस कंट्रोल)
ॲक्सेसचे नियंत्रण (Control of Access)	संसाधनाच्या मालकाद्वारे नियंत्रित	केंद्रिय प्राधिकरणाद्वारे धोरणांनुसार नियंत्रित	संस्थेत परिभाषित केलेल्या भूमिका (Roles) द्वारे नियंत्रित	ॲट्रिब्युट्सवर आधारित (वापरकर्ता, संसाधन, वातावरण, क्रिया)
लवचिकता (Flexibility)	जास्त लवचिक; मालक परवानग्या ठरवतो	अतिशय कठोर; वापरकर्ते परवानग्या बदलू शकत नाहीत	मध्यम लवचिक; भूमिका सहज व्यवस्थापित करता येतात	अतिशय लवचिक; निर्णय परिस्थितीनुसार बदलतात
सुरक्षेची पातळी (Security Level)	कमी ते मध्यम; चुकांमुळे गैरवापराचा धोका	अतिशय जास्त; कठोर व छेडछाड-प्रतिरोधक	जास्त; परवानग्यांचे गट केल्याने चुका कमी होतात	अतिशय जास्त; सूक्ष्म व संदर्भ-जाणून निर्णय
परवानगी देण्याची पद्धत (Permission Assignment)	थेट वापरकर्ते किंवा गटांना	सुरक्षा लेबल्स व क्लिअरन्सवर आधारित	आधी भूमिका, नंतर वापरकर्ते त्या परवानग्या वारशाने घेतात	धोरणांद्वारे ॲट्रिब्युट्सचे मूल्यमापन
वापरकर्त्याचे नियंत्रण (User Control)	जास्त वापरकर्ता नियंत्रण	वापरकर्त्याचे नियंत्रण नाही	मर्यादित वापरकर्ता नियंत्रण	थेट वापरकर्ता नियंत्रण नाही; प्रणाली निर्णय घेते
प्रशासकीय गुंतागुंत (Administrative Complexity)	व्यवस्थापन सोपे	अतिशय गुंतागुंतीचे	मध्यम	अनेक ॲट्रिब्युट्समुळे गुंतागुंतीचे
सामान्य वापर (Common Usage)	UNIX/Linux फाइल परवानग्या, वैयक्तिक प्रणाली	लष्कर, संरक्षण, वर्गीकृत वातावरण	संस्था, उद्योग, महाविद्यालये	क्लाउड प्रणाली, रुग्णालये, संदर्भ-जाणून प्रणाली
निर्णयाचा आधार (Basis for Decision)	वापरकर्ता कोण आहे (ओळख-आधारित)	सुरक्षा क्लिअरन्स + वर्गीकरण	नोकरीची भूमिका व जबाबदाऱ्या	ॲट्रिब्युट्स व धोरण नियम
उदाहरण (Examples)	फाइल वाचन/लेखन/एक्झिक्यूट मालक ठरवतो	Top Secret, Secret, Confidential ॲक्सेस	Teacher, Admin, Manager भूमिका	डॉक्टर फक्त ड्युटीच्या वेळेत व हॉस्पिटल नेटवर्कमधून रेकॉर्ड पाहू शकतो

References:

1. Stallings, W., & Brown, L. (2014). *Computer security: Principles and practice* (3rd ed.). Pearson. ISBN: 978-0-13-377392-7.
2. Kahate, A. (2018). *Cryptography and network security* (3rd ed.; 4th ed.). McGraw-Hill. ISBN: 978-9353163303.
3. Merkow, M., & Breithaupt, J. (2006). *Information security: Principles and practices*. Pearson. ISBN: 978-81-317-1288-7.
4. Pachghare, V. K. (2012). *Cryptography and information security*. Prentice Hall India. ISBN: 978-81-203-5082-3.
5. Gollmann, D. (2011). *Computer security* (3rd ed.). Wiley. ISBN: 978-0-470-74115-3.
6. YouTube. (2019). Simulation of intrusion detection system in MANET using NetSim. Retrieved from https://www.youtube.com/watch?v=NlpnJE0m-NU
7. NPTEL. (2022). Introduction to Information Security. Retrieved from https://archive.nptel.ac.in/courses/106/106/106106129/
8. Swayam. (2022). Information Technology course. Retrieved from https://onlinecourses.swayam2.ac.in/cec22_cs15/preview
9. YouTube. (2020). Firewall configuration tutorial. Retrieved from https://www.youtube.com/watch?v=T9c5ZpT2FV0
10. Virtual Labs, IIIT Hyderabad. (n.d.). Virtual lab for cryptography experiments. Retrieved from https://cse29-iiith.vlabs.ac.in/List%20of%20experiments.html
11. GeeksforGeeks. (2021). Active and passive attacks in information security. Retrieved from https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/
12. BrightSec. (2023). SQL injection attack explained. Retrieved from https://brightsec.com/blog/sql-injection-attack/

युनिट-3
क्रिप्टोग्राफी
(Cryptography)

विषय निष्पत्ती (Course Outcome):

CO3: एनक्रिप्शन / डिक्रिप्शन तंत्रे अंमलात आणा.

घटक निष्पत्ती (Theory Learning Outcome):

1. एनक्रिप्शन आणि डिक्रिप्शनची प्रक्रिया स्पष्ट करा.
2. दिलेल्या पॅरामिटर्सच्या आधारे सिमेट्रिक आणि ॲसिमेट्रिक क्रिप्टोग्राफीची तुलना करा.
3. दिलेल्या मजकूरावर सब्स्टिट्यूशन तंत्रे वापरा.
4. दिलेल्या मजकूरावर ट्रान्सपोझिशन तंत्रे लागू करा.
5. स्टेगनोग्राफीची संकल्पना स्पष्ट करा.

3.1 परिचय (Introduction)

प्लेन टेक्स्ट, सायफर टेक्स्ट, क्रिप्टोग्राफी, क्रिप्टॲनॅलिसिस, क्रिप्टोलॉजी, एनक्रिप्शन, डिक्रिप्शन.

a. प्लेन टेक्स्ट (Plain Text)

प्लेन टेक्स्ट म्हणजे मूळ वाचण्यायोग्य संदेश किंवा डेटा, जो कोणतेही डिक्रिप्शन न करता मानवांना समजतो.

प्लेन टेक्स्ट म्हणजे कोणतीही माहिती जी कोणतेही सुरक्षा उपाय लागू करण्यापूर्वी तिच्या नैसर्गिक आणि समजण्याजोग्या स्वरूपात असते. ही माहिती एनक्रिप्शन प्रक्रियेचा इनपुट असते. प्लेन टेक्स्टमध्ये अक्षरे, संख्या, फाइल्स किंवा संवादाच्या वेळी संरक्षण आवश्यक असलेला कोणताही डेटा असू शकतो. प्लेन टेक्स्ट सहज वाचता येत असल्यामुळे, असुरक्षित नेटवर्कवर पाठवताना तो हल्ल्यांसाठी अत्यंत संवेदनशील असतो. त्यामुळे पाठवण्यापूर्वी त्याचे एनक्रिप्शन करणे आवश्यक असते.

b. सायफर टेक्स्ट (Cipher Text)

सायफर टेक्स्ट म्हणजे प्लेन टेक्स्टचे एनक्रिप्शन केल्यानंतर मिळणारा वाचता न येणारा डेटा होय. सायफर टेक्स्ट हा अर्थहीन अक्षरांचा समूह वाटतो, ज्यामुळे अनधिकृत प्रवेश रोखला जातो. फक्त योग्य की (Key) असलेली व्यक्तीच डिक्रिप्शन प्रक्रियेद्वारे त्याला पुन्हा प्लेन टेक्स्टमध्ये रूपांतरित करू शकते. सायफर टेक्स्ट संवादाच्या वेळी मूळ संदेश लपवून ठेवून गोपनीयता (Confidentiality) सुनिश्चित करतो.

c. एनक्रिप्शन (Encryption)

एनक्रिप्शन ही अशी प्रक्रिया आहे ज्यामध्ये वाचण्यायोग्य प्लेन टेक्स्टला एनक्रिप्शन अल्गोरिदम आणि की वापरून वाचता न येणाऱ्या सायफर टेक्स्टमध्ये रूपांतरित केले जाते. ही प्रक्रिया सुनिश्चित करते की योग्य की असलेले अधिकृत वापरकर्तेच मूळ माहिती वापरू शकतील. एनक्रिप्शन हे डेटा साठवण आणि संवादाच्या वेळी संरक्षण करण्यासाठी वापरले जाणारे मुख्य तंत्र आहे. हे संवेदनशील माहिती सुरक्षित स्वरूपात रूपांतरित करून अनधिकृत व्यक्तींना ती समजण्यापासून रोखते. एनक्रिप्शनमध्ये गणितीय अल्गोरिदम्स आणि कीज वापरल्या जातात. सिमेट्रिक एनक्रिप्शनमध्ये एनक्रिप्शन आणि डिक्रिप्शनसाठी एकच की वापरली जाते, तर ॲसिमेट्रिक एनक्रिप्शनमध्ये पब्लिक की आणि प्रायव्हेट की अशा कीजची जोडी वापरली जाते. एनक्रिप्शन असुरक्षित नेटवर्कवर पाठवला जाणारा डेटा सुरक्षित ठेवते आणि ई-मेल्स, ऑनलाइन बँकिंग, क्लाऊड स्टोरेज, सुरक्षित वेबसाईट्स आणि ऑथेन्टिकेशन सिस्टिम्समध्ये मोठ्या प्रमाणावर वापरले जाते.

d. डिक्रिप्शन (Decryption)

डिक्रिप्शन ही अशी प्रक्रिया आहे ज्यामध्ये वाचता न येणाऱ्या सायफर टेक्स्टला डिक्रिप्शन अल्गोरिदम आणि योग्य की वापरून पुन्हा मूळ वाचण्यायोग्य प्लेन टेक्स्टमध्ये रूपांतरित केले जाते. ही एनक्रिप्शनची उलट प्रक्रिया आहे आणि अधिकृत वापरकर्त्यांसाठी मूळ संदेश पुनर्संचयित करते.

डिक्रिप्शन हे सुरक्षित संवाद प्रणालीचे एक अत्यावश्यक घटक आहे. अनधिकृत प्रवेश टाळण्यासाठी डेटा एनक्रिप्ट केल्यानंतर, अपेक्षित प्राप्तकर्ता डिक्रिप्शन प्रक्रियेद्वारे मूळ प्लेन टेक्स्ट मिळवतो. डिक्रिप्शनसाठी योग्य की आवश्यक

असते; की नसल्यास सायफर टेक्स्ट वाचता येत नाही. सिमेट्रिक-की प्रणालीमध्ये एनक्रिप्शन आणि डिक्रिप्शनसाठी एकच की वापरली जाते, तर ॲसिमेट्रिक-की प्रणालीमध्ये पब्लिक कीने एनक्रिप्ट केलेला डेटा प्रायव्हेट कीने डिक्रिप्ट केला जातो. डिक्रिप्शनमुळे माहिती गोपनीय राहते आणि फक्त अधिकृत व्यक्तींनाच उपलब्ध होते.

e. क्रिप्टोग्राफी (Cryptography)

क्रिप्टोग्राफी ही माहिती सुरक्षित ठेवण्याची शास्त्रशाखा आहे, ज्यामध्ये गणितीय अल्गोरिदम्स आणि कीज वापरून वाचण्यायोग्य प्लेन टेक्स्टला वाचता न येणाऱ्या सायफर टेक्स्टमध्ये रूपांतरित केले जाते. योग्य की असलेले अधिकृत वापरकर्तेच सायफर टेक्स्ट पुन्हा प्लेन टेक्स्टमध्ये रूपांतरित करू शकतात. क्रिप्टोग्राफी कॉन्फिडेन्शियलिटी / गोपनीयता (Confidentiality), इंटेग्रिटी / अखंडता (Integrity), ऑथेंटिकेशन / प्रमाणीकरण (Authentication) आणि नॉन-रिप्युडिएशन सुनिश्चित करते. क्रिप्टोग्राफी असुरक्षित नेटवर्कवर सुरक्षित संवाद उपलब्ध करून देते. प्रेषक (Sender) एनक्रिप्शन अल्गोरिदम आणि की वापरून प्लेन टेक्स्टला सायफर टेक्स्टमध्ये रूपांतरित करतो, ज्यामुळे अनधिकृत वापरकर्त्यांना संदेश वाचता येत नाही. प्राप्तकर्ता (Receiver) योग्य कीसह डिक्रिप्शन अल्गोरिदम वापरून मूळ माहिती पुन्हा मिळवतो. क्रिप्टोग्राफीचे दोन प्रमुख प्रकार आहेत: सिमेट्रिक-की तंत्रे, ज्यामध्ये एकच की वापरली जाते, आणि ॲसिमेट्रिक-की तंत्रे, ज्यामध्ये पब्लिक की आणि प्रायव्हेट की वापरल्या जातात. यामध्ये डेटा अखंडतेसाठी हॅश फंक्शन्स आणि प्रमाणीकरणासाठी डिजिटल सिग्नेचर्सचाही समावेश होतो. क्रिप्टोग्राफीचा वापर सुरक्षित संवाद, ऑनलाइन बँकिंग, डिजिटल प्रमाणपत्रे आणि डेटा साठवण व प्रसारणाच्या वेळी संवेदनशील माहितीचे संरक्षण करण्यासाठी मोठ्या प्रमाणावर केला जातो.

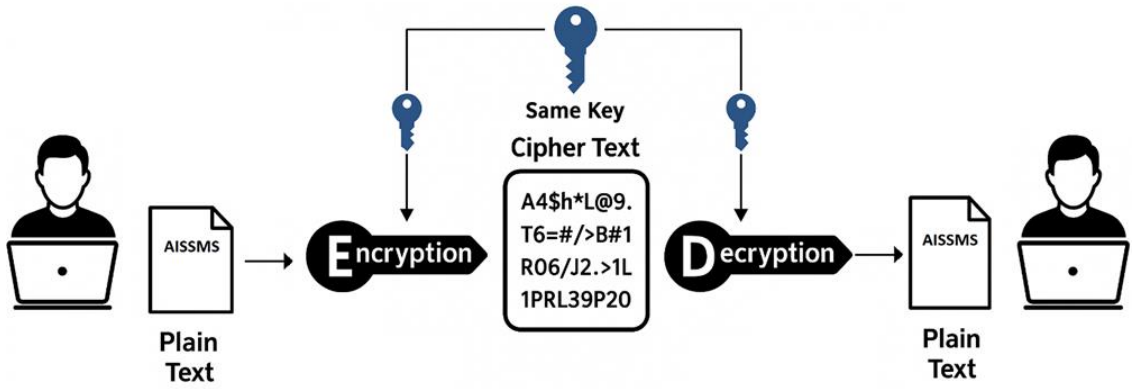


Fig 3.1: क्रिप्टोग्राफी (Cryptography)

क्रिप्टोग्राफीचे घटक (Components of Cryptography)

1. प्लेन टेक्स्ट (Plain Text): प्लेन टेक्स्ट म्हणजे मूळ वाचण्यायोग्य संदेश किंवा डेटा.
   उदाहरण: "AISSMS"
2. सायफर टेक्स्ट (Cipher Text): सायफर टेक्स्ट म्हणजे प्लेन टेक्स्टचे एनक्रिप्शन केल्यानंतर मिळणारा, वाचता न येणारा स्वरूपातील डेटा.
   उदाहरण: "8fh#K92! lmP"
3. एनक्रिप्शन (Encryption): की (Key) वापरून प्लेन टेक्स्टचे सायफर टेक्स्टमध्ये रूपांतर करण्याची प्रक्रिया.
   सूत्र: Plain Text + Key → Encryption Algorithm → Cipher Text
4. डिक्रिप्शन (Decryption): सायफर टेक्स्टचे पुन्हा मूळ वाचण्यायोग्य प्लेन टेक्स्टमध्ये रूपांतर करण्याची प्रक्रिया.
   सूत्र: Cipher Text + Key → Decryption Algorithm → Plain Text
5. की (Key): एनक्रिप्शन आणि डिक्रिप्शन प्रक्रियेत वापरली जाणारी गुप्त मूल्य (Secret Value).

f. क्रिप्टॲनॅलिसिस (Cryptanalysis)

क्रिप्टॲनॅलिसिस म्हणजे एनक्रिप्ट केलेल्या संदेशांचे विश्लेषण करून, की माहिती नसतानाही, क्रिप्टोग्राफिक प्रणाली तोडण्याचा आणि मूळ प्लेन टेक्स्ट पुनर्प्राप्त करण्याचा अभ्यास व प्रक्रिया होय. यामध्ये एनक्रिप्शन अल्गोरिदम्स किंवा कीजमधील कमकुवतपणा शोधण्यासाठी वापरल्या जाणाऱ्या विविध पद्धती आणि गणितीय तंत्रांचा समावेश होतो.

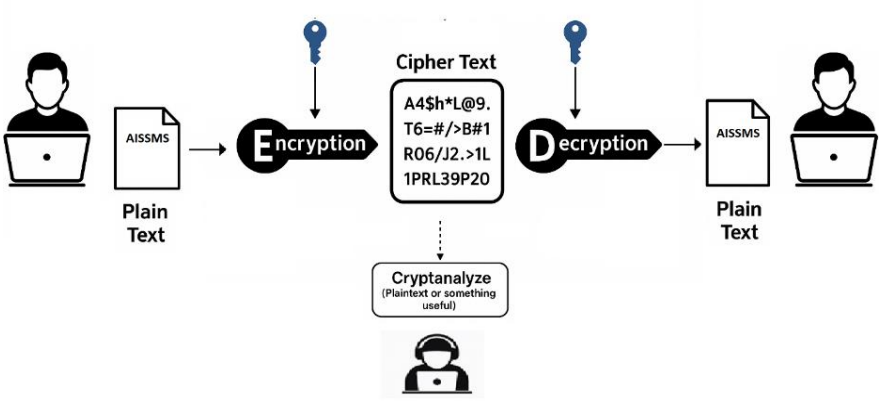


Fig 3.2: क्रिप्टॲनॅलिसिस (Cryptanalysis)

क्रिप्टॲनॅलिसिस हे क्रिप्टोग्राफिक अल्गोरिदम्स, प्रोटोकॉल्स किंवा त्यांच्या अंमलबजावणीतील असुरक्षितता (vulnerabilities) शोधण्यावर लक्ष केंद्रित करते. याचा मुख्य उद्देश अनधिकृत प्रवेशाशिवाय मूळ प्लेन टेक्स्ट किंवा एनक्रिप्शनसाठी वापरलेली की शोधणे हा असतो. क्रिप्टॲनॅलिसिसमध्ये ब्रूट फोर्स, फ्रिक्वेन्सी ॲनालिसिस, डिफरेंशियल ॲनालिसिस आणि स्टॅटिस्टिकल अटॅक्स यांसारख्या विविध तंत्रांचा वापर केला जातो. हे क्रिप्टोग्राफिक सिस्टिम्सची ताकद तपासण्यास मदत करते, म्हणजेच त्या हल्ल्यांविरुद्ध किती प्रतिरोधक आहेत हे समजते. प्रभावी क्रिप्टॲनॅलिसिसमुळे सुरक्षा तज्ज्ञांना कमकुवत एनक्रिप्शन पद्धती ओळखता येतात आणि सिस्टिमची सुरक्षा सुधारता येते. हल्लेखोर (Attackers) कोड्स तोडण्यासाठी क्रिप्टॲनॅलिसिसचा वापर करतात, तर सुरक्षा व्यावसायिक (Security Professionals) अल्गोरिदम्स विश्वासार्ह आणि तोडणे कठीण आहेत याची खात्री करण्यासाठी त्याचा उपयोग करतात.

g. क्रिप्टोलॉजी (Cryptology)

क्रिप्टोलॉजी म्हणजे सुरक्षित संवादाचा व्यापक वैज्ञानिक अभ्यास होय, ज्यामध्ये क्रिप्टोग्राफी (सुरक्षित प्रणाली तयार करणे) आणि क्रिप्टॲनॅलिसिस (त्या प्रणाली तोडणे) या दोन्हींचा समावेश होतो. ही एक संयुक्त शाखा आहे जी माहितीचे संरक्षण करणे आणि एनक्रिप्शन तंत्रांची ताकद विश्लेषित करणे यांशी संबंधित आहे.

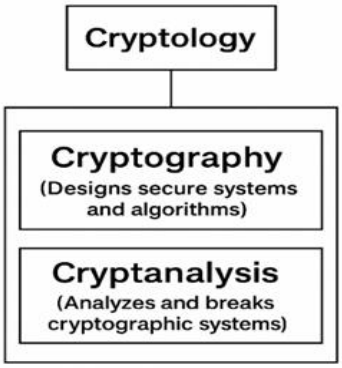


Fig 3.3: क्रिप्टोलॉजी (Cryptology)

क्रिप्टोलॉजी (Cryptology) ही एक व्यापक शास्त्रशाखा आहे जी माहितीचे संरक्षण करण्यासाठी वापरल्या जाणाऱ्या सुरक्षा तंत्रांची रचना (design), विश्लेषण (analysis) आणि मूल्यमापन (evaluation) यांचा समावेश करते. यामध्ये कॉन्फिडेन्शियलिटी / गोपनीयता (Confidentiality), इंटेग्रिटी / अखंडता (Integrity), ऑथेंटिकेशन / प्रमाणीकरण (Authentication) सुनिश्चित करणारे एनक्रिप्शन अल्गोरिदम्स विकसित करणे तसेच त्या अल्गोरिदम्सचे मूल्यमापन किंवा त्यांना तोडण्यासाठी वापरल्या जाणाऱ्या विश्लेषणात्मक पद्धतींचा समावेश होतो. क्रिप्टोलॉजी सुरक्षित संवाद प्रणाली, डिजिटल सुरक्षा, आधुनिक संगणन आणि सायबरसिक्युरिटीमध्ये महत्त्वाची भूमिका बजावते. ती डेटा अनधिकृत प्रवेशापासून सुरक्षित ठेवते तसेच प्रणालींमधील असुरक्षितता तपासण्यास मदत करते. क्रिप्टोलॉजीअंतर्गत क्रिप्टोग्राफी आणि क्रिप्टॲनॅलिसिस या दोन्ही शाखा एकत्रितपणे कार्य करून अधिक मजबूत आणि विश्वासार्ह सुरक्षा यंत्रणा तयार करतात.

उदाहरण: एखादा सुरक्षा संशोधक ऑनलाइन व्यवहारांचे संरक्षण करण्यासाठी नवीन एनक्रिप्शन अल्गोरिदम विकसित करतो (क्रिप्टोग्राफी). दुसरा तज्ज्ञ विविध अटॅक तंत्रांचा वापर करून तो अल्गोरिदम तोडण्याचा प्रयत्न करतो (क्रिप्टअॅनॅलिसिस). ही दोन्ही कार्ये क्रिप्टोलॉजी या व्यापक क्षेत्रात येतात.

3.2 सिमेट्रिक आणि ॲसिमेट्रिक क्रिप्टोग्राफी (Symmetric and Asymmetric cryptography)

3.2.1 सिमेट्रिक क्रिप्टोग्राफी (Symmetric Cryptography- Introduction, working, key management)

सिमेट्रिक क्रिप्टोग्राफीमध्ये एनक्रिप्शन आणि डिक्रिप्शन या दोन्ही प्रक्रियांसाठी एकच सामायिक की (single shared key) वापरली जाते. प्रेषक (sender) आणि प्राप्तकर्ता (receiver) या दोघांकडेही तीच गुप्त की असणे आवश्यक असते. ही पद्धत जलद (fast) असून मोठ्या प्रमाणातील डेटाचे एनक्रिप्शन करण्यासाठी योग्य आहे. मात्र, संवाद करणाऱ्या दोन्ही पक्षांमध्ये ही गुप्त की सुरक्षितरीत्या शेअर करणे हे या पद्धतीतील मुख्य आव्हान आहे.

सिमेट्रिक क्रिप्टोग्राफीची कार्यपद्धती (Working of Symmetric Cryptography)

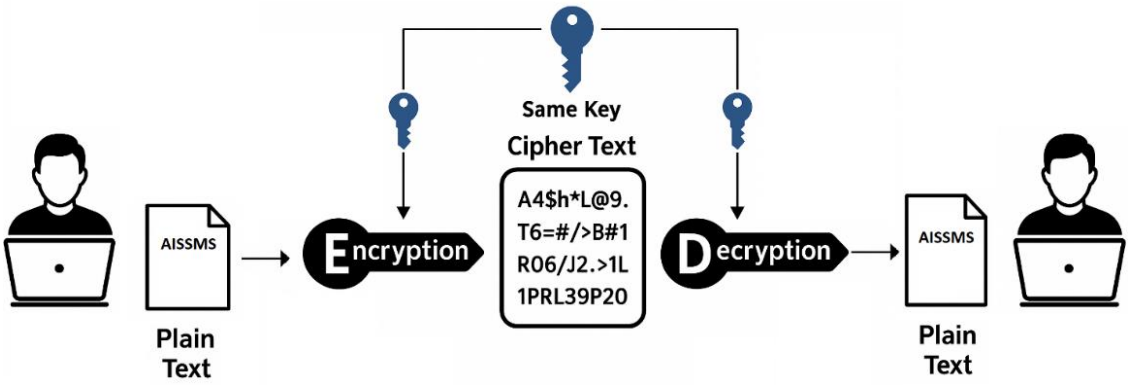


Fig 3.4: सिमेट्रिक क्रिप्टोग्राफीची कार्यपद्धती (Working of Symmetric Cryptography)

स्टेप-बाय-स्टेप कार्यपद्धती (Step-by-Step Working)

1. सेन्डर (Sender) प्लेन टेक्स्ट तयार करतो.
2. सेन्डर एनक्रिप्शन अल्गोरिदम + गुप्त की (Secret Key) वापरतो.
3. आउटपुट सायफर टेक्स्ट बनतो.
4. रिसिव्हर (Receiver) डिक्रिप्शन अल्गोरिदम + तीच गुप्त की वापरतो.
5. रिसिव्हर पुन्हा प्लेन टेक्स्ट प्राप्त होतो.

सिमेट्रिक की व्यवस्थापन (Symmetric Key Management)

- तीच की सेन्डर आणि रिसिव्हर यांच्यात सुरक्षितरीत्या शेअर केली पाहिजे.
- की वितरण (Key Distribution) हे आव्हानात्मक असते, कारण की उघड झाल्यास संपूर्ण प्रणाली धोक्यात येते.
- सुरक्षित चॅनेल्स (उदा. सुरक्षित कुरिअर, एनक्रिप्टेड चॅनेल्स) सहसा आवश्यक असतात.
- की वारंवार बदलल्या पाहिजेत.

3.2.2 ॲसिमेट्रिक क्रिप्टोग्राफी (Asymmetric Cryptography)

ॲसिमेट्रिक क्रिप्टोग्राफीमध्ये दोन वेगवेगळ्या कीज वापरल्या जातात: एनक्रिप्शनसाठी पब्लिक की (Public Key) आणि डिक्रिप्शनसाठी प्रायव्हेट की (Private Key). या कीज एक गणितीय जोडी (Mathematical Pair) तयार करतात. पब्लिक की उघडपणे शेअर केली जाते, तर प्रायव्हेट की गुप्त ठेवली जाते. ॲसिमेट्रिक क्रिप्टोग्राफी उच्च स्तराची सुरक्षा प्रदान करते आणि सिमेट्रिक प्रणालीतील की वितरणाची समस्या सोडवते.

ॲसिमेट्रिक क्रिप्टोग्राफीची कार्यपद्धती (Working of Asymmetric Cryptography)

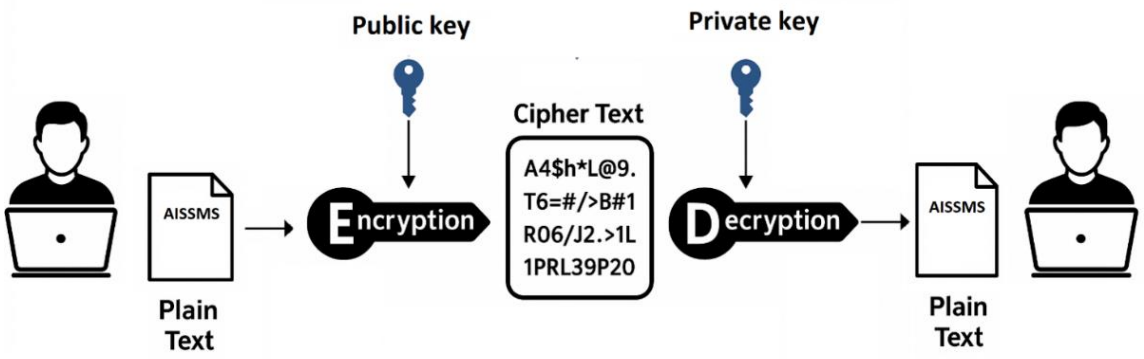


Fig 3.5: ॲसिमेट्रिक क्रिप्टोग्राफीची कार्यपद्धती (Working of Asymmetric Cryptography)

स्टेप-बाय-स्टेप कार्यपद्धती (Step-by-Step Working)

1. रिसिव्हर (Receiver) एक पब्लिक की आणि एक प्रायव्हेट की निर्माण करतो.
2. रिसिव्हर पब्लिक की प्रेषकासोबत शेअर करतो.
3. सेन्डर (Sender) पब्लिक की वापरून प्लेन टेक्स्टचे एनक्रिप्शन करतो.
4. रिसिव्हर प्रायव्हेट की वापरून सायफर टेक्स्टचे डिक्रिप्शन करतो.

ॲसिमेट्रिक की व्यवस्थापन (Asymmetric Key Management)

- पब्लिक कीज मुक्तपणे वितरित करता येतात.
- प्रायव्हेट कीज सुरक्षितरीत्या साठवणे आवश्यक असते (उदा. हार्डवेअर टोकन्स, सुरक्षित व्हॉल्ट्स).
- की पेअर्स एकत्रितपणे तयार केल्या जातात आणि गणितीयदृष्ट्या एकमेकांशी संबंधित असतात.
- की रद्द करणे (Revocation) आणि नूतनीकरण (Renewal) हे प्रमाणपत्रांद्वारे (Certificates) हाताळले जाते.

3.2.3 पब्लिक की वितरण (Public Key Distribution – Asymmetric Cryptography)

पब्लिक की वितरणामुळे की सुरक्षितरीत्या शेअर करण्याची समस्या सोडवली जाते. यासाठी विविध पद्धती वापरल्या जातात:

1. **पब्लिक ॲनाउन्समेंट्स (Public Announcements)**
   वापरकर्ता आपली पब्लिक की उघडपणे प्रकाशित करतो, जसे की वेबसाईट किंवा मेसेज बोर्डवर. जोखीम (Risk): हल्लेखोर बनावट (Fake) कीज वितरित करू शकतात.
2. **पब्लिक की डिरेक्टरीज (Public Key Directories)**
   अधिकृत डिरेक्टरीजमध्ये वापरकर्त्यांच्या पब्लिक कीज साठवलेल्या असतात. वापरकर्ते या प्रमाणित (Authenticated) स्रोतांमधून कीज प्राप्त करू शकतात.
3. **पब्लिक की अथॉरिटीज (Public Key Authorities)**
   विश्वसनीय अथॉरिटी वापरकर्त्यांची ओळख तपासते आणि त्यांना त्यांच्या पब्लिक कीशी जोडते. ही अथॉरिटी साइन केलेले प्रतिसाद (Signed Responses) पाठवते, ज्यामुळे प्रमाणीकरण (Authenticity) सुनिश्चित होते.
4. **पब्लिक की इन्फ्रास्ट्रक्चर (Public Key Infrastructure – PKI)**
   - विश्वसनीय सर्टिफिकेट अथॉरिटीज (CAs) कडून जारी केलेली डिजिटल प्रमाणपत्रे वापरली जातात.
   - प्रमाणपत्रांमध्ये पब्लिक की आणि मालकाची ओळख समाविष्ट असते.
   - जागतिक स्तरावर विश्वासार्ह आणि सुरक्षित पब्लिक की वितरण सुनिश्चित करते.
   - SSL/TLS, बँकिंग, ऑनलाइन ऑथेन्टिकेशन आणि इतर अनेक ठिकाणी वापरले जाते.

Table 3.1: सिमेट्रिक आणि ॲसिमेट्रिक क्रिप्टोग्राफी यांच्यातील तुलना (Comparison between Symmetric and Asymmetric Cryptography)

निकष (Criteria)	सिमेट्रिक क्रिप्टोग्राफी (Symmetric cryptography)	ॲसिमेट्रिक क्रिप्टोग्राफी (Asymmetric cryptography)
कींची संख्या (Number of Keys)	एक की वापरली जाते (एनक्रिप्शन आणि डिक्रिप्शनसाठी तीच की).	दोन की वापरल्या जातात: पब्लिक की (एनक्रिप्शन) आणि प्रायव्हेट की (डिक्रिप्शन).
गती (Speed)	जलद (मोठ्या प्रमाणातील डेटासाठी योग्य).	मंद (जटिल गणितीय क्रिया).
सुरक्षेची पातळी (Security Level)	कमी सुरक्षित (की लीक झाल्यास प्रणाली धोक्यात येते).	अधिक सुरक्षित (प्रायव्हेट की कधीही शेअर केली जात नाही).
की वितरण (Key Distribution)	कठीण — गुप्त की सुरक्षितरीत्या शेअर करावी लागते.	सोपे — पब्लिक की मुक्तपणे वितरित करता येते.
की व्यवस्थापन (Key Management)	सुरक्षित शेअरिंग आणि वारंवार की बदल आवश्यक.	पब्लिक की व्यवस्थापन प्रमाणपत्रांद्वारे (PKI) केले जाते.
कार्यपद्धती (Working Principle)	तीच की एनक्रिप्शन आणि डिक्रिप्शन करते.	पब्लिक की एनक्रिप्शन करते आणि प्रायव्हेट की डिक्रिप्शन करते.
अल्गोरिदम्स (Algorithms)	AES, DES, RC5, Blowfish.	RSA, Diffie-Hellman, ECC.

3.3 सब्स्टिट्यूशन टेक्निक्स (Substitution techniques)

3.3.1 सीझर सायफर (Caesar Cipher)

सीझर सायफर ही एक सब्स्टिट्यूशन एनक्रिप्शन तंत्र आहे, ज्यामध्ये प्लेन टेक्स्टमधील प्रत्येक अक्षर वर्णमालेतील ठरावीक संख्येने पुढे किंवा मागे हलवले जाते. हलवलेल्या स्थानांची संख्या म्हणजेच की (Key) होय. ही पद्धत क्रिप्टोग्राफीमधील सर्वात सोपी आणि जुनी पद्धत मानली जाते. हा एक मोनो-अल्फाबेटिक सायफर आहे, ज्यामध्ये प्लेन टेक्स्टमधील प्रत्येक अक्षर दुसऱ्या अक्षराने बदलले जाते आणि त्यातून सायफर टेक्स्ट तयार होतो. ही सब्स्टिट्यूशन सायफरची सर्वात सोपी पद्धत आहे. हा क्रिप्टोसिस्टम सामान्यतः शिफ्ट सायफर (Shift Cipher) म्हणून ओळखला जातो. या पद्धतीत प्रत्येक अक्षर दुसऱ्या अक्षराने बदलले जाते, जे 0 ते 25 या दरम्यान ठरावीक संख्येने हलवलेले असते. या पद्धतीमध्ये सेन्डर (Sender) आणि रिसिव्हर (Receiver) हे वर्णमाला किती स्थानांनी हलवायची यावर आधीच सहमती दर्शवतात. ही संख्या 0 ते 25 दरम्यान असते आणि तीच एनक्रिप्शनसाठीची की (Key) बनते. जेव्हा शिफ्टची संख्या 3 असते, तेव्हा या शिफ्ट सायफरला विशेषतः सीझर सायफर (Caesar Cipher) असे संबोधले जाते.

शिफ्ट सायफरची प्रक्रिया (Process of Shift Cipher):

- प्लेन टेक्स्टमधील एखादे अक्षर एनक्रिप्ट करण्यासाठी, प्रेषक स्लायडिंग रूलरला प्लेन टेक्स्ट अक्षरांच्या पहिल्या संचाखाली ठेवतो आणि गुप्त शिफ्टच्या स्थानांनुसार तो डावीकडे (LEFT) सरकवतो.
- त्यानंतर, स्लायडिंग रूलरखाली असलेले संबंधित अक्षर हे सायफर टेक्स्टमधील अक्षर बनते.

एनक्रिप्शन सूत्र (Encryption Formula):

$$C = (P + K)\ mod\ 26$$

डिक्रिप्शन सूत्र (Decryption Formula):

$$P = (C - K)\ mod\ 26$$

जिथे, P = प्लेनटेक्स्ट अक्षर, C = सायफरटेक्स्ट अक्षर, K = की (शिफ्ट मूल्य).

उदाहरण:एनक्रिप्शन: प्लेनटेक्स्ट = AISSMS

चला शिफ्ट की K = 3 निवडूया (सीझरची पारंपरिक पद्धत).

Letter	Position (P)	Calculation	Result
A	0	(0 + 3) mod 26 = 3	D
I	8	(8 + 3) mod 26 = 11	L
S	18	(18 + 3) mod 26 = 21	V
S	18	(18 + 3) mod 26 = 21	V
M	12	(12 + 3) mod 26 = 15	P
S	18	(18 + 3) mod 26 = 21	V

सायफरटेक्स्ट = DLVVPV

डिक्रिप्शन: आता आपण सायफरटेक्स्ट DLVVPV घेतो आणि डिक्रिप्शन सूत्र लागू करतो:

Letter	Position (C)	Calculation	Result
D	3	(3 − 3) mod 26 = 0	A
L	11	(11 − 3) mod 26 = 8	I
V	21	(21 − 3) mod 26 = 18	S
V	21	(21 − 3) mod 26 = 18	S
P	15	(15 − 3) mod 26 = 12	M
V	21	(21 − 3) mod 26 = 18	S

रिकव्हर्ड प्लेनटेक्स्ट = AISSMS

3.3.2 प्लेफेअर सायफर (Playfair Cipher)

प्लेफेअर सायफर ही एक डायग्राफ सब्स्टिट्यूशन सायफर आहे, जी एकेक अक्षराऐवजी अक्षरांच्या जोड्या (pairs of letters) एनक्रिप्ट करते. यात कीवर्ड (Keyword) वापरून तयार केलेल्या 5×5 की मॅट्रिक्स चा उपयोग करून प्रत्येक अक्षरजोडीचे सब्स्टिट्यूशन करून सायफरटेक्स्ट तयार केला जातो. अक्षरांच्या जोड्यांवर काम केल्यामुळे, ही पद्धत साध्या मोनो-अल्फाबेटिक सायफर्सपेक्षा अधिक सुरक्षित ठरते.

प्लेफेअर सायफरमध्ये प्लेनटेक्स्टला अक्षरांच्या जोड्यांमध्ये (डायग्राफ्स) विभागले जाते आणि कीवर्ड वापरून तयार केलेल्या 5×5 मॅट्रिक्स च्या आधारे प्रत्येक जोडीचे सब्स्टिट्यूशन केले जाते. यामध्ये I आणि J या अक्षरांना एकच मानले जाते, त्यामुळे एकूण 25 अक्षरे वापरली जातात. जर एखाद्या जोडीमध्ये एकच अक्षर पुन्हा आले असेल, तर त्या दोन अक्षरांच्या मध्ये X घातले जाते. प्लेनटेक्स्टमध्ये अक्षरांची संख्या विषम (odd) असल्यास, शेवटी X जोडले जाते. या सायफरमध्ये तीन नियम लागू केले जातात: सेम रो (Same Row), सेम कॉलम (Same Column), आणि रेक्टँगल सब्स्टिट्यूशन (Rectangle Substitution). एकेक अक्षराऐवजी अक्षरांच्या जोड्या एनक्रिप्ट केल्यामुळे, प्लेफेअर सायफर साध्या सब्स्टिट्यूशन सायफर्सपेक्षा तोडणे अधिक कठीण असते, कारण तो अक्षरांची वारंवारता (letter frequency) लपवतो.

5×5 की मॅट्रिक्स (कीवर्ड: MONARCHY)

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

स्पष्टीकरण (Explanation)

1. MONARCHY या कीवर्डचा वापर करून मॅट्रिक्स ओळींनुसार (row-wise) भरला जातो (कोणतीही अक्षरे पुनरावृत्त नाहीत).
2. उरलेली न वापरलेली वर्णमालेतील अक्षरे उरलेली जागा भरतात (I/J एकत्र धरले जातात).
3. प्रत्येक प्लेनटेक्स्ट जोडी (pair) या मॅट्रिक्समध्ये शोधली जाते आणि खालील नियमांनुसार सब्स्टिट्यूशन केले जाते:

- सेम रो (Same Row) → प्रत्येक अक्षराच्या उजवीकडील अक्षराने बदलले जाते
- सेम कॉलम (Same Column) → प्रत्येक अक्षराच्या खालील अक्षराने बदलले जाते
- रेक्टँगल नियम (Rectangle Rule) → तयार झालेल्या आयताच्या विरुद्ध कोपऱ्यातील, त्याच ओळीत असलेले अक्षर वापरले जाते

उदाहरण – प्लेफेअर सायफर (Example – Playfair Cipher)

प्लेनटेक्स्ट: AISSMS

स्टेप 1: अक्षरांच्या जोड्या तयार करा (Form Letter Pairs)

प्लेनटेक्स्टला दोन अक्षरांच्या जोड्यांमध्ये (डायग्राफ्स) विभागा: AI SS MS

एकसारखी दोन अक्षरे असलेली जोडी (SS) मान्य नाही, त्यामुळे त्यांच्यामध्ये X घातले जाते: AI SX MS

एनक्रिप्शनसाठी अंतिम जोड्या: AI SX MS

स्टेप 2: की टेबल वापरा (Use the Key Table)

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

लक्षात ठेवा: I/J एकत्र धरले जातात.

स्टेप 3: प्रत्येक जोडी एनक्रिप्ट करा (Encrypt Each Pair)

जोडी 1: AI

- A → ओळ 1, स्तंभ 4
- I → ओळ 3, स्तंभ 4

दोन्ही अक्षरे एकाच स्तंभात आहेत, त्यामुळे प्रत्येक अक्षराच्या खालील अक्षराने बदल करा:

- A → B
- I → S

AI → BS

जोडी 2: SX

- S → ओळ 4, स्तंभ 4
- X → ओळ 5, स्तंभ 4

दोन्ही अक्षरे एकाच स्तंभात आहेत, त्यामुळे खाली सरकवा:

- S → X
- X → A

SX → XA

जोडी 3: MS

- M → ओळ 1, स्तंभ 1
- S → ओळ 4, स्तंभ 4

भिन्न ओळ व स्तंभ → रेक्टँगल नियम

- M स्तंभ बदलून S च्या स्तंभात → T
- S स्तंभ बदलून M च्या स्तंभात → L

MS → TL

अंतिम सायफरटेक्स्ट (Final Cipher text): BSXATL

3.3.3 विजनेरे सायफर (Vigenère Cipher)

विजनेरे सायफर ही एक पॉली-अल्फाबेटिक सब्स्टिट्यूशन सायफर आहे, ज्यामध्ये प्लेनटेक्स्ट एनक्रिप्ट करण्यासाठी पुनरावृत्ती होणारा कीवर्ड (repeating keyword) वापरला जातो. प्लेनटेक्स्टमधील प्रत्येक अक्षर संबंधित की अक्षरावर आधारित ठरावीक प्रमाणात शिफ्ट केले जाते. यामुळे ही पद्धत सीझर सायफरसारख्या साध्या मोनो-अल्फाबेटिक सायफर्सपेक्षा अधिक सुरक्षित ठरते.

तुम्ही याची कल्पना 26×26 टेबल म्हणून करू शकता, ज्यामध्ये शिफ्ट केलेल्या वर्णमाला असतात:

वरची ओळ (Top row): A B C D … Z (प्लेन), डावी स्तंभ (Left column): A B C D … Z (की)

आतील भाग (Inside): ओळ = की अक्षर, स्तंभ = प्लेनटेक्स्ट अक्षर → सायफरटेक्स्ट अक्षर

KEY \ PLAIN	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

एनक्रिप्ट करण्यासाठी (To encrypt):

- ओळ शोधा = की अक्षर (key letter)
- स्तंभ शोधा = प्लेनटेक्स्ट अक्षर (plaintext letter)
- इंटरसेक्शन पॉइंट = सायफरटेक्स्ट अक्षर (ciphertext letter)

उदाहरण: विजनेरे सायफर (Vigenère Cipher) – टेबल वापरून (Tabula Recta पद्धत)

प्लेनटेक्स्ट: AISSMS, की: POLY

स्टेप 1: की पुनरावृत्त करा (Repeat the Key)

प्लेनटेक्स्टमध्ये 6 अक्षरे असल्यामुळे, कीची लांबी जुळवण्यासाठी की पुन्हा लिहा:

Plaintext: A I S S M S

Key: P O L Y P O

स्टेप 2: विजनेरे टेबल वापरा (Use the Vigenère Table – Tabula Recta)

टेबल कसे वाचावे (How to Read the Table)

- वरची ओळ = प्लेनटेक्स्ट अक्षर (P)
- डावा स्तंभ = की अक्षर (K)
- इंटरसेक्शन पॉइंट = सायफरटेक्स्ट अक्षर (C)

टेबल वापरून स्टेप-बाय-स्टेप (Step-by-Step Using the Table)

जोडी: A आणि P

- प्लेनटेक्स्ट = A (स्तंभ A)
- की = P (ओळ P)
- टेबल इंटरसेक्शन पॉइंट = P

निकाल: A → P

जोडी: I आणि O

- प्लेनटेक्स्ट = I (स्तंभ I)
- की = O (ओळ O)
- टेबल इंटरसेक्शन पॉइंट = W

निकाल: I → W

जोडी: S आणि L

- प्लेनटेक्स्ट = S (स्तंभ S)
- की = L (ओळ L)
- टेबल इंटरसेक्शन पॉइंट = D

निकाल: S → D

जोडी: S आणि Y

- प्लेनटेक्स्ट = S (स्तंभ S)
- की = Y (ओळ Y)
- टेबल इंटरसेक्शन पॉइंट = Q

निकाल: S → Q

जोडी: M आणि P

- प्लेनटेक्स्ट = M (स्तंभ M)
- की = P (ओळ P)
- टेबल इंटरसेक्शन पॉइंट = B

निकाल: M → B

जोडी: S आणि O

- प्लेनटेक्स्ट = S (स्तंभ S)
- की = O (ओळ O)
- टेबल इंटरसेक्शन पॉइंट = G

निकाल: S → G

अंतिम सायफरटेक्स्ट (Final Ciphertext): PWDQBG

अंतिम उत्तर (Final Answer):

Plaintext	A	I	S	S	M	S
Key	P	O	L	Y	P	O
Cipher	P	W	D	Q	B	G

3.3.4 व्हर्नम सायफर (Vernam Cipher – One-Time Pad)

व्हर्नम सायफर ही गिल्बर्ट व्हर्नम यांनी 1917 मध्ये सादर केलेली सिमेट्रिक की स्ट्रीम सायफर पद्धत आहे. या पद्धतीमध्ये प्लेनटेक्स्टमधील प्रत्येक बिट आणि कीमधील संबंधित बिट यांच्यात XOR (Exclusive OR) ऑपरेशन वापरून डेटा एनक्रिप्ट केला जातो. साध्या सब्स्टिट्यूशन सायफर्सच्या तुलनेत, यामध्ये एनक्रिप्शन आणि डिक्रिप्शनसाठी एकच XOR प्रक्रिया वापरली जाते. ही पद्धत अनेकदा वन-टाइम पॅड (One-Time Pad) म्हणून ओळखली जाते. या तंत्रामध्ये प्लेनटेक्स्टला पूर्णपणे रँडम आणि संदेशाइतकीच लांबी असलेल्या कीसोबत एकत्र केले जाते. बायनरी स्वरूपात, एनक्रिप्शन XOR वापरून केले जाते, तर वर्णमाला-आधारित आवृत्त्यांमध्ये modulo-26 addition वापरले जाऊ शकते. प्लेनटेक्स्टमधील प्रत्येक अक्षरासाठी वेगळी आणि रँडम की अक्षर वापरल्यामुळे कोणतेही पॅटर्न तयार होत नाहीत, त्यामुळे क्रिप्टॲनॅलिसिस साठी काहीही उपलब्ध राहत नाही. व्हर्नम सायफरला तेव्हाच खरा वन-टाइम पॅड मानले जाते, जेव्हा की पूर्णपणे रँडम असते, फक्त एकदाच वापरली जाते आणि काटेकोरपणे गुप्त ठेवली जाते. या आदर्श परिस्थितींमध्ये, ही पद्धत परफेक्ट सिक्युरिटी प्रदान करते आणि गणितीयदृष्ट्या तोडता न येणारी (unbreakable) मानली जाते, ज्यामुळे पूर्ण गोपनीयता सुनिश्चित होते.

व्हर्नम सायफरची प्रक्रिया (Process of Vernam Cipher)

1. की निवड (Key Selection):
   प्लेनटेक्स्टइतकीच लांबी असलेली की निवडा. जर की पूर्णपणे रँडम असेल आणि पुन्हा कधीही वापरली गेली नाही, तर ही सायफर पद्धत वन-टाइम पॅड (OTP) बनते.
2. प्लेनटेक्स्ट आणि कीचे बायनरी/संख्यात्मक रूपांतरण (Convert Plaintext and Key to Binary/Numbers):
   प्लेनटेक्स्ट अक्षरे आणि की अक्षरे ASCII बायनरी कोड्स म्हणून दर्शवा (किंवा modulo-26 वापरत असाल तर A=0, B=1, …, Z=25).
3. एनक्रिप्शन (XOR ऑपरेशन):
   प्लेनटेक्स्ट आणि कीमधील प्रत्येक बिटवर बिटवाईज XOR ($\oplus$) ऑपरेशन लागू करा.
   $$C = P \oplus K$$
4. सायफरटेक्स्ट निर्मिती (Ciphertext Formation):
   सर्व XOR परिणाम एकत्र करून बायनरी स्वरूपात सायफरटेक्स्ट मिळवा. बायनरीला पुन्हा अक्षरांमध्ये रूपांतरित करा (ते रँडमसारखे दिसू शकते).
5. डिक्रिप्शन (Decryption):
   प्राप्तकर्ता (Receiver) तीच की वापरून पुन्हा XOR ऑपरेशन लागू करतो:
   $$P = C \oplus K$$
   XOR उलट करता येणारे (reversible) असल्यामुळे, तीच प्रक्रिया पुन्हा लागू केल्यास मूळ प्लेनटेक्स्ट पुनर्प्राप्त होतो.
   जिथे, P = प्लेनटेक्स्ट अक्षर, C = सायफरटेक्स्ट अक्षर, K = की (शिफ्ट मूल्य), $\oplus$ = XOR.

उदाहरण: एनक्रिप्शन (Example: Encryption)

प्लेनटेक्स्ट = AISSMS

प्लेनटेक्स्ट → संख्या (A=0, B=1, …, Z=25)

A = 0, I = 8, S = 18, S = 18, M = 12,S = 18

म्हणून,

Plaintext = 0 8 18 18 12 18

की निवडा (Choose a Key – same length as plaintext)

Key = XMCKLQ

X = 23, M = 12, C = 2, K = 10, L = 11, Q = 16

म्हणून,

Key = 23 12 2 10 11 16

एनक्रिप्शन सूत्र (Encryption Formula)

$$C = (P + K) mod\ 26$$

आता गणना करा (Now compute):

- A (0) + X (23) = 23 → X
- I (8) + M (12) = 20 → U
- S (18) + C (2) = 20 → U
- S (18) + K (10) = 28 mod 26 = 2 → C
- M (12) + L (11) = 23 → X
- S (18) + Q (16) = 34 mod 26 = 8 → I

सायफरटेक्स्ट = XUUCXI

डिक्रिप्शन (Decryption)

दिलेला सायफरटेक्स्ट (Given Ciphertext): XUUCXI

सायफरटेक्स्ट → संख्या (Convert Ciphertext to Numbers)

(A=0, B=1, …, Z=25)

Letter	X	U	U	C	X	I
Value	23	20	20	2	23	8

म्हणून,

Ciphertext = 23 20 20 2 23 8

की (एनक्रिप्शनसाठी वापरलेलीच की)

Key = XMCKLQ

Letter	X	M	C	K	L	Q
Value	23	12	2	10	11	16

म्हणून,

Key = 23 12 2 10 11 16

डिक्रिप्शन सूत्र (Decryption Formula)

$$P = (C - K) mod\ 26$$

जिथे: P = प्लेनटेक्स्ट मूल्य, C = सायफरटेक्स्ट मूल्य, K = की मूल्य

डिक्रिप्शनची गणना करा

Step	C	K	C - K	Result (mod 26)	Letter
1	23	23	0	0	A
2	20	12	8	8	I
3	20	2	18	18	S
4	2	10	-8 → (-8 + 26 = 18)	18	S
5	23	11	12	12	M
6	8	16	-8 → (-8 + 26 = 18)	18	S

रिकव्हर्ड प्लेनटेक्स्ट: AISSMS

3.4 ट्रान्सपोजिशन टेक्निक्स (Transposition techniques)

3.4.1 रेलफेन्स तंत्र (Rail Fence Technique)

रेल फेन्स सायफर ही एक ट्रान्सपोझिशन सायफर पद्धत आहे, ज्यामध्ये प्लेनटेक्स्टमधील अक्षरे अनेक ओळींमध्ये झिग-झॅग (रेल) पॅटर्नमध्ये लिहिली जातात आणि नंतर ओळीनुसार (row-by-row) वाचून सायफरटेक्स्ट तयार केला जातो. या पद्धतीमध्ये अक्षरे बदलली जात नाहीत, फक्त त्यांची मांडणी बदलली जाते. रेल फेन्स तंत्रामध्ये संदेश एनक्रिप्ट करण्यासाठी प्लेनटेक्स्ट ठरावीक संख्येच्या ओळींमध्ये (ज्यांना "रेल्स" म्हटले जाते) तिरकस (diagonally) स्वरूपात लिहिला जातो आणि नंतर प्रत्येक ओळ आडवी (horizontally) वाचली जाते. अक्षरांची फक्त स्थानं बदलली जातात, अक्षरे स्वतः बदलत नसल्यामुळे ही पद्धत ट्रान्सपोझिशन सायफर म्हणून ओळखली जाते, सब्स्टिट्यूशन सायफर नाही. रेल्सची संख्या हीच की (Key) म्हणून कार्य करते. रेल्सची संख्या जितकी जास्त, तितका झिग-झॅग पॅटर्न अधिक गुंतागुंतीचा होतो. डिक्रिप्शन

दरम्यान, सायफरटेक्स्ट वापरून आणि रेल्सच्या संख्येच्या आधारे पुन्हा झिग-झॅग पॅटर्न तयार करून मूळ संदेश पुनर्संचयित केला जातो. ही पद्धत सोपी असली तरी केवळ मूलभूत सुरक्षा प्रदान करते, कारण विश्लेषणाद्वारे पॅटर्न उघड होऊ शकतात.

उदाहरण (Example):

- की निवडा = रेल्सची संख्या.
- प्लेनटेक्स्ट रेल्सवर झिग-झॅग पद्धतीने लिहा.
- मजकूर ओळीनुसार वाचा → सायफरटेक्स्ट.

डिक्रिप्शनसाठी: सायफरटेक्स्ट आणि रेल्सची संख्या वापरून झिग-झॅग पॅटर्न पुन्हा तयार करा.

उदाहरण (2-रेल सायफर):

प्लेनटेक्स्ट: HELLO WORLD

मांडणी (Arrangement):

Position	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Rail 1	H	.	L	.	O	.	O	.	L	.
Rail 2	.	E	.	L	.	W	.	R	.	D

सायफरटेक्स्ट: HLOOLELWRD

3.4.2 सिंपल कॉलमनर ट्रान्सपोझिशन (Simple Columnar Transposition)

साधी कॉलमनर ट्रान्सपोझिशन ही एक ट्रान्सपोझिशन सायफर पद्धत आहे, ज्यामध्ये प्लेनटेक्स्ट दिलेल्या कीवर्डखाली ओळींमध्ये लिहिला जातो आणि कीवर्डच्या वर्णमालेनुसार (alphabetical sequence) ठरवलेल्या क्रमाने स्तंभ वाचून सायफरटेक्स्ट तयार केला जातो. या पद्धतीमध्ये अक्षरे बदलली जात नाहीत—फक्त त्यांची मांडणी बदलली जाते. या तंत्रामध्ये प्लेनटेक्स्ट निवडलेल्या कीवर्डखाली आयताकृती टेबलमध्ये (rectangular table) ओळींनुसार (row-wise) मांडला जातो. त्यानंतर कीवर्डमधील अक्षरे वर्णमालेनुसार क्रमबद्ध केली जातात आणि त्या क्रमाने टेबलमधील स्तंभ वाचले जातात. यामुळे पुनर्रचित सायफरटेक्स्ट तयार होतो. ही एक शुद्ध ट्रान्सपोझिशन सायफर असल्यामुळे अक्षरांची वारंवारता (frequency) बदलत नाही. या पद्धतीची सुरक्षा कीवर्डच्या लांबीवर आणि गुंतागुंतीवर अवलंबून असते. डिक्रिप्शनसाठी, त्याच की क्रमाचा वापर करून सायफरटेक्स्ट पुन्हा मूळ टेबलमध्ये मांडला जातो.

उदाहरण (Example):

प्लेनटेक्स्ट: POLYTECHNIC, की (Key): COMP

स्टेप 1: कीला क्रमांक द्या (Number the Key)

कीवर्डमधील अक्षरे वर्णमालेनुसार लावा:

Key = C O M P

C → 1, M → 2, O → 3, P → 4

म्हणून, Key = 1 3 2 4

स्टेप 2: प्लेनटेक्स्ट ग्रीडमध्ये मांडणी करा (Arrange Plaintext in Grid)

- प्लेनटेक्स्टची लांबी = 11 अक्षरे
- कीची लांबी = 4 → ग्रीडमध्ये 4 स्तंभ

प्लेनटेक्स्ट ओळींनुसार लिहा आणि रिकामी जागा भरण्यासाठी X जोडा:

Key: 1 3 2 4

C	**O**	**M**	**P**
1	**3**	**2**	**4**
P	O	L	Y
T	E	C	H
N	I	C	X

स्टेप 3: स्तंभ क्रमाने वाचा (Read Columns in Order)
की क्रमाप्रमाणे स्तंभांची पुनर्रचना करा (1 → 2 → 3 → 4):

- स्तंभ नाव 1 → P T N
- स्तंभ नाव 2 → L C C
- स्तंभ नाव 3 → O E I
- स्तंभ नाव 4 → Y H X

स्टेप 4: सायफरटेक्स्ट (Ciphertext)
आता स्तंभानुसार वाचा: PTNLCCOEIYHX
अंतिम सायफरटेक्स्ट = PTNLCCOEIYHX

3.5 स्टेगनोग्राफी: स्टेगनोग्राफीचा आढावा (Overview of Steganography)

स्टेगनोग्राफी ही अशी तंत्रज्ञान पद्धत आहे ज्यामध्ये गुप्त माहिती मजकूर, प्रतिमा, ऑडिओ, व्हिडिओ किंवा नेटवर्क डेटा यांसारख्या कव्हर मीडियममध्ये अशा प्रकारे लपवली जाते की संदेश अस्तित्वात आहे हेच लपून राहते. यामध्ये डेटाला गोंधळात टाकणे (scramble) हा उद्देश नसून, संवाद सामान्य आणि लक्षात न येणारा वाटावा हा मुख्य उद्देश असतो. आधुनिक स्टेगनोग्राफी तंत्रांमध्ये डिजिटल फाइल्स जसे की प्रतिमा, ऑडिओ, व्हिडिओ आणि नेटवर्क पॅकेट्स यांचा वापर केला जातो. यामधील एक सामान्य पद्धत म्हणजे लीस्ट सिग्निफिकंट बिट (LSB) पद्धत, ज्यामध्ये डिजिटल डेटामध्ये अतिशय सूक्ष्म बदल केले जातात, जे दृश्य किंवा श्राव्य स्वरूपात लक्षात येत नाहीत. स्टेगनोग्राफीचा वापर क्रिप्टोग्राफीसोबत देखील केला जाऊ शकतो. म्हणजे आधी संदेशाचे एनक्रिप्शन करणे आणि नंतर तो लपवणे ज्यामुळे अधिक उच्च स्तराची गोपनीयता आणि गुप्तता (stealth) साध्य होते. ही स्तरबद्ध पद्धत (layered approach) आधुनिक माहिती सुरक्षा तत्त्वांशी सुसंगत आहे, जसे की कॉन्फिडेन्शियलिटी / गोपनीयता (Confidentiality), इंटेग्रिटी / अखंडता (Integrity), ऑथेंटिकेशन / प्रमाणीकरण (Authentication), आणि नॉन-रिप्युडिएशन (Non-repudiation), ज्यांचा उल्लेख विविध संदर्भ साहित्यात करण्यात आला आहे.

स्टेगनोग्राफी प्रक्रिया (Steganography Process)

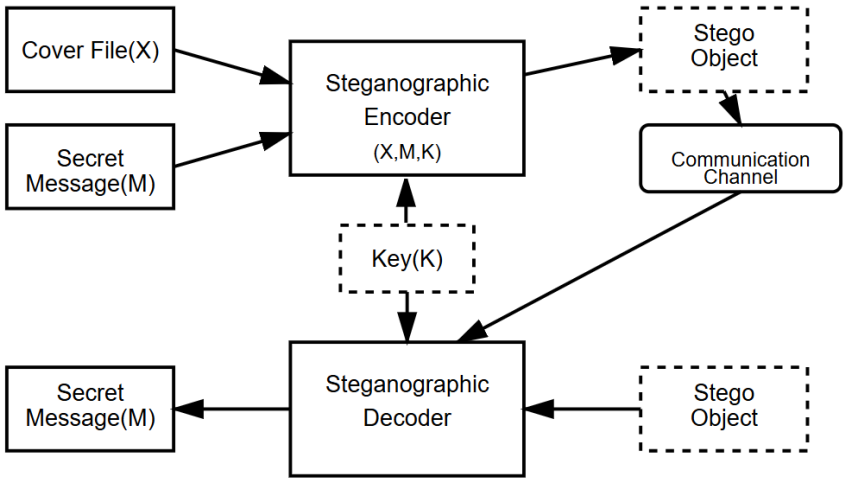


Fig 3.6: स्टेगनोग्राफी प्रक्रिया आकृती (Steganography Process Diagram)

ही आकृती स्टेगनोग्राफिक कम्युनिकेशन सिस्टिमचा संपूर्ण कार्यप्रवाह दर्शवते, ज्यामध्ये सुरक्षित आणि गुप्त प्रसारणासाठी गुप्त संदेश कव्हर फाइलमध्ये लपवला जातो. सर्वप्रथम, कव्हर फाइल (X) आणि गुप्त संदेश (M) हे इनपुट्स म्हणून स्टेगनोग्राफिक एन्कोडरकडे दिले जातात, तसेच अतिरिक्त सुरक्षेसाठी ऐच्छिक की (K) वापरली जाऊ शकते. एन्कोडर गुप्त संदेश कव्हर फाइलमध्ये एम्बेड करतो आणि त्यातून स्टेगो ऑब्जेक्ट तयार होते, जे सामान्य फाइलसारखे दिसते आणि त्यामध्ये लपवलेला डेटा आहे हे उघड होत नाही. हे स्टेगो ऑब्जेक्ट नंतर कम्युनिकेशन चॅनेल (जसे की नेटवर्क किंवा स्टोरेज मीडियम) द्वारे पाठवले जाते. प्राप्तकर्त्याच्या टोकाला, स्टेगनोग्राफिक डिकोडर स्टेगो ऑब्जेक्ट प्राप्त करतो आणि आवश्यक असल्यास तीच की वापरून मूळ गुप्त संदेश (M) काढून पुन्हा तयार करतो. या संपूर्ण प्रक्रियेत, फक्त

संदेश एनक्रिप्ट करणे नव्हे तर संवाद अस्तित्वात आहे हेच लपवणे हा मुख्य उद्देश असतो, ज्यामुळे अनपेक्षित निरीक्षकांना संदेश लक्षात येत नाही, पण अपेक्षित प्राप्तकर्त्याला तो पुनर्प्राप्त करता येतो.

स्टेगनोग्राफी टेक्निक्स (Steganography Techniques)

स्टेगनोग्राफी तंत्रे गुप्त डेटा लपवण्यासाठी वापरल्या जाणाऱ्या कव्हर ऑब्जेक्टच्या प्रकारावर अवलंबून असतात. व्यापकपणे, त्यांचे खालील पाच प्रकार आहेत:

1. टेक्स्ट स्टेगनोग्राफी
2. इमेज स्टेगनोग्राफी
3. व्हिडिओ स्टेगनोग्राफी
4. ऑडिओ स्टेगनोग्राफी
5. नेटवर्क (प्रोटोकॉल) स्टेगनोग्राफी

1. टेक्स्ट स्टेगनोग्राफी (Text Steganography)

टेक्स्ट स्टेगनोग्राफीमध्ये मजकूर-आधारित दस्तऐवजांमध्ये माहिती लपवली जाते. यामध्ये मजकूर अशा प्रकारे बदलला किंवा तयार केला जातो की लपवलेला संदेश लक्षात येत नाही. यामध्ये फॉरमॅट बदलणे, अक्षरे किंवा शब्द बदलणे, किंवा विशिष्ट टेक्स्ट पॅटर्न तयार करणे यांचा समावेश होऊ शकतो.

सामान्य तंत्रे (Common Techniques):

- फॉरमॅट-आधारित पद्धती (Format-Based Methods) – स्पेसिंग, अलाइनमेंट, फॉन्ट्स किंवा विरामचिन्हे बदलणे.
- रँडम आणि स्टॅटिस्टिकल जनरेशन – रँडम किंवा सांख्यिकीयदृष्ट्या समान टेक्स्ट पॅटर्न तयार करणे.
- लिंग्विस्टिक पद्धती (Linguistic Methods) – व्याकरण नियम, समानार्थी शब्द किंवा वाक्यरचना वापरून डेटा एम्बेड करणे.

2. इमेज स्टेगनोग्राफी (Image Steganography)

इमेज स्टेगनोग्राफीमध्ये डिजिटल प्रतिमांमध्ये डेटा लपवला जातो. प्रतिमांमध्ये मोठ्या प्रमाणावर बायनरी डेटा असल्यामुळे, चित्रात दृश्य बदल न करता माहिती एम्बेड करण्याची मोठी क्षमता असते.

सामान्य तंत्रे (Common Techniques):

- लीस्ट सिग्निफिकंट बिट (LSB) इन्सर्शन
- मास्किंग आणि फिल्टरिंग
- रिडंडंट पॅटर्न एन्कोडिंग
- एन्क्रिप्ट अँड स्कॅटर पद्धती
- कोडिंग आणि कोसाईन ट्रान्सफॉर्म तंत्रे

3. ऑडिओ स्टेगनोग्राफी (Audio Steganography)

ऑडिओ स्टेगनोग्राफीमध्ये गुप्त माहिती ऑडिओ सिग्नलमध्ये एम्बेड केली जाते, ज्यामध्ये अंतर्गत बायनरी डेटामध्ये बदल केले जातात. मानवी ऐकण्याची संवेदनशीलता जास्त असल्यामुळे, ही प्रक्रिया इमेज-आधारित स्टेगनोग्राफीपेक्षा अधिक गुंतागुंतीची असते.

सामान्य पद्धती (Common Methods):

- लीस्ट सिग्निफिकंट बिट (LSB) एन्कोडिंग
- पॅरिटी एन्कोडिंग
- फेज कोडिंग
- स्प्रेड स्पेक्ट्रम तंत्रे,

ही पद्धत WAV, AU, आणि MP3 अशा फॉरमॅट्समध्ये वापरली जाऊ शकते.

4. व्हिडिओ स्टेगनोग्राफी (Video Steganography)

व्हिडिओ स्टेगनोग्राफीमध्ये डिजिटल व्हिडिओ फाइल्समध्ये लपवलेला डेटा एम्बेड केला जातो. व्हिडिओमध्ये प्रतिमा आणि ऑडिओ दोन्ही स्ट्रीम्स असतात, त्यामुळे माहिती लपवण्यासाठी मोठी क्षमता उपलब्ध होते.

दोन मुख्य पद्धती (Two Main Approaches):

- कच्च्या (uncompressed) व्हिडिओमध्ये डेटा एम्बेड करून नंतर कंप्रेशन करणे
- आधीच कंप्रेस केलेल्या व्हिडिओ स्ट्रीममध्ये थेट डेटा एम्बेड करणे

ही पद्धत इमेज आणि ऑडिओ स्टेगनोग्राफीचे संयोजन म्हणून पाहिली जाऊ शकते.

5. नेटवर्क (प्रोटोकॉल) स्टेगनोग्राफी (Network Steganography)

नेटवर्क स्टेगनोग्राफीमध्ये TCP, UDP, आणि ICMP यांसारख्या नेटवर्क कम्युनिकेशन प्रोटोकॉल्समध्ये डेटा लपवला जातो. माहिती पॅकेट हेडर्स, न वापरलेले फील्ड्स किंवा प्रोटोकॉल वर्तनामध्ये एम्बेड करून OSI मॉडेलमध्ये गुप्त कम्युनिकेशन चॅनेल्स तयार केली जातात.

उदाहरण: TCP/IP हेडरमधील काही ऐच्छिक (optional) फील्ड्स वापरून डेटा लपवता येतो.

References:

1. Stallings, W., & Brown, L. (2014). Computer security: Principles and practice (3rd ed.). Pearson. ISBN: 978-0-13-377392-7.
2. Kahate, A. (2018). Cryptography and network security (3rd ed.; 4th ed.). McGraw-Hill. ISBN: 978-9353163303.
3. Merkow, M., & Breithaupt, J. (2006). Information security: Principles and practices. Pearson. ISBN: 978-81-317-1288-7.
4. Pachghare, V. K. (2012). Cryptography and information security. Prentice Hall India. ISBN: 978-81-203-5082-3.
5. Gollmann, D. (2011). Computer security (3rd ed.). Wiley. ISBN: 978-0-470-74115-3.
6. YouTube. (2019). Simulation of intrusion detection system in MANET using NetSim. Retrieved from https://www.youtube.com/watch?v=NlpnJE0m-NU
7. NPTEL. (2022). Introduction to Information Security. Retrieved from https://archive.nptel.ac.in/courses/106/106/106106129/
8. Swayam. (2022). Information Technology course. Retrieved from https://onlinecourses.swayam2.ac.in/cec22_cs15/preview
9. YouTube. (2020). Firewall configuration tutorial. Retrieved from https://www.youtube.com/watch?v=T9c5ZpT2FV0
10. Virtual Labs, IIIT Hyderabad. (n.d.). Virtual lab for cryptography experiments. Retrieved from https://cse29-iiith.vlabs.ac.in/List%20of%20experiments.html
11. GeeksforGeeks. (2021). Active and passive attacks in information security. Retrieved from https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/
12. BrightSec. (2023). SQL injection attack explained. Retrieved from https://brightsec.com/blog/sql-injection-attack/

युनिट-4
फायरवॉल अँड एनक्रिप्शन अल्गोरिदम्स
(Firewall and Encryption Algorithms)

विषय निष्पत्ती (Course Outcome):

CO4: सायबर-हल्ले रोखण्यासाठी साधने आणि तंत्रे वापरा.

घटक निष्पत्ती (Theory Learning Outcome):

1. हार्डवेअर आणि सॉफ्टवेअर फायरवॉल्स यांमधील फरक स्पष्ट करा.
2. विविध फायरवॉल पॉलिसीज स्पष्ट करा.
3. दिलेल्या पॅरामिटर्सच्या आधारे DES, AES आणि RSA अल्गोरिदम्सची तुलना करा.
4. दिलेल्या मजकूरावर डिफी-हेलमन (Diffie-Hellman) की एक्सचेंज अल्गोरिदम लागू करा.
5. दिलेल्या मजकूरासाठी हॅश फंक्शन अल्गोरिदम वापरून हॅश व्हॅल्यू काढा.
6. डिजिटल सिग्नेचरची कार्यपद्धती स्पष्ट करा.

4.1 फायरवॉल (Firewall)

फायरवॉल ही एक नेटवर्क सुरक्षा यंत्रणा आहे जी हार्डवेअर, सॉफ्टवेअर किंवा दोन्हींच्या संयोजनात अंमलात आणली जाते. ती विश्वसनीय अंतर्गत नेटवर्क (उदा. LAN) आणि अविश्वसनीय बाह्य नेटवर्क (सामान्यतः इंटरनेट) यांच्यातील ट्रॅफिकचे निरीक्षण, फिल्टरिंग आणि नियंत्रण करते. असुरक्षिततेच्या महत्त्वाच्या ठिकाणी (critical point of vulnerability) बसवलेला फायरवॉल पूर्वनिश्चित सुरक्षा पॉलिसीज अंमलात आणतो, ज्यामुळे नेटवर्क संसाधनांची कॉन्फिडेन्शियलिटी /गोपनीयता (Confidentiality), इंटेग्रिटी /अखंडता (Integrity) आणि अव्हेलेबिलिटी / उपलब्धता (Availability) सुनिश्चित होते.

फायरवॉलची सामान्य क्रिया (Firewall actions) यामध्ये समाविष्ट आहेत:

- ॲक्सेप्ट (Accept): पॅकेट किंवा कनेक्शनला परवानगी देणे.
- रिजेक्ट (Reject): पॅकेट ब्लॉक करणे आणि त्रुटी प्रतिसाद पाठवणे (उदा. ICMP unreachable).
- ड्रॉप (Drop): प्रेषकाला कोणतीही माहिती न देता पॅकेट शांतपणे (silently) टाकून देणे.

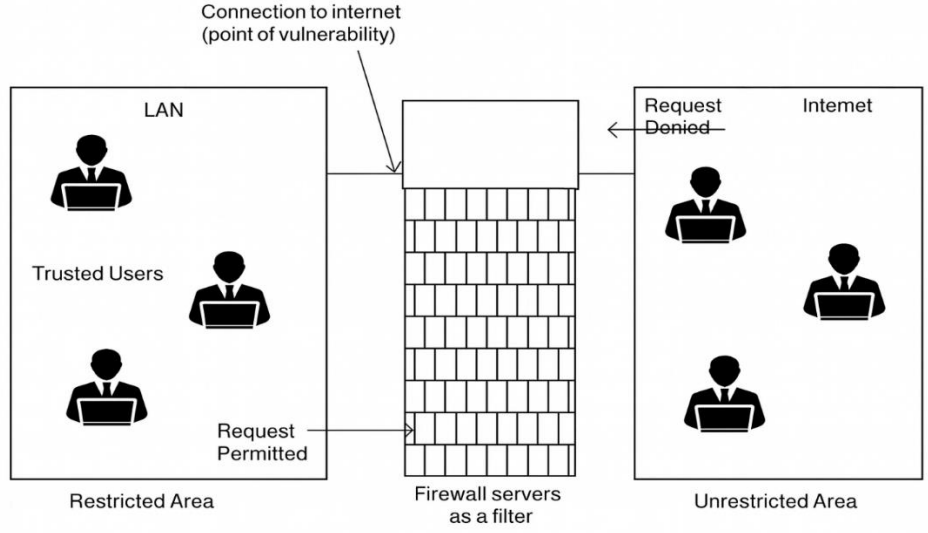


Fig 4.1: फायरवॉल आर्किटेक्चर आकृती (Firewall Architecture Diagram)

ही आकृती लोकल एरिया नेटवर्क (LAN) चे संरक्षण कसे केले जाते हे दर्शवते, जिथे फायरवॉल मर्यादित अंतर्गत क्षेत्र (प्रायव्हेट नेटवर्क) आणि अनियंत्रित इंटरनेट (पब्लिक नेटवर्क) यांच्यामध्ये सुरक्षा अडथळा म्हणून कार्य करतो. LAN मधील विश्वासार्ह (trusted) वापरकर्ते पाठवलेले विनंत्या फायरवॉलमधून जाण्यास परवानगी दिली जाते, तर फायरवॉल सर्व ट्रॅफिकचे काळजीपूर्वक फिल्टरिंग करतो. इंटरनेटवरील अविश्वसनीय (untrusted) वापरकर्त्यांकडून येणाऱ्या विनंत्या फायरवॉल ब्लॉक किंवा नाकारतो, ज्यामुळे अंतर्गत नेटवर्कमध्ये अनधिकृत प्रवेश रोखला जातो. LAN आणि इंटरनेट

यांच्यातील कनेक्शन पॉइंटला असुरक्षिततेचा बिंदू (point of vulnerability) म्हणून दर्शवले आहे, ज्यामुळे फायरवॉल नेटवर्क सुरक्षेसाठी किती आवश्यक आहे हे अधोरेखित होते. एकूणच, ही आकृती दाखवते की फायरवॉलमुळे LAN आणि बाह्य इंटरनेट यांच्यात केवळ सुरक्षित आणि अधिकृत कम्युनिकेशनच होऊ शकते.

4.1.1 फायरवॉलची गरज (Need of Firewall)

1. **अनधिकृत प्रवेश रोखण्यासाठी (To Prevent Unauthorized Access):** फायरवॉल अनधिकृत वापरकर्त्यांना अंतर्गत नेटवर्कमध्ये प्रवेश करण्यापासून रोखतो. तो येणाऱ्या पॅकेट्सचे फिल्टरिंग करतो आणि फक्त विश्वासार्ह ट्रॅफिकला परवानगी देतो.
   उदाहरण: पोर्ट 22 (SSH) वरचा सर्व बाह्य प्रवेश ब्लॉक करणे, ज्यामुळे हल्लेखोर अंतर्गत सर्व्हरमध्ये लॉग-इन करू शकत नाहीत.
2. **सुरक्षा धोरणे अंमलात आणण्यासाठी (To Enforce Security Policies):** संस्था कोणत्या सेवा (HTTP, DNS, ई-मेल इ.) परवानगीयोग्य आहेत हे नियमांद्वारे निश्चित करतात. फायरवॉल हे नियम सातत्याने लागू करतो.
   उदाहरण: वेब सर्व्हरसाठी फक्त पोर्ट 80/443 परवानगी देणे आणि इतर सर्व पोर्ट्स ब्लॉक करणे.
3. **इनबाउंड आणि आउटबाउंड ट्रॅफिक नियंत्रित करण्यासाठी (To Control Inbound and Outbound Traffic):** फायरवॉल नेटवर्कमध्ये येणारा आणि बाहेर जाणारा—दोन्ही प्रकारचा ट्रॅफिक मॉनिटर करतो. यामुळे डेटा लीक होणे टाळले जाते आणि घातक इनबाउंड ट्रॅफिक रोखला जातो.
   उदाहरण: LAN मधील मालवेअरने संवेदनशील डेटा बाहेरील हल्लेखोराकडे पाठवणे थांबवणे.
4. **मालवेअर आणि हल्ल्यांपासून संरक्षणासाठी (To Protect Against Malware and Attacks):** फायरवॉल पोर्ट स्कॅनिंग, DoS हल्ले किंवा संशयास्पद पॅकेट्स यांसारख्या घातक क्रियाकलापांची ओळख करून त्यांना ब्लॉक करतो.
   उदाहरण: वारंवार कनेक्शन प्रयत्न करणाऱ्या (port scan) IP कडील पॅकेट्स ड्रॉप करणे.
5. **नेटवर्क सेगमेंटेशन तयार करण्यासाठी (To Create Network Segmentation):** फायरवॉल नेटवर्कला विविध झोन्समध्ये (DMZ, अंतर्गत LAN, सर्व्हर झोन) विभागतो, ज्यामुळे सुरक्षा भंगाचा परिणाम कमी होतो.
   उदाहरण: वेब सर्व्हर DMZ मध्ये ठेवणे, जेणेकरून तो हॅक झाला तरी हल्लेखोर अंतर्गत LAN पर्यंत पोहोचू शकत नाही.
6. **लॉगिंग, मॉनिटरिंग आणि ऑडिटिंगसाठी (For Logging, Monitoring & Auditing):** फायरवॉल परवानगी दिलेला आणि नाकारलेला सर्व ट्रॅफिक लॉग करतो, जे घुसखोरी शोधण्यासाठी आणि फॉरेन्सिक तपासासाठी उपयुक्त ठरते.
   उदाहरण: संशयास्पद IP कडून वारंवार लॉग-इन प्रयत्न दर्शवणारे फायरवॉल लॉग्स.
7. **सुरक्षा धोके कमी करण्यासाठी आणि गोपनीय डेटा संरक्षित करण्यासाठी (To Reduce Security Risks & Protect Confidential Data):** घातक ट्रॅफिक ब्लॉक करून फायरवॉल संवेदनशील माहितीचे संरक्षण करतो आणि एकूण सायबरसिक्युरिटी धोके कमी करतो.
   उदाहरण: गोपनीय ग्राहक माहिती असलेल्या अंतर्गत डेटाबेसमध्ये बाह्य वापरकर्त्यांना प्रवेश मिळू न देणे.

4.1.2 फायरवॉलचे प्रकार (Types of Firewalls):

a. पॅकेट फिल्टर्स फायरवॉल (Packet Filters Firewall)

पॅकेट फिल्टरिंग फायरवॉल प्रत्येक येणाऱ्या (incoming) आणि जाणाऱ्या (outgoing) पॅकेटची स्वतंत्रपणे तपासणी करतो आणि पूर्वनिश्चित फिल्टरिंग नियमांनुसार ते परवानगी देतो किंवा ब्लॉक करतो. हा फायरवॉल मुख्यतः OSI मॉडेलच्या नेटवर्क लेयर (L3) आणि ट्रान्सपोर्ट लेयर (L4) वर कार्य करतो.

पॅकेट फिल्टर्स फायरवॉलची कार्ये (Function of Packet Filters Firewall):

1. हेडर माहितीवर आधारित पॅकेट्स फिल्टर करणे
   ते खालील गोष्टी तपासतात:
   - स्रोत IP पत्ता (Source IP Address)
   - गंतव्य IP पत्ता (Destination IP Address)

- प्रोटोकॉल (TCP, UDP, ICMP)
- स्रोत पोर्ट नंबर (Source Port Number)
- गंतव्य पोर्ट नंबर (Destination Port Number)
- TCP फ्लॅग्स (SYN, ACK इ.)

2. नियमसंचानुसार पॅकेट्सना परवानगी देणे किंवा ब्लॉक करणे
   क्रियेचे परिणाम खालीलप्रमाणे असू शकतात:
   - Accept → ट्रॅफिकला परवानगी देणे
   - Reject → ट्रॅफिक ब्लॉक करून त्रुटी संदेश पाठवणे
   - Drop → कोणताही प्रतिसाद न देता पॅकेट शांतपणे ब्लॉक करणे
3. मूलभूत सीमा सुरक्षा (Basic Boundary Security) प्रदान करणे
   LAN आणि इंटरनेट यांच्या मध्ये ठेवलेले असल्यामुळे, हे फायरवॉल अनधिकृत प्रवेश रोखण्यास मदत करतात.

पॅकेट फिल्टरिंगमध्ये वापरले जाणारे नियम (Rules Used in Packet Filtering)

पॅकेट फिल्टर्स ॲक्सेस **कंट्रोल लिस्ट्स** (ACLs) वापरतात. प्रत्येक नियमामध्ये खालील घटक असतात:

1. निवड निकष (Selection Criteria / Match Condition)
   उदाहरणे:
   - जर Source IP = 192.168.1.10
   - जर Protocol = TCP
   - जर Destination Port = 80
2. ॲक्शन फील्ड (Action Field)
   - ALLOW (Permit)
   - DENY (Block)

नियम वरून खाली (top to bottom) तपासले जातात आणि पहिला जुळणारा नियम अंतिम क्रिया ठरवतो.

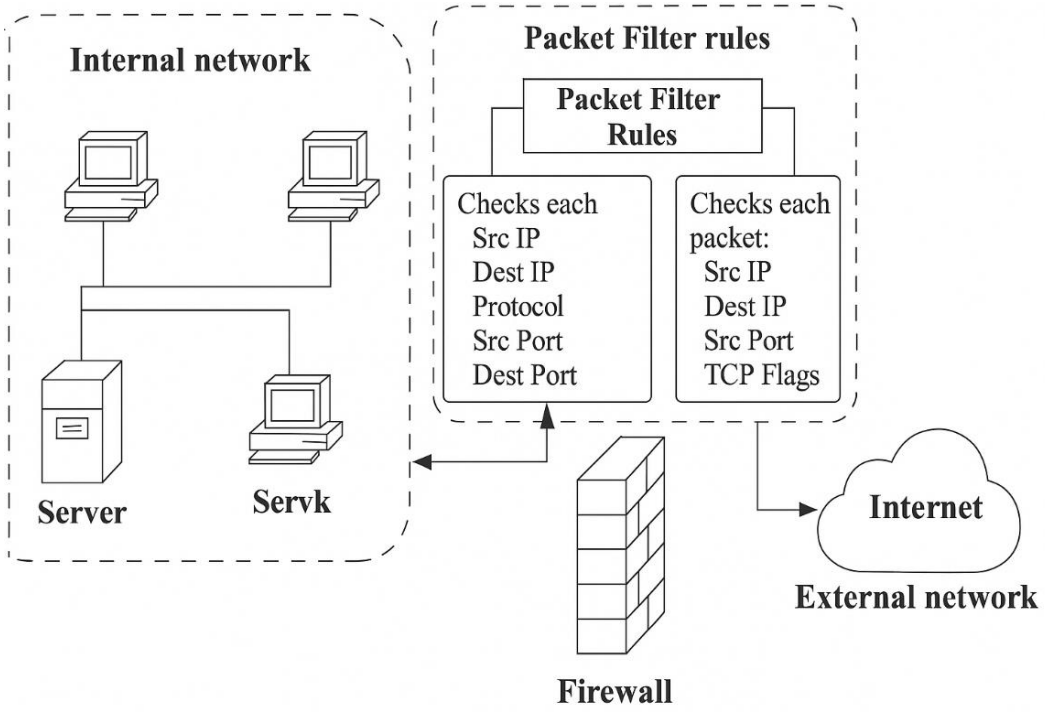


Fig 4.2: पॅकेट फिल्टरिंग फायरवॉल आर्किटेक्चर (Packet Filtering Firewall Architecture)

ही आकृती पॅकेट फिल्टरिंग फायरवॉलचे आर्किटेक्चर दर्शवते, जे अंतर्गत नेटवर्क आणि बाह्य इंटरनेट यांच्या मध्ये स्थित असते. अंतर्गत नेटवर्कमध्ये सर्व्हर्स आणि वर्कस्टेशन्स असतात, ज्यांचा सर्व ट्रॅफिक बाह्य नेटवर्कपर्यंत पोहोचण्यापूर्वी

फायरवॉलमधून जावा लागतो. या प्रणालीच्या केंद्रस्थानी पॅकेट फिल्टर राउटर असतो, जो पूर्वनिश्चित फिल्टरिंग नियमांचा संच वापरून प्रत्येक येणाऱ्या आणि जाणाऱ्या पॅकेटची तपासणी करतो.

हे नियम खालील महत्त्वाची हेडर माहिती तपासतात:

- सोर्स आयपी (Source IP)
- डेस्टिनेशन आयपी (Destination IP)
- प्रोटोकॉल (Protocol)
- सोर्स पोर्ट (Source Port)
- डेस्टिनेशन पोर्ट (Destination Port)
- TCP फ्लॅग्स (TCP Flags)

नेटवर्क, डेटा लिंक आणि फिजिकल लेयर्सवर ही माहिती तपासून, फायरवॉल केवळ वैध आणि सुरक्षित ट्रॅफिकलाच परवानगी देतो, ज्यामुळे बाह्य नेटवर्कमधून येणाऱ्या अनधिकृत प्रवेश आणि संभाव्य धोक्यांपासून अंतर्गत नेटवर्कचे संरक्षण होते.

b. स्टेटफुल पॅकेट फिल्टर्स फायरवॉल (Stateful Packet Filters Firewall)

स्टेटफुल पॅकेट फिल्टरिंग फायरवॉल हा साध्या पॅकेट फिल्टर्सपेक्षा अधिक प्रगत असून, तो पॅकेट हेडर्स तपासण्याबरोबरच नेटवर्क कनेक्शन्सची स्थिती (state) — जसे की TCP स्ट्रीम्स — यांचे निरीक्षण करतो. स्टेटलेस फिल्टर्सप्रमाणे प्रत्येक पॅकेट स्वतंत्रपणे न तपासता, स्टेटफुल फायरवॉल स्टेट टेबल राखतो, ज्यामध्ये सक्रिय सत्रे (active sessions) आणि त्यांची वैशिष्ट्ये नोंदवलेली असतात. यामुळे फायरवॉल अधिक हुशार आणि संदर्भ-जाणून (context-aware) निर्णय घेऊ शकतो. स्टेटफुल फायरवॉल प्रामुख्याने OSI मॉडेलच्या नेटवर्क लेयर (L3) आणि ट्रान्सपोर्ट लेयर (L4) वर कार्य करतात, परंतु त्यांची निर्णय प्रक्रिया अनेक पॅकेट्समधील कनेक्शन वर्तन ट्रॅक करण्यावर आधारित असते.

स्टेटफुल पॅकेट फिल्टर्सची कार्ये (Function of Stateful Packet Filters)

1. सक्रिय कनेक्शन्सची स्थिती ट्रॅक करणे (Track the state of active connections)
   फायरवॉल स्टेट टेबल राखतो, ज्यामध्ये खालील तपशील असतात:
   - स्रोत आणि गंतव्य IP पत्ते
   - स्रोत आणि गंतव्य पोर्ट क्रमांक
   - TCP कनेक्शनची स्थिती (SYN-SENT, ESTABLISHED, FIN-WAIT इ.)
   - पॅकेट सिक्वेन्स नंबर

   यामुळे एखादे पॅकेट वैध आणि स्थापित (established) सत्राचा भाग आहे की नाही हे फायरवॉल ठरवू शकतो.
2. नियम आणि कनेक्शन स्थिती यांच्या आधारे पॅकेट्सना परवानगी देणे किंवा ब्लॉक करणे
   नियम-आधारित फिल्टरिंगसोबत (stateless filters प्रमाणे), स्टेटफुल फायरवॉल खालील बाबी तपासतो:
   - पॅकेट एखाद्या विद्यमान सत्राशी (existing session) जुळते का
   - ते वैध कनेक्शनची सुरुवात (valid connection initiation) आहे का
   - ते अपेक्षित प्रोटोकॉल वर्तनाशी (expected protocol behavior) सुसंगत आहे का

   आधीच मंजूर (approved) सत्राशी संबंधित पॅकेट्सना जलद प्रक्रियेसह परवानगी दिली जाते.
3. अनधिकृत किंवा घातक कनेक्शन्स रोखणे (Prevent unauthorized or malicious connections)
   स्टेटफुल फिल्टरिंग खालील हल्ले रोखण्यास मदत करते:
   - IP Spoofing
   - अनधिकृत सत्र इंजेक्शन (Unauthorized Session Injection)
   - हाफ-ओपन कनेक्शन एक्स्प्लॉइट्स (Half-open Connection Exploits)

   फायरवॉल केवळ स्टेट टेबलमध्ये नोंदवलेल्या सत्र स्थितीशी सुसंगत असलेली पॅकेट्सच परवानगी देतो.

स्टेटफुल पॅकेट फिल्टरिंगमध्ये वापरले जाणारे नियम (Rules Used in Stateful Packet Filtering)

स्टेटफुल फायरवॉल देखील ॲक्सेस कंट्रोल लिस्ट्स (ACLs) वापरतात, परंतु त्यामध्ये कनेक्शन जागरूकता (connection awareness) समाविष्ट असते.

प्रत्येक नियमामध्ये खालील घटक असतात:

1. निवड निकष (Selection Criteria / Match Condition)
   उदाहरणे:
   - जर Protocol = TCP AND State = NEW
   - जर Destination Port = 443 AND State = ESTABLISHED
   - जर येणारे पॅकेट कोणत्याही सक्रिय सत्राशी जुळत नसेल → DROP
2. ॲक्शन फील्ड (Action Field)
   - ALLOW (जर नियम जुळला आणि स्थिती वैध असेल)
   - DENY (जर नियम किंवा स्थिती अवैध असेल)

   फायरवॉल सक्रिय सत्रे ट्रॅक करत असल्यामुळे, स्टेटलेस फिल्टर्सच्या तुलनेत कमी स्पष्ट नियमांची गरज असते.

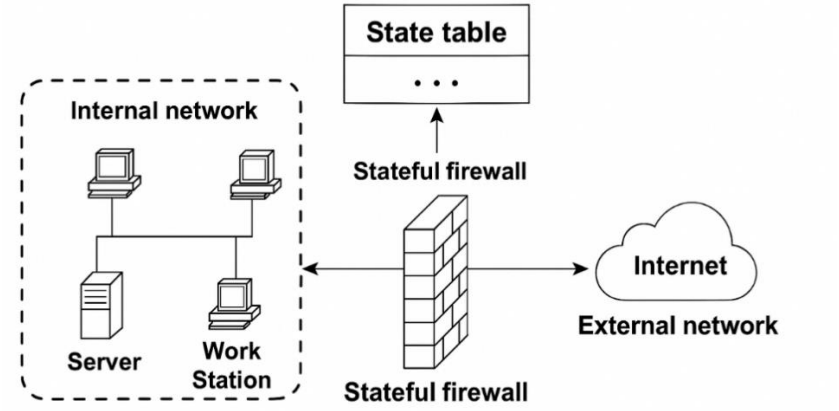


Fig 4.3: स्टेटफुल पॅकेट फिल्टरिंग आर्किटेक्चर (Stateful Packet Filtering Architecture)

या आर्किटेक्चरमध्ये खालील घटक असतात:

- अंतर्गत नेटवर्क (सर्व्हर्स, वर्कस्टेशन्स)
- LAN आणि इंटरनेटच्या मध्ये असलेला स्टेटफुल इन्स्पेक्शन फायरवॉल
- फायरवॉलमधील स्टेट टेबल, ज्यामध्ये सक्रिय सत्रांची नोंद ठेवली जाते
- रूल इंजिन, जे ACLs लागू करते

पॅकेट्सचा प्रवाह कसा होतो (How packets flow):

1. नवीन कनेक्शनचा प्रयत्न झाल्यास (उदा. SYN पॅकेट), फायरवॉल नियम तपासतो.
2. परवानगी दिल्यास, स्टेट टेबलमध्ये नवीन स्टेट एन्ट्री तयार केली जाते.
3. पुढील पॅकेट्स (SYN-ACK, ACK, डेटा, FIN) स्टेट टेबलशी जुळवली जातात.
4. जर पॅकेट कोणत्याही ओळखल्या गेलेल्या सत्राचा भाग नसेल किंवा अपेक्षित स्थितीचे उल्लंघन करत असेल → ते ड्रॉप केले जाते.

यामुळे साध्या पॅकेट फिल्टरिंगपेक्षा अधिक मजबूत सुरक्षा मिळते.

3. ॲप्लिकेशन गेटवेज़ फायरवॉल (Application Gateways Firewall)

ॲप्लिकेशन गेटवे, ज्याला ॲप्लिकेशन-लेव्हल गेटवे किंवा प्रॉक्सी फायरवॉल असेही म्हणतात, हा असा फायरवॉल आहे जो OSI मॉडेलच्या ॲप्लिकेशन लेयर (लेयर 7) वर कार्य करतो. अंतर्गत आणि बाह्य होस्ट्समध्ये थेट संवाद होऊ न देता, हा गेटवे मध्यस्थ (Proxy) म्हणून काम करतो. तो ॲप्लिकेशन-विशिष्ट ट्रॅफिक स्वीकारतो, तपासतो आणि पुढे पाठवतो. डेटाचा प्रत्यक्ष मजकूर (फक्त हेडर्स नव्हे) तपासला जात असल्यामुळे, हा फायरवॉल डीप पॅकेट इन्स्पेक्शन प्रदान करतो आणि पॅकेट फिल्टर्स व स्टेटफुल फिल्टर्सपेक्षा अधिक मजबूत सुरक्षा देतो.

ॲप्लिकेशन गेटवेज़ची कार्ये (Function of Application Gateways)

1. अंतर्गत आणि बाह्य होस्ट्समधील ट्रॅफिकचे प्रॉक्सींग करणे
   गेटवे दोन स्वतंत्र कनेक्शन्स तयार करतो:
   - एक अंतर्गत क्लायंट आणि गेटवे यांच्यात

- दुसरे गेटवे आणि बाह्य सर्व्हर यांच्यात

यामुळे विश्वासार्ह नेटवर्क आणि अविश्वसनीय बाह्य नेटवर्क यांच्यात थेट संपर्क होत नाही.

2. ॲप्लिकेशन-लेयर डेटाची तपासणी करणे
   हे फायरवॉल फक्त IP किंवा पोर्ट माहिती नव्हे, तर संदेशातील प्रत्यक्ष मजकूर तपासू शकतात.
   तपासता येणारे प्रोटोकॉल्स:
   - HTTP
   - FTP
   - Telnet
   - SMTP
3. कठोर वापरकर्ता प्रमाणीकरण अंमलात आणणे
   ट्रॅफिकला परवानगी देण्यापूर्वी गेटवे खालील गोष्टी मागू शकतो:
   - वापरकर्तानाव / पासवर्ड
   - वन-टाइम PIN
   - मल्टी-फॅक्टर ऑथेन्टिकेशन
4. ॲप्लिकेशन-लेयर हल्ल्यांपासून संरक्षण देणे
   डीप इन्स्पेक्शनमुळे खालील गोष्टी ओळखता येतात:
   - घातक कमांड्स (उदा. FTP, SMTP मध्ये)
   - SQL Injection प्रयत्न
   - असुरक्षित HTTP मेथड्स
   - मालवेअर-इंजेक्टेड पेलोड्स

ॲप्लिकेशन गेटवेज़मध्ये वापरले जाणारे नियम (Rules Used in Application Gateways)

ॲप्लिकेशन गेटवे साध्या IP/पोर्ट नियमांऐवजी ॲप्लिकेशन-विशिष्ट नियम वापरतात.

1. निवड निकष (Selection Criteria / Match Condition)
   उदाहरणे:
   - जर HTTP रिक्वेस्टमध्ये ब्लॉक केलेले URL कीवर्ड्स असतील
   - जर FTP कमांड = PUT (फक्त GET ला परवानगी)
   - जर ई-मेल ॲटॅचमेंटमध्ये executable फाइल्स असतील
2. ॲक्शन फील्ड (Action Field)
   - ॲप्लिकेशन रिक्वेस्टला ALLOW करणे
   - रिक्वेस्ट DENY करणे
   - संशयास्पद वर्तन LOG करणे
   - ॲडमिनिस्ट्रेटर्सना ALERT देणे

हे नियम पॅकेट फिल्टर्सपेक्षा खूपच खोल स्तरावर कार्य करतात.

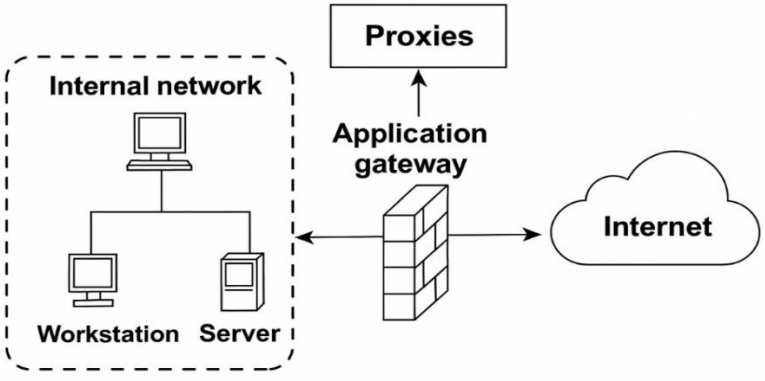


Fig 4.4: ॲप्लिकेशन गेटवे आर्किटेक्चर (Application Gateway Architecture)

- अंतर्गत क्लायंट्स (वापरकर्ते) ॲप्लिकेशन रिक्वेस्ट्स पाठवतात
- LAN आणि इंटरनेटच्या सीमारेषेवर असलेला ॲप्लिकेशन गेटवे / प्रॉक्सी सर्व्हर
- गेटवे रिक्वेस्ट्स स्वीकारतो, त्यांची पडताळणी करतो आणि पुढे फॉरवर्ड करतो
- बाह्य सर्व्हर्स फक्त प्रॉक्सीशीच संवाद साधतात, अंतर्गत नेटवर्कशी थेट कधीही नाही

प्रॉक्सी ॲप्लिकेशन लेयरवर संपूर्ण संदेशांची तपासणी करतो आणि त्यानंतरच त्यांना पुढे जाण्याची परवानगी देतो. यामुळे केवळ सुरक्षित, वैध आणि पॉलिसीनुसार असलेलाच ट्रॅफिक बाह्य गंतव्यापर्यंत पोहोचतो.

d. सर्किट गेटवेज़ (Circuit Gateways / Circuit-Level Firewalls)

सर्किट गेटवे, ज्याला सर्किट-लेव्हल गेटवे असेही म्हणतात, हा असा फायरवॉल आहे जो OSI मॉडेलच्या ट्रान्सपोर्ट लेयर (लेयर 4) वर कार्य करतो. हा फायरवॉल प्रत्यक्ष ॲप्लिकेशन डेटा तपासत नाही; त्याऐवजी TCP/UDP सत्र स्थापन प्रक्रियेचे (session setup) निरीक्षण करून कनेक्शन वैध आहे की नाही हे ठरवतो. सर्किट गेटवे अंतर्गत आणि बाह्य होस्ट्समध्ये थेट एंड-टू-एंड कनेक्शनला परवानगी देत नाही. त्याऐवजी, तो दोन टोकांदरम्यान व्हर्च्युअल सर्किट तयार करतो आणि डेटा पेलोड तपासणी न करता पॅकेट्स रिले करतो. म्हणूनच, यांना कधी कधी "पाईप प्रॉक्सीज़ (pipe proxies)" असेही म्हटले जाते.

सर्किट गेटवेज़ची कार्ये (Function of Circuit Gateways)

1. सत्र सुरूवातीची पडताळणी करणे (Validate Session Initiation)
   हे फायरवॉल TCP थ्री-वे हँडशेक तपासतात:
   - SYN
   - SYN-ACK
   - ACK

   जर हँडशेक वैध असेल आणि फायरवॉल नियमांशी जुळत असेल, तर सर्किट स्थापन केले जाते.
2. दोन स्वतंत्र TCP कनेक्शन्स तयार करणे
   एक कनेक्शन: अंतर्गत क्लायंट → गेटवे
   दुसरे कनेक्शन: गेटवे → बाह्य सर्व्हर
   फायरवॉल या दोन्ही कनेक्शन्समध्ये पॅकेट्स रिले करतो, परंतु पेलोड डेटा तपासत नाही.
3. सत्र स्थितीवर आधारित मूलभूत फिल्टरिंग अंमलात आणणे
   हे फायरवॉल खालील गोष्टी तपासतात:
   - कनेक्शन रिक्वेस्ट्स (NEW connection)
   - स्थापित सत्रे (Established sessions)

   अवैध किंवा चुकीच्या स्वरूपातील (malformed) सत्र प्रयत्न ब्लॉक केले जातात.
4. अनामिकता (Anonymity) प्रदान करणे
   बाह्य सर्व्हर्सना फक्त गेटवेचा IP पत्ता दिसतो, अंतर्गत होस्टचा IP पत्ता दिसत नाही.

सर्किट-लेव्हल गेटवेज़मध्ये वापरले जाणारे नियम (Rules Used in Circuit-Level Gateways)

सर्किट-लेव्हल गेटवे ॲप्लिकेशन गेटवेच्या तुलनेत **सोपे नियमसंच** वापरतात.

1. निवड निकष (Selection Criteria / Match Condition)
   उदाहरणे:
   - जर State = NEW AND Destination Port = 443
   - जर State = ESTABLISHED (TCP साठी)
   - जर सत्र सुरूवात अवैध असेल → DENY
2. ॲक्शन फील्ड (Action Field)
   - सत्राला ALLOW करणे
   - सत्र DENY करणे
   - कनेक्शन प्रयत्न LOG करणे

सर्किट गेटवे प्रामुख्याने सत्र माहितीवर अवलंबून असल्यामुळे, कमी नियमांची गरज असते.

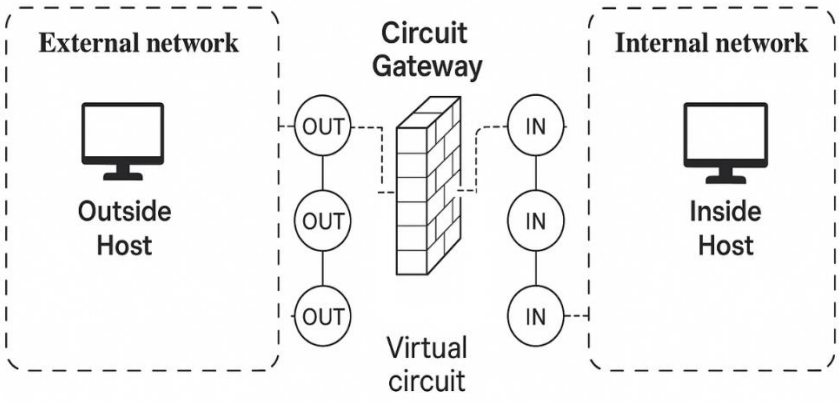


Fig 4.5: सर्किट गेटवे आर्किटेक्चर (Circuit Gateway Architecture)

ही आकृती सर्किट गेटवे कसा बाह्य होस्ट आणि अंतर्गत होस्ट यांच्या मध्ये स्थित असतो हे दर्शवते, जिथे संवादासाठी एक सुरक्षित व्हर्च्युअल सर्किट तयार केले जाते. बाह्य नेटवर्कमधील ट्रॅफिक "OUT" पोर्ट्समधून प्रवेश करते, गेटवे द्वारे प्रक्रिया केली जाते आणि नंतर संबंधित "IN" पोर्ट्समधून अंतर्गत नेटवर्ककडे फॉरवर्ड केली जाते. गेटवे सेशन लेयरवर कनेक्शनची पडताळणी करतो, ज्यामुळे बाह्य होस्ट्स कधीही थेट अंतर्गत होस्ट्सपर्यंत पोहोचू शकत नाहीत. यामुळे नियंत्रित आणि सुरक्षित कम्युनिकेशन सुनिश्चित होते.

Table 4.1: हार्डवेअर फायरवॉल आणि सॉफ्टवेअर फायरवॉल यांमधील फरक (Difference between Hardware Firewall and Software Firewall)

मुद्दा (Point)	हार्डवेअर फायरवॉल (Hardware Firewall)	सॉफ्टवेअर फायरवॉल (Software Firewall)
व्याख्या (Definition)	अंतर्गत नेटवर्क आणि बाह्य नेटवर्क यांच्यामध्ये ठेवलेले ट्रॅफिक फिल्टर करणारे भौतिक उपकरण.	संगणक किंवा सर्व्हरवर इन्स्टॉल केलेला प्रोग्राम जो स्थानिक ट्रॅफिकचे निरीक्षण व नियंत्रण करतो.
स्थान (Location)	नेटवर्कच्या सीमारेषेवर (Network Perimeter) कार्य करते.	होस्ट संगणकावर (वैयक्तिक सिस्टिमवर) कार्य करते.
डिप्लॉयमेंट (Deployment)	संपूर्ण नेटवर्कचे एकाच वेळी संरक्षण करते.	ज्या डिव्हाइसवर इन्स्टॉल आहे त्याच डिव्हाइसचे संरक्षण करते.
कार्यक्षमता (Performance)	साधारणतः जलद; समर्पित हार्डवेअर वापरते, सिस्टिम लोड कमी करते.	CPU आणि RAM वापरत असल्यामुळे सिस्टिम मंद होऊ शकते.
सेटअप व कॉन्फिगरेशन (Setup & Configuration)	अधिक गुंतागुंतीचे; नेटवर्किंग ज्ञान आवश्यक.	सामान्य सॉफ्टवेअरप्रमाणे इन्स्टॉल व कॉन्फिगर करणे सोपे.
सुरक्षेची पातळी (Security Level)	नेटवर्क-स्तरावर मजबूत व सातत्यपूर्ण संरक्षण देते.	वैयक्तिक सिस्टिम-स्तरावर संरक्षण देते.
ट्रॅफिक मॉनिटरिंग (Traffic Monitoring)	मोठ्या प्रमाणातील ट्रॅफिक मॉनिटर करते; संस्थांसाठी योग्य.	एका होस्टसाठी ट्रॅफिक मॉनिटर करते.
उदाहरण उपकरणे/सॉफ्टवेअर (Examples)	Cisco ASA, SonicWall, Fortinet, WatchGuard.	Windows Defender Firewall, ZoneAlarm, Norton Firewall.
अंतर्गत धोकेपासून संरक्षण (Protection from Internal Threats)	कमी प्रभावी; प्रामुख्याने बाह्य धोक्यांपासून संरक्षण.	अंतर्गत नेटवर्कमधील धोक्यांपासून डिव्हाइसचे प्रभावी संरक्षण.
स्केलेबिलिटी (Scalability)	अनेक डिव्हाइसेस व नेटवर्कसाठी उच्च स्केलेबिलिटी.	एका होस्ट डिव्हाइसच्या क्षमतेपुरती मर्यादित.

4.2 फायरवॉल पॉलिसीज (Firewall policies)

4.2.1 फायरवॉल पॉलिसीज (Firewall Policies)

फायरवॉल पॉलिसी म्हणजे नियमांचा संच जो फायरवॉल नेटवर्क ट्रॅफिकचे निरीक्षण, फिल्टरिंग आणि नियंत्रण कसे करेल हे ठरवतो. हे नियम LAN, DMZ आणि इंटरनेट यांसारख्या वेगवेगळ्या नेटवर्क झोन्समधील कोणत्या प्रकारचा ट्रॅफिक परवानगीयोग्य आहे किंवा नाकारला जाईल हे निश्चित करतात. सुयोग्यरित्या डिझाइन केलेली फायरवॉल पॉलिसी नेटवर्क सुरक्षा वाढवते, धोके कमी करते आणि फायरवॉलची कार्यक्षमता सुधारते.

1. लीस्ट प्रिव्हिलेज पॉलिसी वापरा – फक्त आवश्यक ट्रॅफिकला परवानगी द्या; उर्वरित सर्व ट्रॅफिक नाकारून अटॅक सर्फेस कमी करा.
2. तार्किक विभागणी करा – नेटवर्कला झोन्समध्ये (LAN, DMZ इ.) विभाजित करा, जेणेकरून ट्रॅफिक फ्लो नियंत्रित करता येईल.
3. विशिष्ट नियम आधी ठेवा – फायरवॉल नियम वरून खाली प्रक्रिया करतो, त्यामुळे विशिष्ट नियम सामान्य नियमांपूर्वी असणे आवश्यक आहे.
4. ॲड्रेस सेट्स वापरा – अनेक IP पत्ते किंवा नेटवर्क्स गटबद्ध करून स्वतंत्र नियमांची संख्या कमी करा.
5. सर्व्हिस सेट्स वापरा – संबंधित सेवा (HTTP, HTTPS, DNS) एकत्र करून पॉलिसी तयार करणे सोपे करा आणि मेमरी वापर कमी करा.
6. कमी झोन पेअर्स वापरा – स्रोत–गंतव्य झोन संयोजन कमी ठेवल्याने मेमरी वाचते आणि कार्यक्षमता वाढते.
7. स्पष्ट ड्रॉप नियम वापरा – शेवटी "deny all" नियम जोडा, जेणेकरून वर्गीकृत न झालेला किंवा नको असलेला ट्रॅफिक ब्लॉक होईल.
8. लॉगिंग वापरा – ऑडिटिंग आणि ट्रबलशूटिंगसाठी फायरवॉल क्रियाकलापांचे लॉग ठेवा (प्राधान्याने session close logging).
9. नेटवर्क टाइम प्रोटोकॉल (NTP) वापरा – अचूक लॉग्स आणि पॉलिसी शेड्युलिंगसाठी फायरवॉलचा वेळ समक्रमित ठेवा.
10. मेमरी वापर तपासा – पॉलिसी लागू करण्यापूर्वी आणि नंतर मेमरी वापर मॉनिटर करा, जेणेकरून परफॉर्मन्स समस्या टाळता येतील.

4.2.2 फायरवॉल कॉन्फिगरेशन (Firewall Configuration)

फायरवॉल खालील तीन सामान्य आर्किटेक्चर्स वापरून कॉन्फिगर केला जाऊ शकतो. या प्रत्येकामध्ये पॅकेट फिल्टरिंग आणि गेटवे सेवांचा वापर करून अंतर्गत नेटवर्कचे संरक्षण केले जाते.

ही कॉन्फिगरेशन्स आहेत:

1. स्क्रीनड होस्ट फायरवॉल – सिंगल-होम्ड बॅस्टियन होस्ट
2. स्क्रीनड होस्ट फायरवॉल – ड्युअल-होम्ड बॅस्टियन होस्ट
3. स्क्रीनड सबनेट फायरवॉल कॉन्फिगरेशन

1. स्क्रीनड होस्ट फायरवॉल – सिंगल-होम्ड बॅस्टियन कॉन्फिगरेशन (Single-Homed Bastion Configuration)

या कॉन्फिगरेशनमध्ये फायरवॉलमध्ये खालील दोन मुख्य घटक असतात:

1. पॅकेट-फिल्टरिंग राउटर
2. ॲप्लिकेशन गेटवे (बॅस्टियन होस्ट)

कार्यपद्धती (Working):

- पॅकेट-फिल्टरिंग राउटर प्रत्येक येणाऱ्या पॅकेटचा डेस्टिनेशन IP पत्ता तपासून फक्त ॲप्लिकेशन गेटवेकडे जाणाऱ्या ट्रॅफिकला परवानगी देतो.
- त्याचप्रमाणे, प्रत्येक जाणाऱ्या पॅकेटचा सोर्स IP पत्ता तपासून फक्त ॲप्लिकेशन गेटवेकडून येणाऱ्या ट्रॅफिकला परवानगी देतो.
- ॲप्लिकेशन गेटवे ऑथेन्टिकेशन आणि प्रॉक्सी कार्ये पार पाडतो.

मर्यादा (Limitation):

अंतर्गत वापरकर्ते पॅकेट फिल्टर आणि ॲप्लिकेशन गेटवे या दोन्हींशी जोडलेले असतात. त्यामुळे जर पॅकेट-फिल्टरिंग राउटर कॉम्प्रोमाइज झाला, तर संपूर्ण अंतर्गत नेटवर्क हल्लेखोरासाठी उघडे पडू शकते.

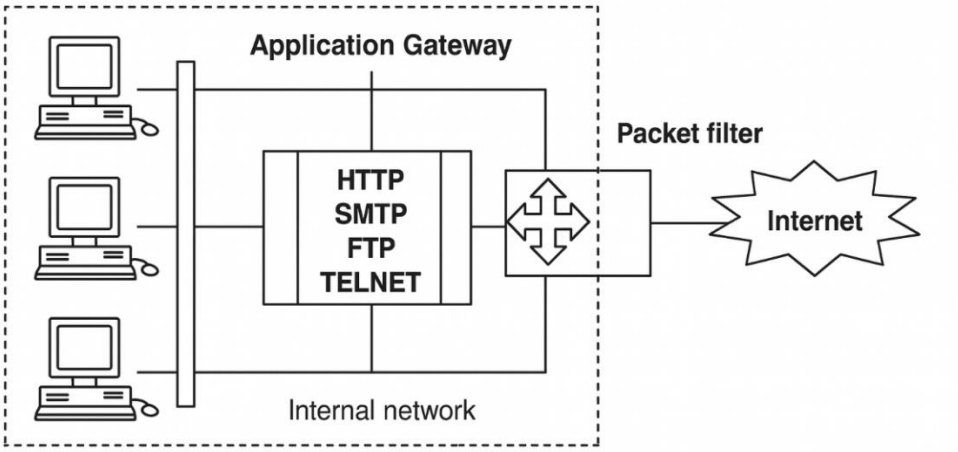


Fig 4.6: सिंगल-होम्ड बॅस्टियन कॉन्फिगरेशन (Single-Homed Bastion Configuration)

2. स्क्रीनड होस्ट फायरवॉल – ड्युअल-होम्ड बॅस्टियन कॉन्फिगरेशन (Screened Host Firewall – Dual-Homed Bastion Configuration)

ही कॉन्फिगरेशन सिंगल-होम्ड बॅस्टियन सेटअपमधील मर्यादा दूर करण्यासाठी डिझाइन करण्यात आली आहे.

कार्यपद्धती (Working):

- या सेटअपमध्ये अंतर्गत होस्ट्स आणि पॅकेट-फिल्टरिंग राउटर यांच्यातील थेट कनेक्शन्स काढून टाकली जातात.
- पॅकेट फिल्टर फक्त ॲप्लिकेशन गेटवेशी जोडलेला असतो, तर ॲप्लिकेशन गेटवे अंतर्गत नेटवर्कशी स्वतंत्र कनेक्शन ठेवतो.
- जर पॅकेट फिल्टर कॉम्प्रोमाइज झाला, तरी हल्लेखोराला फक्त ॲप्लिकेशन गेटवेच दिसतो आणि अंतर्गत होस्ट्स सुरक्षित राहतात.

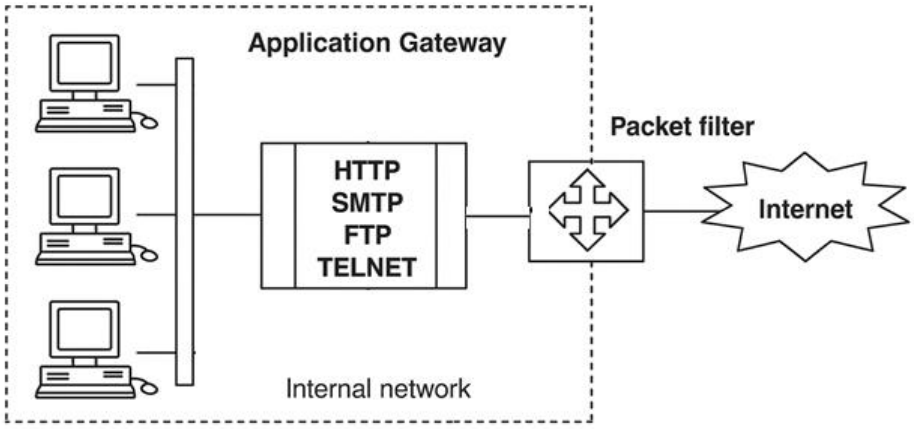


Fig 4.7: ड्युअल-होम्ड बॅस्टियन कॉन्फिगरेशन (Dual-Homed Bastion Configuration)

3. स्क्रीनड सबनेट फायरवॉल कॉन्फिगरेशन (Screened Subnet Firewall Configuration)

ही कॉन्फिगरेशन सर्व फायरवॉल आर्किटेक्चर्सपैकी सर्वाधिक सुरक्षा स्तर प्रदान करते.

कार्यपद्धती (Working):

- या सेटअपमध्ये दोन पॅकेट फिल्टर्स वापरले जातात:
  1. इंटरनेट आणि ॲप्लिकेशन गेटवे यांच्यामध्ये एक
  2. ॲप्लिकेशन गेटवे आणि अंतर्गत नेटवर्क यांच्यामध्ये दुसरा
- यामुळे एक स्वतंत्र स्क्रीनड सबनेट तयार होते, ज्याला सामान्यतः DMZ (डिमिलिट्राइझ्ड झोन) असे म्हणतात.

- परिणामी, हल्लेखोराला तीन सुरक्षा स्तर (layers of defense) पार करावे लागतात, ज्यामुळे एकूण सुरक्षा लक्षणीयरीत्या वाढते.

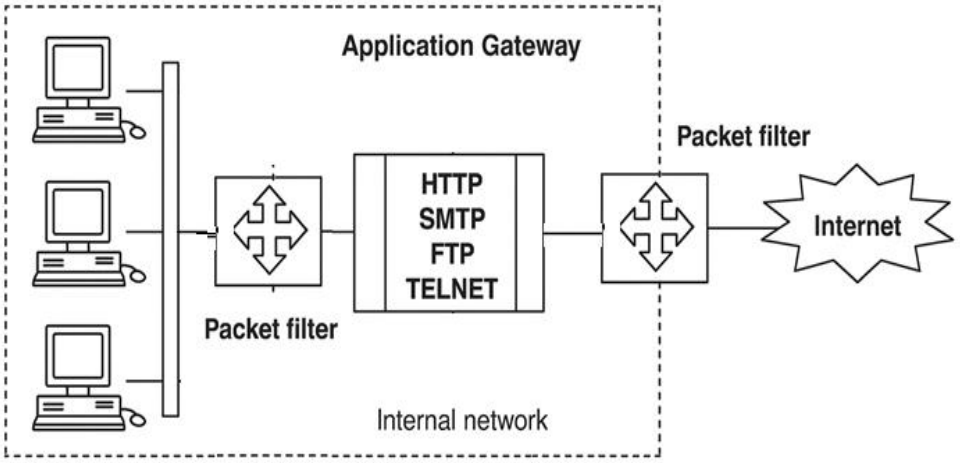


Fig 4.8: स्क्रीनड सबनेट फायरवॉल कॉन्फिगरेशन (Screened Subnet Firewall Configuration)

4.2.3 मर्यादा (Limitations)

1. फायरवॉल अंतर्गत धोक्यांपासून संरक्षण करू शकत नाहीत – ते प्रामुख्याने बाह्य ट्रॅफिक मॉनिटर करतात, अंतर्गत वापरकर्त्यांच्या गैरवापरावर नियंत्रण ठेवत नाहीत.
   उदाहरण: कर्मचारी जाणीवपूर्वक फाइल्स डिलीट करतो.
2. परवानगी दिलेल्या सेवांमधून होणारे हल्ले फायरवॉल रोखू शकत नाही – जर एखादी सेवा परवानगीयोग्य असेल, तर घातक ट्रॅफिकही त्यातून जाऊ शकते.
   उदाहरण: HTTPS (443) पोर्ट खुला असल्यामुळे मालवेअर आत प्रवेश करते.
3. पॅकेट फिल्टर्स पेलोड / कंटेंट तपासत नाहीत – ते फक्त IP, पोर्ट आणि प्रोटोकॉल हेडर्स तपासतात.
   उदाहरण: HTTP मधील घातक स्क्रिप्ट फायरवॉलमधून पास होते.
4. एन्क्रिप्टेड ट्रॅफिकची तपासणी शक्य नाही – SSL/TLS एन्क्रिप्टेड पॅकेट्समधील मजकूर फायरवॉल पाहू शकत नाही.
   उदाहरण: एन्क्रिप्टेड ट्रॅफिकमध्ये लपलेला व्हायरस फायरवॉल बायपास करतो.
5. प्रोटोकॉल टनेलिंगमुळे फायरवॉल नियम बायपास होऊ शकतात – हल्लेखोर परवानगी असलेल्या प्रोटोकॉलमध्ये ट्रॅफिक लपवतात.
   उदाहरण: HTTP मध्ये टनेल केलेले मालवेअर फिल्टरिंग टाळते.
6. वापरकर्त्याद्वारे आणलेले मालवेअर फायरवॉल थांबवू शकत नाही – फायरवॉल फाइल्स किंवा अॅटॅचमेंट्स व्हायरससाठी स्कॅन करत नाही.
   उदाहरण: वापरकर्ता ई-मेलमधून संक्रमित फाइल डाउनलोड करतो.
7. वैध क्रेडेन्शियल्स वापरून होणारे हल्ले रोखता येत नाहीत – ऑथेन्टिकेटेड ट्रॅफिक फायरवॉलला वैध वाटतो.
   उदाहरण: हॅकर चोरी केलेले युजरनेम/पासवर्ड वापरून लॉग-इन करतो.
8. विश्वसनीय होस्ट्समधील घातक क्रियाकलाप ओळखता येत नाहीत – अंतर्गत कॉम्प्रोमाइज झालेले सिस्टिम्स सुरक्षित मानले जातात.
   उदाहरण: संक्रमित अंतर्गत PC LAN वर हल्ले सुरू करतो.
9. योग्य कॉन्फिगरेशनवर मोठ्या प्रमाणात अवलंबित्व – चुकीचे कॉन्फिगरेशन फायरवॉलची सुरक्षा कमी करू शकते.
   उदाहरण: अॅडमिन चुकून सर्व इनबाउंड ट्रॅफिकला परवानगी देतो.
10. सोशल इंजिनिअरिंग हल्ले थांबवता येत नाहीत – हे हल्ले मानवी वर्तनावर आधारित असतात, नेटवर्क ट्रॅफिकवर नाहीत.
    उदाहरण: वापरकर्ता फिशिंग कॉलरला पासवर्ड सांगतो.

4.2.4 डिमिलिट्राइझ्ड झोन (DMZ)

डिमिलिट्राइझ्ड झोन (DMZ) हा कंपनीच्या खाजगी अंतर्गत नेटवर्क (LAN) आणि सार्वजनिक बाह्य नेटवर्क (इंटरनेट) यांच्या मध्ये ठेवलेला एक विशेष नेटवर्क विभाग आहे. तो बफर किंवा न्यूट्रल झोन म्हणून कार्य करतो, ज्यामुळे बाह्य वापरकर्त्यांना अंतर्गत सिस्टिम्समध्ये थेट प्रवेश करता येत नाही.

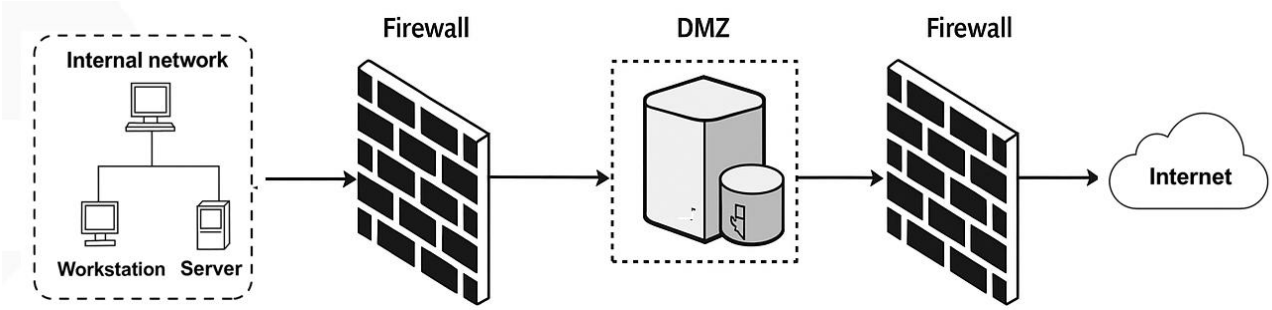


Fig 4.9: डिमिलिट्राइझ्ड झोन (DMZ)

ही आकृती एक सुरक्षित नेटवर्क आर्किटेक्चर दर्शवते, जिथे वर्कस्टेशन्स आणि सर्व्हर्स असलेले अंतर्गत नेटवर्क इंटरनेटशी जोडण्यापूर्वी अनेक सुरक्षा स्तरांनी संरक्षित केलेले असते. अंतर्गत नेटवर्कमधून बाहेर जाणारा ट्रॅफिक प्रथम फायरवॉलमधून जातो, जो प्रवेश फिल्टर करून फक्त अधिकृत कम्युनिकेशनलाच परवानगी देतो. त्यानंतर तो DMZ (डिमिलिट्राइझ्ड झोन) मध्ये पोहोचतो, जो एक अर्ध-संरक्षित (semi-protected) क्षेत्र आहे आणि पब्लिक-फेसिंग सिस्टिम्स होस्ट करतो, परंतु त्यांना अंतर्गत नेटवर्कपासून वेगळे ठेवतो. DMZ नंतर ट्रॅफिक दुसऱ्या फायरवॉलमधून जातो, जो इंटरनेटपर्यंत पोहोचण्यापूर्वी आणखी एक संरक्षण स्तर जोडतो. ही ड्युअल-फायरवॉल रचना अंतर्गत सिस्टिम्स थेट बाह्य नेटवर्कसमोर उघड न करता एकूण सुरक्षा वाढवते. DMZ ही फायरवॉल डिझाइनची ऐच्छिक पण अधिक सुरक्षित वाढ (extension) आहे. ती प्रॉक्सी लेयरप्रमाणे कार्य करू शकते आणि अंतर्गत डेटासाठी अतिरिक्त संरक्षण प्रदान करते. DMZ म्हणजे खाजगी नेटवर्क आणि सार्वजनिक नेटवर्क यांच्या मध्ये ठेवलेला एक संगणक होस्ट किंवा लहान, वेगळे नेटवर्क होय. याचा उद्देश बाह्य वापरकर्त्यांना कंपनीच्या अंतर्गत डेटा सर्व्हर्सपर्यंत थेट पोहोचू न देणे हा आहे.

सामान्य DMZ सेटअपमध्ये, एक समर्पित होस्ट अंतर्गत वापरकर्त्यांकडून येणाऱ्या पब्लिक वेबसाइट्सच्या विनंत्या स्वीकारतो. हा DMZ होस्ट अंतर्गत वापरकर्त्यांच्या वतीने सार्वजनिक नेटवर्कवर सत्रे (sessions) सुरू करतो आणि मध्यस्थ (intermediary) म्हणून कार्य करतो. महत्त्वाचे म्हणजे, DMZ होस्ट खाजगी नेटवर्कमध्ये परत सत्र सुरू करू शकत नाही, ज्यामुळे अंतर्गत संसाधनांचे मजबूत संरक्षण सुनिश्चित होते. तो फक्त अंतर्गत होस्टने सुरुवातीला मागितलेली पॅकेट्सच पुढे फॉरवर्ड करू शकतो. त्याचप्रमाणे, बाह्य (पब्लिक) वापरकर्ते फक्त DMZ होस्टशीच संवाद साधू शकतात, उदाहरणार्थ DMZ मध्ये ठेवलेल्या वेब सर्व्हरशी. DMZ मध्ये कंपनीच्या वेब पानांसारखी सार्वजनिकरित्या उपलब्ध माहिती साठवली जाऊ शकते. DMZ जर हल्लेखोराकडून कॉम्प्रोमाइज झाली तरी, त्याचा परिणाम फक्त तिथे होस्ट केलेल्या वेब पानांपुरताच मर्यादित राहतो; कंपनीचा उर्वरित अंतर्गत डेटा सुरक्षित राहतो.

उदाहरणे (Examples)

1. **वेब सर्व्हर्स (Web Servers)**
   अंतर्गत डेटाबेस सर्व्हर्सशी संवाद साधणारे वेब सर्व्हर्स DMZ मध्ये सुरक्षितपणे तैनात केले जाऊ शकतात. या सेटअपमुळे सुरक्षा वाढते, कारण संवेदनशील माहिती अंतर्गत डेटाबेस सर्व्हरवरच साठवलेली असते, पब्लिक-फेसिंग वेब सर्व्हरवर नाही. वेब सर्व्हर थेट किंवा ॲप्लिकेशन फायरवॉल्सद्वारे अंतर्गत डेटाबेसमध्ये प्रवेश करू शकतो, तरीही DMZ एक अतिरिक्त संरक्षण स्तर प्रदान करते. वेब सर्व्हर कॉम्प्रोमाइज झाला तरी, हल्लेखोर अंतर्गत डेटाबेस किंवा इतर अंतर्गत सिस्टिम्समध्ये थेट प्रवेश करू शकत नाहीत.
2. **DNS सर्व्हर्स (DNS Servers)**
   DNS सर्व्हर पब्लिक IP पत्ते आणि त्यांच्याशी संबंधित होस्टनेम्सचा डेटाबेस राखतो आणि गरज पडल्यास होस्टनेम्सना IP पत्त्यांमध्ये रूपांतरित करतो. DNS सर्व्हर DMZ मध्ये ठेवण्यामुळे बाह्य DNS क्वेरीज कधीही अंतर्गत नेटवर्कला स्पर्श करत नाहीत. विश्वसनीयता आणि सुरक्षा वाढवण्यासाठी, संस्था अनेकदा अंतर्गत नेटवर्कमध्ये दुसरा DNS सर्व्हर तैनात करतात, ज्यामुळे DMZ सर्व्हरवर हल्ला झाला तरी अंतर्गत नेम रिझोल्यूशन सुरक्षित राहते.

3. प्रॉक्सी सर्व्हर्स (Proxy Servers)

प्रॉक्सी सर्व्हर्स सहसा फायरवॉल्ससोबत DMZ मध्ये तैनात केले जातात. जेव्हा अंतर्गत वापरकर्ते बाह्य वेबसाइट्सवर प्रवेश मागतात, तेव्हा प्रॉक्सी वेब पेज मिळवतो आणि नंतर ते विनंती करणाऱ्या संगणकाला फॉरवर्ड करतो. प्रॉक्सी सर्व्हर्स क्लायंट्सच्या वतीने कनेक्शन्स स्थापन करतात, ज्यामुळे अंतर्गत होस्ट्स आणि बाह्य सर्व्हर्स यांच्यात थेट संपर्क होत नाही. ते अंतर्गत नेटवर्कचे संरक्षण करतात, गोपनीयता (privacy) सुधारतात, आणि वेब कंटेंट कॅशिंगद्वारे बँडविड्थ वापर कमी करतात.

4.3 एन्क्रिप्शन अल्गोरिदम (Encryption Algorithm)

4.3.1 डेटा एनक्रिप्शन स्टँडर्ड अल्गोरिदम (Data Encryption Standard Algorithm)

डेटा एनक्रिप्शन स्टँडर्ड (DES) हा सुरक्षित डेटा एन्क्रिप्शनसाठी विकसित केलेला सिमेट्रिक की ब्लॉक सायफर आहे. कालांतराने, कमी की लांबीमुळे DES वर शक्तिशाली ब्रूट-फोर्स हल्ले शक्य झाले, त्यामुळे त्याची लोकप्रियता कमी झाली. DES हा एक ब्लॉक सायफर आहे, म्हणजे तो डेटा निश्चित आकाराच्या 64-बिट ब्लॉक्समध्ये एन्क्रिप्ट करतो. प्रत्येक 64-बिट प्लेनटेक्स्ट ब्लॉक हा 56-बिट की वापरून 64-बिट सायफरटेक्स्ट ब्लॉकमध्ये रूपांतरित केला जातो. एन्क्रिप्शन आणि डिक्रिप्शन या दोन्ही प्रक्रियांसाठी तीच की आणि तोच अल्गोरिदम वापरला जातो, फक्त कार्यपद्धतीत थोडा फरक असतो.

DES की साइज (DES Key Size)

DES मध्ये सामान्यतः 56-बिट की वापरली जाते असे म्हटले जाते, परंतु प्रत्यक्षात प्रारंभिक की 64 बिट्सची असते. DES प्रक्रिया सुरू होण्यापूर्वी, प्रत्येक 8वा बिट काढून टाकला जातो (discard केला जातो):

1	2	3	4	5	6	7	~~8~~	9	10	11	12	13	14	15	~~16~~
17	18	19	20	21	22	23	~~24~~	25	26	27	28	29	30	31	~~32~~
33	34	35	36	37	38	39	~~40~~	41	42	43	44	45	46	47	~~48~~
49	50	51	52	53	54	55	~~56~~	57	58	59	60	61	62	63	~~64~~

- स्थिती क्रमांक 8, 16, 24, 32, 40, 48, 56 आणि 64 वरील बिट्स काढून टाकले जातात. म्हणून प्रभावी (effective) की साइज 56 बिट्स होते, आणि हेच 56 बिट्स DES मधील सर्व अंतर्गत ऑपरेशन्समध्ये वापरले जातात.

DES चे मूलभूत तत्त्वे (Core Principles of DES)

DES हे क्रिप्टोग्राफीच्या दोन मूलभूत तत्त्वांवर आधारित आहे:

1. सब्स्टिट्यूशन (Confusion)
2. ट्रान्सपोझिशन (Diffusion)

ही दोन्ही ऑपरेशन्स 16 राउंड्समध्ये पुन्हा-पुन्हा लागू केली जातात, आणि प्रत्येक राउंड एकूण एन्क्रिप्शन अधिक मजबूत करतो.

DES एन्क्रिप्शन प्रक्रियेचे वर्णन (Description of DES Encryption Process)

DES अल्गोरिदम सिमेट्रिक की आणि निश्चित क्रमाने केलेल्या ऑपरेशन्सच्या मालिकेचा वापर करून 64-बिट प्लेनटेक्स्ट ब्लॉकला 64-बिट सायफरटेक्स्ट ब्लॉकमध्ये एन्क्रिप्ट करतो.

Fig 4.10: DES एन्क्रिप्शन प्रक्रिया (DES Encryption Process)

1. **64-बिट प्लेनटेक्स्ट इनपुट (64-bit Plaintext Input)**
   DES प्रक्रिया 64-बिट प्लेनटेक्स्ट ब्लॉकपासून सुरू होते. हा ब्लॉक निश्चित ऑपरेशन्सच्या क्रमाद्वारे रूपांतरणासाठी तयार केला जातो.
2. **इनिशियल पर्म्युटेशन (IP) (Initial Permutation)**
   प्लेनटेक्स्टला इनिशियल पर्म्युटेशन (IP) मधून पास केले जाते, ज्यामध्ये पूर्वनिश्चित टेबलनुसार सर्व 64 बिट्सची पुनर्रचना (rearrangement) केली जाते. ही पर्म्युटेशन स्वतःहून थेट सुरक्षा वाढवत नाही, परंतु पुढील राउंड्समध्ये कार्यक्षम प्रक्रिया होण्यासाठी डेटाची रचना (data structure) तयार करते.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

3. LPT आणि RPT मध्ये विभाजन (Split into LPT and RPT)

इनिशियल परम्युटेशन (Initial Permutation – IP) नंतर मिळालेला 64-बिट ब्लॉक दोन समान भागांमध्ये विभागला जातो:

• डावा प्लेन टेक्स्ट / Left Plain Text (LPT) → 32 बिट्स

• उजवा प्लेन टेक्स्ट / Right Plain Text (RPT) → 32 बिट्स

हे दोन भाग DES (डेटा एन्क्रिप्शन स्टँडर्ड) मध्ये वापरल्या जाणाऱ्या फायस्टेल स्ट्रक्चर (Feistel Structure) चा आधार बनतात.

LPT					RPT			
58	50	42	34		26	18	10	2
60	52	44	36		28	20	12	4
62	54	46	38		30	22	14	6
64	56	48	40		32	24	16	8
57	49	41	33		25	17	9	1
59	51	43	35		27	19	11	3
61	53	45	37		29	21	13	5
63	55	47	39		31	23	15	7

4. सोळा फायस्टेल राऊंड्सची प्रक्रिया (Sixteen Feistel Rounds of Processing)

DES (डेटा एन्क्रिप्शन स्टँडर्ड) अल्गोरिदमचा मुख्य भाग 16 फायस्टेल राऊंड्सचा बनलेला आहे. प्रत्येक राऊंडमध्ये डिफ्युजन (Diffusion) आणि कन्फ्युजन (Confusion) प्रदान करण्यासाठी विविध क्रिप्टोग्राफिक ऑपरेशन्स लागू केली जातात.

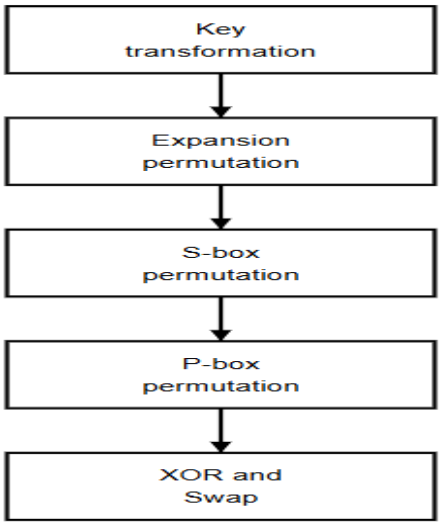


Fig 4.11: DES राउंड (DES Round)

प्रत्येक राउंडमध्ये:

a) की ट्रान्सफॉर्मेशन (Key Transformation)

प्रारंभिक 64-बिट की मधून प्रत्येक 8वा बिट काढून टाकून ती प्रथम 56 बिट्सपर्यंत कमी केली जाते. त्यामुळे DES ऑपरेशन्ससाठी वापरली जाणारी 56-बिट प्रभावी की (effective key) तयार होते. या 56-बिट की मधून प्रत्येक राउंडसाठी एक युनिक 48-बिट सबकी (subkey) तयार केली जाते. या प्रक्रियेला की ट्रान्सफॉर्मेशन (key transformation) असे म्हणतात.

ही ट्रान्सफॉर्मेशन प्रक्रिया करण्यासाठी, 56-बिट की दोन समान भागांमध्ये विभागली जाते:

- 28 बिट्स
- 28 बिट्स

प्रत्येक राउंडमध्ये, या दोन्ही भागांवर सर्क्युलर लेफ्ट शिफ्ट (circular left shift) लागू केला जातो. शिफ्टची संख्या राउंड क्रमांकावर अवलंबून असते.

- राउंड 1, 2, 9 आणि 16 साठी, भागांना एक स्थान (1 position) डावीकडे शिफ्ट केले जाते.
- इतर सर्व राउंड्ससाठी, भागांना दोन स्थानांनी (2 positions) डावीकडे शिफ्ट केले जाते.

Round	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Key Bits Shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

योग्य सर्क्युलर शिफ्ट केल्यानंतर, 56-बिट की मधून 48 बिट्सची निवड केली जाते. या 48 बिट्सची निवड आकृतीमध्ये दाखवलेल्या टेबलनुसार ठरवली जाते. उदाहरणार्थ, शिफ्टनंतर बिट क्रमांक 14 पहिल्या स्थानावर ठेवला जातो, बिट क्रमांक 17 दुसऱ्या स्थानावर ठेवला जातो, आणि त्याचप्रमाणे पुढील बिट्सची मांडणी केली जाते. टेबलकडे बारकाईने पाहिल्यास असे लक्षात येते की त्यामध्ये फक्त 48 स्थानांचीच यादी दिलेली आहे, म्हणजेच 8 बिट्स काढून टाकले जातात. उदाहरणार्थ, बिट क्रमांक 18 टेबलमध्ये दिसत नाही, यावरून तो या प्रक्रियेदरम्यान काढून टाकलेल्या बिट्सपैकी एक आहे हे स्पष्ट होते. या टप्प्यात पर्म्युटेशन (Permutation) आणि 56-बिट की मधून 48-बिट उपसंचाची (subset) निवड दोन्ही गोष्टी समाविष्ट असल्यामुळे, या प्रक्रियेला कंप्रेशन पर्म्युटेशन (Compression Permutation) असे म्हणतात.

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

या कंप्रेशन पर्म्युटेशन तंत्रामुळे, DES च्या प्रत्येक राउंडमध्ये की बिट्सचा वेगळा उपसंच (subset) वापरला जातो. सबकीजमधील ही विविधता (variation) अल्गोरिदमची गुंतागुंत लक्षणीयरीत्या वाढवते आणि DES क्रॅक करणे अधिक कठीण बनवते.

b) एक्स्पान्शन (E-box) (Expansion)

इनिशियल पर्म्युटेशननंतर, 64-बिट प्लेनटेक्स्ट दोन 32-बिट भागांमध्ये विभागला जातो:

- लेफ्ट प्लेनटेक्स्ट (LPT)
- राइट प्लेनटेक्स्ट (RPT)

एक्स्पान्शन पर्म्युटेशन दरम्यान, RPT ला 32 बिट्सवरून 48 बिट्सपर्यंत विस्तारित (expand) केले जाते. या प्रक्रियेत बिट्सची पुनर्रचना (rearrangement) देखील केली जात असल्यामुळे, याला एक्स्पान्शन पर्म्युटेशन असे म्हणतात. ही एक्स्पान्शन प्रक्रिया करण्यासाठी, 32-बिट RPT ला आठ ब्लॉक्समध्ये विभागले जाते, आणि प्रत्येक ब्लॉकमध्ये 4 बिट्स असतात. प्रत्येक 4-बिट ब्लॉक नंतर 6-बिट ब्लॉकमध्ये रूपांतरित केला जातो, म्हणजेच प्रत्येक ब्लॉकमध्ये 2 अतिरिक्त बिट्स जोडले जातात. यामुळे RPT चा आकार 32 बिट्सवरून 48 बिट्सपर्यंत वाढतो, आणि तो DES प्रक्रियेच्या पुढील टप्प्यासाठी तयार होतो.

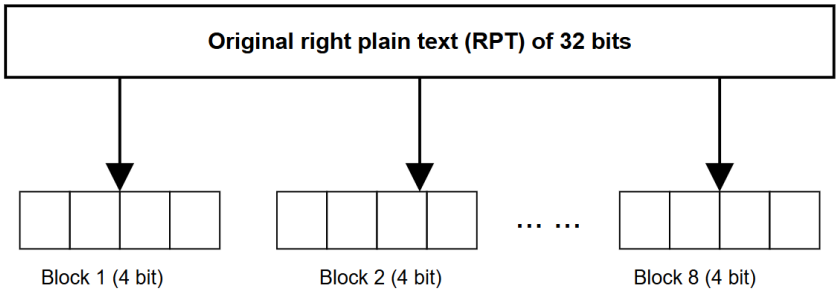
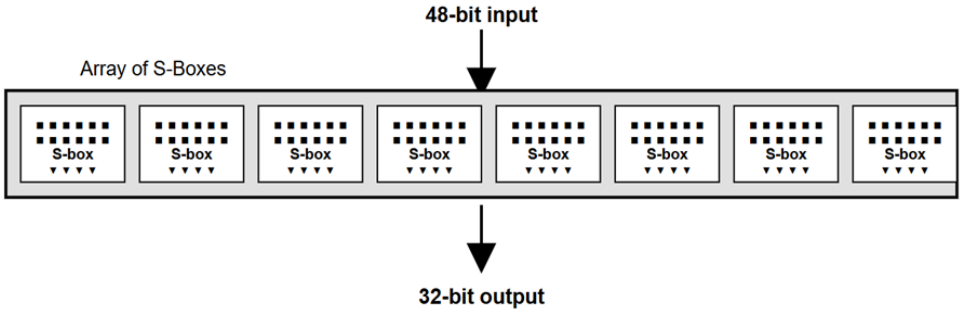


Fig 4.12: एक्स्पान्शन (E-box) (Expansion)

या प्रक्रियेमुळे इनपुट बिट्सचे एक्स्पान्शन (विस्तार) आणि पर्म्युटेशन (पुनर्रचना) दोन्ही होतात आणि आउटपुट तयार होते. की ट्रान्सफॉर्मेशन प्रक्रियेत 56-बिट की चे 48 बिट्समध्ये कंप्रेशन केले जाते. त्याचप्रमाणे, एक्स्पान्शन पर्म्युटेशन दरम्यान 32-बिट RPT चे 48 बिट्समध्ये विस्तार केले जाते. एकदा दोन्ही मूल्ये 48 बिट्सची झाल्यानंतर, 48-बिट सबकी आणि 48-बिट विस्तारित RPT यांचा XOR केला जातो. या XOR ऑपरेशनचा परिणाम DES अल्गोरिदमच्या पुढील टप्प्याकडे पाठवला जातो, ज्याला S-बॉक्स सब्स्टिट्यूशन (S-Box Substitution) असे म्हणतात.

c) S-बॉक्स सब्स्टिट्यूशन (S-box Substitution)

S-बॉक्सेस DES अल्गोरिदममध्ये प्रत्यक्ष मिक्सिंग (mixing) म्हणजेच कन्फ्युजन (confusion) कार्य करतात. DES मध्ये आठ S-बॉक्सेस वापरले जातात, आणि प्रत्येक S-बॉक्स 6-बिट इनपुट स्वीकारतो आणि 4-बिट आउटपुट तयार करतो. प्रत्येक S-बॉक्सद्वारे केलेले रूपांतरण नॉन-लिनिअर (non-linear) असते, ज्यामुळे ते DES सुरक्षेला मजबूत करण्यासाठी एक अत्यंत महत्त्वाचा घटक ठरते.



S-बॉक्स कसा कार्य करतो याचा नियम खाली दर्शविला आहे.

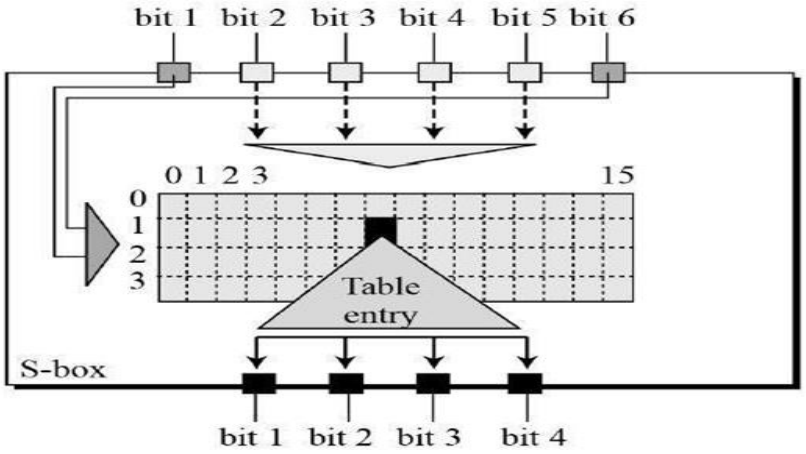


Fig 4.13: S-बॉक्स सब्स्टिट्यूशन (S-box Substitution)

DES मध्ये एकूण आठ S-बॉक्स टेबल्स असतात. प्रत्येक S-बॉक्स 4-बिट आउटपुट तयार करतो, आणि सर्व आठ S-बॉक्सेसचे आउटपुट एकत्र करून 32-बिट ब्लॉक तयार केला जातो.

d) P-बॉक्स पर्म्युटेशन (P-box Permutation)

32-बिट S-बॉक्स आउटपुट ला स्ट्रेट पर्म्युटेशन टेबल वापरून पुनर्रचित (rearranged) केले जाते. ही प्रक्रिया बिट्सच्या स्थानांचे मिश्रण करून डिफ्युजन (diffusion) प्रदान करते.

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

e) XOR + स्वॅप (XOR + Swap)

P-बॉक्स आउटपुट आणि लेफ्ट हाफ (LPT) यांचा XOR केला जातो. यानंतर लेफ्ट आणि राइट हाफ्सची अदलाबदल (swap) केली जाते, ज्यामुळे पुढील राउंड्समध्ये बदल सर्व ब्लॉक्समध्ये प्रसारित होतात.

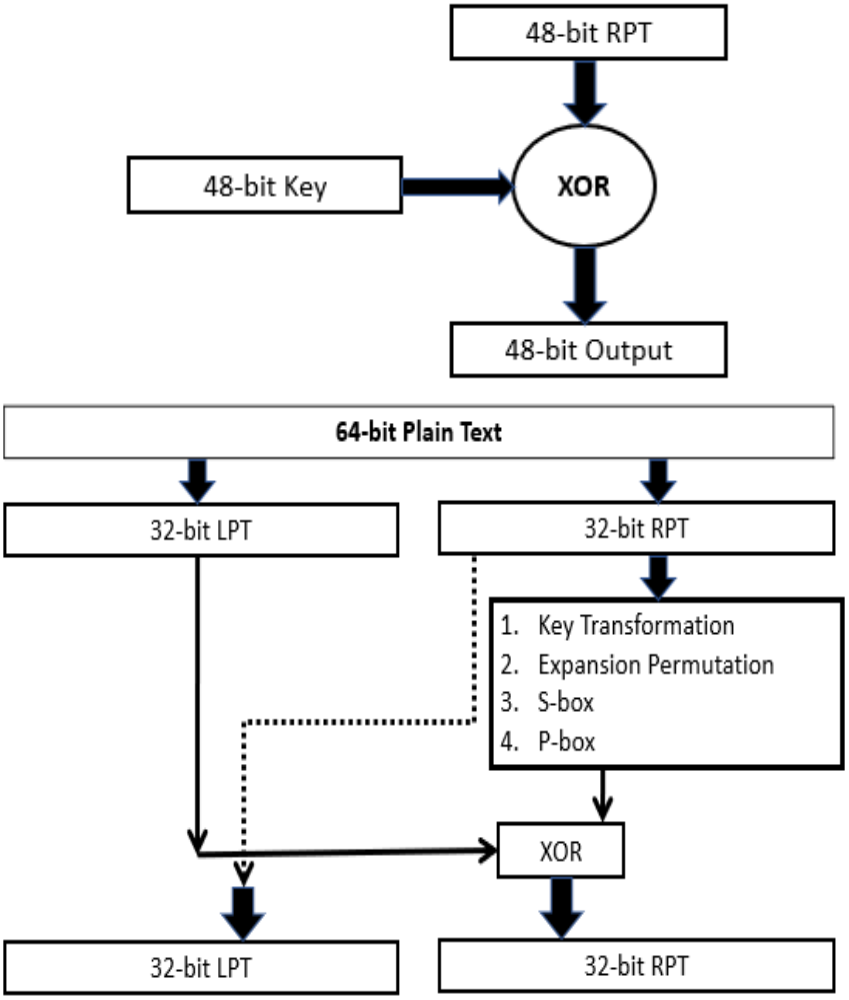


Fig 4.14: XOR + स्वॅप (XOR + Swap)

ही प्रक्रिया सर्व 16 राउंड्ससाठी पुन्हा पुन्हा केली जाते.

5. LPT आणि RPT एकत्र करणे (Combine LPT and RPT)

16वा राउंड पूर्ण झाल्यानंतर, अंतिम LPT आणि RPT ब्लॉक्स एकत्र करून एक 64-बिट ब्लॉक तयार केला जातो. (अंतिम राउंडनंतर कोणताही स्वॅप केला जात नाही.)

6. फायनल पर्म्युटेशन (IP^{-1}) (Final Permutation)

एकत्रित 64-बिट ब्लॉक ला इनिशियल पर्म्युटेशनच्या उलट (Inverse of Initial Permutation – IP^{-1}) मधून पास केले जाते. IP^{-1} बिट्सची स्थिती पुनर्स्थापित करून अंतिम एन्क्रिप्टेड आउटपुट तयार करते.

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

7. 64-बिट सायफरटेक्स्ट आउटपुट (64-bit Ciphertext Output)

IP^{-1} चा परिणाम म्हणजे 64-बिट सायफरटेक्स्ट, जो मूळ प्लेनटेक्स्टची एन्क्रिप्ट केलेली आवृत्ती असते.

4.3.2 अॅडव्हान्स्ड एनक्रिप्शन स्टँडर्ड अल्गोरिदम (Advanced Encryption Standard (AES) algorithm)

AES (अॅडव्हान्स्ड एनक्रिप्शन स्टँडर्ड) हा सिमेट्रिक की ब्लॉक सायफर आहे, जो NIST ने 2001 मध्ये DES चा उत्तराधिकारी म्हणून सादर केला. मोठ्या की साइजेस आणि अधिक गुंतागुंतीच्या अंतर्गत रचनेमुळे AES अधिक मजबूत, जलद आणि सुरक्षित एन्क्रिप्शन प्रदान करतो.

AES चा मोठ्या प्रमाणावर वापर खालील आधुनिक सुरक्षा अनुप्रयोगांमध्ये केला जातो:

- Wi-Fi सुरक्षा (WPA2/WPA3)
- SSL/TLS प्रोटोकॉल्स
- VPNs
- मोबाइल डिव्हाइस एन्क्रिप्शन
- डिस्क एन्क्रिप्शन

सिमेट्रिक सायफर असल्यामुळे, AES मध्ये एन्क्रिप्शन आणि डिक्रिप्शनसाठी एकच की वापरली जाते आणि तो 128-बिट डेटा ब्लॉक्सवर कार्य करतो. AES 128, 192 आणि 256 बिट्सच्या की साइजेसला समर्थन देतो, ज्यासाठी अनुक्रमे 10, 12 आणि 14 प्रोसेसिंग राउंड्स आवश्यक असतात. हा अल्गोरिदम Substitution–Permutation Network (SPN) वर आधारित असून, तो मजबूत कन्फ्युजन (confusion) आणि डिफ्युजन (diffusion) सुनिश्चित करतो, ज्यामुळे AES हे DES पेक्षा खूपच अधिक सुरक्षित ठरते. आंतरिकरित्या, AES डेटा 4 × 4 बाइट मॅट्रिक्स म्हणून दर्शवतो, ज्याला State असे म्हणतात, आणि प्रत्येक एन्क्रिप्शन व डिक्रिप्शन राउंडदरम्यान त्यावर विविध ट्रान्सफॉर्मेशन्स लागू केल्या जातात. AES एन्क्रिप्शन आणि डिक्रिप्शन प्रक्रिया (AES Encryption and Decryption Process) AES (अॅडव्हान्स्ड एनक्रिप्शन स्टँडर्ड) अल्गोरिदम एन्क्रिप्शन आणि डिक्रिप्शनसाठी निश्चित ट्रान्सफॉर्मेशन राउंड्सच्या मालिकेचा वापर करतो. आकृतीमध्ये दाखवलेला फ्लोचार्ट एन्क्रिप्शन (डावीकडे) आणि डिक्रिप्शन (उजवीकडे) या दोन्ही प्रक्रिया दर्शवतो. AES 128-बिट डेटा ब्लॉकवर कार्य करतो, जो 4 × 4 बाइट मॅट्रिक्स (State) मध्ये मांडलेला असतो, आणि मूळ सायफर की पासून व्युत्पन्न (derived) केलेल्या अनेक राउंड कीज वापरतो.

AES स्टेट मॅट्रिक्स (AES State Matrix)

AES 128-बिट प्लेनटेक्स्टला 4 × 4 बाइट मॅट्रिक्समध्ये आयोजित करतो:

b0	b4	b8	b12
b1	b5	b9	b13
b2	b6	b10	b14
b3	b7	b11	b15

सर्व AES ट्रान्सफॉर्मेशन स्टेप्स या मॅट्रिक्सवरच कार्य करतात.

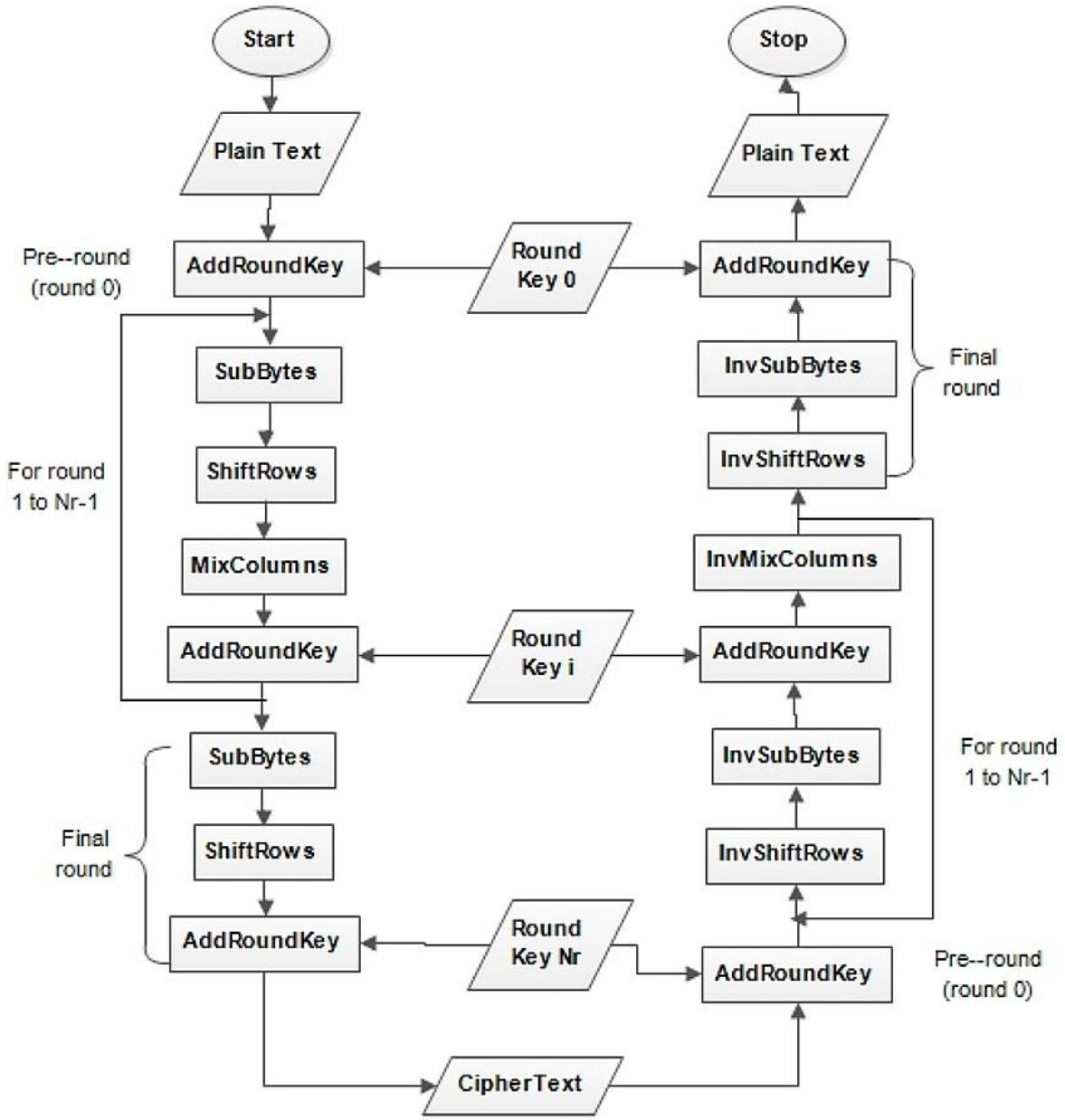


Fig 4.15: AES एन्क्रिप्शन आणि डिक्रिप्शन प्रक्रिया (AES Encryption and Decryption Process)

1. AES एन्क्रिप्शन प्रक्रिया (AES Encryption Process)

AES एन्क्रिप्शनमध्ये खालील टप्पे समाविष्ट असतात:

(a) प्री-राउंड ट्रान्सफॉर्मेशन (Round 0)

- AddRoundKey

प्लेनटेक्स्ट आणि प्रारंभिक राउंड की (Round Key 0) यांचा XOR केला जातो. हा टप्पा एन्क्रिप्शनची प्रक्रिया सुरुवातीपासूनच कीवर अवलंबून आहे याची खात्री करतो.

(b) स्टँडर्ड राउंड्स (Round 1 ते Round Nr−1)

प्रत्येक राउंडमध्ये खालील चार ऑपरेशन्स असतात:

1. SubBytes
   - एक नॉन-लिनिअर सब्स्टिट्यूशन स्टेप.
   - State मधील प्रत्येक बाइट AES S-Box वापरून बदलला जातो.
2. ShiftRows
   - एक ट्रान्सपोझिशन स्टेप.

- State मधील रांगा वेगवेगळ्या ऑफसेट्सने डावीकडे (left) सायक्लिकली शिफ्ट केल्या जातात.

3. MixColumns
- प्रत्येक स्तंभावर (column) केली जाणारी मिक्सिंग ऑपरेशन.
- $GF(2^8)$ मध्ये गणिती पद्धतीने बाइट्स एकत्र करून डिफ्युजन (diffusion) वाढवते.

4. AddRoundKey
- चालू State आणि संबंधित राउंड सबकी (Round Key i) यांचा XOR केला जातो.

(c) अंतिम राउंड (Final Round – Round Nr)

AES एन्क्रिप्शनच्या शेवटच्या राउंडमध्ये MixColumns स्टेप वगळली जाते.

अंतिम राउंडमधील ऑपरेशन्स:

1. SubBytes
2. ShiftRows
3. AddRoundKey (Round Key Nr वापरून)

या अंतिम AddRoundKey नंतर मिळणारा आउटपुट म्हणजे Ciphertext असतो.

2. AES डिक्रिप्शन प्रक्रिया (AES Decryption Process)

डिक्रिप्शन प्रक्रिया ही एन्क्रिप्शनच्या उलट क्रमाने, तीच राउंड कीज वापरून, ऑपरेशन्स रिव्हर्स करून केली जाते.

(a) प्री-राउंड ट्रान्सफॉर्मेशन (Round 0)

- AddRoundKey

सायफरटेक्स्ट आणि Round Key Nr (शेवटची राउंड की) यांचा XOR केला जातो.

(b) स्टँडर्ड राउंड्स (Round 1 ते Nr−1)

प्रत्येक राउंडमध्ये एन्क्रिप्शनच्या इन्व्हर्स ऑपरेशन्स केल्या जातात:

1. InvSubBytes
   - प्रत्येक बाइटवर इन्व्हर्स S-Box लागू केला जातो.
2. InvShiftRows
   - रांगा उजवीकडे (right) शिफ्ट केल्या जातात *(एन्क्रिप्शनच्या उलट प्रक्रिया)*.
3. InvMixColumns
   - MixColumns ट्रान्सफॉर्मेशन उलटवते.
4. AddRoundKey
   - संबंधित राउंड की (Round Key i) सोबत XOR.

(c) अंतिम राउंड (Inverse Final Round)

डिक्रिप्शनच्या अंतिम राउंडमध्ये InvMixColumns स्टेप वगळली जाते.

अंतिम राउंडमधील ऑपरेशन्स:

1. InvSubBytes
2. InvShiftRows
3. AddRoundKey (Round Key 0 वापरून)

या टप्प्यानंतर मूळ प्लेनटेक्स्ट पुनर्स्थापित (restore) होतो.

4.3.3 रिव्हेस्ट–शामीर–ॲडेलमन अल्गोरिदम (Rivest-Shamir-Adleman (RSA) algorithm)

RSA हा एक पब्लिक-की (ॲसिमेट्रिक) क्रिप्टोग्राफिक अल्गोरिदम आहे, जो Ron Rivest, Adi Shamir आणि Leonard Adleman यांनी 1977 मध्ये शोधला. RSA चा मोठ्या प्रमाणावर वापर पुढील गोष्टींसाठी केला जातो: सुरक्षित डेटा ट्रान्समिशन, डिजिटल सिग्नेचर्स, की एक्सचेंज, ई-मेल सुरक्षा, TLS/SSL

RSA मध्ये दोन वेगवेगळ्या कीज वापरल्या जातात:

- पब्लिक की (Public Key) → एन्क्रिप्शनसाठी वापरली जाते
- प्रायव्हेट की (Private Key) → डिक्रिप्शनसाठी वापरली जाते

RSA ची सुरक्षा फार मोठ्या अभाज्य (prime) संख्यांचे गुणाकार फॅक्टरायझेशन करणे अत्यंत कठीण असते या गणिती तत्त्वावर आधारित आहे.

RSA खालील तत्त्वावर कार्य करते:

एन्क्रिप्शन: $C = M^e \ mod \ n$

डिक्रिप्शन: $M = C^d \ mod \ n$

जिथे: M = प्लेनटेक्स्ट (plaintext), C = सायफरटेक्स्ट (ciphertext), e = पब्लिक एक्स्पोनंट (public exponent), d = प्रायव्हेट एक्स्पोनंट (private exponent), n = p × q = दोन मोठ्या अभाज्य संख्यांचा गुणाकार.

फक्त प्रायव्हेट की धारकच d काढू शकतो, त्यामुळे RSA सुरक्षित (secure) ठरते.

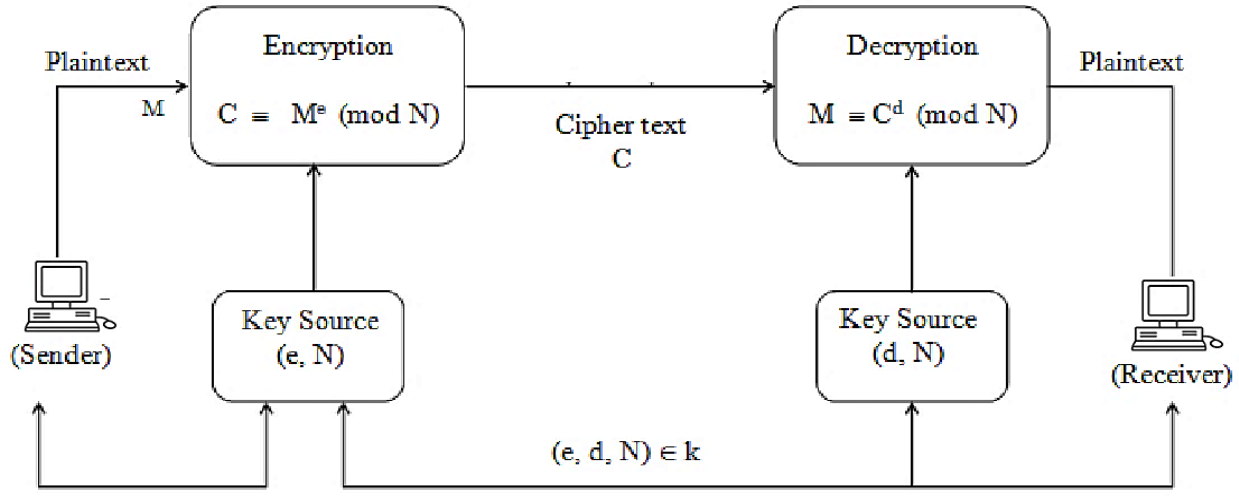


Fig 4.16: RSA एन्क्रिप्शन आणि डिक्रिप्शन प्रक्रिया (RSA Encryption and Decryption Process)

RSA स्टेप्स (RSA Steps)

RSA मध्ये तीन मुख्य टप्पे (phases) असतात:

स्टेप 1: की जनरेशन (Key Generation)

- दोन मोठ्या अभाज्य (prime) संख्या निवडा: p आणि q
  मॉड्युलस काढा: $n = p \times q$
- युलरचे टोटिएंट फंक्शन (Euler's Totient Function) काढा:
  $$\emptyset\ (n) = (p-1)(q-1)$$
- पब्लिक की एक्स्पोनंट (e) निवडा, असा की:
  - $1 < e < \emptyset\ (n)$
  - $gcd\ (e, \emptyset\ (n)) = 1$ (i.e $e \ and \ \emptyset\ (n) \ are \ co-prime$)

  सामान्यतः वापरले जाणारे मूल्य: e = 65537
- प्रायव्हेट की एक्स्पोनंट (d) काढा: $d \times e \ = 1 \ mod \ \emptyset(n)$ (d *हे* e *चे मॉड्युलर इन्व्हर्स असते*)

स्टेप 2: एन्क्रिप्शन (Encryption)

दिलेल्या प्लेनटेक्स्ट M साठी, सायफरटेक्स्ट C खालीलप्रमाणे काढले जाते:

$$C = M^e \ mod \ n$$

यासाठी पब्लिक की (e, n) वापरली जाते.

स्टेप 3: डिक्रिप्शन (Decryption)

रिसिव्हर प्रायव्हेट की (d, n) वापरून प्लेनटेक्स्ट पुनर्प्राप्त करतो:

$$M = C^d \ mod \ n$$

Table 4.2: DES, AES आणि RSA अल्गोरिदम्सची तुलना (Comparison of DES, AES, and RSA Algorithms)

पॅरामिटर (Parameter)	DES (डेटा एन्क्रिप्शन स्टँडर्ड)	AES (ॲडव्हान्स्ड एन्क्रिप्शन स्टँडर्ड)	RSA (रिव्हेस्ट–शॅमिर–ॲडेलमन)
अल्गोरिदमचा प्रकार (Type of Algorithm)	सिमेट्रिक की ब्लॉक सायफर	सिमेट्रिक की ब्लॉक सायफर	ॲसिमेट्रिक की अल्गोरिदम
विकसक (Developer)	IBM आणि NSA (1977)	NIST (2001), Rijndael वर आधारित	Rivest, Shamir, Adleman (1977)
की साइज (Key Size)	56-बिट प्रभावी की	128, 192 किंवा 256-बिट	1024–4096 बिट्स (सामान्यतः)
ब्लॉक साइज (Block Size)	64-बिट ब्लॉक	128-बिट ब्लॉक	ब्लॉक-आधारित नाही (मोठ्या पूर्णांकांवर कार्य)
राउंड्सची संख्या (No. of Rounds)	16 राउंड्स	10, 12 किंवा 14 राउंड्स (की साइजवर अवलंबून)	राउंड-आधारित नाही
वापरलेली रचना (Structure Used)	फिस्टेल नेटवर्क (Feistel Network)	सब्स्टिट्यूशन–पर्म्युटेशन नेटवर्क (SPN)	गणितीय संख्या सिद्धांत (Modular Exponentiation)
गती (Speed)	जलद पण कालबाह्य	अतिशय जलद आणि कार्यक्षम	जड गणनांमुळे मंद
सुरक्षेची पातळी (Security Level)	कमी (ब्रूट-फोर्स हल्ल्यांसाठी असुरक्षित)	उच्च सुरक्षा	अतिशय उच्च सुरक्षा (की साइजवर अवलंबून)
ऑपरेशन्सचा प्रकार (Type of Operations)	XOR, पर्म्युटेशन, सब्स्टिट्यूशन, फिस्टेल राउंड्स	SubBytes, ShiftRows, MixColumns, AddRoundKey	मॉड्युलर एक्स्पोनेंशिएशन, प्राईम फॅक्टरायझेशन
कीचा वापर (Use of Keys)	एन्क्रिप्शन व डिक्रिप्शनसाठी तीच की	एन्क्रिप्शन व डिक्रिप्शनसाठी तीच की	एन्क्रिप्शनसाठी पब्लिक की, डिक्रिप्शनसाठी प्रायव्हेट की
बलस्थान (Strengths)	साधे, ऐतिहासिकदृष्ट्या महत्त्वाचे	मजबूत, जलद, सुरक्षित, मोठ्या प्रमाणावर वापरले जाते	मजबूत सुरक्षा, ऑथेन्टिकेशनसाठी योग्य
मर्यादा (Weaknesses)	लहान की साइज → असुरक्षित	अतिशय लहान डिव्हाइसेससाठी संगणकीयदृष्ट्या जड	मोठ्या डेटासाठी मंद; मोठ्या की साइजची गरज
उदाहरण अनुप्रयोग (Example Applications)	जुनी UNIX प्रणाली, बँकिंग ATMs (legacy)	TLS/SSL, Wi-Fi WPA2/WPA3, VPN	डिजिटल सिग्नेचर्स, PGP, SSL सर्टिफिकेट्स

4.4 डिफी–हेलमन की एक्सचेंज अल्गोरिदम (Diffie-Hellman Key Exchange Algorithm)

डिफी–हेलमन की एक्सचेंज (DHKE) ही क्रिप्टोग्राफीमधील एक पद्धत आहे, जी असुरक्षित कम्युनिकेशन चॅनलवर दोन पक्षांना सुरक्षितपणे एक सामायिक गुप्त की (shared secret key) स्थापन करण्यास सक्षम करते. ही सामायिक की पुढील कम्युनिकेशन एन्क्रिप्ट करण्यासाठी वापरली जाऊ शकते. हा अल्गोरिदम 1976 मध्ये Whitfield Diffie आणि Martin Hellman यांनी सादर केला, आणि तो पब्लिक की क्रिप्टोग्राफीच्या पहिल्या व्यावहारिक अंमलबजावण्यांपैकी एक मानला जातो. डिफी–हेलमन अल्गोरिदम हा मॉड्युलर अंकगणितातील डिस्क्रीट लॉगरिदम प्रॉब्लेम (Discrete Logarithm Problem – DLP) सोडविण्याच्या कठीणतेवर आधारित आहे.

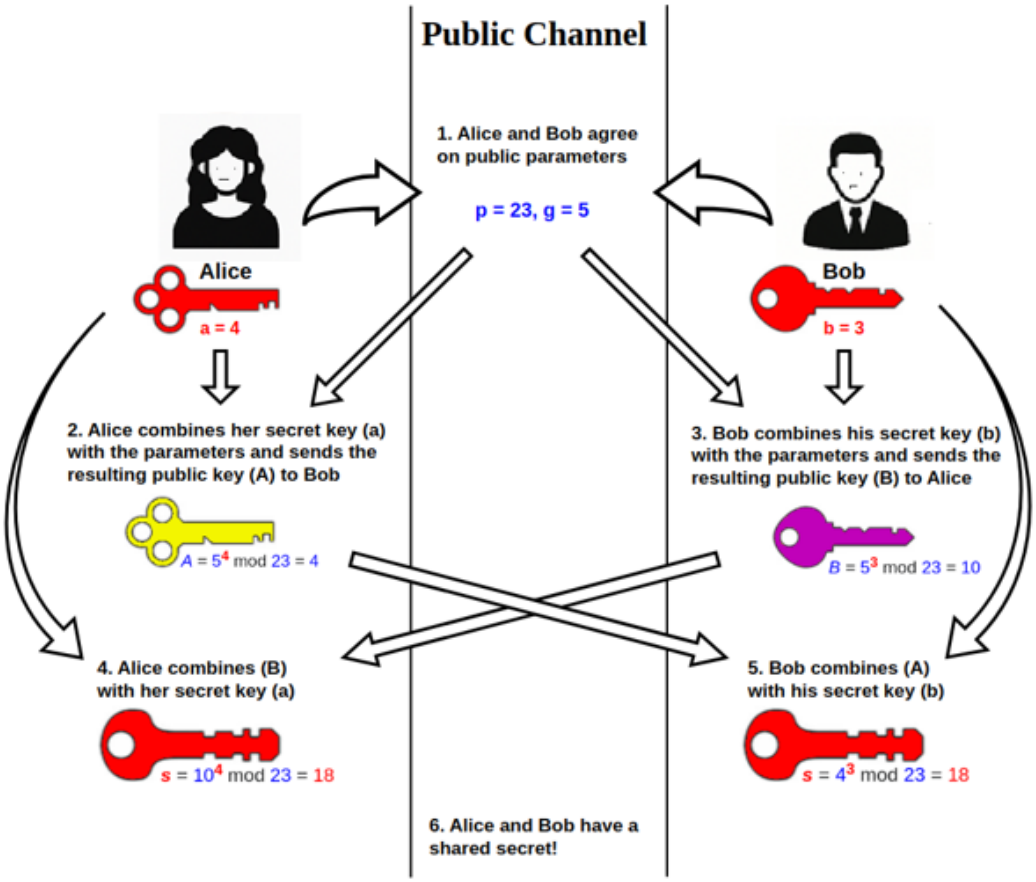


Fig 4.17: डिफी–हेलमन की एक्सचेंज अल्गोरिदम (Diffie-Hellman Key Exchange Algorithm)

दोन पक्ष (उदा. A आणि B) खालील पब्लिक पॅरामिटर्सवर सहमती दर्शवतात:

- एक मोठी अभाज्य संख्या p
- p मॉड्युलोचा प्रिमिटिव्ह रूट (किंवा जनरेटर) g

ही मूल्ये (p, g) सार्वजनिकरित्या ज्ञात असतात.

प्रत्येक पक्ष प्रायव्हेट की निवडतो:

- Alice निवडते a (गुप्त)
- Bob निवडतो b (गुप्त)

प्रत्येक जण पब्लिक की काढतो:

- Alice काढते:

$$A = g^a \ mod \ p$$

- Bob काढतो:

$$B = g^b \ mod \ p$$

यानंतर ते ही मूल्ये एकमेकांशी एक्सचेंज करतात.

प्रत्येक पक्ष सामायिक गुप्त की (Shared Secret) काढतो:

- Alice काढते:

$$S = B^a \ mod \ p$$

- Bob काढतो:

$$S = A^b \ mod \ p$$

दोन्ही मूल्ये गणिती दृष्ट्या समान असतात:

$$S = g^{ab} \ mod \ p$$

आता Alice आणि Bob दोघांकडेही तीच गुप्त की S असते, आणि ती कधीही थेट पाठवलेली नसते.

उदाहरण:

पब्लिक पॅरामिटर्स:

- अभाज्य p = 23
- जनरेटर g = 5

प्रायव्हेट कीज:

- Alice निवडते: a=6
- Bob निवडतो: b=15

पब्लिक कीज:

- Alice काढते:

$$A = g^a \ mod \ p = 5^6 \ mod \ 23 = 15625 \ mod \ 23 = 8$$

- Bob काढतो:

$$B = g^b \ mod \ p = \ 5^{15} \ mod \ 23 = \ 30517578125 \ mod \ 23 = 19$$

म्हणून Alice 8 पाठवते, आणि Bob 19 पाठवतो.

सामायिक गुप्त की (Shared Secret):

- Alice काढते:

$$S = B^a \ mod \ p = \ 19^6 \ mod \ 23 = \ 47045881 \ mod \ 23 = 2$$

- Bob काढतो:

$$S = A^b \ mod \ p = 8^{15} \ mod \ 23 = \ 35184372088832 \ mod \ 23 = 2$$

आता Alice आणि Bob दोघांकडेही सामायिक गुप्त की = 2 आहे, जी एन्क्रिप्शनसाठी वापरली जाऊ शकते.

4.5 हॅश फंक्शन (Hash Function)

4.5.1 परिचय (Introduction)

हॅश फंक्शन ही एक क्रिप्टोग्राफिक अल्गोरिदम आहे, जी कोणत्याही लांबीचा इनपुट मेसेज स्वीकारते आणि त्यापासून निश्चित लांबीचा आउटपुट तयार करते. या आउटपुटला हॅश व्हॅल्यू (Hash Value), मेसेज डायजेस्ट (Message Digest) किंवा फिंगरप्रिंट (Fingerprint) असे म्हणतात.

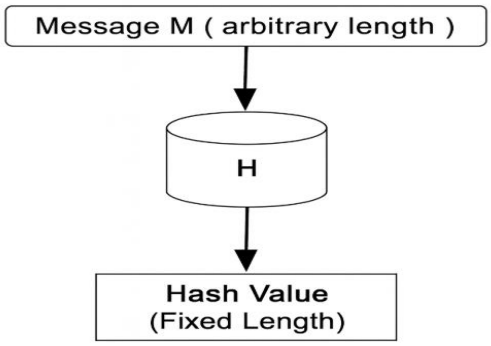


Fig 4.18: हॅश फंक्शन (Hash Function)

हॅश फंक्शन्स या एकमार्गी (One-Way) स्वरूपाच्या असतात, म्हणजेच हॅश व्हॅल्यूवरून मूळ मेसेज पुन्हा मिळवणे संगणकीय दृष्ट्या अशक्य (Computationally Infeasible) असते. हॅश फंक्शनचा वापर प्रमाणीकरण (Authentication), डिजिटल सिग्नेचर (Digital Signatures), डेटा इंटिग्रिटी तपासणी (Integrity Checking), पासवर्ड स्टोरेज (Password Storage) तसेच विविध सिक्युरिटी प्रोटोकॉल्समध्ये जसे की SSL/TLS, IPSec आणि PGP यांसाठी मोठ्या प्रमाणावर केला जातो.

4.5.2. हॅश फंक्शनची वैशिष्ट्ये (Features of Hash Functions)

1. निश्चित लांबीचा आउटपुट (Fixed-Length Output)
   इनपुट मेसेजची लांबी कितीही असली तरी हॅश फंक्शन नेहमी निश्चित लांबीचा आउटपुट तयार करते.

उदाहरण:

- MD5 → 128-बिट आउटपुट
- SHA-1 → 160-बिट आउटपुट
- SHA-256 → 256-बिट आउटपुट

यामुळे डेटा प्रोसेसिंग कार्यक्षम (Efficient) आणि एकसमान (Uniform) होते.

2. निर्धारिक स्वरूप (Deterministic)
   समान इनपुट दिल्यास हॅश फंक्शन नेहमी समान हॅश व्हॅल्यू तयार करते. यामुळे डेटा इंटिग्रिटी तपासणी (Data Integrity Checking) सुसंगतपणे करता येते.
3. प्री-इमेज रेझिस्टन्स / एकमार्गी गुणधर्म (Pre-image Resistance / One-Way Property)
   दिलेल्या हॅश व्हॅल्यू H साठी अशी कोणतीही मेसेज M शोधणे संगणकीय दृष्ट्या अशक्य असते की:
   $$H = Hash(M)$$
   हा गुणधर्म डेटा रिव्हर्स-इंजिनिअरिंग रोखतो, जो पासवर्ड सिक्युरिटीसाठी अत्यंत महत्त्वाचा आहे.
4. सेकंड प्री-इमेज रेझिस्टन्स (Second Pre-image Resistance)
   दिलेल्या इनपुट M_1 साठी वेगळी मेसेज M_2 अशी शोधणे अशक्य असते की:
   $$Hash(M_1) = Hash(M_2)$$
   यामुळे मेसेज सब्स्टिट्यूशन अटॅक (Message Substitution Attacks) टाळले जातात.
5. कोलिजन रेझिस्टन्स (Collision Resistance)
   दोन वेगवेगळ्या मेसेजेस M_1 आणि M_2 साठी समान हॅश व्हॅल्यू शोधणे अत्यंत कठीण असले पाहिजे, म्हणजे:
   $$Hash(M_1) = Hash(M_2)$$
   यामुळे हॅश व्हॅल्यूची युनिकनेस (Uniqueness) सुनिश्चित होते.
6. ॲव्हलांच इफेक्ट (Avalanche Effect)
   इनपुटमध्ये अगदी छोटासा बदल (उदा. 1 बिट) केल्यास हॅश व्हॅल्यू पूर्णपणे वेगळी तयार झाली पाहिजे. यामुळे अनपेक्षितता (Unpredictability) आणि सिक्युरिटी वाढते.
7. संगणकीय कार्यक्षमता (Computational Efficiency)
   हॅशिंग प्रक्रिया जलद आणि कार्यक्षम असावी, विशेषतः मोठ्या डेटासाठी. TLS, IPSec आणि Blockchain सारखे प्रोटोकॉल्स जलद हॅशिंगचा वापर करून मोठ्या ट्रॅफिकवर प्रक्रिया करतात.
8. नॉन-रिव्हर्सिबल / एकमार्गी फंक्शन (Non-reversible / One-Way Function)
   हॅश फंक्शन्स अशा प्रकारे डिझाइन केलेले असतात की त्यांची उलट प्रक्रिया (Reverse Process) करणे संगणकीय दृष्ट्या अशक्य असते. हा गुणधर्म सुरक्षित पासवर्ड स्टोरेजसाठी अत्यावश्यक आहे.
9. युनिफॉर्म डिस्ट्रीब्युशन (Uniform Distribution)
   हॅश व्हॅल्यूज संपूर्ण रेंजमध्ये समान प्रमाणात वितरित झाल्या पाहिजेत, जेणेकरून अटॅकर्सना पॅटर्नचा फायदा घेता येणार नाही.
10. साधे आणि सहज अंमलबजावणीयोग्य (Simple and Easy to Implement)
    हॅश अल्गोरिदम्स सॉफ्टवेअर आणि हार्डवेअर दोन्हीमध्ये कार्यक्षमतेने अंमलात आणता येणे आवश्यक आहे, उदा. राऊटर्स, फायरवॉल्स आणि क्रिप्टोग्राफिक मॉड्यूल्स यामध्ये.

4.5.3. MD5 (मेसेज डायजेस्ट मेथड 5 | Message Digest Method 5)

MD5 ही एक क्रिप्टोग्राफिक हॅश फंक्शन आहे, जी Ron Rivest यांनी 1991 मध्ये विकसित केली. ही कोणत्याही लांबीचा इनपुट मेसेज स्वीकारते आणि त्यापासून 128-बिट (16-बाइट) हॅश व्हॅल्यू तयार करते, ज्याला मेसेज डायजेस्ट (Message Digest) असे म्हणतात.

MD5 चा ऐतिहासिक वापर पुढील क्षेत्रांमध्ये केला गेला आहे:

- डिजिटल सिग्नेचर्स (Digital Signatures)
- डेटा इंटिग्रिटी व्हेरिफिकेशन (Data Integrity Verification)

- पासवर्ड हॅशिंग (Password Hashing)
- फाइल चेकसम युटिलिटीज (File Checksum Utilities)

जरी MD5 ला आता कोलिजन अटॅक्स (Collision Attacks) साठी असुरक्षित (Cryptographically Insecure) मानले जात असले, तरी ज्या ठिकाणी उच्च स्तराची सुरक्षा आवश्यक नाही अशा अनुप्रयोगांमध्ये ते अजूनही उपयुक्त आहे. विशेषतः, अपघाती डेटा करप्शन (Accidental Data Corruption) ओळखण्यासाठी MD5 चा चेकसम म्हणून वापर केला जाऊ शकतो. त्याच्या कमकुवतपणांनंतरही, MD5 चा वापर काही नॉन-क्रिप्टोग्राफिक अनुप्रयोगांमध्ये केला जातो. उदाहरणार्थ, डिस्ट्रिब्यूटेड डेटाबेसमध्ये पार्टिशन्स निवडण्यासाठी MD5 वापरले जाते, कारण त्याचा वेग (Speed) आणि कमी संगणकीय खर्च (Low Computational Cost) हे आधुनिक Secure Hash Algorithms च्या तुलनेत फायदेशीर ठरतात.

MD5 अल्गोरिदम (MD5 Algorithm — Step-by-Step)

स्टेप 1: पॅडिंग (Padding)

MD5 प्रोसेसिंगसाठी मेसेज तयार करण्यासाठी मूळ मेसेजमध्ये पॅडिंग जोडले जाते.

• मेसेजच्या शेवटी 1 ते 512 बिट्सपर्यंत पॅडिंग जोडले जाते.

• पॅडिंगनंतर, मेसेजची एकूण लांबी ही 512 च्या पटीपेक्षा 64 बिट्सने कमी असली पाहिजे.

याचा अर्थ अंतिम पॅड केलेल्या मेसेजची लांबी खालील अट पूर्ण करते:

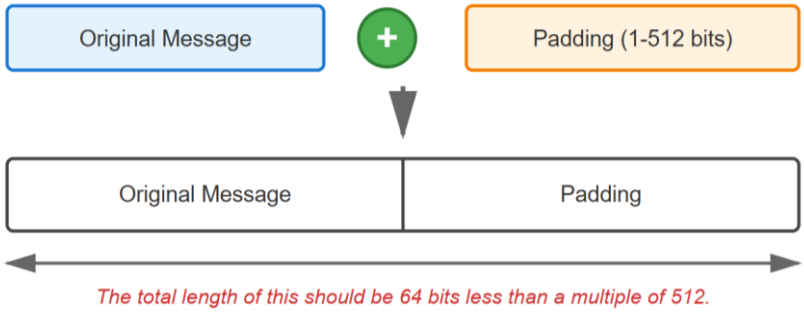


Fig 4.19: पॅडिंग (Padding)

उदाहरणे (Examples):

- 448 बिट्स (कारण 448 = 512 − 64)
- 960 बिट्स (कारण 960 = [2 × 512] − 64)
- 1472 बिट्स (कारण 1472 = [3 × 512] − 64)

टीप (Note): मूळ मेसेजची लांबी आधीच 512 बिट्सच्या पटीत असली तरीही पॅडिंग नेहमी जोडले जाते.

स्टेप 2: लांबी जोडणे (Append Length)

पॅडिंग केल्यानंतर, MD5 मूळ मेसेजची (पॅडिंगपूर्वीची) लांबी डेटाच्या शेवटी जोडते.

- मूळ मेसेजची लांबी (बिट्समध्ये) मोजली जाते.
- ही लांबी 64-बिट व्हॅल्यू म्हणून दर्शवली जाते.
- ही 64-बिट लांबीची व्हॅल्यू मेसेज + पॅडिंग यांच्या शेवटी जोडली जाते.

जर मूळ मेसेजची लांबी 64 बिट्सपेक्षा जास्त असेल (म्हणजेच 2^{64} पेक्षा मोठी असेल), तर लांबीतील फक्त सर्वात कमी महत्त्वाचे (Least Significant) 64 बिट्स वापरले जातात. म्हणजेच, मेसेजची लांबी 2^{64} ने मॉड्युलो (Modulo 2^{64}) घेतली जाते. 64-बिट लांबीची व्हॅल्यू जोडल्यावर, मेसेज पुढील स्वरूपाचा बनतो:

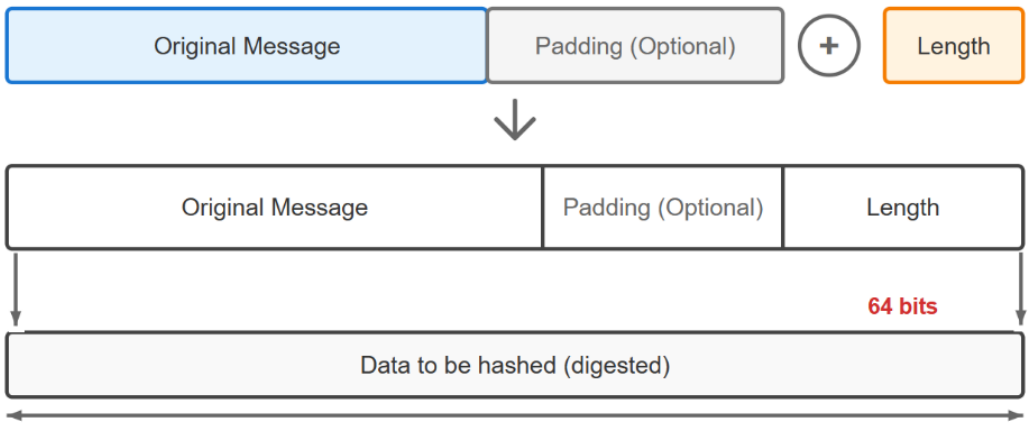


Fig 4.20: 64-बिट मेसेज (64-Bit Message)

यामुळे MD5 अल्गोरिदमद्वारे प्रक्रिया करण्यासाठी अंतिम मेसेज तयार होतो.

महत्त्वाचा मुद्दा (Key Point): लांबीचे फील्ड जोडल्यावर मेसेजचा एकूण आकार 512 बिट्सच्या पटीत येतो आणि तो हॅशिंगसाठी तयार होतो.

स्टेप 3: इनपुटला 512-बिट ब्लॉक्समध्ये विभागणे (Divide the Input into 512-bit Blocks)

मेसेजला पॅडिंग करून आणि 64-बिट लांबीची व्हॅल्यू जोडल्यानंतर, अंतिम मेसेजची लांबी 512 बिट्सच्या पटीत होते. यानंतर हा मेसेज निश्चित आकाराच्या ब्लॉक्समध्ये विभागला जातो, ज्यामध्ये प्रत्येक ब्लॉक नेमका 512 बिट्स लांबीचा असतो.

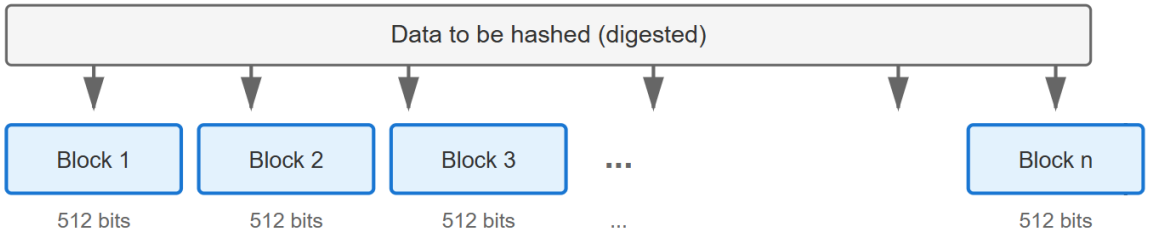


Fig 4.21: 512-बिट ब्लॉक्स (512-bit Blocks)

हॅशिंग दरम्यान प्रत्येक 512-बिट ब्लॉक MD5 कंप्रेशन फंक्शनद्वारे क्रमाने (Sequentially) प्रोसेस केला जातो.

स्टेप 4: चेनिंग व्हेरिएबल्सची सुरुवात (Initialize Chaining Variables)

मेसेज ब्लॉक्स प्रोसेस करण्यापूर्वी, MD5 चार 32-बिट चेनिंग व्हेरिएबल्सची सुरुवात करते. हे व्हेरिएबल्स हॅशिंग प्रक्रियेची प्रारंभिक स्थिती (Starting State) म्हणून कार्य करतात आणि प्रत्येक 512-बिट ब्लॉक प्रोसेस झाल्यानंतर अपडेट केली जातात.

प्रारंभिक व्हॅल्यूज (Hexadecimal मध्ये):

- A = 0x67452301
- B = 0xefcdab89
- C = 0x98badcfe
- D = 0x10325476

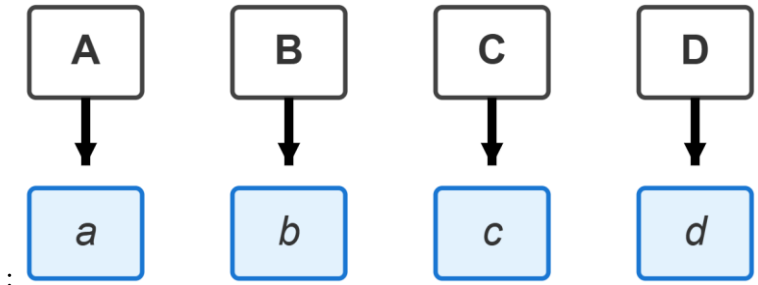
हे कॉन्स्टंट्स MD5 अल्गोरिदमद्वारे पूर्वनिश्चित (Predefined) केलेले आहेत आणि प्रत्येक हॅशिंग ऑपरेशनसाठी समानच राहतात. अल्गोरिदम प्रत्येक ब्लॉक प्रोसेस करत असताना ही व्हेरिएबल्स सातत्याने बदलत जातात, आणि त्यांची अंतिम एकत्रित व्हॅल्यूच 128-बिट MD5 हॅश तयार करते.

स्टेप 5: ब्लॉक्स प्रोसेस करणे (Process Blocks)

प्रत्येक 512-बिट मेसेज ब्लॉकसाठी पुढील टप्पे पार पाडले जातात:

1. चेनिंग व्हेरिएबल्स तात्पुरत्या रजिस्टरमध्ये कॉपी करणे (Copy chaining variables into temporary registers)

MD5 चेनिंग व्हेरिएबल्स A, B, C आणि D यांच्या सध्याच्या व्हॅल्यूज तात्पुरत्या व्हेरिएबल्समध्ये कॉपी केल्या जातात



:

Fig 4.22: चेनिंग व्हेरिएबल्स (Chaining Variables)

ही तात्पुरती व्हेरिएबल्स ब्लॉकच्या प्रोसेसिंग दरम्यान बदलली जातात, तर मूळ चेनिंग व्हेरिएबल्स पुढील अपडेटसाठी जतन (Preserve) करून ठेवली जातात.

2. 512-बिट ब्लॉकला 16 उप-ब्लॉक्समध्ये विभागणे (Divide the 512-bit Block into 16 Sub-blocks)
प्रत्येक 512-बिट मेसेज ब्लॉकला 16 उप-ब्लॉक्समध्ये विभागले जाते, आणि प्रत्येक उप-ब्लॉकची लांबी 32 बिट्स असते:

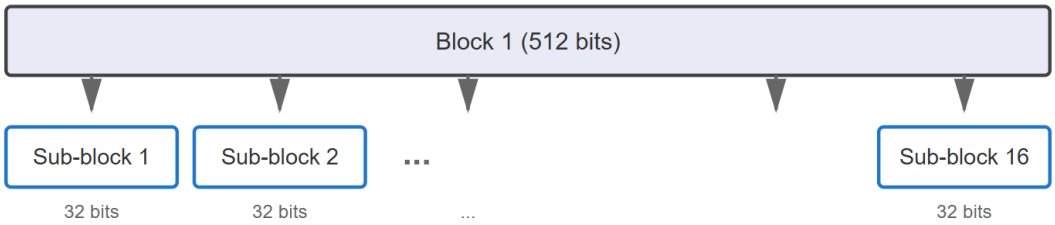


Fig 4.23: 16 उप-ब्लॉक्स (16 Sub-blocks)

हे 16 उप-ब्लॉक्स (M_0 ते M_{15}) MD5 च्या राऊंड ऑपरेशन्स दरम्यान एकामागोमाग एक वापरले जातात.

3. राऊंडमधील संकल्पनात्मक प्रक्रिया (Conceptual Process Within a Round)
प्रत्येक MD5 राऊंडमध्ये मेसेजचे 16 उप-ब्लॉक्स तसेच पूर्वनिश्चित (Predefined) कॉन्स्टंट्स वापरून प्रक्रिया केली जाते.
या प्रक्रियेदरम्यान चेनिंग व्हेरिएबल्स (a, b, c, d) वारंवार अपडेट केली जातात. ही अपडेट प्रक्रिया पुढील घटकांच्या संयोजनावर आधारित असते: ॲडिशन (Additions), नॉन-लिनिअर फंक्शन्स (Non-linear Functions), मेसेज वर्ड्स (Message Words), कॉन्स्टंट्स (Constants), सर्क्युलर शिफ्ट्स (Circular Shifts), या सर्व ऑपरेशन्समुळे MD5 हॅशिंग प्रक्रिया अधिक गुंतागुंतीची आणि सुरक्षित बनते.

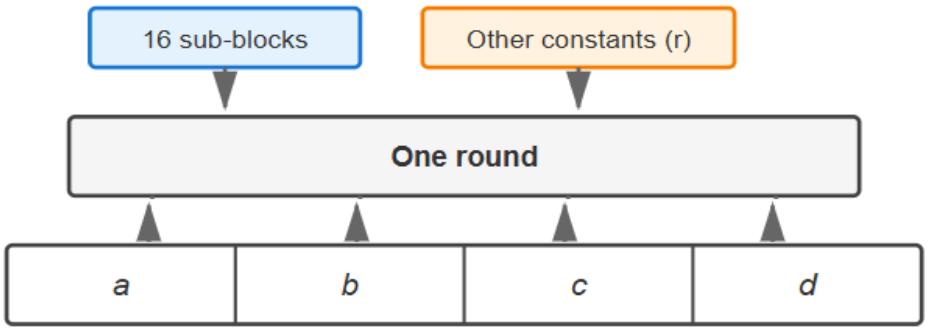


Fig 4.24: राऊंडमधील संकल्पनात्मक प्रक्रिया (Conceptual Process Within a Round)

एक MD5 ऑपरेशनचे गणितीय रूप (Mathematical Expression of a Single MD5 Operation)
एक MD5 ऑपरेशन खालीलप्रमाणे गणितीय स्वरूपात दर्शवता येते:

$$a = b + ((a + Process\ P\ (b, c, d) + M[i] + t[k]) <<< s)$$

जिथे:

- a, b, c, d → चेनिंग व्हेरिएबल्स (Chaining Variables)
- P(b, c, d) → राऊंड-विशिष्ट नॉन-लिनिअर फंक्शन (Round-specific Non-linear Function)
- M[i] → सध्याच्या 512-बिट मेसेज ब्लॉकमधील i वा 32-बिट उप-ब्लॉक
- t[k] → कॉन्स्टंट व्हॅल्यू (64 पूर्वनिश्चित कॉन्स्टंट्सच्या टेबलमधून)
- <<< s → s बिट्सने केलेला सर्क्युलर लेफ्ट शिफ्ट / रोटेशन (Circular Left Shift)

प्रत्येक राऊंडमध्ये ही ऑपरेशन अनेक वेळा लागू केली जाते, परंतु दरवेळी खालील घटक बदलले जातात:

- मेसेज वर्ड्स (M[i])
- कॉन्स्टंट्स (t[k])
- शिफ्ट अमाउंट्स (s)
- नॉन-लिनिअर फंक्शन्स (P)

सर्व चार राऊंड्स पूर्ण झाल्यानंतर तात्पुरती व्हेरिएबल्स (a, b, c, d) मध्ये अपडेट झालेल्या व्हॅल्यूज असतात, ज्या पुढे मुख्य चेनिंग व्हेरिएबल्समध्ये जोडल्या जातात.

स्टेप 6: चेनिंग व्हेरिएबल्स अपडेट करणे (Update Chaining Variables)

एका 512-बिट ब्लॉकसाठी MD5 चे सर्व चार राऊंड्स पूर्ण झाल्यानंतर, प्रोसेसिंग दरम्यान बदललेल्या तात्पुरत्या व्हेरिएबल्स a, b, c, d मूळ चेनिंग व्हेरिएबल्स A, B, C, D मध्ये परत जोडल्या जातात. यामुळे पुढील ब्लॉकसाठी MD5 ची स्टेट (State) अपडेट होते.

अपडेट खालीलप्रमाणे केली जाते:

$$A = A + a$$
$$B = B + b$$
$$C = C + c$$
$$D = D + d$$

(सर्व ॲडिशन्स modulo 2^{32} *प्रमाणे केली जातात.)*

या स्टेप चा उद्देश (Purpose of This Step)

- एका ब्लॉकचा आउटपुट पुढील ब्लॉकच्या इनपुटवर प्रभाव टाकतो.
- MD5 ला आवश्यक असलेला चेनिंग इफेक्ट (Chaining Effect) तयार होतो, जो त्याची क्रिप्टोग्राफिक रचना निश्चित करतो.
- अंतिम ब्लॉक प्रोसेस झाल्यानंतर A, B, C आणि D यांच्या व्हॅल्यूज एकत्रितपणे 128-बिट MD5 डायजेस्ट तयार करतात.

अंतिम MD5 हॅश (Final MD5 Hash)

अंतिम आउटपुट खालीलप्रमाणे तयार होतो: **MD5 Hash = A || B || C || D**

येथे प्रत्येक व्हॅल्यू 32-बिट वर्ड म्हणून little-endian फॉरमॅटमध्ये दर्शवली जाते. यामुळे एकूण 128-बिट (16-बाइट) MD5 हॅश व्हॅल्यू तयार होते.

4.5.2. SHA (सिक्युअर हॅशिंग अल्गोरिदम | Secure Hashing Algorithm)

सिक्युअर हॅश अल्गोरिदम (SHA) हा क्रिप्टोग्राफिक हॅश फंक्शन्सचा एक समूह (Family) आहे, जो नॅशनल इन्स्टिटयूट ऑफ स्टँडर्ड्स अँड टेकनॉलॉजि (National Institute of Standards and Technology) (NIST) आणि नॅशनल सिक्युरिटी एजन्सी National Security Agency (NSA) यांनी विकसित केला आहे. SHA अल्गोरिदम्स कोणत्याही लांबीचा मेसेज स्वीकारतात आणि त्यापासून निश्चित लांबीची हॅश व्हॅल्यू तयार करतात. यांचा वापर मोठ्या प्रमाणावर डिजिटल सिग्नेचर्स (Digital Signatures), ऑथेंटिकेशन (Authentication), इंटिग्रिटी व्हेरिफिकेशन (Integrity Verification), TLS/SSL, ब्लॉकचेन (Blockchain) तसेच विविध क्रिप्टोग्राफिक प्रोटोकॉल्समध्ये केला जातो.

SHA अल्गोरिदम कुटुंब (SHA Family of Algorithms)

1. SHA-0 (रद्द करण्यात आलेले | Withdrawn)
   - पहिली आवृत्ती (1993)
   - डिझाइनमधील त्रुटीमुळे (Design Flaw) रद्द करण्यात आली
2. SHA-1
   - 160-बिट हॅश आउटपुट
   - 512-बिट ब्लॉक्स प्रोसेस करते
   - कोलिजन अटॅक्समुळे आता कमजोर (Weak) मानले जाते
3. SHA-2 कुटुंब (SHA-2 Family)
   यामध्ये SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 यांचा समावेश होतो.
   - मजबूत (Strong) आणि मोठ्या प्रमाणावर वापरले जाणारे
   - आउटपुट लांबी: 224, 256, 384, 512 बिट्स
4. SHA-3 कुटुंब (SHA-3 Family)
   - Keccak अल्गोरिदमवर आधारित
   - अत्यंत सुरक्षित आणि आधुनिक डिझाइन

SHA-1 अल्गोरिदम — (SHA-1 Algorithm — Step-by-Step)

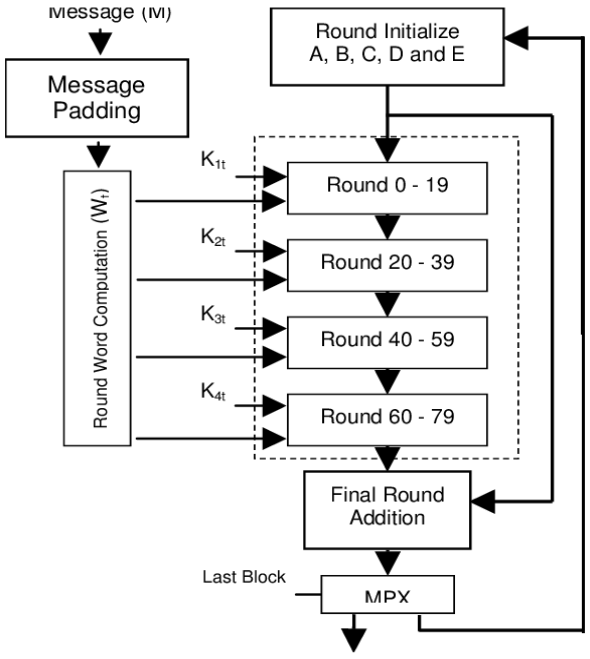


Fig 4.25: सिक्युअर हॅशिंग अल्गोरिदम (Secure Hashing Algorithm)

1. मेसेज (Message – M)
   हा मूळ इनपुट मेसेज आहे, ज्याचे रूपांतर निश्चित लांबीच्या हॅश व्हॅल्यूमध्ये केले जाते.
2. मेसेज पॅडिंग (Message Padding)
   प्रोसेसिंगपूर्वी मेसेजमध्ये पॅडिंग जोडले जाते, जेणेकरून त्याची लांबी 448 mod 512 शी सुसंगत (Congruent) होते. यामुळे अंतिम पॅड केलेला मेसेज अचूकपणे 512-बिट ब्लॉक्समध्ये विभागता येतो.
3. राऊंड वर्ड कॅलक्युलेशन (Round Word Computation – W_t)
   पॅडिंगनंतर:
   - मेसेज 512-बिट ब्लॉक्समध्ये विभागला जातो.
   - प्रत्येक ब्लॉक पुढे 16 वर्ड्समध्ये विभागला जातो, ज्यातील प्रत्येक वर्ड 32 बिट्सचा असतो.
   - हे 16 वर्ड्स पुढे विस्तारून (Expand करून) 80 32-बिट वर्ड्स तयार केले जातात. हे विस्तारित वर्ड्स अल्गोरिदमच्या 80 राऊंड्ससाठी इनपुट म्हणून वापरले जातात.

4. राऊंड इनिशियलायझेशन (Round Initialization – A, B, C, D, E)
   पाच वर्किंग व्हेरिएबल्स — A, B, C, D आणि E — पूर्वनिश्चित (Predefined) कॉन्स्टंट व्हॅल्यूजने इनिशियलाइझ केली जातात. ही व्हेरिएबल्स प्रत्येक राऊंडमध्ये ट्रान्सफॉर्म होत जातात आणि हळूहळू अंतिम हॅश व्हॅल्यू तयार करतात.
5. राऊंड कॉन्स्टंट्स (Round Constants – K_t)
   SHA-1 मध्ये 80 राऊंड्स दरम्यान चार कॉन्स्टंट व्हॅल्यूज वापरल्या जातात. प्रत्येक कॉन्स्टंट ठराविक राऊंड्ससाठी लागू असते:
   • K_1 → राऊंड्स 0–19
   • K_2 → राऊंड्स 20–39
   • K_3 → राऊंड्स 40–59
   • K_4 → राऊंड्स 60–79 या कॉन्स्टंट्समुळे वेगवेगळ्या टप्प्यांमध्ये ट्रान्सफॉर्मेशनची पद्धत बदलते.
6. राऊंड्स 0–79 (Rounds 0–79)
   SHA-1 मध्ये एकूण 80 पुनरावृत्ती (Iterative) राऊंड्स केले जातात, जे चार टप्प्यांमध्ये विभागलेले असतात (प्रत्येक टप्पा K_1 ते K_4 शी संबंधित).
   प्रत्येक राऊंडमध्ये:
   • लॉजिकल फंक्शन्स आणि बिटवाइज ऑपरेशन्स लागू केली जातात.
   • वर्किंग व्हेरिएबल्स (A–E) सध्याच्या वर्ड W_t आणि योग्य कॉन्स्टंट K_t वापरून अपडेट केली जातात.
   ही पुनरावृत्ती प्रक्रिया मेसेज कंप्रेशनचा मुख्य भाग आहे.
7. अंतिम राऊंड ॲडिशन (Final Round Addition)
   सर्व 80 राऊंड्स पूर्ण झाल्यानंतर:
   • A, B, C, D आणि E यांच्या अंतिम व्हॅल्यूज सुरुवातीच्या हॅश व्हॅल्यूजमध्ये जोडल्या जातात.
   • यामुळे अपडेटेड हॅश स्टेट (Updated Hash State) तयार होते.
8. MPX मल्टिप्लेक्सिंग (Multiplexing)
   अंतिम टप्प्यात वर्किंग व्हेरिएबल्सच्या अपडेटेड व्हॅल्यूज एकत्र केल्या जातात आणि त्यातून 160-बिट मेसेज डायजेस्ट तयार होतो, जो SHA-1 हॅश आउटपुट म्हणून ओळखला जातो.

4.6 डिजिटल सिग्नेचर (Digital Signature)

4.6.1. परिचय (Introduction)

डिजिटल सिग्नेचर ही एक सुरक्षित इलेक्ट्रॉनिक स्वाक्षरी आहे, जी प्रेषकाच्या प्रायव्हेट की (Private Key) चा वापर करून मेसेज डायजेस्ट (Message Digest) एन्क्रिप्ट करून तयार केली जाते. ही प्रेषकाची ओळख (Sender's Identity) पडताळून पाहते, ट्रान्समिशनदरम्यान मेसेजमध्ये कोणताही बदल झाला नाही याची खात्री (Integrity) देते, तसेच नॉन-रिप्युडिएशन (Non-repudiation) प्रदान करते. म्हणूनच डिजिटल सिग्नेचरचा वापर सुरक्षित इलेक्ट्रॉनिक व्यवहारांमध्ये (Secure Electronic Transactions) मोठ्या प्रमाणावर केला जातो.

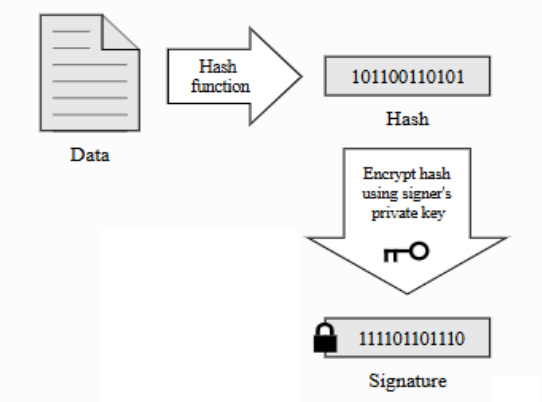


Fig 4.26: डिजिटल सिग्नेचर (Digital Signature)

डिजिटल सिग्नेचर तयार करण्याची प्रक्रिया मूळ डेटापासून सुरू होते. प्रथम, हा डेटा हॅशिंग अल्गोरिदममधून पास केला जातो, ज्यामुळे एक युनिक आणि एकमार्गी (One-Way) हॅश व्हॅल्यू तयार होते. ही हॅश व्हॅल्यू डेटाचे निश्चित आणि संक्षिप्त (Fixed, Compact) रूप दर्शवते. यानंतर प्रेषक ही हॅश व्हॅल्यू स्वतःच्या प्रायव्हेट की (Private Key) वापरून एन्क्रिप्ट करतो. प्रायव्हेट की फक्त प्रेषकाकडेच असल्यामुळे, ही एन्क्रिप्ट केलेली हॅश व्हॅल्यू डेटा खरोखरच त्या प्रेषकाकडून आला आहे याचा ठोस पुरावा देते. या एन्क्रिप्ट केलेल्या हॅशला डिजिटल सिग्नेचर (Digital Signature) असे म्हणतात. हे डिजिटल सिग्नेचर मूळ डेटासोबत रिसिव्हरकडे पाठवले जाते. त्यामुळे रिसिव्हरला मेसेजची ऑथेंटिसिटी (Authenticity) म्हणजे प्रेषकाची ओळख आणि इंटिग्रिटी (Integrity) म्हणजे मेसेजमध्ये कोणताही बदल झाला नाही याची पडताळणी करता येते.

4.6.2. डिजिटल सिग्नेचरचे कार्य (Working of Digital Signature)

डिजिटल सिग्नेचर ही एक क्रिप्टोग्राफिक यंत्रणा (Cryptographic Mechanism) आहे, जी इलेक्ट्रॉनिक मेसेजेस किंवा डॉक्युमेंट्ससाठी ऑथेंटिकेशन (Authentication), इंटिग्रिटी (Integrity) आणि नॉन-रिप्युडिएशन (Non-repudiation) सुनिश्चित करते. डिजिटल सिग्नेचरचे कार्य हॅश फंक्शन्स (Hash Functions), मेसेज डायजेस्ट (Message Digest) आणि असिमेट्रिक की क्रिप्टोग्राफी (Asymmetric Key Cryptography) म्हणजेच पब्लिक की (Public Key) आणि प्रायव्हेट की (Private Key) यांच्या साहाय्याने केले जाते.

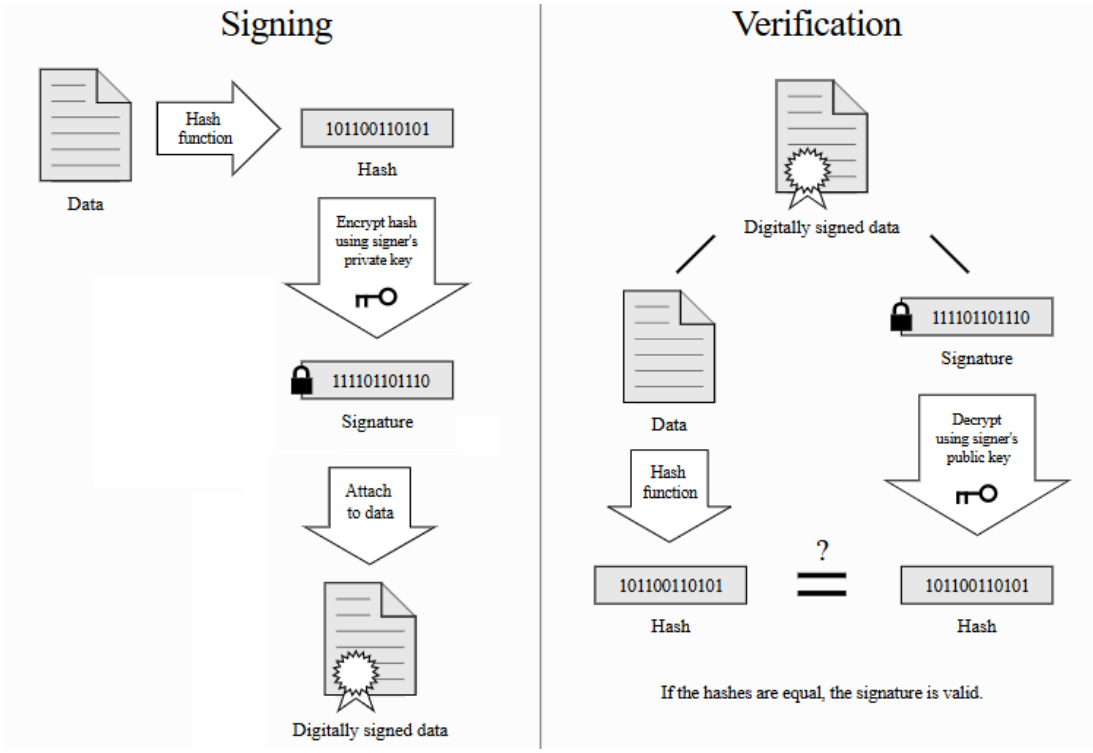


Fig 4.27: डिजिटल सिग्नेचरचे कार्य (Working of Digital Signature)

1. **की जनरेशन (Key Generation)**
   डिजिटल सिग्नेचर वापरण्यापूर्वी प्रेषक कींची एक जोडी (Key Pair) तयार करतो:
   - प्रायव्हेट की (Private Key) → डिजिटल सिग्नेचर तयार करण्यासाठी वापरली जाते
   - पब्लिक की (Public Key) → सिग्नेचरची पडताळणी करण्यासाठी इतरांना दिली जाते

   यामुळे ऑथेंटिसिटी (Authenticity) आणि ट्रस्ट (Trust) स्थापित होतो.
2. **डिजिटल सिग्नेचर तयार करणे – साइनिंग प्रक्रिया (Digital Signature Creation / Signing Process)**
   स्टेप 1: मेसेज डायजेस्ट तयार करणे (Generation of Message Digest)
   - प्रेषक मूळ मेसेजवर हॅश फंक्शन (उदा. SHA-256) लागू करतो.
   - यामुळे निश्चित लांबीचा आउटपुट तयार होतो, ज्याला मेसेज डायजेस्ट (Message Digest – MD) म्हणतात.
   - हा डायजेस्ट मेसेजच्या मजकुराचे युनिक प्रतिनिधित्व करतो.

   स्टेप 2: प्रेषकाच्या प्रायव्हेट की ने एन्क्रिप्शन (Encryption using Sender's Private Key)
   - प्रेषक मेसेज डायजेस्ट स्वतःच्या प्रायव्हेट की चा वापर करून एन्क्रिप्ट करतो.

- एन्क्रिप्ट केलेला डायजेस्ट म्हणजेच डिजिटल सिग्नेचर होय.

स्टेप 3: डेटा पाठवणे (Sending Data)

प्रेषक खालील माहिती रिसिव्हरकडे पाठवतो:

- प्लेनटेक्स्ट मेसेज (Plaintext Message)
- एन्क्रिप्ट केलेला मेसेज डायजेस्ट (डिजिटल सिग्नेचर)
- यामुळे साइनिंग स्टेज पूर्ण होते.

3. डिजिटल सिग्नेचरची पडताळणी – रिसिव्हर साइड (Digital Signature Verification – Receiver Side)

स्टेप 4: रिसिव्हरकडून मेसेज डायजेस्ट तयार करणे (Receiver Generates Message Digest)

- रिसिव्हर प्राप्त झालेल्या प्लेनटेक्स्ट मेसेजवर तोच हॅश फंक्शन लागू करतो.
- यामुळे नवीन मेसेज डायजेस्ट तयार होतो.

स्टेप 5: सिग्नेचर डिक्रिप्ट करणे (Decrypting the Signature)

- रिसिव्हर प्रेषकाची पब्लिक की वापरून डिजिटल सिग्नेचर डिक्रिप्ट करतो.
- यामुळे प्रेषकाने तयार केलेला मूळ मेसेज डायजेस्ट प्राप्त होतो.

स्टेप 6: पडताळणीसाठी तुलना (Comparison for Verification)

रिसिव्हर खालील दोन डायजेस्टची तुलना करतो:

- प्राप्त मेसेजवरून तयार झालेला मेसेज डायजेस्ट, आणि
- सिग्नेचर डिक्रिप्ट करून मिळालेला मेसेज डायजेस्ट

निर्णय (Decision)

- जर दोन्ही डायजेस्ट जुळले → सिग्नेचर VALID
  - मेसेज ऑथेंटिक आहे
  - मेसेजमध्ये कोणताही बदल झालेला नाही
  - प्रेषकाची ओळख सत्यापित होते
- जर डायजेस्ट जुळले नाहीत → सिग्नेचर INVALID
  - साइन केल्यानंतर मेसेजमध्ये बदल झाला आहे
  - सिग्नेचर किंवा मेसेजमध्ये छेडछाड (Tampering) झालेली आहे

4.6.3 डिजिटल सर्टिफिकेट (Digital Certificate)

डिजिटल सर्टिफिकेट हे एक इलेक्ट्रॉनिक डॉक्युमेंट आहे, जे विश्वासार्ह प्राधिकरणाद्वारे म्हणजेच सर्टिफिकेट अथॉरिटी (Certificate Authority – CA) कडून जारी केले जाते. हे एखाद्या व्यक्ती, डिव्हाइस, संस्था किंवा वेबसाईटची ओळख पडताळते आणि त्या ओळखीला पब्लिक की (Public Key) शी जोडते. नेटवर्कवर सुरक्षित आणि विश्वासार्ह कम्युनिकेशन (Secure and Trusted Communication) स्थापित करण्यासाठी डिजिटल सर्टिफिकेटचा वापर केला जातो.

उद्देश (Purpose): डिजिटल सर्टिफिकेट खालील गोष्टी सुनिश्चित करते:

- ऑथेंटिकेशन /प्रमाणीकरण (Authentication) → सर्टिफिकेट मालकाची ओळख निश्चित करते
- इंटिग्रिटी / प्रामाणिकपणा (Integrity) → डेटामध्ये कोणताही बदल झाला नाही याची खात्री देते
- कॉन्फिडेन्शियलिटी / गोपनीयता (Confidentiality) → सुरक्षित एन्क्रिप्शनसाठी सहाय्य करते
- नॉन-रिप्युडिएशन / नाकारता न येणे (Non-repudiation) → सर्टिफिकेट मालक स्वतःची ओळख नाकारू शकत नाही

डिजिटल सर्टिफिकेटचे प्रकार (Types of Digital Certificates)

- SSL/TLS सर्टिफिकेट्स – वेबसाईट्ससाठी (HTTPS सिक्युरिटी)
- कोड साइनिंग सर्टिफिकेट्स (Code Signing Certificates) – सॉफ्टवेअर प्रकाशकांसाठी
- ई-मेल सर्टिफिकेट्स (S/MIME) – सुरक्षित ई-मेल कम्युनिकेशनसाठी
- डॉक्युमेंट साइनिंग सर्टिफिकेट्स – PDF, Office डॉक्युमेंट्ससाठी
- क्लायंट ऑथेंटिकेशन सर्टिफिकेट्स

डिजिटल सर्टिफिकेट X.509

X.509 हा पब्लिक की सर्टिफिकेट्ससाठीचा एक आंतरराष्ट्रीय मानक (International Standard) आहे, जो HTTPS, SSL/TLS, ई-मेल सिक्युरिटी, VPNs आणि डिजिटल सिग्नेचर्स यांसारख्या सुरक्षित कम्युनिकेशन सिस्टिम्समध्ये ओळख पडताळणीसाठी वापरला जातो. X.509 हा अत्यंत मोठ्या प्रमाणावर वापरला जाणारा मानक आहे, जो डिजिटल सर्टिफिकेट्सची रचना (Structure) आणि फॉरमॅट (Format) निश्चित करतो. या सर्टिफिकेट्समध्ये सर्टिफिकेट मालकाची ओळख आणि त्याची पब्लिक की असते, आणि ती सर्टिफिकेट अथॉरिटी (CA) या विश्वासार्ह संस्थेद्वारे जारी व डिजिटल साइन केलेली असतात. जेव्हा तुम्ही एखादी सुरक्षित वेबसाईट (HTTPS) भेट देता, तेव्हा तुमचा ब्राऊजर X.509 सर्टिफिकेटचा वापर करून ती वेबसाईट खरी (Legitimate) आहे का आणि कनेक्शन एन्क्रिप्टेड आहे का हे तपासतो. X.509 सर्टिफिकेट्स म्हणजे इंटरनेटवरील डिजिटल ओळखपत्रे (Digital ID Cards) आहेत. ती तुमची ओळख सिद्ध करतात आणि तुमची ओळख तुमच्या पब्लिक की शी जोडून सुरक्षित कम्युनिकेशन शक्य करतात.

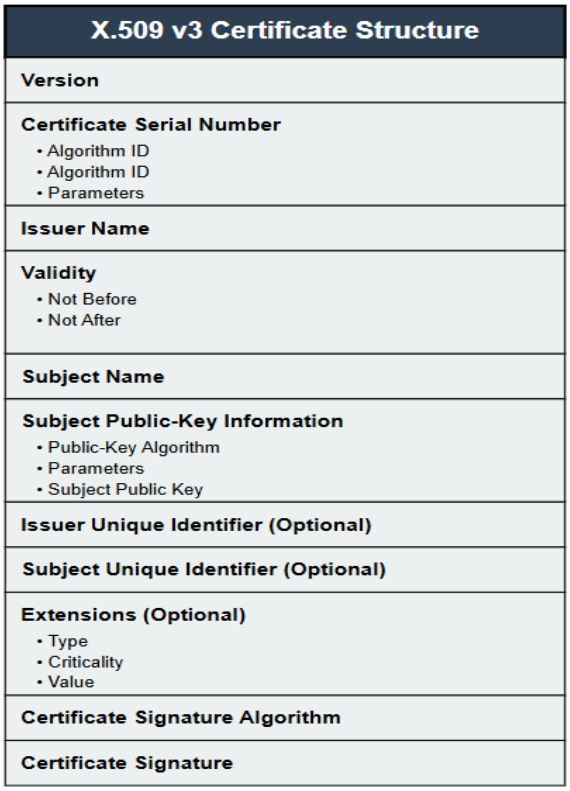


Fig 4.28: X.509 सर्टिफिकेट (X.509 Certificate)

X.509 Version 3 डिजिटल सर्टिफिकेट हे HTTPS, ई-मेल सिक्युरिटी, VPN ऑथेंटिकेशन इत्यादी PKI (Public Key Infrastructure) सिस्टिम्समध्ये वापरले जाते. आकृतीतील प्रत्येक विभाग सर्टिफिकेटमध्ये समाविष्ट असलेल्या विशिष्ट घटकाचे प्रतिनिधित्व करतो.

X.509 सर्टिफिकेटचे मुख्य घटक (Key Components of an X.509 Certificate)

1. **व्हर्जन (Version)**
   हा फील्ड सर्टिफिकेटचे व्हर्जन दर्शवतो. X.509 v3 सर्टिफिकेट्स प्रामुख्याने वापरले जातात, कारण त्यामध्ये एक्स्टेन्शन्स (Extensions) सपोर्ट केले जातात.
2. **सर्टिफिकेट सिरीयल नंबर (Certificate Serial Number)**
   हा सर्टिफिकेट अथॉरिटी (CA) कडून दिलेला एक युनिक नंबर असतो. सर्टिफिकेट ओळखण्यासाठी आणि व्यवस्थापनासाठी (विशेषतः रिव्होकेशनसाठी) याचा वापर केला जातो.
3. **अल्गोरिदम आयडी, अल्गोरिदम आयडी, पॅरामिटर्स (Algorithm ID, Algorithm ID, Parameters)**
   हा भाग सिग्नेचर अल्गोरिदम आयडेंटिफायर (Signature Algorithm Identifier) शी संबंधित असतो, ज्यामध्ये पुढील घटक असतात:

- Algorithm ID → उदा. RSA, ECDSA
- Algorithm ID (Hash) → उदा. SHA-256
- Parameters → अल्गोरिदमसाठी आवश्यक असलेली अतिरिक्त माहिती

यावरून CA ने सर्टिफिकेट साइन करण्यासाठी कोणता अल्गोरिदम वापरला आहे हे कळते.

4. **इश्यूअर नेम (Issuer Name)**
   हा सर्टिफिकेट जारी करणाऱ्या सर्टिफिकेट अथॉरिटीची ओळख दर्शवतो.
   उदाहरण फील्ड्स:
   - CN (Common Name)
   - O (Organization)
   - C (Country)

   या विभागातून सर्टिफिकेट कोणी जारी केले आहे हे समजते.
5. **वैधता कालावधी (Validity)**
   या विभागात खालील 2 फील्ड्स असतात:
   - Not Before → सर्टिफिकेट वैध होण्याची सुरुवात तारीख/वेळ
   - Not After → सर्टिफिकेटची समाप्ती तारीख/वेळ

   या दोन्ही मिळून सर्टिफिकेटचा Validity Period ठरतो.
6. **सब्जेक्ट नेम (Subject Name)**
   हा विभाग सर्टिफिकेट मालकाची (Subject) ओळख दर्शवतो.
   उदाहरणे:
   - वेबसाईटसाठी : CN = www.example.com
   - व्यक्तीसाठी: CN = User Name
7. **सब्जेक्ट पब्लिक-की माहिती (Subject Public-Key Information)**
   या ब्लॉकमध्ये सर्टिफिकेट मालकाची पब्लिक की आणि तिच्याशी संबंधित माहिती असते.
   यामध्ये समावेश होतो:
   - Public-Key Algorithm → कीचा प्रकार (RSA, EC इ.)
   - Parameters → अल्गोरिदम-विशिष्ट व्हॅल्यूज
   - Subject Public Key → प्रत्यक्ष पब्लिक की

   हीच की इतर लोक सर्टिफिकेट मालकाच्या सिग्नेचरची पडताळणी करण्यासाठी वापरतात.
8. **इश्यूअर युनिक आयडेंटिफायर (Issuer Unique Identifier) – ऐच्छिक**
   हा एक जुना आणि सध्या क्वचित वापरला जाणारा फील्ड आहे. इश्यूअरचे नाव बदलल्यास त्याची युनिक ओळख ठेवण्यासाठी वापरला जातो.
9. **सब्जेक्ट युनिक आयडेंटिफायर (Subject Unique Identifier) – ऐच्छिक**
   हा फील्ड देखील क्वचित वापरला जातो. एकाच नावाच्या अनेक एंटिटीज असतील तर सब्जेक्टला वेगळे ओळखण्यासाठी उपयोगी पडतो.
10. **एक्स्टेन्शन्स (Extensions) – ऐच्छिक पण महत्त्वाचे**
    हा विभाग फक्त X.509 v3 सर्टिफिकेट्समध्ये उपलब्ध असतो.
    एक्स्टेन्शन्समध्ये समावेश:
    - Type → एक्स्टेन्शनचा प्रकार (उदा. KeyUsage, BasicConstraints)
    - Criticality → ॲप्लिकेशनने हे एक्स्टेन्शन समजणे आवश्यक आहे की नाही
    - Value → प्रत्यक्ष एक्स्टेन्शन डेटा
    - सामान्य एक्स्टेन्शन्स:
    - सब्जेक्ट अल्टरनेटिव्ह नेम (SAN)

- की युसेज
- सर्टिफिकेट पॉलिसीज
- सीआरएल डिस्ट्रीब्युशन पॉइंट्स

एक्स्टेन्शन्समुळे v3 सर्टिफिकेट्स अधिक लवचिक (Flexible) बनतात.

11. **सर्टिफिकेट सिग्नेचर अल्गोरिदम (Certificate Signature Algorithm)**
    हा फील्ड डिजिटल सिग्नेचर तयार करण्यासाठी वापरलेल्या अल्गोरिदमची पुनरावृत्ती करतो. तो वर दिलेल्या Algorithm ID शी जुळलेला असणे आवश्यक आहे.
12. **सर्टिफिकेट सिग्नेचर (Certificate Signature)**
    हा सर्टिफिकेटमधील अंतिम भाग आहे. यामध्ये CA कडून तयार केलेला डिजिटल सिग्नेचर असतो. तो सर्टिफिकेटची इंटिग्रिटी (Integrity) आणि ऑथेंटिसिटी (Authenticity) सुनिश्चित करतो. जर सर्टिफिकेटमधील कोणताही फील्ड बदलला गेला, तर हा सिग्नेचर अवैध (Invalid) ठरतो.
    X.509 कुठे वापरले जाते (Where X.509 is Used)
    - HTTPS / SSL / TLS (वेबसाईट सिक्युरिटी)
    - डिजिटल सिग्नेचर्स (Digital Signatures)
    - ई-मेल एन्क्रिप्शन (S/MIME)
    - VPN ऑथेंटिकेशन
    - सुरक्षित सॉफ्टवेअर वितरण (Secure Software Distribution)

References:

1. Stallings, W., & Brown, L. (2014). *Computer Security: Principles and Practice* (3rd ed.). Pearson. ISBN: 978-0-13-377392-7.
2. Kahate, A. (2018). *Cryptography and Network Security* (3rd & 4th ed.). McGraw-Hill. ISBN: 978-9353163303.
3. Merkow, M., & Breithaupt, J. (2006). *Information Security: Principles and Practices*. Pearson. ISBN: 978-81-317-1288-7.
4. Pachghare, V. K. (2012). *Cryptography and Information Security*. Prentice Hall India. ISBN: 978-81-203-5082-3.
5. Gollmann, D. (2011). *Computer Security* (3rd ed.). Wiley. ISBN: 978-0-470-74115-3.
6. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
7. RFC 3174 — *US Secure Hash Algorithm 1 (SHA-1)*. Internet Engineering Task Force (IETF). https://www.ietf.org/rfc/rfc3174.txt
8. NPTEL. (2022). *Introduction to Information Security.* https://archive.nptel.ac.in/courses/106/106/106106129/
9. SWAYAM. (2022). *Information Technology Course.* https://onlinecourses.swayam2.ac.in/cec22_cs15/preview
10. Virtual Labs (IIIT Hyderabad). (n.d.). *Virtual Laboratory for Cryptography Experiments.* https://cse29-iiith.vlabs.ac.in/List%20of%20experiments.html

युनिट-5
नेटवर्क अँड डेटाबेस सेक्युरिटी
(Network and Database Security)

विषय निष्पत्ती (Course Outcome):

CO5: नेटवर्क आणि डेटाबेसवर सुरक्षा लागू करणे.

घटक निष्पत्ती (Theory Learning Outcome):

1. नेटवर्क-आधारित (Network-Based) आणि होस्ट-आधारित (Host-Based) IDS ची तुलना करा.
2. नेटवर्क सुरक्षेसाठी Kerberos आणि IP Security (IPSec) प्रोटोकॉल्स वापरा.
3. ई-मेल सुरक्षेसाठी वापरल्या जाणाऱ्या दिलेल्या प्रोटोकॉलचे स्पष्टीकरण द्या.
4. डेटाबेस सुरक्षेची गरज स्पष्ट करा.
5. क्लाउड सुरक्षा स्पष्ट करा. हार्डवेअर आणि सॉफ्टवेअर फायरवॉलमधील फरक सांगा.

5.1 इंट्रूजन डिटेक्शन सिस्टीम (Intrusion Detection System – IDS):

इंट्रूजन डिटेक्शन सिस्टीम (IDS) ही एक सुरक्षा यंत्रणा आहे, जी नेटवर्क ट्रॅफिक किंवा होस्टवरील ॲक्टिव्हिटीजचे सतत निरीक्षण करून दुर्भावनायुक्त वर्तन (Malicious Behavior), सिक्युरिटी पॉलिसीचे उल्लंघन (Policy Violations) किंवा संभाव्य घुसखोरीचे प्रयत्न (Attempted Intrusions) ओळखते. IDS ही सिस्टीम इव्हेंट्सचे सतत विश्लेषण करते आणि संशयास्पद ॲक्टिव्हिटी आढळल्यास त्वरित अलर्ट्स (Alerts) निर्माण करते. IDS चे मुख्य उद्दिष्ट हल्ले ओळखणे (Detect) हे आहे, त्यांना थेट रोखणे (Prevent) नव्हे. IDS तंत्रज्ञानाचे मुख्यतः दोन प्रकार केले जातात: नेटवर्क-आधारित IDS (Network-based IDS – NIDS) आणि होस्ट-आधारित IDS (Host-based IDS – HIDS). तसेच, डिटेक्शनसाठी सिग्नेचर-आधारित (Signature-based), ॲनॉमली -आधारित (Anomaly-based) आणि हायब्रिड (Hybrid) पद्धती वापरल्या जातात. अलर्ट्स तयार करून IDS इन्सिडेंट रिस्पॉन्स (Incident Response), डिजिटल फॉरेन्सिक्स (Digital Forensics) आणि कॉम्प्लायन्स रिपोर्टिंग (Compliance Reporting) यांना मदत करते. जरी IDS थेट हल्ले थांबवू शकत नसले, तरी लवकर सूचना देऊन आणि ॲडमिनिस्ट्रेटर्सना योग्य सुधारात्मक कारवाई करण्यास मदत करून संपूर्ण सुरक्षा व्यवस्थेला अधिक मजबूत बनवते.

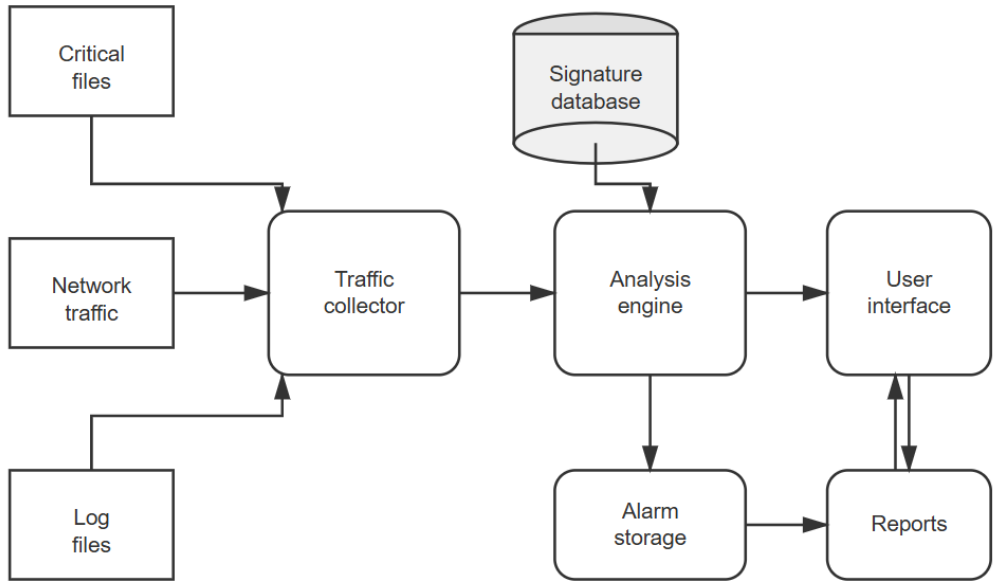


Fig 5.1: इंट्रूजन डिटेक्शन सिस्टीम (Intrusion Detection System – IDS)

1. **नेटवर्क ट्रॅफिक / क्रिटिकल फाइल्स / लॉग फाइल्स (Network Traffic / Critical Files / Log Files)**
   हे IDS साठी इनपुट स्रोत (Input Sources) आहेत.
   - नेटवर्क ट्रॅफिक: नेटवर्कमधून जाणारे रॉ पॅकेट्स जसे की TCP, UDP, ICMP, HTTP इत्यादी.

- क्रिटिकल फाइल्स: महत्त्वाच्या सिस्टम किंवा ॲप्लिकेशन फाइल्स, ज्यावर अनधिकृत बदल झाला आहे का हे तपासले जाते (मुख्यतः HIDS चे कार्य).
- लॉग फाइल्स: सिस्टम लॉग्स, ॲप्लिकेशन लॉग्स, ऑथेंटिकेशन लॉग्स, ज्यांच्या आधारे असामान्य किंवा दुर्भावनायुक्त ॲक्टिव्हिटी ओळखली जाते.

हे सर्व डेटा स्रोत IDS मध्ये मॉनिटरिंगसाठी माहिती पुरवतात.

2. **ट्रॅफिक कलेक्टर (Traffic Collector)**

हा IDS चा सेन्सर (Sensor) घटक आहे. तो पुढील गोष्टी गोळा करतो:

- नेटवर्कमधील पॅकेट्स
- फाइल सिस्टीममधील बदल
- लॉग एंट्रीज

याची मुख्य भूमिका रॉ डेटा कॅप्चर करून तो पुढील प्रक्रियेसाठी मानक (Standard) स्वरूपात रूपांतरित करणे ही आहे.

3. **ॲनालिसिस इंजिन (Analysis Engine)**

हा IDS चा मुख्य (Core) घटक असून प्रत्यक्ष इंट्रूजन डिटेक्शन येथेच होते. तो खालील पद्धती वापरतो:

- सिग्नेचर-आधारित डिटेक्शन (Signature-based Detection): ट्रॅफिक पॅटर्नची तुलना ज्ञात हल्ल्यांच्या सिग्नेचर्सशी करणे.
- ॲनॉमली-आधारित डिटेक्शन (Anomaly-based Detection): सामान्य वर्तनापासून झालेल्या विचलनांची ओळख करणे.
- स्टेटफुल ॲनालिसिस (Stateful Analysis): प्रोटोकॉलचे वर्तन वैध आहे की नाही हे तपासणे.

ॲनालिसिस इंजिन ठरवते की एखादा इव्हेंट सामान्य आहे की संशयास्पद.

4. **सिग्नेचर डेटाबेस (Signature Database)**

हा ज्ञात हल्ल्यांच्या पॅटर्न्सचा संग्रह आहे, जो व्हायरस सिग्नेचर्ससारखा असतो. यामध्ये खालील हल्ल्यांचे नियम (Rules) असतात:

- पोर्ट स्कॅन
- मालवेअर सिग्नेचर्स
- DoS हल्ल्यांचे पॅटर्न्स
- SQL Injection पॅटर्न्स
- बफर ओव्हरफ्लो
- इतर ज्ञात इंट्रूजन्स

ॲनालिसिस इंजिन सतत येणाऱ्या ट्रॅफिकची तुलना या डेटाबेसशी करत असते.

5. **अलार्म स्टोरेज (Alarm Storage)**

ॲनालिसिस इंजिनने संशयास्पद किंवा दुर्भावनायुक्त वर्तन ओळखल्यास अलार्म तयार केला जातो आणि तो येथे साठवला जातो. अलार्म स्टोरेजमध्ये पुढील नोंदी असतात:

- हल्ल्याची तारीख आणि वेळ
- सोर्स आणि डेस्टिनेशन IP ॲड्रेस
- हल्ल्याचा प्रकार
- तीव्रता (Severity)

सिक्युरिटी ॲडमिनिस्ट्रेटर्स हे अलार्म्स तपास, चौकशी आणि फॉरेन्सिक विश्लेषणासाठी वापरतात.

6. **युजर इंटरफेस (User Interface)**

हा तो भाग आहे जिथे सिस्टम ॲडमिनिस्ट्रेटर IDS चे आउटपुट पाहतो. युजर इंटरफेसद्वारे पुढील गोष्टी करता येतात:

- अलार्म्स पाहणे
- लाईव्ह ट्रॅफिक मॉनिटर करणे

- सिग्नेचर अपडेट्स मॅनेज करणे
- IDS नियम कॉन्फिगर करणे

7. **रिपोर्ट्स (Reports)**

IDS खालील बाबींचा सविस्तर अहवाल (Reports) तयार करते:

- ओळखलेले हल्ले
- ट्रॅफिक आकडेवारी
- ट्रेंड ॲनालिसिस
- फॉल्स पॉझिटिव्ह आणि फॉल्स निगेटिव्ह

हे रिपोर्ट्स ॲडमिनिस्ट्रेटर्सना धोके समजून घेण्यास आणि संपूर्ण सुरक्षा व्यवस्था सुधारण्यास मदत करतात.

5.1.1 नेटवर्क-आधारित इंट्रूजन डिटेक्शन सिस्टीम (Network-Based Intrusion Detection System – NIDS)

नेटवर्क-आधारित इंट्रूजन डिटेक्शन सिस्टीम (NIDS) ही अशी सुरक्षा प्रणाली आहे जी नेटवर्कमधील महत्त्वाच्या ठिकाणी (उदा. राऊटर्स, स्विचेस किंवा गेटवे) नेटवर्क ट्रॅफिकचे निरीक्षण व विश्लेषण करते, जेणेकरून दुर्भावनायुक्त ॲक्टिव्हिटी, हल्ले किंवा सिक्युरिटी पॉलिसीचे उल्लंघन ओळखता येईल. NIDS नेटवर्कमधून वाहणाऱ्या पॅकेट्सना निष्क्रियपणे (Passively) ऐकते आणि संशयास्पद किंवा असामान्य पॅटर्न्स ओळखते. ती पॅकेट हेडर्स आणि पेलोड्सचे निरीक्षण करते, त्यांची तुलना ज्ञात हल्ल्यांच्या सिग्नेचर्सशी करते आणि ट्रॅफिकच्या वर्तनाचे विश्लेषण करून स्कॅनिंग, इंट्रूजनचे प्रयत्न, डिनायल-ऑफ-सर्व्हिस (DoS) हल्ले किंवा प्रोटोकॉलचा गैरवापर ओळखते. NIDS रिअल-टाइममध्ये कार्य करते आणि साधारणपणे DMZ (Demilitarized Zone) किंवा अंतर्गत नेटवर्क सेगमेंट्ससारख्या धोरणात्मक (Strategic) ठिकाणी स्थापित केली जाते. संपूर्ण नेटवर्क सेगमेंटचे निरीक्षण केल्यामुळे NIDS व्यापक दृश्यमानता (Broad Visibility) प्रदान करते, मात्र एन्क्रिप्टेड ट्रॅफिक किंवा अतिवेगवान (High-Speed) नेटवर्क्समध्ये तिची कार्यक्षमता मर्यादित ठरू शकते. NIDS ही लेयर्ड सिक्युरिटी (Layered Security) चा महत्त्वाचा भाग आहे. ती फायरवॉल्स आणि होस्ट-आधारित IDS यांना पूरक ठरते, कारण ती परिमिती संरक्षण (Perimeter Defenses) चुकवून जाणाऱ्या धोक्यांची ओळख करून देते.

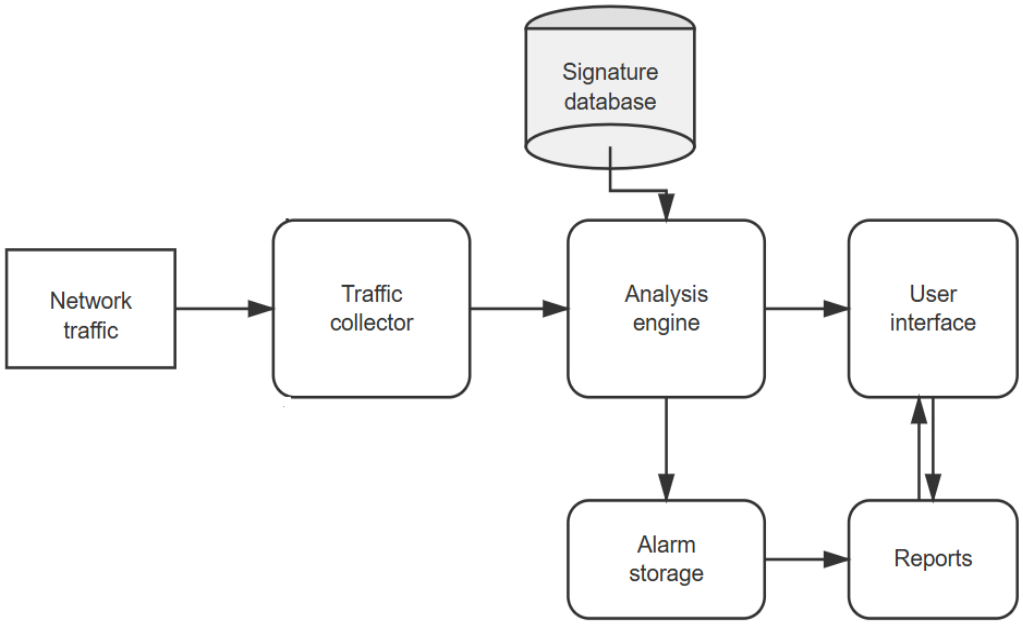


Fig 5.2: नेटवर्क-आधारित इंट्रूजन डिटेक्शन सिस्टीम (Network-based Intrusion Detection System – NIDS)

नेटवर्क-आधारित IDS चे घटक (Network-based IDS Components)

1. **नेटवर्क ट्रॅफिक (Network Traffic)**

नेटवर्कमधून येणारी आणि जाणारी सर्व डेटा पॅकेट्स येथे कॅप्चर केली जातात. ही रॉ पॅकेट्स IDS साठी मुख्य इनपुट म्हणून वापरली जातात.

2. **ट्रॅफिक कलेक्टर (Traffic Collector)**
   हा मॉड्यूल नेटवर्कमधील पॅकेट्स कॅप्चर करून त्यांची नोंद (Log) ठेवतो. तो डेटा मानक (Standard) स्वरूपात व्यवस्थित करतो, जेणेकरून ॲनालिसिस इंजिन त्यावर प्रक्रिया करू शकेल. हा घटक IDS साठी सेन्सरप्रमाणे कार्य करतो.
3. **ॲनालिसिस इंजिन (Analysis Engine)**
   हा IDS चा मुख्य डिटेक्शन घटक आहे. तो पुढील प्रकारचे विश्लेषण करतो: सिग्नेचर-आधारित डिटेक्शन, ज्यामध्ये ट्रॅफिक पॅटर्नची तुलना ज्ञात हल्ल्यांच्या सिग्नेचर्सशी केली जाते. ॲनॉमली-आधारित डिटेक्शन, ज्यामध्ये सामान्य वर्तनापासून झालेली विचलने ओळखली जातात. प्रोटोकॉल किंवा स्टेट ॲनालिसिस, ज्यामध्ये प्रोटोकॉल फ्लो योग्य आहे की नाही हे तपासले जाते. संशयास्पद ॲक्टिव्हिटी आढळल्यास ॲनालिसिस इंजिन अलार्म तयार करते.
4. **सिग्नेचर डेटाबेस (Signature Database)**
   हा ज्ञात हल्ल्यांच्या पॅटर्न्सचा संग्रह असतो. यामध्ये पोर्ट स्कॅनिंग, DoS हल्ल्यांचे पॅटर्न्स, SQL Injection सिग्नेचर्स, मालवेअर वर्तन आणि एक्सप्लॉईट फिंगरप्रिंट्स यांचा समावेश असतो. ॲनालिसिस इंजिन सतत येणाऱ्या ट्रॅफिकची तुलना या डेटाबेसशी करत असते.
5. **अलार्म स्टोरेज (Alarm Storage)**
   ॲनालिसिस इंजिनने इंट्रूजन ओळखल्यावर तयार झालेला अलार्म येथे साठवला जातो. यामध्ये हल्ल्याची वेळ, सोर्स आणि डेस्टिनेशन IP, तीव्रता (Severity) आणि हल्ल्याचा प्रकार यांसारखी माहिती असते. ही नोंद ॲडमिनिस्ट्रेटर्सना मागील अलर्ट्सचा आढावा घेण्यासाठी आणि फॉरेन्सिक विश्लेषणासाठी उपयुक्त ठरते.
6. **युजर इंटरफेस (User Interface)**
   हा ग्राफिकल किंवा कमांड-लाईन कन्सोल असतो, जिथे ॲडमिनिस्ट्रेटर IDS शी संवाद साधतो. याच्या मदतीने अलर्ट्स पाहणे, सिस्टम स्टेटस तपासणे, IDS कॉन्फिगरेशन मॅनेज करणे आणि सिग्नेचर्स अपडेट करणे शक्य होते.
7. **रिपोर्ट्स (Reports)**
   रिपोर्ट्समध्ये IDS ने शोधलेल्या माहितीचा सारांश दिला जातो. यामध्ये अलर्ट्सची संख्या, हल्ल्यांचे प्रकार, ट्रॅफिक आकडेवारी आणि फॉल्स पॉझिटिव्ह व फॉल्स निगेटिव्ह यांचा समावेश असतो. हे रिपोर्ट्स ऑडिटिंग, मॉनिटरिंग आणि भविष्यातील सिक्युरिटी नियोजनासाठी उपयोगी पडतात.

NIDS चे फायदे (Advantages of NIDS)

1. संपूर्ण नेटवर्क सेगमेंटचे निरीक्षण
   एकच NIDS सेन्सर नेटवर्कवरील अनेक डिव्हाइसेसचा ट्रॅफिक निरीक्षण करू शकतो, त्यामुळे संपूर्ण नेटवर्कवर व्यापक दृश्यमानता मिळते.
2. होस्टच्या कार्यक्षमतेवर परिणाम होत नाही
   NIDS हे नेटवर्कवर कार्य करते, स्वतंत्र संगणकांवर नाही, त्यामुळे होस्टच्या CPU किंवा मेमरी संसाधनांचा वापर होत नाही.
3. नेटवर्क हल्ल्यांची लवकर ओळख
   NIDS खालीलप्रमाणे हल्ले त्वरीत ओळखू शकते: पोर्ट स्कॅनिंग, DDoS हल्ले, वर्मचा प्रसार आणि मालवेअर कम्युनिकेशन. यामुळे लवकर सूचना मिळते आणि त्वरित प्रतिसाद देणे शक्य होते.
4. केंद्रीकृत मॉनिटरिंग
   संपूर्ण नेटवर्क ॲक्टिव्हिटी एक किंवा काही सेन्सर्सद्वारे मॉनिटर केली जाते, ज्यामुळे व्यवस्थापन अधिक सोपे आणि कार्यक्षम होते.
5. निष्क्रिय कार्यपद्धती (Passive Operation)
   NIDS ट्रॅफिकची प्रत (Copy) विश्लेषित करते, त्यामुळे कम्युनिकेशनमध्ये अडथळा येत नाही किंवा नेटवर्कचा वेग कमी होत नाही.
6. सिग्नेचर-आधारित अचूकता
   ज्ञात हल्ल्यांसाठी NIDS अद्ययावत सिग्नेचर डेटाबेस वापरून उच्च अचूकतेने डिटेक्शन करते.

NIDS चे तोटे (Disadvantages of NIDS)

1. एन्क्रिप्टेड ट्रॅफिक तपासता येत नाही
   HTTPS, SSL/TLS किंवा VPN ने एन्क्रिप्ट केलेले पॅकेट्स NIDS वाचू शकत नाही, त्यामुळे एन्क्रिप्टेड नेटवर्कमध्ये हल्ले ओळखणे कठीण होते.
2. ॲनॉमली डिटेक्शनमध्ये जास्त फॉल्स पॉझिटिव्ह्स
   सामान्य पण असामान्य वाटणारे ट्रॅफिक पॅटर्न्स अलर्ट ट्रिगर करू शकतात, ज्यामुळे ॲलर्ट फॅटिग निर्माण होते.
3. लोकल होस्टवरील हल्ले चुकू शकतात
   होस्टच्या आत होणारी दुर्भावनायुक्त ॲक्टिव्हिटी जसे की फाइल टॅम्परिंग किंवा प्रिव्हिलेज एस्कलेशन NIDS ओळखू शकत नाही.
4. हाय-स्पीड नेटवर्क हाताळणे कठीण
   अत्यंत वेगवान नेटवर्कमध्ये NIDS काही पॅकेट्स ड्रॉप करू शकते किंवा रिअल-टाइममध्ये संपूर्ण विश्लेषण करू शकत नाही.
5. हल्ले थेट रोखू शकत नाही
   NIDS ही फक्त डिटेक्शन सिस्टीम आहे. ती हल्ल्यांची सूचना देते, पण त्यांना ब्लॉक करत नाही (IPS प्रमाणे नाही).
6. सतत सिग्नेचर अपडेट्सची गरज
   नवीन धोके वारंवार उद्भवतात. सिग्नेचर अपडेट्स नसतील तर Zero-day अटॅक्स ओळखण्यात NIDS अपयशी ठरू शकते.

5.1.2 होस्ट-आधारित इंट्रूजन डिटेक्शन सिस्टीम (Host-Based Intrusion Detection System – HIDS)

होस्ट-आधारित इंट्रूजन डिटेक्शन सिस्टीम (HIDS) ही एक सुरक्षा साधन (Security Tool) आहे, जी एखाद्या विशिष्ट होस्ट किंवा डिव्हाइसवर (उदा. सर्व्हर, वर्कस्टेशन किंवा लॅपटॉप) इन्स्टॉल केली जाते. ती स्थानिक सिस्टम ॲक्टिव्हिटीचे निरीक्षण करते, जसे की लॉग फाइल्स, फाइल इंटिग्रिटी, युजर ॲक्शन्स, कॉन्फिगरेशन आणि सिस्टम प्रोसेसेस, जेणेकरून अनधिकृत किंवा दुर्भावनायुक्त वर्तन ओळखता येईल. HIDS ही थेट त्या होस्ट मशीनवर कार्य करते जिथे ती इन्स्टॉल केलेली असते. ती सिस्टम लॉग्स, युजर ॲक्टिव्हिटीज, क्रिटिकल फाइल्समधील बदल, रनिंग प्रोसेसेस, रजिस्ट्रि मॉडिफिकेशन्स आणि कॉन्फिगरेशन बदलांचे निरीक्षण करते. नेटवर्क-आधारित IDS (NIDS) नेटवर्क ट्रॅफिकचे विश्लेषण करते, तर HIDS अंतर्गत सिस्टम ॲक्टिव्हिटीवर लक्ष केंद्रित करते. म्हणूनच HIDS प्रिव्हिलेज एस्कलेशन, फाइल टॅम्परिंग, अनधिकृत प्रवेश आणि मालवेअर संसर्ग यांसारख्या इंट्रूजन्स ओळखण्यात अधिक प्रभावी ठरते. HIDS मध्ये प्रामुख्याने फाइल इंटिग्रिटी चेकिंग (उदा. MD5/SHA हॅशेसची तुलना), लॉग ॲनालिसिस, बिहेवियर मॉनिटरिंग आणि रूल-आधारित डिटेक्शन पद्धती वापरल्या जातात. नेटवर्क संरक्षण यंत्रणा चुकवून होणारे हल्ले ओळखण्यासाठी HIDS विशेषतः उपयुक्त आहे. मात्र, HIDS फक्त ज्या होस्टवर ती इन्स्टॉल केलेली असते त्या होस्टचेच निरीक्षण करते आणि संपूर्ण नेटवर्क-लेव्हल धोके ओळखू शकत नाही.

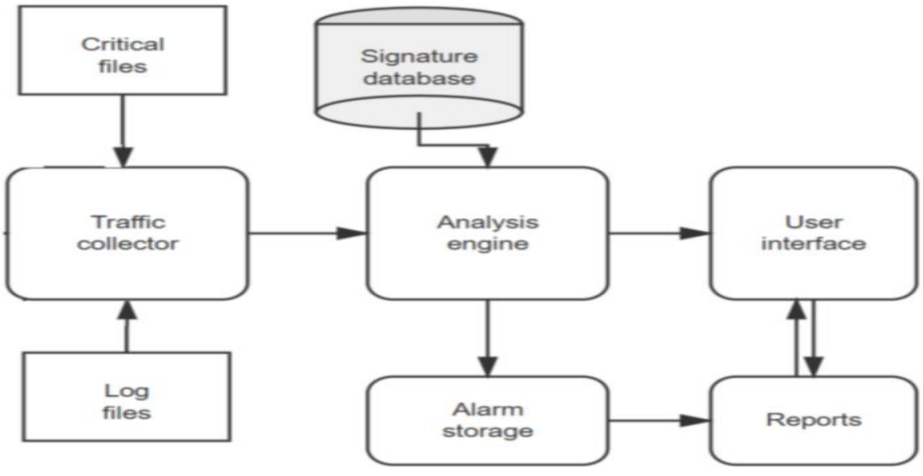


Fig 5.3: होस्ट-आधारित इंट्रूजन डिटेक्शन सिस्टीम (Host-based Intrusion Detection System – HIDS)

1. **क्रिटिकल फाइल्स (Critical Files)**
   या महत्त्वाच्या सिस्टम फाइल्स असतात, जसे की कॉन्फिगरेशन फाइल्स आणि सिक्युरिटी फाइल्स. या फाइल्समध्ये कोणताही बदल झाला आहे का यावर सतत लक्ष ठेवले जाते, कारण अनधिकृत बदल हे इंट्रूजनचे लक्षण असू शकतात.
2. **लॉग फाइल्स (Log Files)**
   सिस्टम लॉग्स, ॲप्लिकेशन लॉग्स आणि सिक्युरिटी लॉग्स गोळा केले जातात. या लॉग्समध्ये युजर ॲक्टिव्हिटीज, लॉगिन प्रयत्न, त्रुटी (Errors) आणि सिस्टम इव्हेंट्सची नोंद असते, जी असामान्य वर्तन ओळखण्यासाठी वापरली जाते.
3. **ट्रॅफिक कलेक्टर (Traffic Collector)**
   हा IDS चा सेन्सर घटक आहे. तो पुढील माहिती गोळा करतो: क्रिटिकल फाइल्समधील बदल, लॉग फाइल्स आणि सिस्टम ॲक्टिव्हिटी. ही माहिती पुढील तपासणीसाठी ॲनालिसिस इंजिनकडे पाठवली जाते.
4. **सिग्नेचर डेटाबेस (Signature Database)**
   या डेटाबेसमध्ये ज्ञात हल्ल्यांचे पॅटर्न्स साठवलेले असतात, उदा. पोर्ट स्कॅनिंग, मालवेअर सिग्नेचर्स, SQL Injection वर्तन आणि DoS हल्ल्यांचे पॅटर्न्स. ॲनालिसिस इंजिन गोळा केलेल्या डेटाची तुलना या सिग्नेचर्सशी करून इंट्रूजन ओळखते.
5. **ॲनालिसिस इंजिन (Analysis Engine)**
   हा IDS चा मुख्य घटक आहे. तो सिग्नेचर-आधारित डिटेक्शन आणि ॲनॉमली डिटेक्शन या पद्धती वापरतो. संशयास्पद ॲक्टिव्हिटी आढळल्यास अलार्म तयार केला जातो.
6. **अलार्म स्टोरेज (Alarm Storage)**
   ॲनालिसिस इंजिनद्वारे तयार झालेले अलार्म्स येथे साठवले जातात. यामध्ये हल्ल्याची वेळ, सोर्स आणि टार्गेट सिस्टम, हल्ल्याचा प्रकार आणि तीव्रता यांचा समावेश असतो. हे अलार्म्स ॲडमिनिस्ट्रेटर्स तपासणीसाठी वापरतात.
7. **युजर इंटरफेस (User Interface)**
   येथे सिस्टम ॲडमिनिस्ट्रेटर IDS शी संवाद साधतो. अलर्ट्स पाहणे, सिस्टम स्टेटस मॉनिटर करणे, सिग्नेचर्स अपडेट करणे आणि IDS नियम कॉन्फिगर करणे या सुविधा उपलब्ध असतात.
8. **रिपोर्ट्स (Reports)**
   IDS च्या कार्याचा सारांश रिपोर्ट्स स्वरूपात तयार केला जातो. यामध्ये अटॅक ट्रेंड्स, ट्रॅफिक आकडेवारी, अलर्ट्सची संख्या आणि फॉल्स पॉझिटिव्ह / फॉल्स निगेटिव्ह यांचा समावेश असतो. हे रिपोर्ट्स ऑडिटिंग आणि नेटवर्क सिक्युरिटी सुधारण्यासाठी उपयुक्त ठरतात.

होस्ट-आधारित इंट्रूजन डिटेक्शन सिस्टीम चे फायदे (Advantages of HIDS)

1. लोकल हल्ले प्रभावीपणे ओळखते
   HIDS होस्टच्या आत होणारे हल्ले जसे की अनधिकृत फाइल बदल, प्रिव्हिलेज एस्कलेशन किंवा मालवेअर एक्झिक्युशन प्रभावीपणे ओळखू शकते.
2. सिस्टम इंटिग्रिटीचे निरीक्षण
   HIDS क्रिटिकल फाइल्स, सिस्टम कॉन्फिगरेशन्स आणि लॉग्स तपासते, त्यामुळे फाइल टॅम्परिंग किंवा रूटकिट अटॅक्स ओळखण्यात ती उपयुक्त ठरते.
3. एन्क्रिप्टेड ट्रॅफिकवर कार्यक्षम
   NIDS प्रमाणे पॅकेट इन्स्पेक्शनवर अवलंबून न राहता HIDS थेट होस्टवरील ॲक्टिव्हिटीचे निरीक्षण करते. म्हणून HTTPS/SSL ने एन्क्रिप्ट केलेल्या ट्रॅफिकमध्येही HIDS संशयास्पद ॲक्टिव्हिटी ओळखू शकते.
4. होस्ट वर्तनासाठी कमी फॉल्स निगेटिव्ह्स
   सविस्तर सिस्टम लॉग्स आणि प्रोसेसेसचे विश्लेषण केल्यामुळे, नेटवर्क-आधारित सिस्टीम्सकडून चुकणारे लपलेले किंवा सूक्ष्म हल्ले HIDS ओळखू शकते.
5. फॉरेन्सिक विश्लेषणासाठी उपयुक्त
   HIDS प्रोसेसेस, युजर्स, फाइल ॲक्सेस आणि सिस्टम बदलांची सविस्तर नोंद ठेवते, जी घटनेनंतरच्या तपासासाठी अत्यंत उपयुक्त ठरते.

6. इनसाइडर थ्रेट्स ओळखते
   HIDS सिस्टिममधील दुर्भावनायुक्त कर्मचारी किंवा अनधिकृत युजर्सविरुद्ध प्रभावी ठरते.

होस्ट-आधारित इंट्रूजन डिटेक्शन सिस्टीम चे तोटे (Disadvantages of HIDS)

1. फक्त एका होस्टपुरते मर्यादित
   HIDS फक्त ज्या सिस्टमवर इन्स्टॉल केलेले असते त्या होस्टचेच निरीक्षण करते, संपूर्ण नेटवर्कचे नाही. अनेक डिव्हाइसेस सुरक्षित ठेवण्यासाठी अनेक HIDS एजंट्सची आवश्यकता असते.
2. जास्त संसाधनांचा वापर
   HIDS CPU, मेमरी आणि डिस्क I/O संसाधने वापरते, ज्यामुळे होस्ट मशीनची कार्यक्षमता कमी होऊ शकते.
3. हल्लेखोरांकडून डिसेबल होण्याची शक्यता
   HIDS ज्या होस्टवर चालते, त्याच होस्टवर हल्लेखोर किंवा मालवेअर असल्यास ती बदलली किंवा निष्क्रिय (Disable) केली जाऊ शकते.
4. मोठ्या नेटवर्कमध्ये व्यवस्थापन कठीण
   प्रत्येक मशीनवर स्वतंत्र इन्स्टॉलेशन, कॉन्फिगरेशन आणि अपडेट्स करावी लागतात, त्यामुळे मोठ्या नेटवर्कमध्ये HIDS चे व्यवस्थापन क्लिष्ट होते.
5. नेटवर्क-लेव्हल हल्ले ओळखू शकत नाही
   पोर्ट स्कॅनिंग किंवा DDoS सारखे होस्टच्या बाहेर होणारे हल्ले HIDS ला दिसत नाहीत.
6. मोठ्या प्रमाणात लॉग्स तयार होतात
   अत्यधिक लॉग डेटा तयार झाल्यामुळे, योग्य फिल्टरिंग आणि व्यवस्थापन नसेल तर ॲडमिनिस्ट्रेटर्सवर ताण येऊ शकतो.

Table 5.1: नेटवर्क-आधारित IDS (NIDS) आणि होस्ट-आधारित IDS (HIDS) यांची तुलना (Comparison of Network-Based IDS and Host-Based IDS)

निकष (Parameters)	नेटवर्क-आधारित IDS (NIDS)	होस्ट-आधारित IDS (HIDS)
स्थान (Location)	नेटवर्कमधील धोरणात्मक ठिकाणी (उदा. राऊटर्स, स्विचेस) स्थापित केले जाते.	प्रत्येक स्वतंत्र होस्टवर (सर्व्हर किंवा संगणकावर) थेट इन्स्टॉल केले जाते.
निरीक्षण केलेला डेटा (Data Monitored)	नेटवर्कमधून वाहणाऱ्या डेटा पॅकेट्सचे निरीक्षण करते.	सिस्टम लॉग्स, फाइल्स, प्रोसेसेस आणि सिस्टम कॉल्स यांचे निरीक्षण करते.
संरक्षणाची व्याप्ती (Scope of Protection)	संपूर्ण नेटवर्क सेगमेंटचे संरक्षण करते.	फक्त एका होस्टचे संरक्षण करते.
शोध क्षमता (Detection Capability)	बाह्य हल्ले, नेटवर्क स्कॅनिंग आणि DoS हल्ले ओळखण्यात प्रभावी.	अंतर्गत गैरवापर, अनधिकृत फाइल ॲक्सेस आणि रूटकिट्स ओळखण्यात प्रभावी.
संसाधन वापर (Resource Usage)	नेटवर्क हार्डवेअर संसाधने वापरते; होस्टच्या कार्यक्षमतेवर परिणाम होत नाही.	होस्टचा CPU, मेमरी आणि डिस्क संसाधने वापरते; सिस्टमची गती कमी होऊ शकते.
अंमलबजावणीची गुंतागुंत (Deployment Complexity)	एकाच वेळी अनेक मशीनसाठी डिप्लॉय करणे सोपे.	प्रत्येक होस्टवर स्वतंत्र इन्स्टॉलेशन व देखभाल आवश्यक.
दृश्यमानता (Visibility)	HTTPS सारखा एन्क्रिप्टेड ट्रॅफिक पाहू शकत नाही.	एन्क्रिप्शनपूर्वी किंवा डिक्रिप्शननंतर डेटा विश्लेषण करू शकते.
प्रतिसादाचा वेग (Response Speed)	मोठ्या प्रमाणावरील नेटवर्क हल्ल्यांवर जलद प्रतिसाद.	होस्ट-विशिष्ट हल्ले अधिक जलद ओळखते.

उदाहरणे (Examples)	Snort, Suricata, Cisco IDS, Bro/Zeek.	OSSEC, Tripwire, AIDE, Windows Event Auditing.
खर्च (Cost)	तुलनेने महाग; स्वतंत्र हार्डवेअरची गरज भासू शकते.	स्वस्त; सॉफ्टवेअर-आधारित आणि इन्स्टॉल करणे सोपे.
शोध अचूकता (Detection Accuracy)	ट्रॅफिक जास्त असल्यामुळे फॉल्स पॉझिटिव्ह्स जास्त असू शकतात.	सविस्तर होस्ट लॉग्सवर आधारित असल्यामुळे अधिक अचूक.
योग्य वापर (Best Use Cases)	मोठी नेटवर्क्स, एंटरप्राइझ परिमिती संरक्षण.	महत्त्वाचे सर्व्हर्स, वैयक्तिक वर्कस्टेशन्स, फाइल इंटिग्रिटी मॉनिटरिंग.

5.1.3 हनीपॉट्स (Honeypots)

हनीपॉट्स हे "ट्रॅप सिस्टीम्स" आहेत, ज्यांचा उपयोग घुसखोरीचे प्रयत्न (Intrusion Attempts) ओळखण्यासाठी, वळवण्यासाठी (Deflect) किंवा त्यांचे विश्लेषण करण्यासाठी केला जातो. हनीपॉट म्हणजे मुद्दाम असुरक्षित असल्यासारखी भासणारी एक डमी (Decoy) संगणक प्रणाली किंवा नेटवर्क संसाधन, जी हल्लेखोरांना आकर्षित करण्यासाठी डिझाइन केलेली असते. हनीपॉट कोणत्याही वैध (Legitimate) युजरसाठी वापरली जात नाही. तिचा एकमेव उद्देश हल्लेखोरांना आकर्षित करणे, त्यांच्या ॲक्टिव्हिटीची नोंद (Log) ठेवणे आणि दुर्भावनायुक्त वर्तनाचा अभ्यास करणे हा असतो. हनीपॉट्स फसवणूक (Deception) या तत्त्वावर कार्य करतात. यामध्ये मुद्दाम ओपन पोर्ट्स, सर्व्हिसेस किंवा भासमान असुरक्षा (Apparent Vulnerabilities) उघड्या ठेवल्या जातात, जेणेकरून संभाव्य हल्लेखोर आकर्षित होतील. एकदा हल्लेखोर सिस्टीमशी संवाद साधू लागला की, सविस्तर मॉनिटरिंग यंत्रणा त्याच्या सर्व ॲक्टिव्हिटी कॅप्चर करतात. यामध्ये एक्झिक्युट केलेल्या कमांड्स, इंटूजनचे प्रयत्न, मालवेअर डिप्लॉयमेंट, कीस्ट्रोक्स, IP ॲड्रेस आणि एक्सप्लॉईट पॅटर्न्स यांचा समावेश होतो. हनीपॉटमध्ये कोणताही खरा डेटा किंवा वैध युजर ॲक्टिव्हिटी नसल्यामुळे, त्यावर होणारा कोणताही ॲक्सेस प्रयत्न स्वभावतः संशयास्पद असतो. यामुळे प्रत्यक्ष नेटवर्क संसाधनांना धोका न पोहोचवता हल्ले सुरक्षितपणे आयसोलेट (Isolate) आणि कंटेन (Contain) करता येतात. गोळा केलेली माहिती सिक्युरिटी टीमकडून विश्लेषित केली जाते, ज्यामुळे हल्लेखोरांचे वर्तन, तंत्र (Techniques) आणि हल्ल्यांचे टप्पे जसे की रेकॉनिसन्स (Reconnaissance), एक्सप्लॉइटेशन (Exploitation) आणि कमांड एक्झिक्युशन समजून घेता येतात. हे निष्कर्ष IDS, फायरवॉल नियम आणि एकूणच इन्सिडेंट रिस्पॉन्स स्ट्रॅटेजी सुधारण्यासाठी उपयोगी ठरतात. तसेच, हनीपॉट्सवर जेव्हा दुर्भावनायुक्त ॲक्टिव्हिटी होते तेव्हा त्वरित अलर्ट्स तयार होतात. कोणतीही वैध ट्रॅफिक नसल्यामुळे, पारंपरिक IDS सिस्टीम्सच्या तुलनेत हनीपॉट्समध्ये फॉल्स पॉझिटिव्ह्स खूपच कमी असतात.

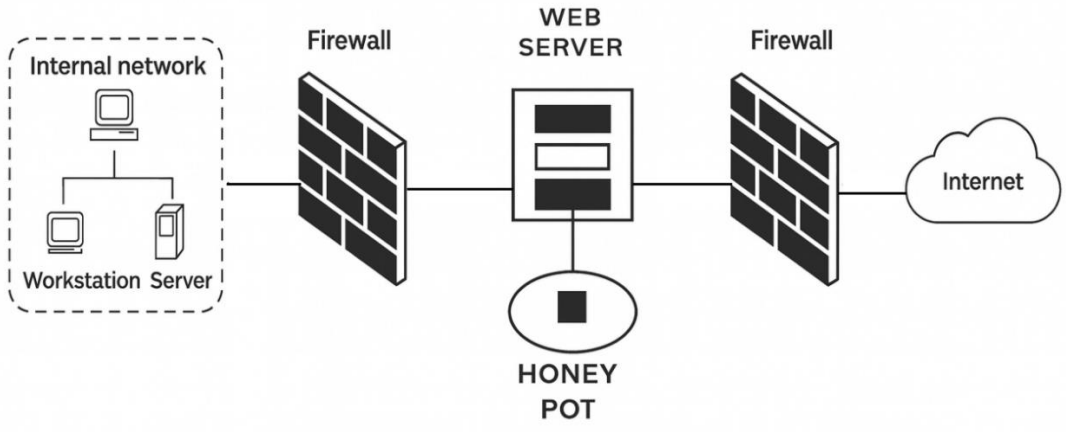


Fig 5.4: हनीपॉट (Honeypot)

या आकृतीमध्ये हनीपॉटची नेटवर्कमधील मांडणी (Placement) दर्शवलेली आहे. हनीपॉट दोन फायरवॉल्सच्या मध्ये ठेवलेला असतो. इंटरनेटवरील हल्लेखोर प्रथम एक्सटर्नल फायरवॉल (External Firewall) पार करतात आणि त्यानंतर वेब सर्व्हर व हनीपॉटपर्यंत पोहोचतात. हनीपॉट असे डिझाइन केलेले असते की ते हल्लेखोरांना आकर्षित करेल आणि त्यांना सापळ्यात (Trap) अडकवेल. हल्लेखोर जेव्हा हनीपॉटशी संवाद साधतात, तेव्हा त्यांच्या सर्व ॲक्टिव्हिटीचे निरीक्षण व नोंद केली जाते. दरम्यान, इंटरनल फायरवॉल (Internal Firewall) हा प्रत्यक्ष कॉर्पोरेट नेटवर्कचे संरक्षण करतो. यामुळे,

जरी हल्लेखोर हनीपॉटशी संपर्क साधत असले तरीही खरे सर्व्हर्स, डेटाबेस आणि अंतर्गत सिस्टम्स सुरक्षित राहतात. या रचनेमुळे हल्लेखोरांचे वर्तन अभ्यासता येते आणि प्रत्यक्ष नेटवर्क संसाधनांना कोणताही धोका पोहोचत नाही.

हनीपॉट्सचे प्रकार (Types of Honeypots)

A. इंटरॅक्शन लेव्हलवर आधारित (Based on Interaction Level)

1. लो-इंटरॅक्शन हनीपॉट्स (Low-Interaction Honeypots)
   - मर्यादित सर्व्हिसेसचे सिम्युलेशन करतात
   - सुरक्षित (Safe) आणि सहज डिप्लॉय करता येतात
   - ऑटोमेटेड हल्ले ओळखण्यासाठी वापरले जातात (उदा. वर्म्स, नेटवर्क स्कॅन्स)
2. हाय-इंटरॅक्शन हनीपॉट्स (High-Interaction Honeypots)
   - प्रत्यक्ष सर्व्हिसेस आणि पूर्ण ऑपरेटिंग सिस्टीम प्रदान करतात
   - हल्लेखोरांना पूर्णपणे इंटरॅक्ट करण्याची मुभा देतात
   - सखोल वर्तनात्मक विश्लेषणासाठी वापरले जातात
   - धोका जास्त असतो, पण अधिक तपशीलवार डेटा मिळतो

B. उद्देशावर आधारित (Based on Purpose)

1. प्रॉडक्शन हनीपॉट्स (Production Honeypots)
   - संस्थांमध्ये वापरले जातात
   - घुसखोरीचे प्रयत्न लवकर ओळखण्यास मदत करतात
2. रिसर्च हनीपॉट्स (Research Honeypots)
   - विद्यापीठे, CERT टीम्स (Computer Emergency Response Team) आणि सायबरसिक्युरिटी संशोधक वापरतात
   - प्रगत हल्ल्यांच्या तंत्रांचा अभ्यास करण्यासाठी वापरले जातात

हनीपॉट्सची उदाहरणे (Examples of Honeypots)

उदाहरण 1: वेब हनीपॉट (Web Honeypot): असुरक्षित लॉगिन पेजेस असलेली बनावट वेबसाईट. SQL Injection, Brute-force अटॅक्स आणि वेब एक्सप्लॉईटेशन प्रयत्न आकर्षित करते.

उदाहरण 2: SSH हनीपॉट (SSH Honeypot): पोर्ट 22 वर SSH चालू असल्यासारखा भासणारा सर्व्हर. पासवर्ड गेसिंग अटॅक्सची नोंद ठेवण्यासाठी वापरला जातो.

उदाहरण 3: मालवेअर हनीपॉट (Malware Honeypot): वर्म्स किंवा व्हायरस आकर्षित करण्यासाठी डिझाइन केलेला डमी संगणक. मालवेअर कलेक्शन आणि विश्लेषणासाठी वापरला जातो.

उदाहरण 4: ई-मेल हनीपॉट / स्पॅम ट्रॅप (Email Honeypot / Spam Trap): बनावट ई-मेल अकाउंट्स तयार करून स्पॅम मेसेजेस गोळा केले जातात. स्पॅमिंग तंत्रांचा अभ्यास करण्यासाठी वापरले जाते.

उदाहरण 5: डेटाबेस हनीपॉट (Database Honeypot): मुद्दाम असुरक्षित ठेवलेला डमी डेटाबेस सर्व्हर. SQL Injection किंवा अनधिकृत डेटा ॲक्सेस प्रयत्न ओळखण्यासाठी वापरला जातो.

उदाहरण 6: इंडस्ट्रियल कंट्रोल हनीपॉट्स (Industrial Control Honeypots / SCADA HoneyNet): वीज ग्रीड्स, फॅक्टरी सिस्टीम्स आणि IoT डिव्हाइसेसवरील हल्ले समजून घेण्यासाठी वापरले जातात.

हनीपॉट्सचे फायदे (Advantages of Honeypots)

- फॉल्स पॉझिटिव्ह्स अत्यंत कमी
- नवीन / Zero-day हल्ले समजून घेण्यास मदत
- हल्लेखोरांचे वर्तन सहजपणे विश्लेषित करता येते
- फॉरेन्सिक तपासणीसाठी उपयुक्त
- प्रॉडक्शन सिस्टीम्सचे संरक्षण (हल्ले वळवून)
- संशोधन आणि अध्यापनासाठी उपयुक्त

हनीपॉट्सच्या मर्यादा (Limitations of Honeypots)

- हनीपॉटवर लक्ष न दिलेले हल्ले ओळखता येत नाहीत
- हाय-इंटरॅक्शन हनीपॉट्ससाठी काळजीपूर्वक आयसोलेशन आवश्यक
- कुशल हल्लेखोर हनीपॉट ओळखू शकतात
- चुकीचे कॉन्फिगरेशन केल्यास सुरक्षा धोका निर्माण होऊ शकतो

5.2 केर्बेरॉस (Kerberos)

5.2.1 केर्बेरॉस: वर्किंग, ऑथेंटिकेशन सर्व्हर (AS), टिकट ग्रॅन्टिंग सर्व्हिस (TGS), सर्व्हिस सर्व्हर (SS)

केर्बेरॉस हा एक नेटवर्क ऑथेंटिकेशन प्रोटोकॉल आहे, जो MIT (Massachusetts Institute of Technology) येथे विकसित करण्यात आला आहे. हा प्रोटोकॉल सिमेट्रिक की क्रिप्टोग्राफी (Symmetric Key Cryptography) चा वापर करून असुरक्षित नेटवर्कवर युजर्स आणि सर्व्हिसेसचे सुरक्षित प्रमाणीकरण करतो.

केर्बेरॉस खालील सुविधा प्रदान करतो

- म्युच्युअल ऑथेंटिकेशन (Mutual Authentication)
- सिंगल साइन-ऑन (Single Sign-On – SSO)
- ईव्ह्सड्रॉपिंग (Eavesdropping) आणि रिप्ले अटॅक्स (Replay Attacks) पासून संरक्षण

केर्बेरॉस मध्ये एक विश्वासार्ह तृतीय पक्ष वापरला जातो, ज्याला Key Distribution Center (KDC) म्हणतात.

KDC मध्ये दोन मुख्य घटक असतात :

1. ऑथेंटिकेशन सर्व्हर Authentication Server (AS)
2. टिकट ग्रॅन्टिंग सर्व्हिस Ticket Granting Server (TGS)

नेटवर्कवरील प्रत्यक्ष सेवा सर्व्हिस सर्व्हर Service Server (SS) द्वारे प्रदान केल्या जातात.

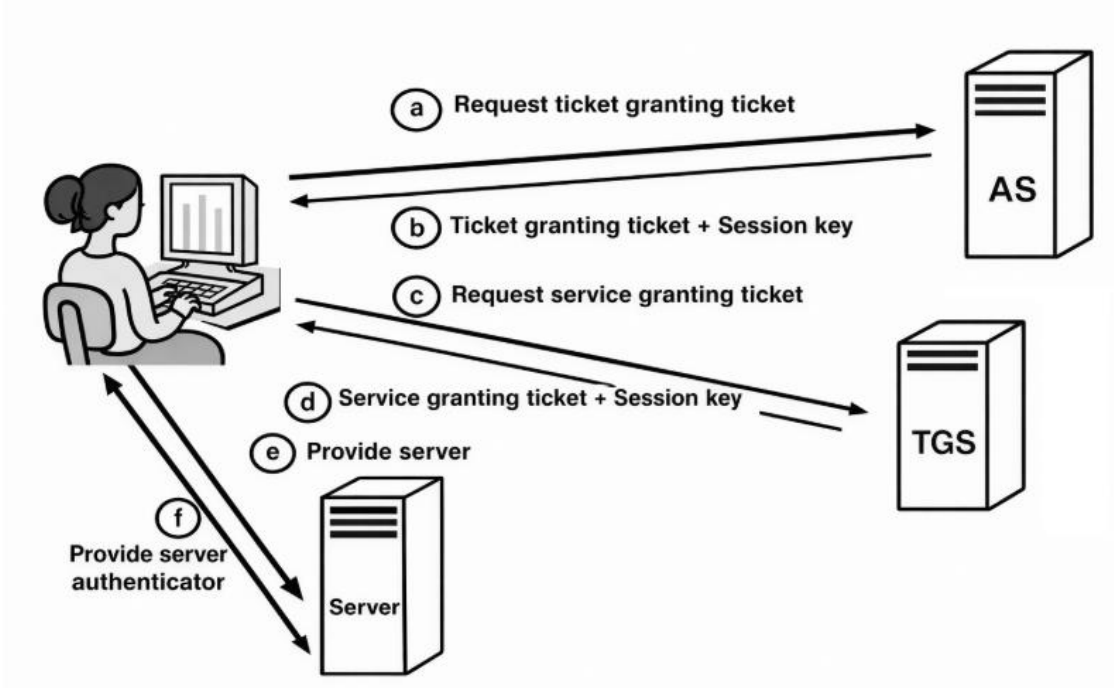


Fig 5.5: केर्बेरॉसचे कार्य (Working of Kerberos)

केर्बेरॉसचे कार्य (स्टेप-बाय-स्टेप)

केर्बेरॉस ऑथेंटिकेशन **(Authentication) तीन टप्प्यांमध्ये (Phases)** होते:

फेज 1: वापरकर्ता लॉगिन आणि AS सोबत प्रमाणीकरण

स्टेप 1: वापरकर्ता प्रवेशाची विनंती करतो

वापरकर्ता क्लायंट मशीनवर आपले यूजरनेम (Username) टाकतो.

स्टेप 2: AS ओळख तपासतो

ऑथेंटिकेशन सर्व्हर Authentication Server (AS) पुढील कार्य करतो:

- डेटाबेसमध्ये वापरकर्त्याची नोंद तपासतो
- तिकीट ग्रॅन्टिंग तिकीट (Ticket Granting Ticket – TGT) तयार करतो
- TGT ला TGS च्या सिक्रेट की (Secret Key) ने एन्क्रिप्ट करतो
- तसेच एक सेशन की (Session Key) पाठवतो, जी वापरकर्त्याच्या पासवर्ड (Password) वरून तयार झालेल्या सिक्रेट कीने एन्क्रिप्ट केलेली असते

स्टेप 3: वापरकर्त्याला TGT मिळतो

क्लायंट वापरकर्त्याच्या पासवर्डवरून तयार झालेल्या कीचा वापर करून संदेश डिक्रिप्ट करतो. पासवर्ड योग्य असल्यास सेशन की (Session Key) मिळते.

TGT मध्ये खालील माहिती असते:

- यूजर आयडी (User ID)
- क्लायंट नेटवर्क ॲड्रेस (Client Network Address)
- व्हॅलिडिटी पिरियड (Validity Period)
- TGS सोबत संवादासाठी सेशन की (Session Key)

फेज 2: TGS कडे प्रवेशाची विनंती

स्टेप 4: क्लायंट सर्व्हिस टिकटसाठी विनंती करतो

वापरकर्त्याला नेटवर्क सेवा वापरायची असल्यास, क्लायंट खालील माहिती टिकिट ग्रॅन्टिंग सर्व्हर (Ticket Granting Server – TGS) कडे पाठवतो:

- TGT
- सर्व्हिस आयडी (Service ID)

स्टेप 5: TGS TGT ची पडताळणी करतो

TGT वैध असल्यास, TGS पुढील गोष्टी तयार करतो:

- मागितलेल्या सेवेकरिता सर्व्हिस टिकट (Service Ticket – ST)
- क्लायंट–सेवा संवादासाठी नवीन सेशन की (Session Key)

सर्व्हिस टिकट Service Server च्या सिक्रेट की (Secret Key) ने एन्क्रिप्ट केलेले असते.

स्टेप 6: क्लायंटला सर्व्हिस टिकट मिळते

सर्व्हिस टिकट (ST) क्लायंटकडे साठवून ठेवले जाते आणि आवश्यकतेनुसार वापरले जाते.

फेज 3: सर्व्हिस सर्व्हर (SS) ला प्रवेश

स्टेप 7: क्लायंट सर्व्हिस टिकट SS कडे पाठवतो

सेवेला प्रवेश करताना, क्लायंट खालील गोष्टी पाठवतो:

- सर्व्हिस टिकट (ST)
- ऑथेंटिकेटर (Authenticator) – (टाइमस्टॅम्प + क्लायंट आयडी), सेशन कीने एन्क्रिप्ट केलेले

स्टेप 8: SS पडताळणी करून क्लायंटचे प्रमाणीकरण करतो

तिकीट आणि ऑथेंटिकेटर जुळल्यास:

- सर्व्हिस सर्व्हर (SS) क्लायंटला स्वीकारतो
- ऐच्छिकरित्या म्युच्युअल ऑथेंटिकेशन साठी उत्तर पाठवतो (टाइमस्टॅम्प – 1)

स्टेप 9: सुरक्षित संवाद सुरू होतो

यानंतर दोन्ही बाजू सेशन की (Session Key) वापरून सुरक्षितपणे संवाद साधतात.

केर्बेरॉस सर्व्हर (Kerberos Servers)

1. **ऑथेंटिकेशन सर्व्हर (Authentication Server – AS)**

   भूमिका (Role): वापरकर्त्याची ओळख (credentials) तपासणे आणि सुरुवातीचे टिकिट ग्रॅन्टिंग तिकीट (Ticket Granting Ticket – TGT) तयार करणे.

जबाबदाऱ्या (Responsibilities):

1. वापरकर्त्याचे प्रमाणीकरण (Authentication) करणे
2. क्लायंट–TGS संवादासाठी सेशन की (Session Key) तयार करणे
3. TGS च्या सिक्रेट की ने एन्क्रिप्ट केलेले TGT जारी करणे
4. नेटवर्कवर थेट पासवर्ड पाठवला जाणार नाही याची खात्री करणे

AS चे आउटपुट (Output of AS):

- टिकिट ग्रॅन्टिंग तिकीट (TGT)
- सेशन की (Client ↔ TGS)

2. टिकट ग्रॅन्टिंग सर्व्हर (Ticket Granting Server – TGS)

भूमिका (Role): विविध नेटवर्क सेवांसाठी सर्व्हिस टिकट (Service Ticket) जारी करणे.

जबाबदाऱ्या (Responsibilities):

1. TGT ची वैधता तपासणे
2. क्लायंट आणि सर्व्हिस सर्व्हर यांच्यातील संवादासाठी नवीन सेशन की तयार करणे
3. सर्व्हिस सर्व्हरच्या सिक्रेट की ने एन्क्रिप्ट केलेले सर्व्हिस टिकट (ST) तयार करणे

TGS चे आउटपुट (Output of TGS):

- सर्व्हिस टिकट (ST)
- सेशन की (Client ↔ Service Server)

3. सर्व्हिस सर्व्हर (Service Server – SS)

भूमिका (Role): प्रत्यक्ष नेटवर्क सेवा पुरवणे (उदा. फाइल सर्व्हर, ई-मेल सर्व्हर, डेटाबेस इ.).

जबाबदाऱ्या (Responsibilities):

1. सर्व्हिस टिकट (ST) ची पडताळणी करणे
2. क्लायंटचा ऑथेंटिकेटर (Authenticator) तपासणे
3. म्युच्युअल ऑथेंटिकेशन (Mutual Authentication) करणे
4. मागितलेल्या सेवेचा सुरक्षित प्रवेश प्रदान करणे

SS चे आउटपुट (Output of SS):

2.4 सुरक्षित सेशन की वापरून सेवा उपलब्ध करून देणे.

5.2.2 आयपी सिक्युरिटी (IP Security)

a. ओव्हरव्ह्यू (Overview)

IP सुरक्षा (IPsec) ही प्रोटोकॉल्सची एक संच (suite) आहे, जी IP कम्युनिकेशन सुरक्षित करण्यासाठी डिझाइन करण्यात आली आहे. IPsec द्वारे कॉन्फिडेन्शिअलिटी (Confidentiality), इंटेग्रिटी (Integrity), ऑथेंटिकेशन (Authentication) आणि रिप्ले अटॅक प्रोटेक्शन (Replay Attack Protection) मिळते. IPsec हे TCP/IP प्रोटोकॉल स्टॅकच्या नेटवर्क लेयरवर (Network Layer) कार्य करते आणि IP-आधारित नेटवर्कवरून जाणाऱ्या सर्व ट्रॅफिकचे संरक्षण करते.IPsec ट्रान्समिशन दरम्यान ट्रान्सपोर्ट लेयर आणि ॲप्लिकेशन लेयरमधील डेटा एन्क्रिप्ट आणि सील करते, ज्यामुळे अनधिकृत व्यक्तींना डेटा ॲक्सेस करता येत नाही. तसेच, ते इंटरनेट लेयरसाठी इंटिग्रिटी संरक्षण देते, म्हणजे ट्रान्झिट दरम्यान IP पॅकेट्समध्ये कोणताही बदल झाला आहे का हे तपासते. IPsec हे पारंपरिक TCP/IP प्रोटोकॉल स्टॅकमधील इंटरनेट लेयर आणि ट्रान्सपोर्ट लेयर यांच्या मध्ये लॉजिकलरित्या स्थित असते. त्यामुळे वरच्या लेयरमधील ॲप्लिकेशन्समध्ये कोणताही बदल न करता सुरक्षा वाढवता येते, ही IPsec ची मोठी जमेची बाजू आहे.

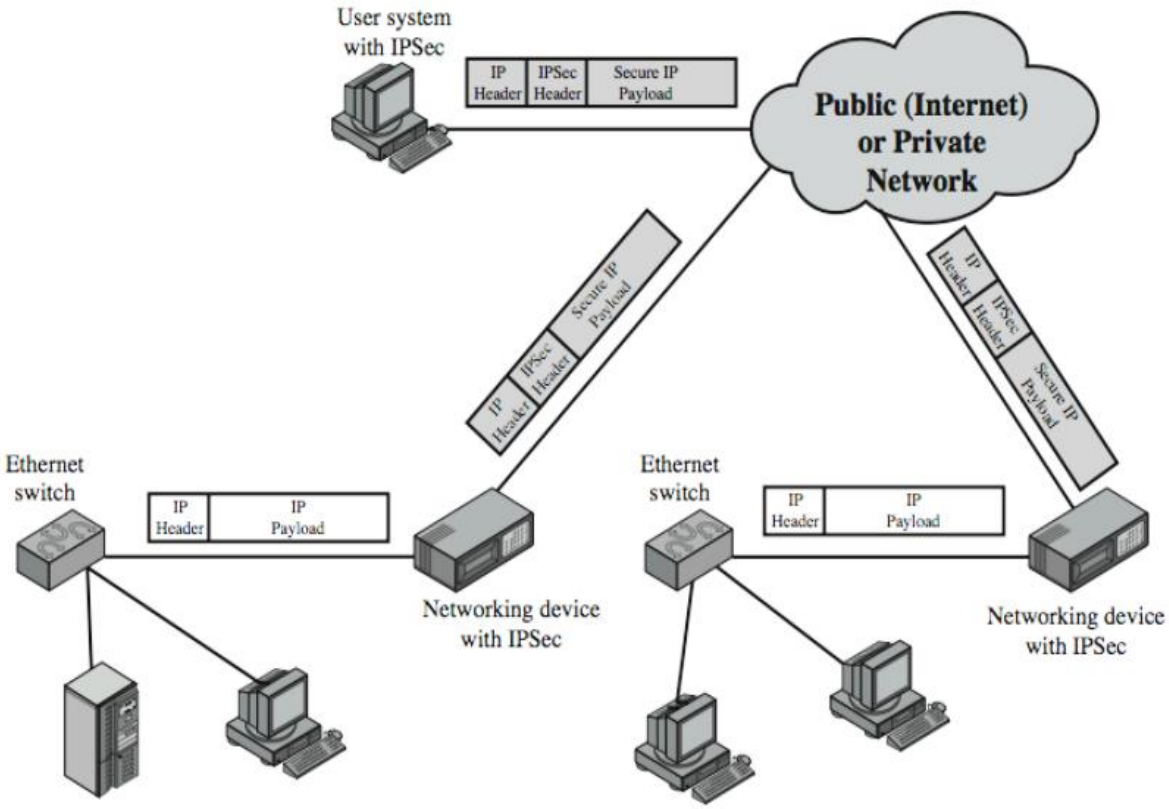


Figure 5.6: IP सुरक्षा (IPsec) चे कार्य (Working of IP Security)

IPsec हे पब्लिक किंवा प्रायव्हेट नेटवर्कवरून युजर सिस्टिम्स आणि नेटवर्किंग डिव्हाइसेस यांच्यातील कम्युनिकेशन सुरक्षित करते. आकृतीच्या वरच्या भागात, IPsec सक्षम असलेली युजर सिस्टिम डेटा पाठवते. हा डेटा पुढील घटकांसह एन्कॅप्सुलेट केला जातो:

1. IP हेडर
- IPsec हेडर (Authentication Header – AH किंवा Encapsulating Security Payload – ESP)
- सुरक्षित IP पेलोड (Secure IP Payload)

हा एन्कॅप्सुलेट केलेला पॅकेट नंतर एक्स्टर्नल नेटवर्क (क्लाऊड) मधून प्रवास करतो, जे इंटरनेट किंवा प्रायव्हेट WAN असू शकते. IPsec लागू असल्यामुळे, हा डेटा एन्क्रिप्शन (Encryption), इंटेग्रिटी चेकिंग (Integrity Checking) आणि ऑथेंटिकेशन (Authentication) यांच्या सहाय्याने सुरक्षित राहतो, जरी तो अनट्रस्टेड नेटवर्कमधून जात असला तरीही. क्लाऊडच्या दोन्ही बाजूंना IPsec सक्षम नेटवर्किंग डिव्हाइसेस (जसे राऊटर्स, फायरवॉल्स किंवा VPN गेटवे) हे सुरक्षित पॅकेट्स प्रोसेस करतात.

2. जेव्हा पॅकेट्स पब्लिक नेटवर्कमध्ये पाठवले जातात, तेव्हा ही डिव्हाइसेस IPsec वापरून त्यांना एन्कॅप्सुलेट करतात, सामान्यतः टनेल मोड (Tunnel Mode) मध्ये.
3. टनेल मोडमध्ये फक्त डेटा (Payload) नाही, तर मूळ IP हेडर देखील संरक्षित केला जातो.

जेव्हा पॅकेट्स डेस्टिनेशन गेटवेवर पोहोचतात, तेव्हा IPsec डी-एन्कॅप्सुलेशन (Decapsulation) होते. यामध्ये IPsec हेडर काढून टाकला जातो आणि मूळ IP पॅकेट पुन्हा प्राप्त केले जाते. आकृतीच्या खालच्या डाव्या आणि उजव्या बाजूला दाखवलेल्या इंटरनल LAN नेटवर्क्समध्ये, डिव्हाइसेस ईथरनेट स्विचेसद्वारे सामान्य IP पॅकेट्स वापरून संवाद साधतात. या पॅकेट्समध्ये फक्त: IP हेडर, IP पेलोड असतो. हे इंटरनल नेटवर्क्स ट्रस्टेड वातावरण असल्यामुळे त्याठिकाणी IPsec ची आवश्यकता नसते. IPsec फक्त तेव्हाच वापरले जाते जेव्हा डेटा दूरस्थ साइट्स किंवा रिमोट युजर्सदरम्यान एक्स्टर्नल नेटवर्कमधून प्रवास करतो. एकूणात, ही आकृती अनसिक्युअर्ड इंटरनल कम्युनिकेशन आणि IPsec-सुरक्षित वाइड-एरिया कम्युनिकेशन यातील फरक स्पष्टपणे दाखवते. तसेच, IPsec कसा एंड-टू-एंड (End-to-End) किंवा साइट-टू-साइट (Site-to-Site) सुरक्षित डेटा ट्रान्सफर शक्य करतो, हे ठळकपणे स्पष्ट करते.

IPsec चे उपयोग (Applications of IPsec)

1. **सुरक्षित रिमोट इंटरनेट ॲक्सेस (Secure Remote Internet Access):** IPsec मुळे वापरकर्ते घर, हॉटेल किंवा दूरस्थ ठिकाणांहून आपल्या संस्थेच्या अंतर्गत नेटवर्कला सुरक्षितपणे प्रवेश करू शकतात. इंटरनेट सर्व्हिस सुप्रोव्हायडर (ISP) च्या माध्यमातून सुरक्षित कनेक्शन स्थापन करून कर्मचारी कॉर्पोरेट रिसोर्सेस, रिमोट डेस्कटॉप्स आणि सर्व्हर्स वापरू शकतात, जणू ते ऑफिसमध्येच उपस्थित आहेत.
2. **रक्षित ब्रांच ऑफिस कनेक्टिव्हिटी (Secure Branch Office Connectivity):** महागड्या leased lines वापरण्याऐवजी, संस्था वेगवेगळ्या शहरांतील ब्रांच ऑफिसेसना IPsec सक्षम VPNs च्या सहाय्याने जोडू शकतात. यामुळे एन्क्रिप्टेड, सुरक्षित आणि खर्च-कार्यक्षम (cost-effective) इंटर-ऑफिस कम्युनिकेशन शक्य होते.
3. **वेगवेगळ्या संस्थांमधील सुरक्षित कम्युनिकेशन (Secure Communication between Different rganizations):** IPsec चा वापर दोन किंवा अधिक संस्थांची नेटवर्क्स सुरक्षितपणे जोडण्यासाठी देखील केला जाऊ शकतो. यामुळे सुरक्षित डेटा एक्सचेंज, सहकार्य (collaboration) आणि पार्टनर इंटिग्रेशन शक्य होते, तसेच अंतर्गत इन्फ्रास्ट्रक्चर थ्रेट्सपासून सुरक्षित राहते.

b. ऑथेंटिकेशन हेडर (Authentication Header – AH)

Authentication Header (AH) हा IPsec मधील दोन मुख्य सिक्युरिटी प्रोटोकॉल्सपैकी एक आहे. तो IP पॅकेट्ससाठी पुढील सुरक्षा प्रदान करतो:

- डेटा ओरिजिन ऑथेंटिकेशन (Data Origin Authentication)
- इंटेग्रिटी (Integrity)
- अँटी-रिप्ले प्रोटेक्शन (Anti-Replay Protection)

मात्र, AH कॉन्फिडेन्शियलिटी प्रदान करत नाही, कारण तो डेटाचे एन्क्रिप्शन करत नाही. म्हणजेच, डेटा बदलला गेला नाही आणि तो योग्य स्रोताकडूनच आला आहे याची खात्री AH देतो, पण डेटा वाचण्यायोग्यच राहतो.

ऑथेंटिकेशन हेडर (AH) फॉरमॅट:

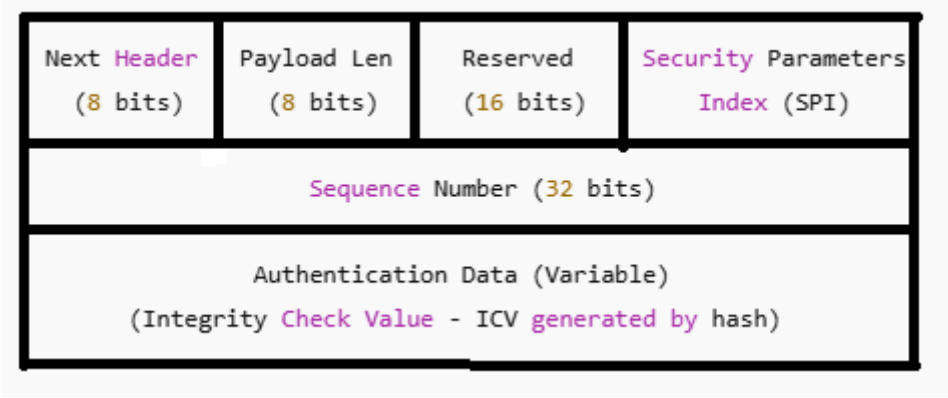


Figure 5.7 : ऑथेंटिकेशन हेडर (AH) फॉरमॅट

IP पॅकेटमधील AH :

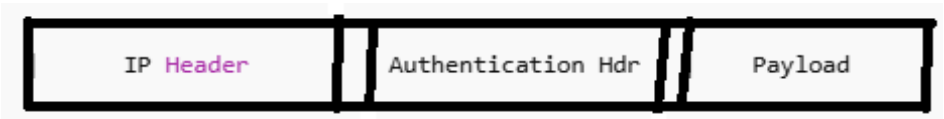


Figure 5.8 : IP पॅकेटमधील AH

1. **Next Header (8 bits)**
   • AH नंतर येणाऱ्या हेडरचा प्रकार दर्शवतो (उदा. TCP, UDP, ICMP).
   • रिसीव्हरला पुढील प्रोटोकॉल योग्यरीत्या समजून घेण्यास मदत करतो.
2. **Payload Length (8 bits)**
   • AH हेडरची लांबी 32-बिट शब्दांमध्ये दर्शवतो (पहिले 32 bits वगळून).
   • रिसीव्हरला Authentication Data कुठे आहे हे शोधण्यास मदत करतो.

3. **Reserved (16 bits)**
   - भविष्यातील वापरासाठी राखीव ठेवलेले फील्ड.
   - सध्या यामध्ये मूल्य शून्य (0) ठेवले जाते.
4. **Security Parameters Index (SPI) (32 bits)**
   - सेंडर आणि रिसीव्हर यांच्यातील Security Association (SA) ओळखतो.
   - कोणती की (Key) आणि कोणते अल्गोरिदम वापरले जात आहेत हे निश्चित करतो.
5. **Sequence Number (32 bits)**
   - सतत वाढत जाणारी (Monotonically increasing) संख्या असते.
   - Replay Attacks टाळण्यासाठी वापरली जाते, म्हणजे प्रत्येक पॅकेट युनिक राहते.
6. **Authentication Data / ICV (Variable length)**
   - Integrity Check Value (ICV) समाविष्ट असते, जी HMAC आणि hashing algorithms (उदा. SHA-1, SHA-256) वापरून काढली जाते.
   - IP Header + AH Header + Payload यांची Integrity आणि Authentication सुनिश्चित करते.
   - रिसीव्हरने पुन्हा ICV काढल्यावर मूल्य जुळले नाही तर → पॅकेट compromise झाले आहे असे मानले जाते.

c. एन्कॅप्स्युलेटिंग सिक्युरिटी पेलोड (Encapsulating Security Payload ESP) प्रोटोकॉल

एन्कॅप्स्युलेटिंग सिक्युरिटी पेलोड (ESP) हा IPsec मधील दोन प्रमुख प्रोटोकॉलपैकी एक आहे. ऑथेंटिकेशन हेडर (AH) फक्त ऑथेंटिकेशन आणि इंटेग्रिटी प्रदान करतो, तर ESP हे त्यापेक्षा अधिक सुरक्षा सुविधा देते. ESP द्वारे पुढील सुरक्षा सेवा मिळतात: कॉन्फिडेन्शिअलिटी (Confidentiality) – डेटाचे एन्क्रिप्शन, डेटा ओरिजिन ऑथेंटिकेशन (Data Origin Authentication), इंटेग्रिटी (Integrity) – डेटामध्ये बदल झाला नाही याची खात्री, अँटी-रिप्ले प्रोटेक्शन (Anti-Replay Protection) – जुन्या पॅकेट्सचा पुन्हा वापर रोखतो. ESP मध्ये डेटा (Payload) एन्क्रिप्ट केला जातो, त्यामुळे अनधिकृत व्यक्तीला मूळ माहिती वाचता येत नाही. यामुळे ESP हा VPNs, सुरक्षित ब्रँच ऑफिस कनेक्टिव्हिटी, आणि रिमोट ॲक्सेस यांसाठी मोठ्या प्रमाणावर वापरला जातो.

ESP मुळे नेटवर्कवरून जाणारा डेटा पूर्णपणे सुरक्षित राहतो आणि गोपनीयतेचे संरक्षण होते, जे AH मध्ये उपलब्ध नसते.

ESP हेडर फॉरमॅट (ESP Header Format)

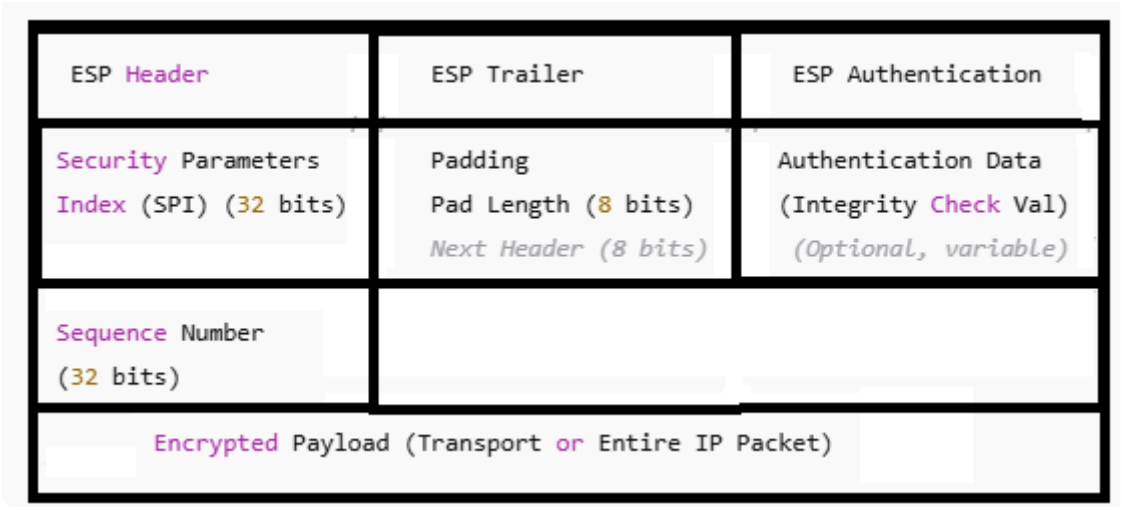


Figure 5.8 : ESP हेडर फॉरमॅट (ESP Header Format)

1. **Security Parameters Index (SPI)**
   - पाठवणारा (Sender) आणि प्राप्तकर्ता (Receiver) यांच्यातील सिक्युरिटी असोसिएशन (Security Association – SA) ओळखतो.
   - कोणत्या की (Keys) आणि अल्गोरिदम्स (Algorithms) वापरले जातील हे निर्दिष्ट करतो.
2. **Sequence Number (सिक्वेन्स नंबर)**
   - प्रत्येक IP पॅकेट वेगळे आहे याची खात्री करून रिप्ले अटॅक्स (Replay Attacks) टाळतो.

3. **Encrypted Payload (एन्क्रिप्टेड पेलोड)**
   - एन्क्रिप्ट केलेला डेटा समाविष्ट असतो (Transport-layer segment किंवा संपूर्ण IP पॅकेट).
   - एन्क्रिप्शनमुळे कॉन्फिडेन्शिअलिटी (Confidentiality) मिळते.
4. **Padding (पॅडिंग)**
   - एन्क्रिप्शन अल्गोरिदमला आवश्यक असलेल्या ब्लॉक साईजशी डेटा जुळवण्यासाठी वापरले जाते.
5. **Pad Length (पॅड लांबी)**
   - किती पॅडिंग बाइट्स जोडले आहेत हे दर्शवते.
6. **Next Header (नेक्स्ट हेडर)**
   - पुढे कोणत्या प्रकारचा डेटा आहे हे ओळखते (TCP, UDP, ICMP).
7. **Authentication Data (Integrity Check Value – ICV)**
   - ऐच्छिक (Optional) फील्ड.
   - इंटेग्रिटी (Integrity) आणि डेटा ओरिजिन ऑथेंटिकेशन (Data Origin Authentication) प्रदान करते.
   - SHA-1, SHA-256 सारख्या हॅशिंग अल्गोरिदम्स वापरून गणना केली जाते.

IPsec चे ऑपरेशन मोड्स (IPsec Modes of Operation)

IPsec दोन मोड्समध्ये कार्य करते:

1. ट्रान्सपोर्ट मोड (Transport Mode)
2. टनल मोड (Tunnel Mode)

हे मोड्स IPsec प्रोटोकॉल्स (AH किंवा ESP) द्वारे IP पॅकेटचा किती भाग सुरक्षित केला जातो हे ठरवतात.

1. ट्रान्सपोर्ट मोड (Transport Mode)

ट्रान्सपोर्ट मोडमध्ये IPsec फक्त IP पॅकेटच्या पेलोड (Payload / डेटा भाग) चे संरक्षण करते. मूळ IP हेडर (Original IP Header) जसा आहे तसाच राहतो आणि त्यात कोणताही बदल केला जात नाही.

ट्रान्सपोर्ट मोड कसा कार्य करतो (How It Works):

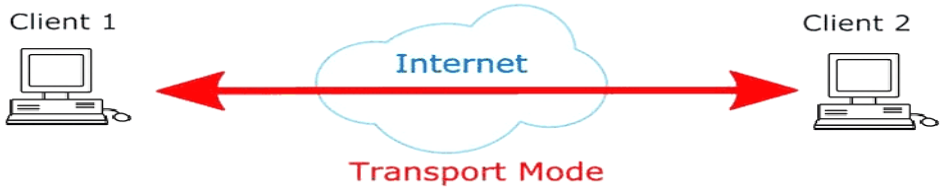


Figure 5.7 : ट्रान्सपोर्ट मोडचे कार्य (Working of Transport Mode)

IPSec ट्रान्सपोर्ट मोड दोन होस्ट्समध्ये (उदा. आकृतीतील Client 1 आणि Client 2) एंड-टू-एंड सुरक्षा प्रदान करतो. या मोडमध्ये IP पॅकेटचा फक्त पेलोड (Payload / डेटा भाग) एन्क्रिप्ट आणि ऑथेंटिकेट केला जातो, तर मूळ IP हेडर जसा आहे तसाच राहतो, त्यामुळे राऊटर्स इंटरनेटवर पॅकेट सामान्यपणे फॉरवर्ड करू शकतात. ट्रान्सपोर्ट मोड प्रामुख्याने नेटवर्क-टू-नेटवर्क ऐवजी डिव्हाइस-टू-डिव्हाइस (Host-to-Host) सुरक्षित संवादासाठी वापरला जातो. तो पॅकेटची एकूण रचना न बदलता कॉन्फिडेन्शिअलिटी (Confidentiality) आणि इंटेग्रिटी (Integrity) प्रदान करतो.

वैशिष्ट्ये (Features):

1. कमी ओव्हरहेड (Lower overhead) → अधिक कार्यक्षम.
2. दोन होस्ट्समध्ये एंड-टू-एंड सुरक्षा प्रदान करतो.
3. ESP फक्त पेलोड एन्क्रिप्ट करतो.
4. AH पेलोड आणि IP हेडरच्या काही भागांचे संरक्षण करतो.

वापराचे प्रकार (Use Cases):

1. होस्ट-टू-होस्ट कम्युनिकेशन
2. खाजगी नेटवर्कमधील सुरक्षित संवाद
3. रिमोट युजर ते सर्व्हर कम्युनिकेशन (जेव्हा दोन्ही IPsec सपोर्ट करतात)

2. टनेल मोड (Tunnel Mode)

टनेल मोडमध्ये IPsec संपूर्ण मूळ IP पॅकेटचे संरक्षण करतो, म्हणजेच IP हेडर + पेलोड (डेटा भाग) दोन्ही सुरक्षित केले जातात. या मोडमध्ये मूळ IP पॅकेट पूर्णपणे एन्कॅप्सुलेट (encapsulate) करून ते नवीन IP पॅकेटच्या आत ठेवले जाते.

टनेल मोड कसा कार्य करतो (How It Works):

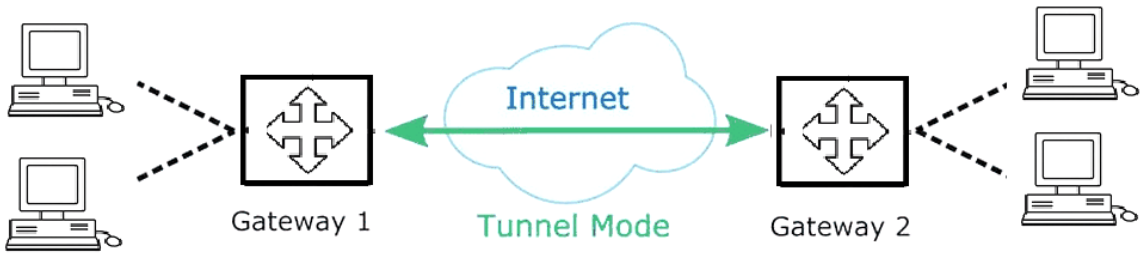


Figure 5.8: टनेल मोडचे कार्य (Working of Tunnel Mode)

IPSec टनेल मोडमध्ये, कम्युनिकेशन हे वैयक्तिक होस्ट्समध्ये नसून दोन गेटवे डिव्हाइसेसमध्ये (उदा. राऊटर्स, फायरवॉल्स) होते. या मोडमध्ये संपूर्ण मूळ IP पॅकेट — म्हणजेच IP हेडर + पेलोड (डेटा) — एन्क्रिप्ट केले जाते आणि नंतर ते नवीन IP पॅकेटच्या आत एन्कॅप्सुलेट केले जाते. यामुळे अंतर्गत नेटवर्कमधील सर्व ट्रॅफिकला उच्च स्तराची सुरक्षा मिळते. टनेल मोड प्रामुख्याने साइट-टू-साइट VPNs साठी वापरला जातो, ज्यामुळे सार्वजनिक इंटरनेटवरून दोन नेटवर्क्समध्ये सुरक्षित कम्युनिकेशन शक्य होते. तसेच, अंतर्गत IP ॲड्रेस लपवले जातात आणि पाठवलेल्या सर्व डेटासाठी कॉन्फिडेन्शिअलिटी (Confidentiality) आणि इंटेग्रिटी (Integrity) सुनिश्चित केली जाते.

वैशिष्ट्ये (Features)

1. अधिक ओव्हरहेड → अधिक सुरक्षित.
2. राऊटर्स, फायरवॉल्स, गेटवे सारख्या नेटवर्क डिव्हाइसेसमध्ये वापरले जाते.
3. गोपनीयतेसाठी अंतर्गत IP ॲड्रेस लपवते.

वापराचे प्रकार (Use Cases)

1. साइट-टू-साइट VPNs (ब्रांच ऑफिस कनेक्टिव्हिटी)
2. संस्था-ते-संस्था (Organization-to-Organization) सुरक्षित कम्युनिकेशन
3. गेटवेच्या माध्यमातून रिमोट ॲक्सेस VPNs

Table 5.2: ट्रान्सपोर्ट मोड आणि टनेल मोड यांची तुलना (Comparison between Transport Mode and Tunnel Mode)

वैशिष्ट्य	ट्रान्सपोर्ट मोड (Transport Mode)	टनेल मोड (Tunnel Mode)
काय संरक्षित केले जाते?	फक्त डेटा (Payload)	संपूर्ण IP पॅकेट
IP हेडर एनक्रिप्ट केले जाते का?	नाही	हो (आतील IP हेडर)
रूटिंगसाठी वापरले जाणारे हेडर	मूळ IP हेडर	नवीन IP हेडर
ओव्हरहेड	कमी	जास्त
वापराचा प्रकार	होस्ट ↔ होस्ट	गेटवे ↔ गेटवे (VPN)
सुरक्षा पातळी	मध्यम	उच्च (संपूर्ण पॅकेट संरक्षण)

5.3 ई-मेल सिक्युरिटी (E-mail Security)

ई-मेल सिक्युरिटी (E-mail Security) प्रामुख्याने इंटरनेटवरून होणारे ई-मेल कम्युनिकेशन सुरक्षित ठेवण्यासाठी वापरली जाते, ज्यामुळे अनधिकृत व्यक्तींना संदेश वाचता किंवा बदलता येत नाही. ई-मेल सुरक्षा यंत्रणांद्वारे ईव्हसड्रॉपिंग, स्पूफिंग, फिशिंग आणि मालवेअर हल्ल्यांपासून संरक्षण मिळते. तसेच, ई-मेलद्वारे पाठवलेल्या माहितीसाठी कॉन्फिडेन्शिअलिटी (Confidentiality), ऑथेंटिकेशन (Authentication), इंटेग्रिटी (Integrity) आणि नॉन-रिप्युडिएशन (Non-Repudiation) सुनिश्चित केली जाते, ज्यामुळे सुरक्षित आणि विश्वासार्ह ई-मेल कम्युनिकेशन शक्य होते.

5.3.1 सिम्पल मेल ट्रान्सफर प्रोटोकॉल (SMTP – Simple Mail Transfer Protocol)

सिम्पल मेल ट्रान्सफर प्रोटोकॉल (SMTP) हा एक मानक प्रोटोकॉल आहे, जो परस्पर जोडलेल्या नेटवर्क्सवरून इलेक्ट्रॉनिक मेल (ई-मेल) पाठवण्यासाठी वापरला जातो. तो TCP/IP मॉडेलच्या ॲप्लिकेशन लेयर (Application Layer) वर कार्य करतो आणि प्रेषकाकडून प्राप्तकर्त्याच्या मेल सर्व्हरपर्यंत ई-मेल विश्वासार्हरीत्या पोहोचवतो. SMTP मध्ये ई-मेल संदेशांची योग्य आणि क्रमबद्ध डिलिव्हरी सुनिश्चित करण्यासाठी TCP (Transmission Control Protocol) चा वापर केला जातो.

SMTP साठी वापरले जाणारे पोर्ट्स :

- पोर्ट 25 → स्टँडर्ड SMTP
- पोर्ट 465 / 587 → सिक्युअर SMTP (SSL/TLS वापरून)

SMTP हे पुश-बेस्ड मॉडेल (Push-based Model) वापरते, म्हणजे ई-मेल प्रेषकाकडून मेल सर्व्हरकडे किंवा एका मेल सर्व्हरकडून दुसऱ्या मेल सर्व्हरकडे *पुश* केले जातात. यामध्ये प्राप्तकर्ता ई-मेल मागवत नाही, तर प्रेषक प्रणाली स्वतःहून ई-मेल पाठवते.

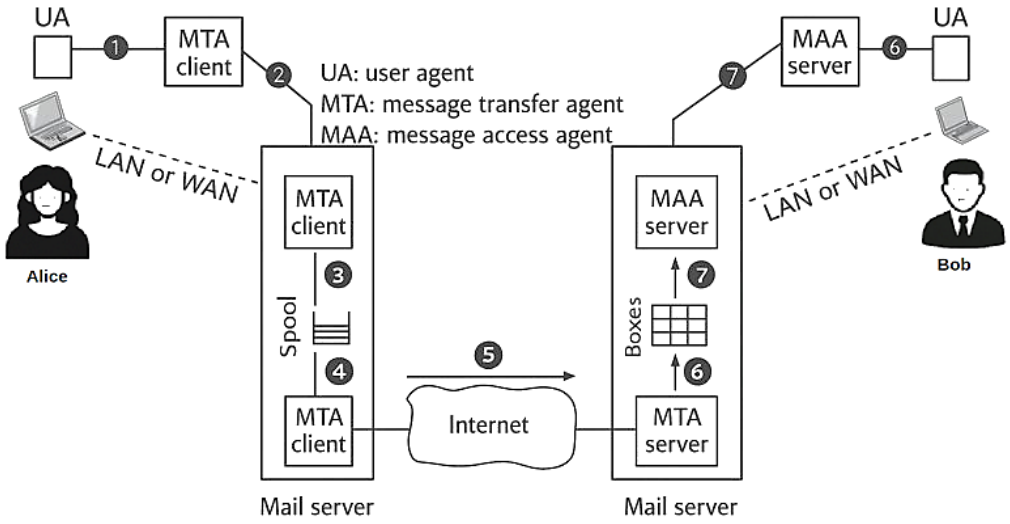


Fig 5.9: SMTP आर्किटेक्चर (SMTP Architecture)

1. **ॲलिस तिच्या User Agent (UA) चा वापर करून ई-मेल तयार करते.**
   User Agent (UA) म्हणजे Outlook, Gmail क्लायंट यांसारखे ॲप्लिकेशन, जे ई-मेल तयार करण्यासाठी व पाठवण्यासाठी वापरले जाते.
2. **ई-मेल MTA Client कडे दिला जातो.**
   Message Transfer Agent (MTA) क्लायंट ॲलिसचा ई-मेल स्वीकारतो आणि तो मेल सर्व्हरकडे पाठवण्यासाठी तयार करतो.
3. **मेल सर्व्हर आउटगोइंग ई-मेल spool area मध्ये साठवतो.**
   ॲलिसच्या बाजूचा MTA Server ई-मेल स्वीकारतो आणि तो तात्पुरता spool (queue) मध्ये ठेवतो.
4. **MTA Server ई-मेल डेस्टिनेशन मेल सर्व्हरकडे फॉरवर्ड करतो.**
   सर्व्हर तयार झाल्यानंतर, तो ई-मेल इंटरनेटद्वारे पुढील मेल सर्व्हरकडे पाठवतो.
5. **ई-मेल इंटरनेटद्वारे बॉबच्या मेल सर्व्हरकडे प्रवास करतो.**
   हा टप्पा म्हणजे इंटरनेटवरून एका MTA Server कडून दुसऱ्या MTA Server कडे होणारा ट्रान्सफर.
6. **बॉबचा मेल सर्व्हर ई-मेल स्वीकारतो आणि बॉबच्या मेलबॉक्समध्ये साठवतो.**
   MTA Server ई-मेल स्वीकारून तो बॉबच्या "Boxes" (मेल स्टोरेज एरिया) मध्ये ठेवतो.
7. **बॉबचा MAA Server ई-मेल मिळवण्यासाठी वापरला जातो.**
   Message Access Agent (MAA) Server (उदा. POP3 / IMAP Server) स्टोरेजमधून ई-मेल घेतो.

8. बॉबचा User Agent ई-मेल डाउनलोड करून दाखवतो.

बॉबच्या डिव्हाइसवरील MAA Client ई-मेल सर्व्हरवरून संदेश डाउनलोड करतो आणि बॉब तो ई-मेल वाचू शकतो.

5.3.2 प्रिटी गुड प्रायव्हसी (Pretty Good Privacy – PGP)

प्रिटी गुड प्रायव्हसी (PGP) हे ई-मेल कम्युनिकेशनसाठी मोठ्या प्रमाणावर वापरले जाणारे एक सुरक्षा (Security) प्रोग्राम आहे. PGP द्वारे ई-मेलसाठी कॉन्फिडेन्शिअलिटी (Confidentiality), ऑथेंटिकेशन (Authentication), इंटेग्रिटी (Integrity) आणि नॉन-रिप्युडिएशन (Non-repudiation) या चारही सुरक्षा सेवा प्रदान केल्या जातात. इंटरनेटवर पाठवले जाणारे संदेश सुरक्षित ठेवण्यासाठी PGP मध्ये खालील क्रिप्टोग्राफिक तंत्रांचा एकत्रित वापर केला जातो:

- सिमेट्रिक-की एन्क्रिप्शन (Symmetric-key Encryption)
- पब्लिक-की एन्क्रिप्शन (Public-key Encryption)
- डिजिटल सिग्नेचर्स (Digital Signatures)
- हॅशिंग (Hashing)

PGP हे **हायब्रिड एन्क्रिप्शन मॉडेल (Hybrid Encryption Model)** अनुसरते. यामध्ये:

- प्रत्यक्ष संदेश (Message) एन्क्रिप्ट करण्यासाठी वेगवान सिमेट्रिक एन्क्रिप्शन अल्गोरिदम वापरला जातो.
- सिमेट्रिक सेशन की (Symmetric Session Key) सुरक्षित करण्यासाठी पब्लिक-की एन्क्रिप्शन अल्गोरिदम (उदा. RSA) वापरला जातो.

या पद्धतीमुळे PGP ला उच्च कार्यक्षमता (Efficiency) आणि मजबूत सुरक्षा (Strong Security) दोन्ही मिळतात.

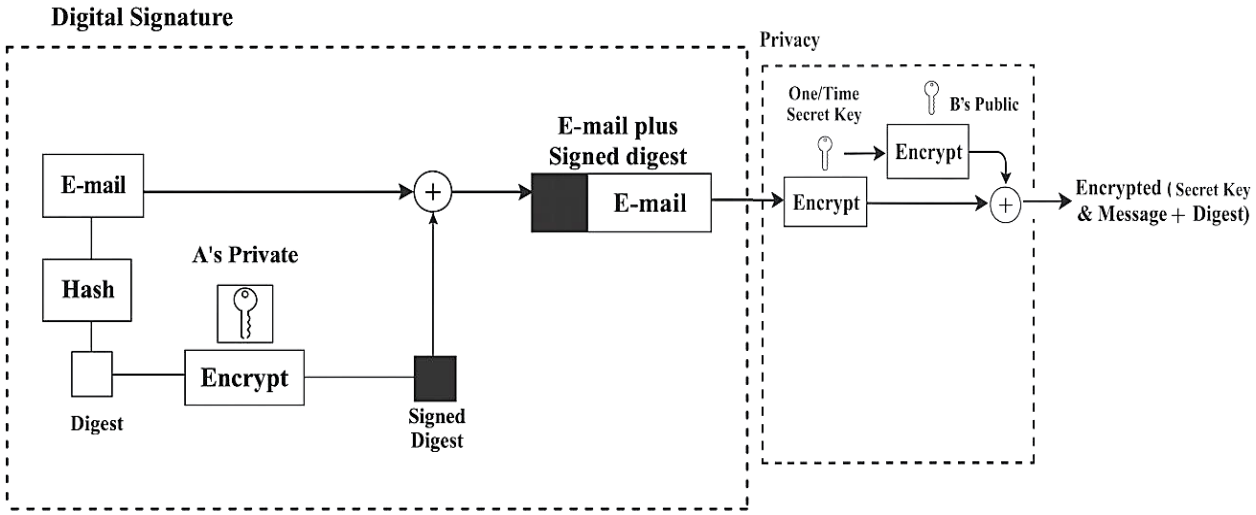


Fig 5.10: सेन्डर साईटवरील PGP चे कार्य (Sender site – A)

प्रिटी गुड प्रायव्हसी (PGP) मध्ये ई-मेल सुरक्षित करण्यासाठी डिजिटल सिग्नेचर (Digital Signature) आणि एन्क्रिप्शन प्रायव्हसी (Encryption / Privacy) यांचा एकत्रित वापर केला जातो.

सेन्डर साईटवरील प्रक्रिया दोन मुख्य भागांमध्ये विभागलेली असते.

I. डिजिटल सिग्नेचर विभाग (DIGITAL SIGNATURE SECTION)

1. सेन्डर ई-मेल संदेश तयार करतो
   प्रक्रियेची सुरुवात सेन्डर A ने तयार केलेल्या प्लेन टेक्स्ट (Plain Text) ई-मेलपासून होते.
2. हॅश फंक्शनद्वारे मेसेज डायजेस्ट तयार होतो
   - ई-मेल संदेश हॅश अल्गोरिदममधून (उदा. SHA, MD5) पास केला जातो.
   - आउटपुट म्हणून निश्चित आकाराचा मेसेज डायजेस्ट (Message Digest) तयार होतो.
   - उद्देश: इंटेग्रिटी (Integrity) सुनिश्चित करणे — संदेशात थोडाही बदल झाला तर डायजेस्ट बदलतो.
3. डायजेस्टला सेन्डर A च्या प्रायव्हेट की ने एन्क्रिप्ट करणे
   - सेन्डर A आपली प्रायव्हेट की (Private Key) वापरून डायजेस्ट एन्क्रिप्ट करतो.

- यामुळे साईन्ड डायजेस्ट (Signed Digest / Digital Signature) तयार होतो.
- उद्देश:
  - ऑथेंटिकेशन (Authentication) — संदेश A कडूनच आला आहे याची खात्री
  - नॉन-रिप्युडिएशन (Non-repudiation) — A संदेश पाठविल्याचे नाकारू शकत नाही
  - इंटेग्रिटी (Integrity) — बदल झाल्यास सिग्नेचर व्हेरिफिकेशन फेल होते

4. ई-मेल + साईन्ड डायजेस्ट एकत्र करणे
   - मूळ ई-मेल आणि त्याचा साईन्ड डायजेस्ट एकत्र जोडले जातात.
   - यामुळे डिजिटली साईन्ड मेसेज (Digitally Signed Message) तयार होतो.
   - येथे डिजिटल सिग्नेचर प्रक्रिया पूर्ण होते.

II. प्रायव्हसी / एन्क्रिप्शन विभाग (PRIVACY / ENCRYPTION SECTION)

5. वन-टाइम सिक्रेट की (Session Key) तयार करणे
   - PGP एक रॅन्डम सिमेट्रिक सिक्रेट की (Session Key) तयार करते.
   - सिमेट्रिक एन्क्रिप्शन जलद असल्यामुळे संपूर्ण संदेश एन्क्रिप्ट करण्यासाठी वापरले जाते.
6. ई-मेल + साईन्ड डायजेस्ट सिक्रेट की ने एन्क्रिप्ट करणे
   - एकत्रित संदेश वन-टाइम सिक्रेट की वापरून एन्क्रिप्ट केला जातो.
   - यामुळे कॉन्फिडेन्शिअलिटी (Confidentiality) मिळते.
7. सिक्रेट की ला रिसिव्हर B च्या पब्लिक की ने एन्क्रिप्ट करणे
   - सिक्रेट की रिसिव्हर B कडे पाठवणे आवश्यक असते.
   - ती B च्या पब्लिक की (Public Key) ने एन्क्रिप्ट केली जाते.
   - त्यामुळे फक्त B च्या प्रायव्हेट की नेच ती डिक्रिप्ट होऊ शकते.
   - यामुळे फक्त योग्य रिसिव्हरलाच संदेश उघडता येतो.
8. एन्क्रिप्टेड मेसेज + एन्क्रिप्टेड सिक्रेट की एकत्र करणे
   अंतिम पाठवला जाणारा डेटा यात समाविष्ट असतो:
   - एन्क्रिप्टेड सिक्रेट की
   - एन्क्रिप्टेड (ई-मेल + साईन्ड डायजेस्ट)

डायग्राममध्ये हे पुढीलप्रमाणे दर्शविलेले असते: Encrypted (Secret Key & Message + Digest)

रिसिव्हर साईटवरील PGP चे कार्य (PGP at the Receiver site – B)

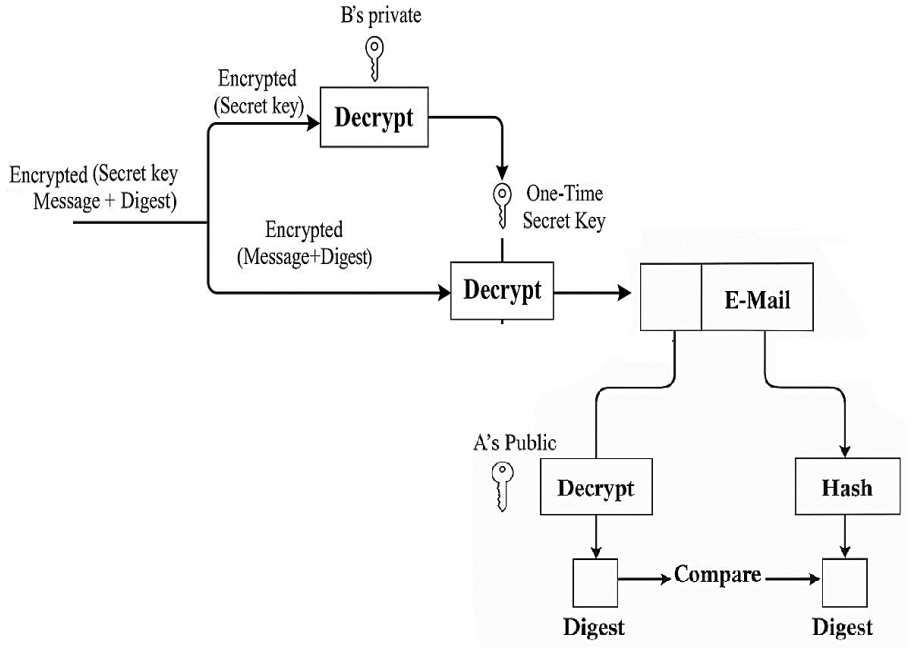


Fig 5.11 : रिसिव्हर साईडवरील PGP चे कार्य (PGP at the Receiver Site – B)

PGP मध्ये रिसिव्हरच्या बाजूला दोन मुख्य प्रक्रिया केल्या जातात:

1. डिक्रिप्शन प्रक्रिया – गोपनीयता सुनिश्चित करण्यासाठी
2. डिजिटल स्वाक्षरी पडताळणी – प्रामाणिकता व अखंडता सुनिश्चित करण्यासाठी

I. डिक्रिप्शन प्रक्रिया

पायरी 1: रिसिव्हर B ला प्राप्त होणारे घटक

रिसिव्हर B ला खालील दोन गोष्टी प्राप्त होतात:

- एन्क्रिप्ट केलेली गुप्त की
- एन्क्रिप्ट केलेला संदेश आणि स्वाक्षरी केलेला डायजेस्ट

हे दोन्ही मिळून सुरक्षित PGP ई-मेल तयार होतो.

पायरी 2: रिसिव्हर B स्वतःच्या खाजगी की ने गुप्त की डिक्रिप्ट करतो

एन्क्रिप्ट गुप्त की → डिक्रिप्शन (B ची खाजगी की) → एकदाच वापरण्याची सत्र-की

- सत्र-की ही B च्या सार्वजनिक की ने एन्क्रिप्ट केलेली असल्यामुळे
  फक्त B ची खाजगी कीच ती डिक्रिप्ट करू शकते. यामुळे संदेशाची गोपनीयता राखली जाते आणि अनधिकृत व्यक्तींना प्रवेश मिळत नाही.

पायरी 3: सत्र-की वापरून संदेश व डायजेस्ट डिक्रिप्ट केला जातो

एन्क्रिप्ट संदेश + डायजेस्ट → डिक्रिप्शन (सत्र-की)

यामुळे ई-मेलचा मूळ मजकूर डिक्रिप्ट होतो. आउटपुट: साधा (Plain) ई-मेल संदेश आणि स्वाक्षरी केलेला डायजेस्ट या टप्प्यावर संदेश वाचता येतो, मात्र अजून त्याची सत्यता तपासणे आवश्यक असते.

II. डिजिटल सिग्नेचर पडताळणी प्रक्रिया

डिक्रिप्शननंतर PGP प्रेषकाची ओळख आणि संदेशाची अखंडता तपासतो.

पायरी 4: संदेशामधून स्वाक्षरी केलेला डायजेस्ट वेगळा काढला जातो

हा डायजेस्ट म्हणजे प्रेषक A ने स्वतःच्या खाजगी की ने एन्क्रिप्ट केलेली हॅश किंमत असते.

पायरी 5: स्वाक्षरी केलेला डायजेस्ट प्रेषक A च्या सार्वजनिक की ने डिक्रिप्ट केला जातो

स्वाक्षरी डायजेस्ट → डिक्रिप्शन (A ची सार्वजनिक की) → मूळ डायजेस्ट

जर डिक्रिप्शन यशस्वी झाले, तर यावरून हे सिद्ध होते की:

– संदेश खरोखरच प्रेषक A कडून आलेला आहे

– प्रेषक A नंतर तो संदेश पाठवला नाही असे नाकारू शकत नाही

पायरी 6: प्राप्त ई-मेलचा स्वतंत्रपणे हॅश तयार केला जातो

ई-मेल संदेश → हॅश फंक्शन → नवीन डायजेस्ट

रिसिव्हर साध्या ई-मेल संदेशावर हॅश फंक्शन वापरून नवीन डायजेस्ट तयार करतो. हा डायजेस्ट संदेशात कोणताही बदल झाला आहे का हे तपासण्यासाठी वापरला जातो. (जर मूळ डायजेस्ट आणि नवीन डायजेस्ट जुळले, तर संदेश बदललेला नाही हे निश्चित होते.)

निष्कर्ष

PGP रिसिव्हरच्या बाजूला डिक्रिप्शनद्वारे संदेशाची गोपनीयता राखतो. आणि डिजिटल स्वाक्षरी पडताळणीद्वारे संदेशाची प्रामाणिकता, अखंडता आणि न नाकारण्याची हमी प्रदान करतो.

5.3.3 सिक्युअर / मल्टिपर्पज इंटरनेट मेल एक्स्टेन्शन्स (Secure/Multipurpose Internet Mail Extensions (S/MIME))

S/MIME (सिक्युअर / मल्टिपर्पज इंटरनेट मेल एक्स्टेन्शन्स) ही ई-मेल कम्युनिकेशन सुरक्षित करण्यासाठी वापरली जाणारी एक उद्योग-मान्य (Industry-standard) तंत्रज्ञान प्रणाली आहे. S/MIME मध्ये पब्लिक-की एन्क्रिप्शन (Public Key Encryption) आणि डिजिटल स्वाक्षरी (Digital Signature) यांचा वापर करून पुढील सुरक्षा सुविधा प्रदान केल्या जातात:

- प्रमाणीकरण / ऑथेंटिकेशन (Authentication)
- संदेशाची अखंडता / इंटेग्रिटी (Integrity)
- डेटा गोपनीयता/ डेटा कॉन्फिडेन्शियलिटी (Data Confidentiality)
- नॉन-रिप्युडिएशन (Non-repudiation)

S/MIME मुळे ई-मेल पाठवणारा आणि प्राप्त करणारा यांची ओळख निश्चित करता येते तसेच संदेशामध्ये ट्रान्समिशनदरम्यान कोणताही बदल झाला नाही याची खात्री मिळते. S/MIME तंत्रज्ञानाला खालील लोकप्रिय ई-मेल क्लायंट्स आणि सिस्टिम्समध्ये मोठ्या प्रमाणावर समर्थन आहे :

Microsoft Outlook, Gmail (वेब आवृत्ती), Thunderbird, Apple Mail तसेच अनेक एंटरप्राइझ मेल सिस्टिम्स. म्हणूनच S/MIME ही सुरक्षित, विश्वासार्ह आणि व्यापकपणे वापरली जाणारी ई-मेल सिक्युरिटी प्रणाली आहे.

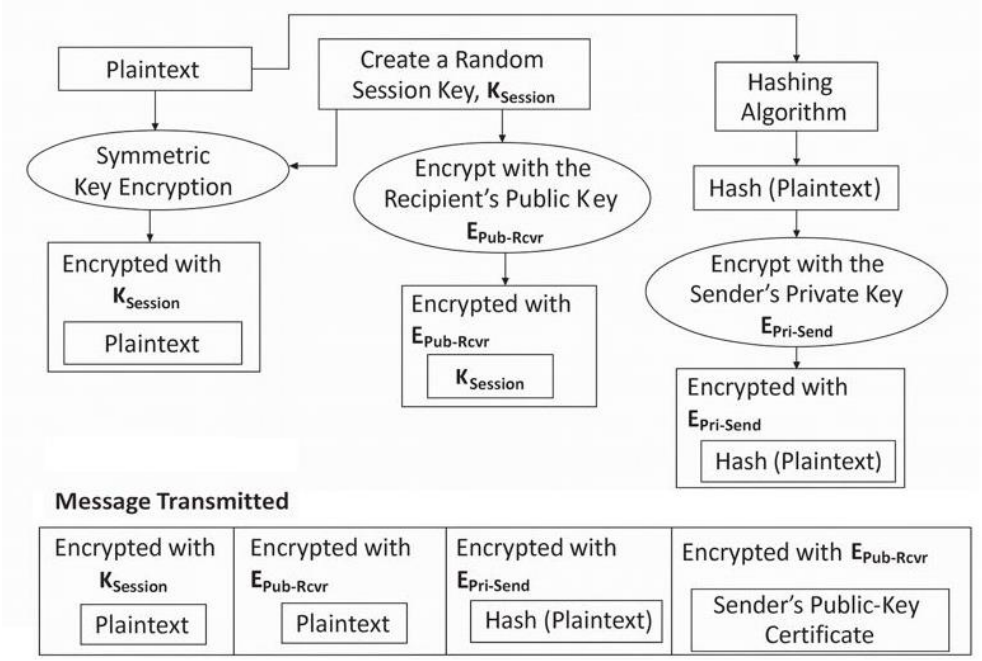


Fig 5.12: सिक्युअर / मल्टिपर्पज इंटरनेट मेल एक्स्टेन्शन्स (S/MIME)

S/MIME चे कार्य (Working of S/MIME)

S/MIME मध्ये सिमेट्रिक क्रिप्टोग्राफी आणि असिमेट्रिक क्रिप्टोग्राफी यांचा संयुक्त वापर करून ई-मेल कम्युनिकेशनसाठी डेटा गोपनीयता (Confidentiality), प्रमाणीकरण (Authentication), संदेशाची अखंडता (Integrity) आणि नॉन-रिप्युडिएशन (Non-repudiation) प्रदान केली जाते.

या प्रक्रियेत दोन मुख्य ऑपरेशन्स केल्या जातात :

1. मेसेज एन्क्रिप्शन (Message Encryption – Confidentiality)
2. डिजिटल स्वाक्षरी (Digital Signature – Authentication आणि Integrity)

या दोन्हींचे परिणाम एकत्र करून अंतिम ई-मेल पाठवला जातो.

1. मेसेज एन्क्रिप्शन (Message Encryption)

ही प्रक्रिया ई-मेलची गोपनीयता सुनिश्चित करते, म्हणजेच फक्त अपेक्षित रिसिव्हरच मेसेज वाचू शकतो.

स्टेप्स :

a. प्लेनटेक्स्ट इनपुट: साध्या (Plaintext) ई-मेल मेसेजपासून प्रक्रिया सुरू होते.

b. रँडम सत्र-की (K_session) तयार करणे:मेसेज एन्क्रिप्ट करण्यासाठी एक नवीन सिमेट्रिक की तयार केली जाते. सिमेट्रिक की वेगवान असल्यामुळे वापरली जाते.

c. सिमेट्रिक एन्क्रिप्शन वापरून मेसेज एन्क्रिप्ट करणे: प्लेनटेक्स्ट मेसेज K_session वापरून एन्क्रिप्ट केला जातो. → आउटपुट : एन्क्रिप्ट केलेला मेसेज

d. रिसिव्हरच्या पब्लिक की ने सत्र-की एन्क्रिप्ट करणे: K_session ही रिसिव्हरच्या पब्लिक की ने एन्क्रिप्ट केली जाते. फक्त रिसिव्हरच स्वतःच्या प्रायव्हेट की ने ती डिक्रिप्ट करू शकतो. → आउटपुट : एन्क्रिप्ट केलेली सत्र-की

2. डिजिटल स्वाक्षरी (Digital Signature)

ही प्रक्रिया प्रमाणीकरण आणि संदेशाची अखंडता सुनिश्चित करते.

a. हॅशिंग अल्गोरिदम वापरणे: प्लेनटेक्स्ट मेसेजवर हॅश फंक्शन लागू करून डायजेस्ट तयार केला जातो.
b. प्रेषकाच्या प्रायव्हेट की ने हॅश एन्क्रिप्ट करणे: हा हॅश प्रेषकाच्या प्रायव्हेट की ने एन्क्रिप्ट केला जातो. यालाच डिजिटल स्वाक्षरी म्हणतात. → आउटपुट : एन्क्रिप्ट केलेला हॅश

3. **पाठवला जाणारा अंतिम संदेश (Message Transmitted)**

अंतिम ई-मेलमध्ये खालील चार घटक असतात :

a. K_session ने एन्क्रिप्ट केलेला मेसेज
b. रिसिव्हरच्या पब्लिक की ने एन्क्रिप्ट केलेली सत्र-की
c. प्रेषकाच्या प्रायव्हेट की ने एन्क्रिप्ट केलेली डिजिटल स्वाक्षरी (हॅश)
d. प्रेषकाचे पब्लिक-की सर्टिफिकेट, ज्यामुळे रिसिव्हर स्वाक्षरी पडताळू शकतो

यामुळे खालील सुरक्षा गुणधर्म मिळतात :

- डेटा गोपनीयता (Confidentiality) – फक्त रिसिव्हरच मेसेज डिक्रिप्ट करू शकतो
- संदेशाची अखंडता (Integrity) – मेसेजमध्ये बदल झाला आहे का हे तपासता येते
- प्रमाणीकरण (Authentication) – मेसेज कोणाकडून आला आहे हे सिद्ध होते
- नॉन-रिप्युडिएशन (Non-repudiation) – प्रेषक मेसेज पाठवला नाही असे नाकारू शकत नाही

5.3.4 प्रायव्हसी एन्हान्स्ड मेल (Privacy Enhanced Mail – PEM)

प्रायव्हसी एन्हान्स्ड मेल (PEM) हा इंटरनेटवरील ई-मेल कम्युनिकेशन सुरक्षित करण्यासाठी Internet Architecture Board (IAB) यांनी स्वीकारलेला एक ई-मेल सुरक्षा मानक (Email Security Standard) आहे. ई-मेलचा वापर मोठ्या प्रमाणावर वाढल्यानंतर अनधिकृत प्रवेश, संदेशातील छेडछाड (Tampering) आणि बनावट ओळख (Impersonation) यापासून संरक्षण करणे आवश्यक झाले. या गरजांमुळे PEM चे विकासकार्य इंटरनेट रिसर्च टास्क फोर्स (IRTF) आणि Privacy and Security Research Group (PSRG) यांनी केले. PEM ची औपचारिक व्याख्या खालील RFC मध्ये दिली आहे: RFC 1421, RFC 1422, RFC 1423 आणि RFC 1424.

PEM द्वारे दिल्या जाणाऱ्या क्रिप्टोग्राफिक सुरक्षा सेवा

PEM खालील तीन प्रमुख सुरक्षा सेवा प्रदान करते:

1. डेटा गोपनीयता (Confidentiality)
2. संदेशाची अखंडता (Integrity)
3. नॉन-रिप्युडिएशन (Non-repudiation)

PEM ची कार्यपद्धती (Working of PEM)

PEM ची कार्यपद्धती उच्च पातळीवर चार सलग टप्प्यांमध्ये पार पडते. रिसिव्हरकडून हेच टप्पे उलट क्रमाने (Reverse Order) पार पाडले जातात, जेणेकरून मूळ प्लेनटेक्स्ट मेसेज प्राप्त करता येतो.

PEM मध्ये खालील क्रिया केल्या जातात:

1. कॅनॉनिकल कन्व्हर्जन (Canonical Conversion)
2. डिजिटल स्वाक्षरी (Digital Signature)
3. एन्क्रिप्शन (Encryption)
4. बेस-64 एन्कोडिंग (Base-64 Encoding)

PEM मधील सुरक्षा मोड्स (Modes of PEM)

कोणते टप्पे वापरले जातात यावरून PEM तीन सुरक्षा मोड्स प्रदान करते:

- फक्त स्वाक्षरी (Signature Only): (स्टेप 1 आणि स्टेप 2 वापरले जातात)

- स्वाक्षरी + बेस-64 एन्कोडिंग :(स्टेप 1, स्टेप 2 आणि स्टेप 4 वापरले जातात)
- स्वाक्षरी + एन्क्रिप्शन + बेस-64 एन्कोडिंग :(स्टेप 1 ते स्टेप 4 सर्व वापरले जातात)

Step 1 : कॅनॉनिकल कन्व्हर्जन (Canonical Conversion)

इंटरनेटवर वेगवेगळ्या आर्किटेक्चर आणि ऑपरेटिंग सिस्टीम असलेल्या संगणकांमध्ये कम्युनिकेशन होते. यामुळे कॅरेक्टर रिप्रेझेंटेशन, लाईन एंडिंग्स आणि मेसेज फॉरमॅटमध्ये फरक असू शकतो. हा फरक मेसेज डायजेस्ट आणि डिजिटल स्वाक्षरी तयार करताना अडचणी निर्माण करतो, कारण प्रेषक आणि रिसिव्हरकडे मेसेजचे स्वरूप एकसारखे असणे आवश्यक असते. म्हणून PEM ई-मेल मेसेजला कॅनॉनिकल फॉर्म मध्ये रूपांतरित करते, म्हणजेच डिव्हाइस किंवा ऑपरेटिंग सिस्टीमपासून स्वतंत्र असे एकसमान स्वरूप तयार केले जाते.

यामुळे खालील गोष्टी सुनिश्चित होतात:

- सुसंगत हॅशिंग (Consistent Hashing)
- विश्वासार्ह डिजिटल स्वाक्षरी निर्मिती व पडताळणी
- सुलभ एन्क्रिप्शन आणि डिक्रिप्शन

Step 2 : डिजिटल स्वाक्षरी (Digital Signature)

PEM मानक डिजिटल स्वाक्षरी तंत्रांचा वापर करते.

a. मेसेज डायजेस्ट जनरेशन (Message Digest Generation): कॅनॉनिकल स्वरूपातील मेसेजवर MD2 किंवा MD5 हॅश अल्गोरिदम वापरून हॅश व्हॅल्यू तयार केली जाते.
b. स्वाक्षरी निर्मिती (Signature Creation): हा मेसेज डायजेस्ट प्रेषकाच्या प्रायव्हेट की ने एन्क्रिप्ट केला जातो. यामुळे प्रेषकाची डिजिटल स्वाक्षरी तयार होते.

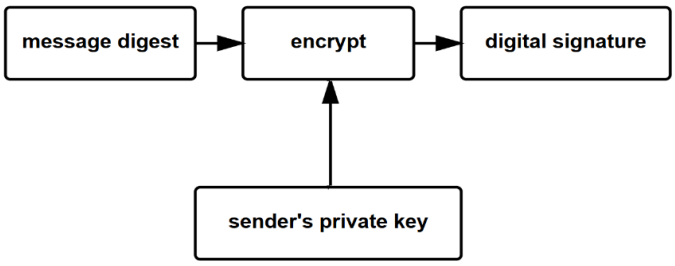


Fig 5.13: डिजिटल स्वाक्षरी (Digital Signature)

यामुळे खालील सुरक्षा सेवा मिळतात :

- प्रमाणीकरण (Authentication)
- नॉन-रिप्युडिएशन (Non-repudiation)
- संदेशाची अखंडता संरक्षण (Integrity Protection)

Step 3: एन्क्रिप्शन (Encryption)

या टप्प्यात मूळ ई-मेल संदेश आणि डिजिटल स्वाक्षरी हे दोन्ही एकत्र करून सिमेट्रिक-की एन्क्रिप्शन (Symmetric-key Encryption) वापरून एन्क्रिप्ट केले जातात. PEM मध्ये खालील एन्क्रिप्शन अल्गोरिदम वापरले जातात :

- DES (Data Encryption Standard) किंवा
- ट्रिपल DES (3DES)
- Cipher Block Chaining (CBC) मोड मध्ये

प्रक्रिया (Process)

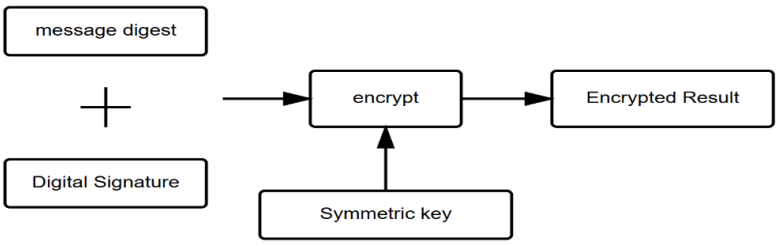


Fig 5.14: एन्क्रिप्शन (Encryption)

1. सिमेट्रिक की तयार केली जाते.
2. एकत्रित संदेश (ई-मेल + डिजिटल स्वाक्षरी) सिमेट्रिक की वापरून एन्क्रिप्ट केला जातो.
3. ही सिमेट्रिक की रिसिव्हरच्या पब्लिक की ने एन्क्रिप्ट केली जाते.

यामुळे डेटा गोपनीयता (Confidentiality) सुनिश्चित होते, कारण फक्त रिसिव्हरच स्वतःच्या प्रायव्हेट की ने सिमेट्रिक की डिक्रिप्ट करू शकतो.

Step 4 : बेस-64 एन्कोडिंग (Base-64 Encoding)

हा PEM मधील अंतिम टप्पा आहे. ई-मेल सिस्टीम्समध्ये कच्चा बायनरी डेटा (Raw Binary Output) विश्वासार्हरीत्या पाठवता येत नाही.

म्हणून PEM मध्ये बेस-64 एन्कोडिंग वापरले जाते, ज्याला खालील नावांनीही ओळखले जाते :

- Radix-64 Encoding
- ASCII Armoring

बेस-64 एन्कोडिंगमध्ये बायनरी डेटाचे ASCII कॅरेक्टर्समध्ये रूपांतर केले जाते, जेणेकरून एन्क्रिप्ट केलेला ई-मेल संदेश कोणत्याही मेल सिस्टीममधून सुरक्षितपणे पाठवता येतो.

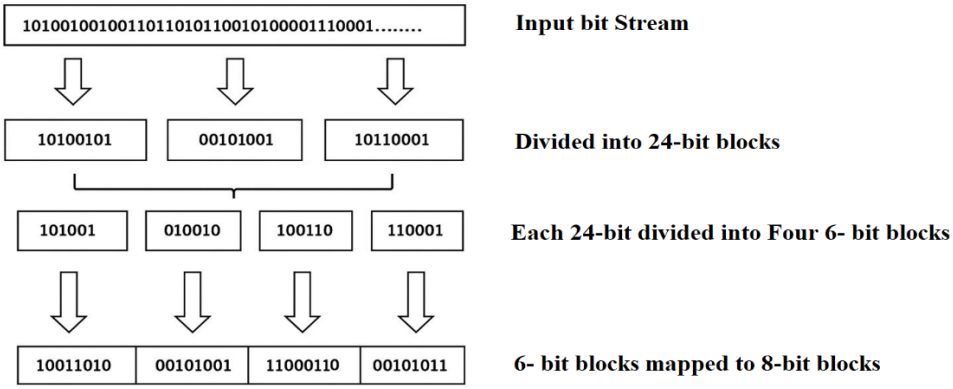


Fig 5.15: ब्लॉक-वाइज रिप्रेझेंटेशन ऑफ बेस 64 एन्कोडिंग (Block-wise Representation of Base64 Encoding)

- बायनरी डेटा 3 बाइट्सच्या (24 बिट्स) ब्लॉक्समध्ये घेतला जातो.
- हे 24 बिट्स 6 बिट्सचे 4 गट (Groups) मध्ये विभागले जातात.
- प्रत्येक 6-बिट गटाला Base-64 लुक-अप टेबलच्या साहाय्याने 8-बिट छापता येणाऱ्या (Printable) कॅरेक्टरमध्ये रूपांतरित केले जाते.

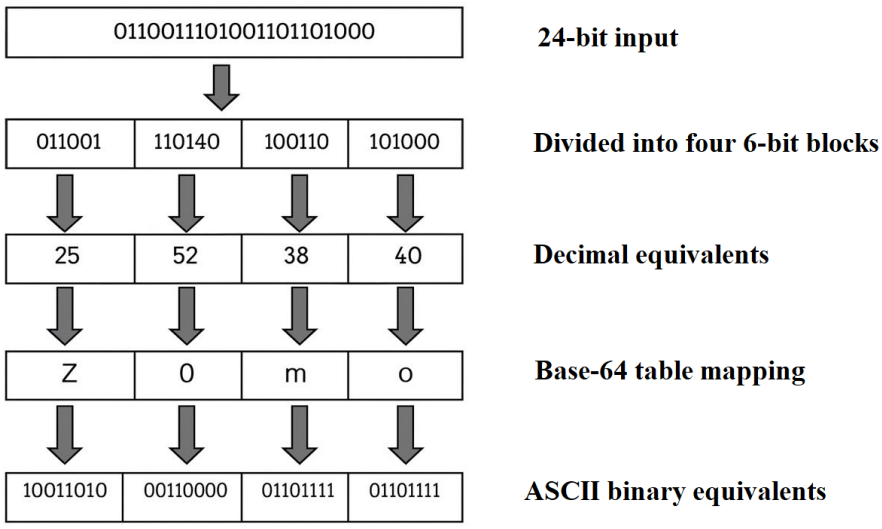


Fig 5.16: बेस-64 एन्कोडिंग प्रोसेस (Base-64 Encoding Process)

Table 5.3: बेस-64 कॅरेक्टर(Base-64 Character)

Char	Dec	Char	Dec	Char	Dec
A	0	W	22	s	44
B	1	X	23	t	45
C	2	Y	24	u	46
D	3	Z	25	v	47
E	4	a	26	w	48
F	5	b	27	x	49
G	6	c	28	y	50
H	7	d	29	z	51
I	8	e	30	0	52
J	9	f	31	1	53
K	10	g	32	2	54
L	11	h	33	3	55
M	12	i	34	4	56
N	13	j	35	5	57
O	14	k	36	6	58
P	15	l	37	7	59
Q	16	m	38	8	60
R	17	n	39	9	61
S	18	o	40	+	62
T	19	p	41	/	63
U	20	q	42	=	Padding
V	21	r	43		

5.4 डेटाबेस सिक्युरिटी (Database Security):

डेटाबेस सिक्युरिटी म्हणजे अनऑथराईज्ड ॲक्सेस, डेटा ब्रीचेस, मिसयूज आणि सायबरअटॅक्स पासून डेटाबेसचे संरक्षण करण्यासाठी वापरली जाणारी टूल्स, कंट्रोल्स, पॉलिसीज आणि टेक्निक्स यांची एकत्रित व्यवस्था होय. यामुळे डेटाबेस सिस्टिम मध्ये साठवलेला डेटा कॉन्फिडेन्शियल, ॲक्युरेट आणि फक्त ऑथराईज्ड युजर्स साठीच उपलब्ध राहतो. डेटाबेस सिक्युरिटी हा इन्फॉर्मेशन सिक्युरिटी चा एक अत्यंत महत्त्वाचा भाग आहे, जो डेटाबेसमध्ये साठवलेल्या डेटाचे इंटेन्शनल किंवा ॲक्सिडेंटल थ्रेट्स पासून संरक्षण करण्यावर लक्ष केंद्रित करतो. यामध्ये ऑथेंटिकेशन, ॲक्सेस कंट्रोल, एन्क्रिप्शन, ऑडिटिंग आणि बॅकअप स्ट्रॅटेजीज यांसारख्या यंत्रणांची अंमलबजावणी केली जाते, जेणेकरून डेटा अनऑथराईज्ड ॲक्सेस आणि करप्शन पासून सुरक्षित राहील. डेटाबेसमध्ये अनेकदा पर्सनल रेकॉर्ड्स, फायनान्शियल डेटा आणि ऑर्गनायझेशनल ॲसेट्स यांसारखी अत्यंत संवेदनशील माहिती साठवलेली असल्यामुळे ते अटॅकर्स साठी मुख्य लक्ष्य (प्राईम टार्गेट) ठरतात. त्यामुळे सुरक्षा उपायांनी पुढील बाबी सुनिश्चित करणे आवश्यक असते:

- कॉन्फिडेन्शियलिटी – ॲक्सेस मर्यादित ठेवून
- इंटेग्रिटी – अनऑथराईज्ड मॉडिफिकेशन रोखून
- ॲव्हेलेबिलिटी – लेजिटिमेट युजर्स साठी डेटा सतत उपलब्ध ठेवून

आधुनिक डीबीएमएसेस (DBMSs) मध्ये रोल-बेस्ड ॲक्सेस कंट्रोल (RBAC), रो-लेव्हल सिक्युरिटी (RLS) आणि एन्क्रिप्शन यांसारखी ॲडव्हान्स्ड सिक्युरिटी फीचर्स समाविष्ट केलेली असतात, ज्यामुळे संरक्षण अधिक मजबूत होते. एक चांगले डिझाइन केलेले डेटाबेस सिक्युरिटी फ्रेमवर्क मध्ये सिक्युअर कॉन्फिगरेशन्स, कंटिन्युअस मॉनिटरिंग आणि रिकव्हरी मेकॅनिझम्स यांचा देखील समावेश असतो, जेणेकरून कोणताही थ्रेट झाला तरी डेटा सुरक्षितपणे रिस्टोअर करता येईल. एकूणच, डेटाबेस सिक्युरिटी ही मल्टी-लेयर्ड डिफेन्स प्रदान करते, जी साठवलेल्या माहितीची रिलायबिलिटी आणि ट्रस्टवर्थिनेस टिकवून ठेवते.

उदाहरण: एका बँकेत ग्राहकांचे खाते तपशील आणि व्यवहार इतिहास डेटाबेसमध्ये साठवलेले असतात. जर योग्य सुरक्षा अंमलात आणली नाही, तर अटॅकर्स क्रेडिट कार्ड नंबर चोरणे, खाते शिल्लक बदलणे किंवा सेवा विस्कळीत करणे शक्य आहे. म्हणूनच मजबूत डेटाबेस सिक्युरिटी अत्यावश्यक आहे.

5.4.1 डेटाबेस सिक्युरिटीची गरज (Need for database security):

1. संवेदनशील आणि गोपनीय डेटा संरक्षणासाठी :(उदा., फायनान्शियल रेकॉर्ड्स, पर्सनल इन्फॉर्मेशन)
2. अनऑथराईज्ड ॲक्सेस टाळण्यासाठी: फक्त वैध युजर्सनाच डेटा पाहता किंवा बदलता येईल याची खात्री करते.
3. डेटा इंटेग्रिटी टिकवून ठेवण्यासाठी: डेटामधील ॲक्सिडेंटल किंवा मॅलिशस बदल रोखते.
4. डेटा ॲव्हेलेबिलिटी सुनिश्चित करण्यासाठी: क्रॅशेस, फेल्युअर्स आणि DoS सारख्या अटॅक्सपासून डेटाबेसचे संरक्षण करते.
5. डेटा ब्रीचेस आणि सायबरअटॅक्स टाळण्यासाठी: जसे की SQL इंजेक्शन, मालवेअर, फिशिंग इत्यादी.
6. इन्सायडर थ्रेट्स नियंत्रणात ठेवण्यासाठी: कर्मचारी किंवा प्रिव्हिलेज्ड युजर्सकडून होणारा मिसयूज रोखण्यासाठी.
7. कायदेशीर आणि नियामक आवश्यकता पूर्ण करण्यासाठी: (उदा., डेटा प्रोटेक्शन लॉज, ऑडिट आवश्यकता)
8. आर्थिक नुकसान आणि प्रतिमेची हानी टाळण्यासाठी: डेटा थेफ्ट किंवा करप्शनमुळे होणारे नुकसान रोखण्यासाठी.
9. सिक्युअर बॅकअप आणि रिकव्हरीला समर्थन देण्यासाठी: डिसॅस्टर्स किंवा फेल्युअर्सनंतर डेटा रिस्टोअर करता येईल याची खात्री करते.
10. योग्य ऑथेंटिकेशन आणि ऑथरायझेशन लागू करण्यासाठी: युजर्सना फक्त आवश्यक त्या परमिशन्सच मिळतील याची खात्री करते.

5.4.2 SQL इंजेक्शन अटॅक (SQL injection attack)

SQL इंजेक्शन हा एक डेटाबेस अटॅक आहे, ज्यामध्ये अटॅकर इनपुट फील्डमध्ये मॅलिशस SQL कमांड्स टाकून डेटाबेसमध्ये फेरफार करतो. SQL इंजेक्शन तेव्हा घडते जेव्हा वेब ॲप्लिकेशन युजर इनपुट योग्य प्रकारे व्हॅलिडेट करत नाही. अटॅकर्स ही व्हल्नरेबिलिटी वापरून लॉगिन फॉर्म्स, सर्च बॉक्सेस किंवा URL पॅरामिटर्स मध्ये हानिकारक SQL कोड टाकतात. त्यानंतर DBMS हा इंजेक्ट केलेला SQL कमांड एक्झिक्यूट करतो, ज्यामुळे अटॅकरला पुढील गोष्टी शक्य होतात :

1. ऑथेंटिकेशन बायपास करणे
2. संवेदनशील डेटा पाहणे
3. रेकॉर्ड्स मॉडिफाय करणे
4. टेबल्स डिलीट करणे
5. अगदी पूर्ण डेटाबेस कंट्रोल मिळवणे

SQL इंजेक्शन हा सर्वात सामान्य सिक्युरिटी थ्रेट्स पैकी एक आहे, कारण अनेक ॲप्लिकेशन्स डायनॅमिक SQL क्वेरीज वर अवलंबून असतात. SQL इंजेक्शन टाळण्यासाठी इनपुट व्हॅलिडेशन, प्रिपेअर्ड स्टेटमेंट्स, पॅरामिटराइज्ड क्वेरीज आणि लीस्ट प्रिव्हिलेज प्रिन्सिपल वापरणे आवश्यक आहे.

उदाहरण: लॉगिन फॉर्म क्वेरी:

```
SELECT * FROM users WHERE username = 'admin' AND password = '1234';
```

अटॅकर खालील इनपुट देतो:

युजरनेम : admin

पासवर्ड : `' OR '1'='1`

रिझल्टिंग क्वेरी:

```
SELECT * FROM users WHERE username='admin' AND password='' OR '1'='1';
```

कारण '1'='1' हे नेहमी true असते, त्यामुळे अटॅकरला अनऑथराईज्ड ॲक्सेस मिळतो.

5.4.3 डेटाबेस एन्क्रिप्शन (database encryption)

डेटाबेस एन्क्रिप्शन म्हणजे डेटाबेसमध्ये साठवलेला किंवा ट्रान्समिट होणारा डेटा क्रिप्टोग्राफिक अल्गोरिदम्स वापरून न वाचता येणाऱ्या फॉरमॅटमध्ये रूपांतरित करण्याची प्रक्रिया होय, ज्यामुळे अनऑथराईज्ड ॲक्सेस पासून डेटाचे संरक्षण

होते. डेटाबेस एन्क्रिप्शनमुळे, जरी एखाद्या अटॅकरला स्टोरेज मीडिया, बॅकअप फाइल्स किंवा कम्युनिकेशन चॅनेल्स ला ॲक्सेस मिळाला तरीही डेटा सुरक्षित राहतो, कारण डिक्रिप्शन की शिवाय तो समजून घेता येत नाही. एन्क्रिप्शन विविध स्तरांवर लागू करता येते, जसे की डिस्क-लेव्हल एन्क्रिप्शन, टेबल-लेव्हल एन्क्रिप्शन, कॉलम-लेव्हल एन्क्रिप्शन किंवा ॲप्लिकेशन-लेव्हल एन्क्रिप्शन. पासवर्ड्स, क्रेडिट कार्ड नंबर आणि पर्सनल आयडेंटिफायर्स यांसारखा संवेदनशील डेटा सामान्यतः प्रायव्हसी आणि रेग्युलेटरी कॉम्प्लायन्स राखण्यासाठी एन्क्रिप्ट केला जातो. आधुनिक DBMSs मध्ये बिल्ट-इन एन्क्रिप्शन टूल्स उपलब्ध असतात, उदा. MySQL AES फंक्शन्स, PostgreSQL pgcrypto आणि Oracle TDE. एन्क्रिप्शनमुळे सुरक्षा वाढते, मात्र सिक्युअर की मॅनेजमेंट प्रॅक्टिसेस वापरून त्याचे काळजीपूर्वक व्यवस्थापन करणे आवश्यक असते.

उदाहरण: डेटाबेसमध्ये क्रेडिट कार्ड नंबर एन्क्रिप्ट करणे:

```
SELECT HEX (AES_ENCRYPT ('4567-8901-2345-6789', 'secretkey'));
```

आउटपुट: 5F8A2C3C9E6F4D8E2B1A7C5D4F9E8B3A

जरी एखाद्या अटॅकरला डेटाबेस ॲक्सेस मिळाला तरी, सिक्रेट की शिवाय एन्क्रिप्ट केलेले व्हॅल्यू वाचता येत नाही.

5.5 क्लाऊड सिक्युरिटी (Cloud security)

क्लाऊड सिक्युरिटी म्हणजे क्लाऊड-बेस्ड डेटा, ॲप्लिकेशन्स आणि सर्व्हिसेस यांचे संरक्षण करण्यासाठी डिझाइन केलेल्या टेक्नॉलॉजीज, कंट्रोल्स, प्रोसेसेस आणि पॉलिसीज यांचा संच होय. क्लाऊड कम्प्युटिंग चा वापर मोठ्या प्रमाणावर स्टोरेज, ॲनालिटिक्स आणि कम्प्युटिंग सर्व्हिसेस साठी केला जात असल्यामुळे, क्लाऊड एन्व्हायर्नमेंट्स सुरक्षित ठेवणे अत्यंत आवश्यक बनते.

5.5.1 क्लाऊड कम्प्युटिंगची एसेन्शियल कॅरेक्टरिस्टिक्स (Cloud security: Essential characteristics)

1. ऑन-डिमांड सेल्फ-सर्व्हिस: युजर्स सर्व्हिस प्रोव्हायडरकडून कोणत्याही मानवी हस्तक्षेपाशिवाय आपोआप कम्प्युटिंग रिसोर्सेस ॲक्सेस करू शकतात.
2. ब्रॉड नेटवर्क ॲक्सेस: सर्व्हिसेस नेटवर्कवर उपलब्ध असतात आणि स्टँडर्ड मेकॅनिझम्स द्वारे ॲक्सेस केल्या जातात (उदा. वेब ब्राउझर्स, मोबाईल ॲप्स).
3. रिसोर्स पूलिंग: कम्प्युटिंग रिसोर्सेस (स्टोरेज, CPU, RAM) हे मल्टी-टेनेन्ट मॉडेल वापरून अनेक युजर्समध्ये पूल आणि शेअर केले जातात.
4. रॅपिड इलॅस्टिसिटी: युजरच्या डिमांडनुसार रिसोर्सेस जलदगतीने वाढवता किंवा कमी करता येतात.
5. मेझर्ड सर्व्हिस: क्लाऊड सिस्टिम्स आपोआप रिसोर्स युसेज मॉनिटर आणि ऑप्टिमाइझ करतात; बिलिंग हे प्रत्यक्ष वापरावर (actual consumption) आधारित असते.

5.5.2 क्लाऊड सर्व्हिस मॉडेल्स (Cloud service model)

a. इन्फ्रास्ट्रक्चर ॲज अ सर्व्हिस (Infrastructure as a Service -IaaS)

इन्फ्रास्ट्रक्चर ॲज अ सर्व्हिस (IaaS) हे एक क्लाऊड कम्प्युटिंग सर्व्हिस मॉडेल आहे, जे व्हर्च्युअल मशिन्स, स्टोरेज आणि नेटवर्किंग यांसारखी मूलभूत कम्प्युटिंग रिसोर्सेस इंटरनेट द्वारे प्रदान करते. हे रिसोर्सेस ऑन-डिमांड उपलब्ध करून दिले जातात आणि सहसा पे-ॲज-यू-गो प्रायसिंग मॉडेलचे अनुसरण करतात. त्यामुळे संस्था महागड्या फिजिकल हार्डवेअर मध्ये गुंतवणूक न करता प्रत्यक्ष वापरानुसार आपले इन्फ्रास्ट्रक्चर स्केल करू शकतात. IaaS मॉडेलमध्ये क्लाऊड व्हेंडर कोअर इन्फ्रास्ट्रक्चर कॉम्पोनंट्सचे होस्टिंग आणि मॅनेजमेंट करतो, ज्यामध्ये सर्व्हर्स, स्टोरेज सिस्टिम्स, नेटवर्किंग डिव्हाइसेस, डेटा सेंटर्स आणि हायपरवायझर (व्हर्च्युअलायझेशन लेयर) यांचा समावेश असतो. यामुळे संस्थांना ऑन-प्रिमायसेस हार्डवेअर मेंटेन करण्याची गरज राहत नाही आणि ऑपरेशनल कॉम्प्लेक्सिटी कमी होते. IaaS हे वेब ॲप्लिकेशन्स आणि एंटरप्राइझ सिस्टिम्स डिप्लॉय व रन करण्यासाठी आवश्यक असलेले फंडामेंटल बिल्डिंग ब्लॉक्स प्रदान करते. हे युजर्सना त्यांच्या व्हर्च्युअलाइज्ड इन्फ्रास्ट्रक्चर वर पूर्ण नियंत्रण देते, ज्यामध्ये ऑपरेटिंग सिस्टिम्स, स्टोरेज कॉन्फिगरेशन्स आणि डिप्लॉय केलेली ॲप्लिकेशन्स यांचा समावेश असतो. या उच्च स्तराच्या कंट्रोल आणि फ्लेक्सिबिलिटी मुळे, IaaS हे कस्टमायझेबल एन्व्हायर्नमेंट्स आणि कम्प्युटिंग रिसोर्सेसचे थेट मॅनेजमेंट आवश्यक असलेल्या संस्थांसाठी अत्यंत उपयुक्त ठरते.

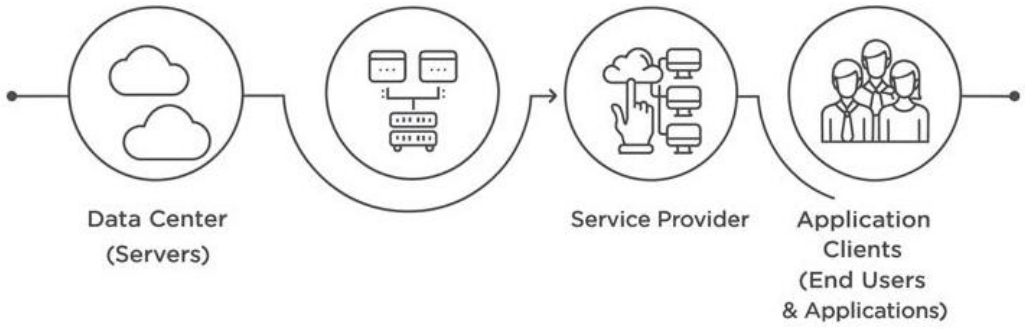


Fig 5.17: इन्फ्रास्ट्रक्चर अॅज अ सर्व्हिस (Infrastructure as a Service)(IaaS)

IaaS मॉडेल इतर क्लाऊड सर्व्हिस मॉडेल्सच्या तुलनेत सर्वात जास्त फ्लेक्सिबिलिटी आणि अॅडमिनिस्ट्रेटिव्ह कंट्रोल प्रदान करते. त्यामुळे स्केलेबिलिटी, रिलायबिलिटी आणि डीप कॉन्फिगरेशन ऑप्शन्स आवश्यक असलेल्या वर्कलोड्ससाठी ते योग्य ठरते.

उदाहरणे: AWS EC2, Google Compute Engine

सिक्युरिटी रिस्पॉन्सिबिलिटी:

- प्रोव्हायडर → फिजिकल सिक्युरिटी, नेटवर्क इन्फ्रास्ट्रक्चर
- कस्टमर → OS सिक्युरिटी, ॲप्स, डेटा सिक्युरिटी

b. प्लॅटफॉर्म अॅज अ सर्व्हिस (Platform as a Service-PaaS)

प्लॅटफॉर्म अॅज अ सर्व्हिस (PaaS) हे एक क्लाऊड कम्प्युटिंग मॉडेल आहे, जे सॉफ्टवेअर ॲप्लिकेशन्स तयार करणे, डिप्लॉय करणे आणि मॅनेज करण्यासाठी एक पूर्ण फ्रेमवर्क प्रदान करते. यामध्ये ॲप्लिकेशन डेव्हलपमेंटसाठी आवश्यक असलेली टूल्स, मिडलवेअर आणि रनटाइम एन्व्हायर्नमेंट्स समाविष्ट असतात. PaaS मुळे डेव्हलपर्स फक्त ॲप्लिकेशन कोड लिहिणे आणि मॅनेज करणे यावर लक्ष केंद्रित करू शकतात, तर क्लाऊड प्रोव्हायडर आपोआप सर्व्हर्स, स्टोरेज, नेटवर्किंग, व्हर्च्युअलायझेशन आणि ऑपरेटिंग सिस्टिम्स यांसारखे अंडरलाईंग इन्फ्रास्ट्रक्चर हाताळतो. हा मॉडेल ऑटोमॅटिक स्केलेबिलिटी ला सपोर्ट करतो, ज्यामुळे डिमांडनुसार ॲप्लिकेशन्स आपोआप स्केल अप किंवा स्केल डाउन होतात, कोणत्याही मॅन्युअल हस्तक्षेपाशिवाय. PaaS सोल्यूशन्स संपूर्ण ॲप्लिकेशन लाईफ-सायकल ला सपोर्ट करणाऱ्या सर्व्हिसेस प्रदान करतात, ज्यामध्ये डेव्हलपमेंट, टेस्टिंग, डिप्लॉयमेंट आणि मेंटेनन्स यांचा समावेश असतो. यामुळे फिजिकल किंवा व्हर्च्युअल इन्फ्रास्ट्रक्चर मेंटेन करण्याचा ओव्हरहेड न ठेवता ॲप्लिकेशन्स तयार करणे, रन करणे आणि मॅनेज करणे अधिक सोपे व जलद होते. एकूणच, PaaS संस्थांना आणि डेव्हलपर्सना रॅपिड इनोव्हेशन, टाइम-टू-मार्केट कमी करणे आणि ऑपरेशनल कॉम्प्लेक्सिटी कमी करणे यासाठी सक्षम बनवते, तसेच त्यांच्या ॲप्लिकेशन्स होस्ट करण्यासाठी एक मजबूत क्लाऊड प्लॅटफॉर्म उपलब्ध करून देते.

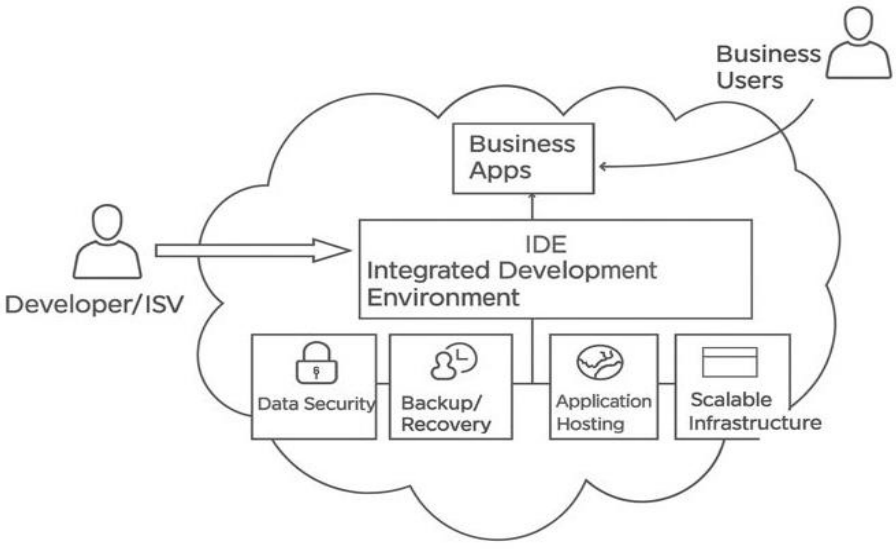


Fig 5.18: प्लॅटफॉर्म अॅज अ सर्व्हिस (Platform as a Service (PaaS))

उदाहरणे: गूगल ॲप इंजिन, मायक्रोसॉफ्ट अझ्युअर ॲप सर्व्हिसेस
सिक्युरिटी रिस्पॉन्सिबिलिटी:

- प्रोव्हायडर → OS, मिडलवेअर, रनटाइम
- कस्टमर → ॲप्लिकेशन-लेव्हल सिक्युरिटी

c. सॉफ्टवेअर ॲज अ सर्व्हिस (Software as a Service- SaaS)

सॉफ्टवेअर ॲज अ सर्व्हिस (SaaS) हे एक वेब-बेस्ड सॉफ्टवेअर डिलिव्हरी मॉडेल आहे, ज्यामध्ये ॲप्लिकेशन्स सर्व्हिस प्रोव्हायडरकडून होस्ट केली जातात आणि इंटरनेट द्वारे युजर्सना उपलब्ध करून दिली जातात. युजर्स वेब ब्राउझर द्वारे सॉफ्टवेअर ॲक्सेस करतात, त्यासाठी ॲप्लिकेशन कुठे होस्ट आहे, कोणत्या ऑपरेटिंग सिस्टिम वर रन होते किंवा कोणत्या प्रोग्रामिंग लँग्वेज मध्ये डेव्हलप केले आहे हे जाणून घेण्याची गरज नसते. SaaS ॲप्लिकेशन्स इंटरनेट कनेक्शन असलेल्या कोणत्याही डिव्हाइसवरून ॲक्सेस करता येतात, त्यामुळे त्या अत्यंत फ्लेक्सिबल आणि कन्व्हिनियंट असतात. हा मॉडेल याची खात्री करतो की युजर्स नेहमीच सॉफ्टवेअरची लेटेस्ट व्हर्जन वापरत आहेत, कारण अपडेट्स, अपग्रेड्स आणि पॅचेस हे थेट SaaS प्रोव्हायडरकडून हाताळले जातात. मेंटेनन्स चे सर्व पैलू,जसे की सिक्युरिटी, बॅकअप्स, परफॉर्मन्स मॉनिटरिंग आणि टेक्निकल सपोर्ट हे प्रोव्हायडरकडून मॅनेज केले जातात. SaaS मॉडेलमध्ये युजर्स अंडरलाईंग क्लाऊड इन्फ्रास्ट्रक्चर वर कोणतेही मॅनेजमेंट किंवा कंट्रोल करत नाहीत, ज्यामध्ये सर्व्हर्स, स्टोरेज, नेटवर्क आणि कम्प्युटिंग रिसोर्सेस यांचा समावेश असतो.

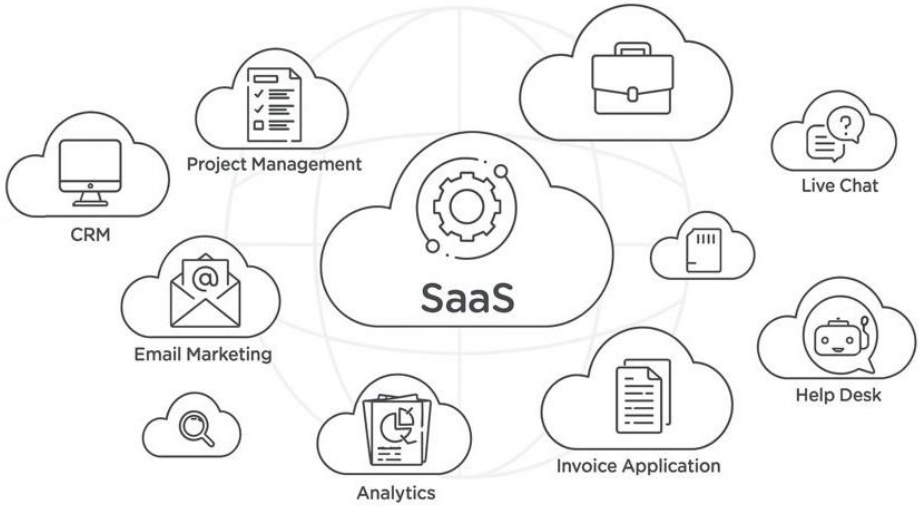


Fig 5.19: सॉफ्टवेअर ॲज अ सर्व्हिस (Software as a Service (SaaS))

उदाहरणे: जीमेल, सेल्सफोर्स
सिक्युरिटी रिस्पॉन्सिबिलिटी:

- प्रोव्हायडर → इन्फ्रास्ट्रक्चर + ॲप्लिकेशन सिक्युरिटी
- कस्टमर → युजर ऑथेंटिकेशन, डेटा हॅण्डलिंग

5.5.3 क्लाऊड डिप्लॉयमेंट मॉडेल्स (Cloud deployment model)

क्लाऊड डिप्लॉयमेंट मॉडेल्स हे क्लाऊड सर्व्हिसेस युजर्सना कशा प्रकारे उपलब्ध करून दिल्या जातात हे परिभाषित करतात, ज्यामध्ये क्लाऊड एन्व्हायर्नमेंटची कॉन्फिगरेशन स्पष्ट केली जाते. हे मॉडेल्स ओनरशिप, इन्फ्रास्ट्रक्चर साईज, कंट्रोलची पातळी आणि इन्फ्रास्ट्रक्चरचे फिजिकल लोकेशन यांसारख्या घटकांवर आधारित वेगवेगळे असतात. सर्वाधिक वापरले जाणारे चार क्लाऊड डिप्लॉयमेंट मॉडेल्स खालीलप्रमाणे आहेत: पब्लिक क्लाऊड, प्रायव्हेट क्लाऊड, हायब्रिड क्लाऊड, कम्युनिटी क्लाऊड.

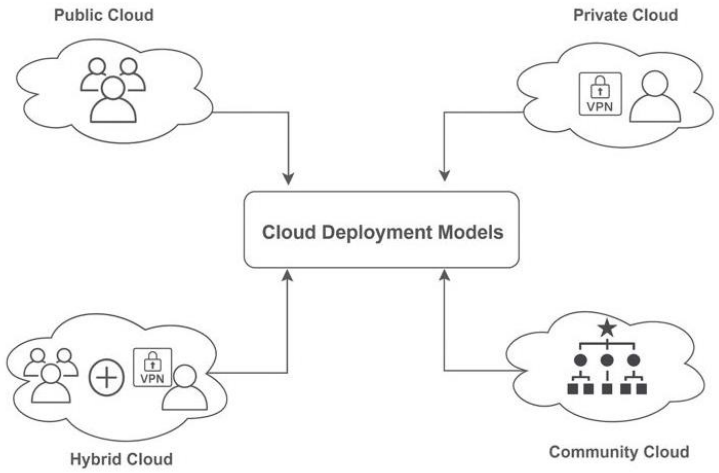


Fig 5.20: क्लाऊड डिप्लॉयमेंट मॉडेल्स (Cloud Deployment Models)

a. पब्लिक क्लाऊड

पब्लिक क्लाऊड कोणत्याही युजर किंवा संस्थेसाठी उपलब्ध असतो, जे व्हर्च्युअल मशिन्स (उदा. Amazon EC2), स्टोरेज किंवा डेटाबेस सर्व्हिसेस यांसारखी कम्प्युटिंग रिसोर्सेस पे-पर-यूज किंवा सबस्क्रिप्शन बेसिसवर वापरू इच्छितात. युजर्स किंवा संस्थांना फिजिकल हार्डवेअर खरेदी किंवा मेंटेन करण्याची गरज नसते; संपूर्ण इन्फ्रास्ट्रक्चर हे क्लाऊड प्रोव्हायडर मॅनेज करतो. पब्लिक क्लाऊड डिप्लॉयमेंट सहसा अशा बिझनेस ऑपरेशन्ससाठी वापरले जाते जिथे प्रायव्हसी ही मोठी चिंता नसते किंवा नॉन–मिशन-क्रिटिकल टास्क्स साठी. हे मल्टी-टेनेन्सी मॉडेल फॉलो करते, ज्यामुळे युजर्स आवश्यकतेनुसार रिसोर्सेस स्केल करू शकतात.

उदाहरणे : एडब्ल्यूएस, अझ्युअर, गूगल क्लाऊड

फायदे (Pros) : कॉस्ट-इफेक्टिव्ह, स्केलेबल

सिक्युरिटी कन्सर्न : मल्टी-टेनेन्सी, डेटा प्रायव्हसी

b. प्रायव्हेट क्लाऊड

प्रायव्हेट क्लाऊड हा पब्लिक क्लाऊडपेक्षा अधिक महाग असतो, परंतु तो संस्थेला अधिक कंट्रोल, सिक्युरिटी आणि प्रायव्हसी प्रदान करतो. पब्लिक क्लाऊडसारखे फायदे असले तरी, यातील मुख्य फरक असा की इन्फ्रास्ट्रक्चर हे फक्त एका टेनेन्ट किंवा संस्थेसाठी समर्पित (डेडिकेटेड) असते आणि इतरांबरोबर शेअर केलेले नसते. प्रायव्हेट क्लाऊड ऑन-प्रिमायसेस होस्ट केला जाऊ शकतो आणि स्वतः संस्था मॅनेज करू शकते किंवा थर्ड-पार्टी क्लाऊड सर्व्हिस प्रोव्हायडर कडून ऑपरेट केला जाऊ शकतो.

फायदे (Pros) : उच्च सिक्युरिटी, उत्तम कंट्रोल

वापर करणारे : बँका, सरकारी संस्था

c. हायब्रिड क्लाऊड

हायब्रिड क्लाऊड मध्ये पब्लिक क्लाऊड आणि प्रायव्हेट क्लाऊड या दोन्ही एन्व्हायर्नमेंट्सचा समावेश असतो. उदाहरणार्थ, एखादी संस्था आपले मिशन-क्रिटिकल वर्कलोड्स सुरक्षित प्रायव्हेट क्लाऊडवर चालवू शकते, तर कमी संवेदनशील ॲप्लिकेशन्स पब्लिक क्लाऊड वर डिप्लॉय करू शकते. हा अप्रोच सिक्युरिटी, स्केलेबिलिटी आणि कॉस्ट एफिशियन्सी यांचा योग्य समतोल साधतो.

फायदे (Pros) : फ्लेक्सिबिलिटी, ऑप्टिमाइझ्ड कॉस्ट आणि सिक्युरिटी

युज केस : संवेदनशील डेटा प्रायव्हेट ठेवून ॲप्स पब्लिक क्लाऊडवर रन करणे

d. कम्युनिटी क्लाऊड

कम्युनिटी क्लाऊड हा प्रायव्हेट क्लाऊडसारखाच असतो, पण त्याचे इन्फ्रास्ट्रक्चर एकाच कम्युनिटी किंवा सेक्टर मधील अनेक संस्थांमध्ये शेअर केलेले असते. या संस्था समान गरजा पूर्ण करण्यासाठी रिसोर्सेस, इन्फ्रास्ट्रक्चर आणि कधी कधी डेटा देखील शेअर करतात.उदाहरणार्थ, एखाद्या देशातील विविध सरकारी विभाग सुरक्षितपणे कॉमन डेटा ॲक्सेस आणि एक्स्चेंज करण्यासाठी एक कम्युनिटी क्लाऊड वापरू शकतात.

5.5.4 क्लाऊड-स्पेसिफिक सिक्युरिटी थ्रेट्स (cloud specific security threats)

1. डेटा ब्रीचेस (Data Breaches)
   कमकुवत ऑथेंटिकेशन किंवा चुकीच्या प्रकारे कॉन्फिगर केलेल्या डेटाबेस मुळे संवेदनशील क्लाऊड डेटावर अनऑथराईज्ड ॲक्सेस मिळणे.
2. डेटा लॉस (Data Loss)
   ॲक्सिडेंटल डिलीशन, मॅलिशस अटॅक्स किंवा फॉल्टी बॅकअप्स मुळे डेटा नष्ट होणे.
3. इन्सिक्युअर APIs (Insecure APIs)
   क्लाऊड सर्व्हिसेस API वापरून कम्युनिकेशन करतात; असुरक्षित APIs चा अटॅकर्स कडून गैरवापर होऊ शकतो.
4. अकाउंट हायजॅकिंग (Account Hijacking)
   अटॅकर्स युजर क्रेडेन्शियल्स मिळवून क्लाऊड रिसोर्सेसवर अनऑथराईज्ड कंट्रोल मिळवतात.
5. इन्सायडर थ्रेट्स (Insider Threats)
   क्लाऊड प्रोव्हायडर किंवा कस्टमरकडील मॅलिशस किंवा केअरलेस एम्प्लॉईज डेटाचा लीक किंवा मिसयूज करू शकतात.
6. डिनायल-ऑफ-सर्व्हिस (DoS) अटॅक्स
   अटॅकर्स क्लाऊड सर्व्हिसेसवर जास्त लोड टाकतात, ज्यामुळे त्या लेजिटिमेट युजर्स साठी अनुपलब्ध होतात.
7. शेअर्ड टेक्नॉलॉजी व्हल्नरेबिलिटीज (Shared Technology Vulnerabilities)
   क्लाऊड इन्फ्रास्ट्रक्चरमध्ये हायपरवायझर्स, व्हर्च्युअल मशिन्स यांसारखे शेअर्ड रिसोर्सेस वापरले जातात; त्यातील कमतरता अनेक टेनेन्ट्स वर परिणाम करू शकते.
8. मिसकॉन्फिगरेशन थ्रेट्स (Misconfiguration Threats)
   क्लाऊड स्टोरेजमधील चुकीच्या सेटिंग्ज (उदा. ओपन S3 बकेट्स) मुळे डेटा सार्वजनिकरित्या उघड होऊ शकतो.
9. लॅक ऑफ व्हिजिबिलिटी ॲण्ड कंट्रोल (Lack of Visibility and Control)
   कस्टमर्सना बॅकएंड ऑपरेशन्स साठी सर्व्हिस प्रोव्हायडर्सवर अवलंबून राहावे लागते, त्यामुळे सिक्युरिटीवरील त्यांचा कंट्रोल कमी होतो.

References:

1. Stallings, W., & Brown, L. (2014). *Computer Security: Principles and Practice* (3rd ed.). Pearson. ISBN: 978-0-13-377392-7.
2. Kahate, A. (2018). *Cryptography and Network Security* (3rd & 4th ed.). McGraw-Hill. ISBN: 978-9353163303.
3. Merkow, M., & Breithaupt, J. (2006). *Information Security: Principles and Practices*. Pearson. ISBN: 978-81-317-1288-7.
4. Pachghare, V. K. (2012). *Cryptography and Information Security*. Prentice Hall India. ISBN: 978-81-203-5082-3.
5. Gollmann, D. (2011). *Computer Security* (3rd ed.). Wiley. ISBN: 978-0-470-74115-3.
6. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
7. NPTEL. (2022). *Introduction to Information Security.* https://archive.nptel.ac.in/courses/106/106/106106129/
8. SWAYAM. (2022). *Information Technology Course.* https://onlinecourses.swayam2.ac.in/cec22_cs15/preview
9. Virtual Labs (IIIT Hyderabad). (n.d.). *Virtual Laboratory for Cryptography Experiments.* https://cse29-iiith.vlabs.ac.in/List%20of%20experiments.html
10. GeeksforGeeks. (2021). *Active and Passive Attacks in Information Security.* https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/