महाराष्ट्र राज्य तंत्रशिक्षण मंडळ, मुंबई

(स्वायत्त) (ISO 9001:2015) (ISO/IEC 27001:2013)

अभियांत्रिकी आणि तंत्रज्ञान पदविका

शिक्षण पुस्तिका

(Learning Material)

INFORMATION SECURITY

(314319)

K Scheme

इन्फॉरमेशन सेक्युरिटी

संगणक अभियांत्रिकी गट

(के स्कीम)

मराठी–इंग्रजी (द्विभाषिक) माध्यम

(अभियांत्रिकी व तंत्रज्ञानातील चौथे सत्र पदविका)

शिक्षण पुस्तिका

(Learning Material)

इन्फॉरमेशन सेक्युरिटी

Information Security (314319)

संगणक अभियांत्रिकी

गट (के-स्कीम)

K-Scheme

मराठी-इंग्रजी (द्विभाषिक) माध्यम

(अभियांत्रिकी व तंत्रज्ञानातील चौथे सत्र पदविका)

महाराष्ट्र राज्य तंत्रशिक्षण मंडळ मुंबई

((स्वायत्त)(ISO 9001:2015) (ISO/IEC 27001:2013)

इन्फॉरमेशन सेक्युरिटी

Information Security (314319)

मार्गदर्शक

प्रा. कुकरे विजय नामदेवराव

विभाग प्रमुख संगणक अभियांत्रिकी

प्रकल्प समन्वयक

प्रा. सोनाली मोरताळे

विभाग प्रमुख इन्फॉरमेशन टेक्नोलॉजि

संकलक

सोनाली मोरताळे
अधिव्याख्याता

मनस्विनी परळीकर
अधिव्याख्याता

गायत्री मुजुमदार
अधिव्याख्याता

माधवी माळी
अधिव्याख्याता

शितल चत्तर
अधिव्याख्याता

महाराष्ट्र राज्य तंत्र शिक्षण मंडळ

(स्वायत्त) (ISO: ९००१:२०१५) (ISO/IES: २७००१-२०१३)

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

दूरध्वनी क्र.: ०२२-६२५४२१७० / १६१

Email : director@msbte.com Web : www.msbte.org.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 असतांना संकल्पनात्मक ज्ञान, सुसंगत संदर्भ, प्रश्न विचारणे, विश्वसनिय 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 खेड्यापाड्यातून विकसित झालेला देश असून ग्रामीण भागातील विद्यार्थ्यांना तांत्रिक शिक्षण घेतांना 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 शैक्षणिक वर्ष २०२१-२२ पासून उपलब्ध करून दिलेला आहे .

राष्ट्रीय शैक्षणिक धोरण-२०२० प्रादेशिक भाषेतील शिक्षणास प्रोत्साहन देते, ज्यामुळे विद्यार्थ्यांना तांत्रिक अभ्यासक्रमांसाठी प्रादेशिक भाषांतुन शिक्षणाचे माध्यम निवडता येते. सदर धोरणामुळे प्रादेशिक भाषांमध्ये तांत्रिक सामग्री आणि अभ्यास सामग्रीचा विकास आणि भाषांतर निर्माण करण्याची आवश्यकता आहे . त्यास अनुसरून मंडळाने मराठी-इंग्रजी द्विभाषिक माध्यमाचा पर्याय द्वितीय व तृतीय वर्षाकरिताही उपलब्ध करून देण्यात आला आहे. तसेच त्याकरिताची शैक्षणिक सामग्रीही संबंधीत भागधारकरांना उपलब्ध करून देण्यात येत 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 सम्पन्न 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 प्रमुख विषयांची मराठी-इंग्रजी द्विभाषिक शैक्षणिक सामुग्री बनविण्यासाठी अध्यापक व सुकाणू समितीचे सदस्य यांनी दर्शविलेले समर्पण व वचनबद्धता कौतुकास पात्र आहे , या सर्वांचे मी मनः पूवक अभिनंदन करतो !

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

अनुक्रमणिका

अ. नु.	युनिटचे नाव	पृष्ठक्रमांक
1	इन्फॉरमेशन सेक्युरिटी चा परिचय **(Introduction to Information Security)**	01
2	युजर ऑथेंटीकेशन अँड ॲक्सेस कंट्रोल **(User authentication and Access Control)**	22
3	क्रिप्टोग्राफीची मूलतत्त्वे **(Fundamentals of Cryptography)**	46
4	एन्क्रिप्शन अल्गोरिदम **(Encryption Algorithm)**	62
5	इन्फॉर्मेशन सेक्युरिटी आणि सायबर कायदा **(Information Security and Cyber Laws)**	82

युनिट - 1
इन्फॉरमेशन सेक्युरिटी चा परिचय
(Introduction to Information Security)

विषय निष्पत्ती (Course Outcome)(CO)

CO1: हल्ल्यांचे (attack)प्रकार ओळखा ज्यामुळे माहितीच्या सुरक्षिततेस धोका निर्माण होतो.

घटक निष्पत्ती(Theory Learning Outcomes)

1. माहिती सुरक्षेची आवश्यकता स्पष्ट करा.
2. माहिती वर्गीकरणासाठी निकष सांगा.
3. माहिती सुरक्षेची मूलभूत तत्त्वे स्पष्ट करा.
4. विविध प्रकारचे हल्ले ओळखा.
5. मालवेयरचे प्रकार नोंदवा.
6. धमकी, असुरक्षितता, योग्य उदाहरणासह जोखीम यांच्यात संबंध स्थापित करा.

1.1 इन्फॉरमेशन सेक्युरिटी (Information Security)

सारांश(Overview)

1.1.1 इन्फॉरमेशनची ओळख (Introduction to Information): इन्फॉरमेशन(Information) हे आउटपुट(output) आहे जे विश्लेषण(analysing),संदर्भित करणे(contextualizing), रचना(structuring), अर्थ लावणे(interpreting) किंवा डेटावर प्रक्रिया करण्याच्या इतर मार्गांनी परिणाम करते.

1.1.2 इन्फॉरमेशन सुरक्षेची आवश्यकता(Need of Information Security) : आपण चोरी आणि सायबर क्राइमसह(cyber crime) विविध प्रकारच्या धोक्यांपासून मौल्यवान(valuable) इन्फॉरमेशन(Information) मालमत्तेचे संरक्षण करण्यासाठी इन्फॉरमेशन(Information) सुरक्षा वापरतो. इन्फॉरमेशनची(Information) सुरक्षा महत्त्वाची का आहे याची काही मुख्य कारणे खाली दिली आहेत.

- **सेन्सीटिव्ह इन्फॉरमेशनचे संरक्षण (Security of sensitive Information)**: सेन्सीटिव्ह (sensititve) इन्फॉरमेशनला (Information) अनधिकृत व्यक्तींकडून ऍक्सेस(access) किंवा मॉडिफाय(modify) होण्यापासून संरक्षण करण्यास इन्फॉरमेशन(Information) सेक्युरिटी मदत करते. यात वैयक्तिक इन्फॉरमेशन (Information), आर्थिक डेटा(financial data) आणि व्यापार रहस्ये (trade secrets)तसेच गोपनीय(confidential) सरकार आणि लष्करी इन्फॉरमेशनचा समावेश असतो .
- **धोका कमी करणे(Mitigating risk)**: इन्फॉरमेशन सुरक्षा उपायांची अंमलबजावणी करून, संस्था सायबर थ्रेट(cyber threat) आणि इतर सुरक्षा घटनांशी संबंधित रिस्क(risk) कमी करू शकतात. यात डेटा उल्लंघन(data breaches), डिनायल ऑफ सर्विस अटॅक(denial-of-service attacks) आणि इतर मॅलीशीअस ऍक्टिव्हिटीचा(malicious activity) धोका कमी होतो.
- **नियमांचे पालन(Compliance with regulations)** : बऱ्याच उद्योग आणि कार्यक्षेत्रांमध्ये सेन्सीटिव्ह इन्फॉरमेशनच्या (sensitive Information)संरक्षणाचे नियमन करणारे विशिष्ट नियम आहेत. इन्फॉरमेशन सेक्युरिटी नियमांचे पालन सुनिश्चित करण्यात मदत करतात त्याचबरोबर दंड आणि कायदेशीर उत्तरदायित्वाचा(legal liability) धोका कमी करतात.
- **प्रतिष्ठेचे संरक्षण(Protecting the Reputation)** : सुरक्षा उल्लंघन एखाद्या संस्थेच्या प्रतिष्ठेचे नुकसान करू शकते आणि व्यवसाय गमावण्यास कारणीभूत ठरू शकते. प्रभावी इन्फॉरमेशन सुरक्षा ,सुरक्षा घटनांचा धोका कमी करून संस्थेच्या प्रतिष्ठेचे संरक्षण करू शकते.
- **बिझनेस कन्टीनुएटी(Business continuity) सुनिश्चित करणे :** सेक्युरिटी इनसिडेन्ट(security incident) झाल्यासही क्रिटिकल(critical) व्यवसाय कार्ये सुरू राहू शकतात यासाठी इन्फॉरमेशन सुरक्षा मदत करते. हे, की

सिस्टम आणि डेटा(key system and data) ॲक्सेस करते आणि कोणत्याही व्यत्ययांचा(disruptions) प्रभाव कमी करते.

1.2 इन्फॉरमेशन वर्गीकरण, इन्फॉरमेशन वर्गीकरणासाठी निकष(Information Classification,Criteria for Information Classification)

1.2.1 इन्फॉरमेशन वर्गीकरण

इन्फॉरमेशनचे वर्गीकरण ही एक प्रक्रिया आहे जी त्याच्या सेन्सीटिव्हिटी (sensitivity) आणि महत्तवाच्या पातळीवर आधारित डेटाचे(data) वर्गीकरण करण्यासाठी इन्फॉरमेशन सुरक्षेमध्ये वापरली जाते. वर्गीकरणाचा उद्देश त्या इन्फॉरमेशनशी संबंधित जोखमीच्या पातळीवर आधारित योग्य सुरक्षा नियंत्रणे लागू करून सेन्सीटिव्ह इन्फॉरमेशनचे(sensitive information) संरक्षण करणे आहे. अशा अनेक भिन्न वर्गीकरण योजना आहेत ज्या संस्था वापरू शकतात, परंतु त्यामध्ये सामान्यत: वर्गीकरणाच्या काही सामान्य स्तरांचा समावेश आहे, जसे की:

- **सार्वजनिक(Public)**: जी इन्फॉरमेशन सेन्सीटिव्ह(sensitive information) नाही आणि कोणाबरोबरही मुक्तपणे शेयर केली जाऊ शकते.
- **अंतर्गत(Internal)**: सेन्सीटिव्हिट(sensitive) परंतु क्रिटिकल(critical) नसलेली इन्फॉरमेशन केवळ संस्थेमध्ये शेअर केली जावी.
- **कॉन्फिडेंशियल(confidential) :** सेन्सीटिव्ह (sensitive) आणि संरक्षणाची आवश्यकता असलेली इन्फॉरमेशन (information) केवळ अधिकृत व्यक्ती किंवा ग्रुप्स(groups) सह शेअर(share) केली जावी.
- **रहस्य(secret)**: जी अत्यंत सेन्सीटिव्ह(sensitive) आहे आणि उच्च पातळीवरील संरक्षणाची आवश्यकता आहे अशी माहिती केवळ अधिकृत व्यक्तींच्या निवडक गटासह शेअर केले जावे.
- **टॉप सीक्रेट(Top-secret) :** ज्या इन्फॉरमेशनचा खुलासा केला तर राष्ट्रीय सुरक्षेचे अपवादात्मक नुकसान होईल अशा इन्फॉरमेशनचा ॲक्सेस अधिकृत व्यक्तींनाच दिला जातो .
- **इन्फॉरमेशनच्या वर्गीकरणात** केवळ अधिकृत व्यक्ती इन्फॉरमेशनमध्ये प्रवेश करू शकतात हे सुनिश्चित करण्यासाठी योग्य वर्गीकरण स्तरासह इन्फॉरमेशनचे लेबलिंग(information lebelling) आणि प्रवेश नियंत्रणे अंमलात आणण्याची प्रक्रिया देखील समाविष्ट आहे. हे फायरवॉल(firewall), इंट्रूशन डिटेक्शन सिस्टम(Intrusion detection system) आणि एन्क्रिप्शन (encryption)सारख्या सुरक्षा तंत्रज्ञानाच्या वापराद्वारे केले जाते.

1.2.2 इन्फॉरमेशन वर्गीकरणासाठी निकष(Criteria of Information Classification):

- **मूल्य(Value)** - खाजगी क्षेत्रातील डेटाचे(data) वर्गीकरण करण्यासाठी हे सर्वात सामान्यपणे वापरले जाणारे निकष आहे. जर एखाद्या संस्थेसाठी इन्फॉरमेशन(information) मौल्यवान असेल तर त्याचे वर्गीकरण करणे आवश्यक आहे.
- **वय** (**Age**)- माहितीचे वर्गीकरण त्या माहितीचे मूल्य कालांतराने कमी झाल्यास कमी केले जाऊ शकते.
- **उपयुक्त जीवन(Useful Life)**- माहिती अधिक उपयुक्त ठरेल जर ती आवश्यकतेनुसार बदल करण्यासाठी उपलब्ध असेल.
- **वैयक्तिक असोसिएशन(Association)** - जर माहिती विशिष्ट व्यक्तीशी संबंधित असेल किंवा ती गोपनीयतेच्या कायद्याने हाताळली जात असेल, तर ती वर्गीकृत केली जाऊ शकते.

1.3 इन्फॉरमेशन सुरक्षेची मूलभूत तत्त्वे: (Basic principles of information security)

कॉन्फिडेन्शिअलीटी(Confidentiality),ऑथेंटिकेशन(Authentication),इंटेग्रिटी(Integrity), अव्हेलेबिलिटी (Availability),ॲक्सेस कंट्रोल्स(Access Controls) , रेपुडीएशन (Repudiation)

इन्फोमेशन सिस्टिम सिक्युरिटी (INFOSEC) म्हणजे संगणक, नेटवर्क(Network) आणि संबंधित डेटाची सुरक्षा प्रदान करण्याची प्रक्रिया आहे. तंत्रज्ञानाच्या वाढीसोबत, ज्या प्रमाणात माहिती विस्तृत नेटवर्कवर साठवली जाते, त्याप्रमाणे ती अनधिकृत व्यक्तींच्या वापरापासून संरक्षण करणे अत्यंत महत्त्वाचे आहे. प्रत्येक संस्थेकडे अशा डेटाचे संच असतात ज्यामध्ये त्यांच्या ॲक्टिव्हिटीबद्दल(Activity) गोपनीय माहिती असते.

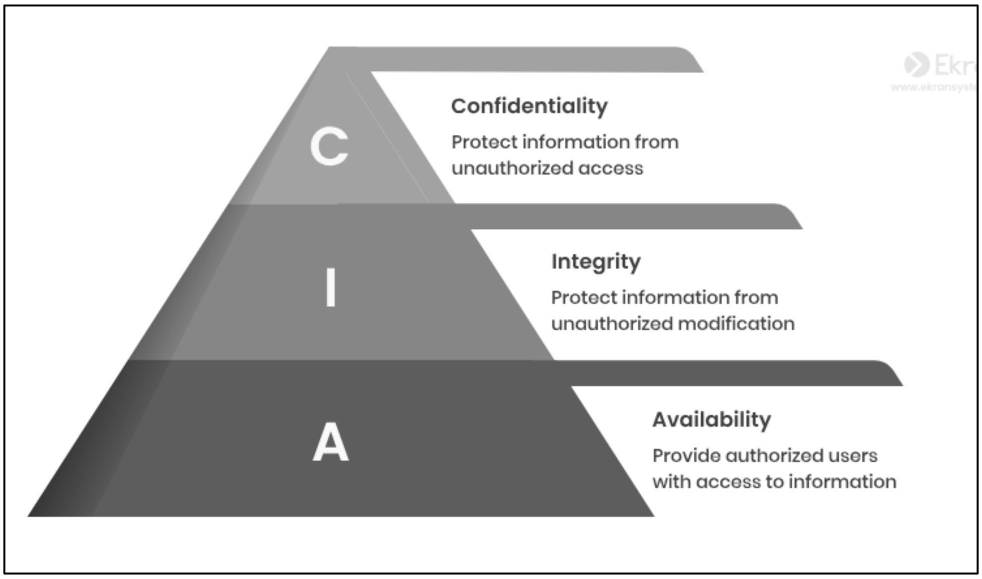


Figure.1.1 CIA Model(Courtesey: https://www.suridata.ai)

- **कॉन्फिडेन्शिअलीटी (Confidentiality):** कॉन्फिडेन्शिअलीटी हे सुनिश्चित करते की सेन्सीटिव्ह इन्फॉरमेशन(sensitive information) अनधिकृत व्यक्ती, घटक किंवा प्रक्रियेस उघड केली जात नाही.
- **अखंडता(Integrity**): अखंडता हे सुनिश्चित करते की डेटा अचूक(data) आणि विश्वासार्ह असावा. हे माहितीतील अनधिकृत बदलांना प्रतिबंधित करते, ज्यामुळे ती माहिती विश्वासार्ह राहते.
- **प्रमाणीकरण**(**Authentication):** प्रमाणीकरण वापरकर्त्यांची, सिस्टमची किंवा उपकरणांची ओळख पडताळते जेणेकरून केवळ अधिकृत संस्थाच संसाधनांमध्ये(resources) प्रवेश करू शकतील याची खात्री होते. हे अनधिकृत प्रवेश प्रतिबंधित करते.
- **नॉन-रिप्यूडिएशन (Non-Repudiation)**: नॉन-रिप्यूडिएशन हे सुनिश्चित करते की एखाद्या व्यवहारामध्ये, संप्रेषणात(transaction) किंवा कृतीत सामील असलेल्या व्यक्ती किंवा घटक त्यांचा सहभाग नाकारू शकत नाहीत. हे डेटाची उत्पत्ती(origin of data) आणि पावती या दोन्हींचा पुरावा प्रदान करते, ज्यामुळे पक्षांना(parties) जबाबदार ठेवणे शक्य होते.
- **ऍक्सेस कंट्रोल(Access-control)**: ऍक्सेस कंट्रोल ही एक सेक्युरिटी स्ट्रॅटेजी (security strategy) आहे जी संगणक प्रणालीमध्ये संसाधने कोण किंवा काय पाहू शकते किंवा काय वापरू शकते यावर नियंत्रण ठेवते. ही एक मूलभूत सुरक्षा संकल्पना आहे जी कंपनी किंवा संस्थेचा धोका कमी करते.

1.4 हल्ल्यांचा प्रकार: ऍक्टिव्ह आणि पॅसीव अटॅक(Active and Passive), डिनायल ऑफ सर्विस (डॉस) अटॅक(Denial of service), डीडीओएस(DDOS), बॅकडोर्स आणि ट्रॅपडोर्स(Backdoors and Trapdoor), स्निफिंग(sniffing), फिशिंग(fishing), स्पूफिंग(Spoofing), मॅन इन मिडल(Man in Middle), रीप्ले(Replay), टीसीपी/आयपी हॅकिंग(TCP/IP Hacking), एन्क्रिप्शन हल्ले(encryption), सोशल इंजिनिअरिंग(Social engineering)

सायबर सिक्युरिटीमध्ये(Social security), सध्याच्या काळातील अनेक प्रकारच्या सायबर थ्रेटस(cyber threat) आहेत जे संगणक सुरक्षा, नेटवर्क(network) सुरक्षा आणि इन्फॉरमेशनच्या सुरक्षिततेशी संबंधित असू शकतात. मुळात थ्रेटस(threats) चे दोन प्रकार आहेत: ऍक्टिव्ह (active)आणि पॅसीव्ह (passive)अटॅक.

1.4.1 ऍक्टिव्ह अटॅक(Active attack):

हल्लेखोर आपल्या संगणक प्रणालीला थेट हानी पोहचवतात त्याला ऍक्टिव्ह अटॅक म्हणतात. ते अनेक समस्या तयार करू शकतात, जसे की क्रॅशिंग फाईल्स (crashing files), डेटा चोरणे इत्यादी. ऍक्टिव्ह अटॅक (Active attack) हे अनधिकृत क्रिया आहेत जी सिस्टम किंवा डेटामध्ये (system and data) बदल करतात. सक्रिय हल्ल्यात, हल्लेखोर(attacker) थेट लक्ष्यावर(target) हस्तक्षेप करतो ज्यामुळे संगणक प्रणाली आणि नेटवर्कमध्ये अनधिकृत प्रवेश मिळवणे किंवा हानी होणे शक्य

होते. यामध्ये शत्रुत्वपूर्ण कोड(injection of hostile) संवादांमध्ये इंजेक्ट करणे, डेटामध्ये बदल करणे, आणि अनधिकृत प्रवेश मिळवण्यासाठी दुसऱ्या व्यक्तीच्या रूपात छुपे राहणे(masquerading) यांचा समावेश होऊ शकतो.
ॲक्टिव्ह अटॅकचे प्रकार खालीलप्रमाणे आहेत:
1. मास्करेड अटॅक (Masquerade Attack)
2. मॉडिफिकेशन ऑफ मॅसेज (Modification of Messages)
3. रिप्यूडिएशन (Repudiation)
4. रीप्ले अटॅक (Replay Attack)
5. डिनायल ऑफ सर्विस (डॉस) अटॅक (Denial of Service (DoS) Attack)

1.मास्करेड अटॅक (Masquerade Attack)

मास्करेड हल्ले(Masquerade attack) हे सायबर हल्ल्यांच्या प्रकारांपैकी एक मानले जातात, ज्यामध्ये हल्लेखोर स्वतःला दुसऱ्या व्यक्तीच्या रूपात लपवतो आणि सिस्टम किंवा डेटामध्ये (system and data)प्रवेश करतो. यामध्ये तो कायदेशीर वापरकर्ता (legal user)किंवा सिस्टम म्हणून नक्कल करू शकतो किंवा दुसऱ्या वापरकर्त्यांपासून संवेदनशील माहिती मिळवण्यासाठी मागणी करू शकतो. यामध्ये लोकांना त्यांची खाजगी माहिती देण्यासाठी किंवा त्यांना सुरक्षित ठिकाणी जाण्याची परवानगी देण्यासाठी प्रत्यक्ष वापरकर्त्यासारखे किंवा सिस्टमच्या एखाद्या घटकासारखे वागणे देखील समाविष्ट असू शकते.

मास्करेड अटॅकचे (Masquerade attack) प्रकार:

- **युझरनेम आणि पासवर्ड मास्करेड(Username and password Masquerade)**: या मास्करेड हल्ल्यात(Masquerade attack), एक व्यक्ती चोरी केलेली किंवा बनावट प्रमाणपत्रे वापरून स्वतःला वैध वापरकर्ता म्हणून प्रमाणित करते, ज्यामुळे तो सिस्टम किंवा ॲप्लिकेशनमध्ये प्रवेश मिळवतो.
- **आयपी ॲड्रेस मास्करेडः (IP address Masquerade attack):** आयपी ऍड्रेस मास्करेड(Masquerade) म्हणजे एक नेटवर्क तंत्रज्ञान जे एका डिव्हाइसचा वास्तविक आयपी ऍड्रेस दुसऱ्या आयपी ऍड्रेस द्वारे लपवते.
- **वेबसाइट मास्करेडः(website Masquerade)**: एक हॅकर(hacker) एक फेक वेबसाइट(fake website) तयार करते जी वापरकर्त्याची इन्फॉरमेशन(information) मिळविण्यासाठी किंवा मालवेयर(malware) डाउनलोड करण्यासाठी कायदेशीर वेबसाइटसारखी दिसते.
- **ईमेल मास्करेडः(Email Masquerade)** हा एक ई-मेल(Email Masquerade) मास्करेड हल्ला आहे, ज्याद्वारे हल्लेखोर(attacker) एक विश्वासार्ह स्रोताचा ई-मेल पाठवतो, ज्यामुळे प्राप्तकर्ता चुकून संवेदनशील माहिती शेअर(share) करू शकतो किंवा मालवेअर डाउनलोड करू शकतो.

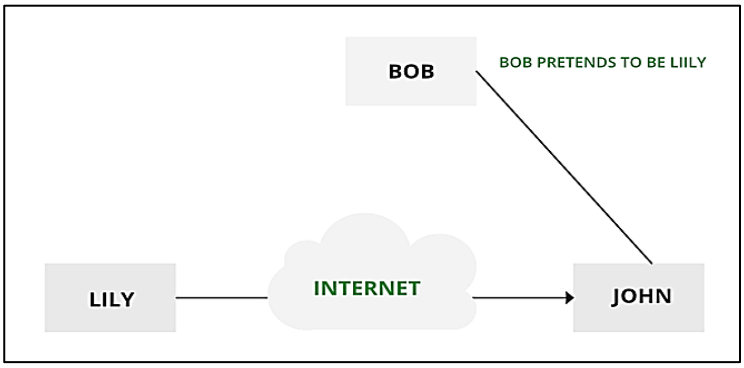


Figure.1.2 Masquerade Attack(Courtesey: https://www.geeksforgeeks.org)

2.मॉडीफिकेशन ऑफ मेसेज(Modification of Messages)

हे तेव्हा घडते जेव्हा कोणीतरी संदेशाच्या(message) भागात परवानगी न घेता बदल करतो, किंवा संदेशांच्या क्रमाचा गोंधळ घालतो, ज्यामुळे अडचण निर्माण होते. कल्पना करा की कोणीतरी गुपचूप आपल्याला पाठवलेला पत्र बदलतो आणि ते वेगळं

काहीतरी सांगायला बनवतो. असा हल्ला माहितीच्या विश्वसनीयतेला धक्का पोहोचवतो. उदाहरणार्थ, "JOHN ला गोपनीय फाइल-X वाचण्याची परवानगी द्या" या संदेशाला बदलून "Smith ला गोपनीय फाइल-X वाचण्याची परवानगी द्या" असं केले जातं.

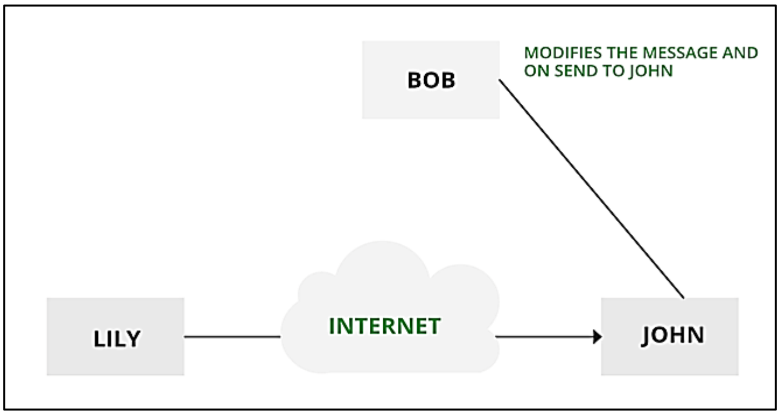


Figure.1.3 Modification of messages(Courtesey: https://www.geeksforgeeks.org)

3.रेपुडीएशन (Repudiation)

रिपुडिएशन हल्ले (Repudiation attack)हे सायबर हल्ल्यांचा एक प्रकार आहेत, ज्यामध्ये एखादी व्यक्ती ऑनलाइन काही हानीकारक क्रिया करते, जसे की वित्तीय व्यवहार करणे किंवा एखादी अशी संदेश पाठवणे जी ती व्यक्ती पाठवू इच्छित नाही, आणि नंतर ती क्रिया केली असल्याचे नाकारते. असे हल्ले, हल्ल्याच्या मूळचा(origin) मागोवा घेण्याच्या क्षमता किंवा दिलेल्या क्रियेसाठी कोण जबाबदार आहे हे ओळखण्यात मोठा अडथळा निर्माण करतात, ज्यामुळे योग्य व्यक्तीला जबाबदार ठरवणे कठीण होऊन जाते.

रेपुडीएशन हल्ल्यांचे (Repudiation attack) प्रकार

- **मेसेज रिप्यूडिएशन हल्ले: (Message repudiation attack)** या हल्ल्यात, एक संदेश(message) हल्लेखोराने पाठवलेला असतो, पण नंतर हल्लेखोर त्या संदेशाच्या पाठवणीचा नाकारतो. हे स्पूफड(spoofed) किंवा बदललेले हेडर्स(headers) वापरून किंवा संदेश प्रणालीतील कमतरतांचा फायदा उठवून साधता येऊ शकते.
- **ट्रान्झॅक्शन रिप्यूडिएशन अटॅक: (Transaction repudiation attack)** या प्रकाराच्या हल्ल्यात, आर्थिक व्यवहार केला जातो आणि काही वेळानंतर जेव्हा त्या व्यवहाराबद्दल पुरावे मागितले जातात, तेव्हा हल्लेखोर त्या विशिष्ट व्यवहाराची कधीही अंमलबजावणी केली नाही असे नकार देतो. हे व्यवहार प्रक्रिया प्रणालीतील कमकुवतपणाचा(vulnerability) फायदा घेत किंवा चोरी केलेली आणि बनवलेली ओळखपत्रे वापरून केले जाऊ शकते, ज्यामुळे व्यवसायाला नुकसान होऊ शकते.
- **डेटा रिपुडिएशन हल्ले**: (**Data repudiation attack**)डेटा रिपुडिएशन अटॅकमध्ये **(**Data repudiation attack) , डेटा बदलला जातो किंवा मिटवला जातो. त्यानंतर हल्लेखोर दावा करतो की त्याने कधीही हे केलेच नाही. हे डेटा संग्रहण प्रणालीतील(data storage system) कमकुवतपणाचा (vulnerability) फायदा घेत किंवा चोरी केलेली किंवा बनवलेली ओळखपत्रे वापरून केले जाऊ शकते.

4.रीप्ले (Replay)

हे एक संदेशाचे निष्क्रियपणे कॅप्चर (passive capturing)करणे आहे, ज्याचा उद्देश अधिकृत(authorized) परिणाम साधण्यासाठी त्याला प्रसारित(production) करण्यासाठीआहे. त्यामुळे, या प्रकाराच्या हल्ल्यात, हल्लेखोराचा मुख्य उद्देश म्हणजे त्या विशिष्ट नेटवर्कवर मूळतः असलेल्या डेटाची एक कॉपी साठवणे आणि नंतर ती वैयक्तिक वापरासाठी वापरणे. एकदा डेटा लीक झाल्यावर, तो त्याच्या वापरकर्त्यांसाठी असुरक्षित साधन बनतो.

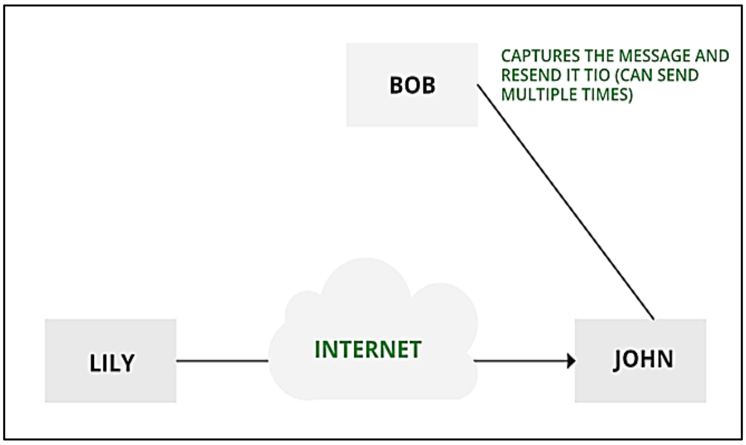


Figure.1.4 Replay(Courtesey: https://www.geeksforgeeks.org)

5.डिनायल ऑफ सर्व्हिस अटॅक (डॉस) (Denial of Service):

डिनायल ऑफ सर्व्हिस(Denial of Service) (DoS) हे एक सायबर सुरक्षा हल्ल्याचे रूप आहे, ज्यात प्रणाली किंवा नेटवर्कच्या इच्छित वापरकर्त्यांना ट्रॅफिक किंवा विनंत्यांद्वारे(request) प्रवेश नाकारला जातो. या DoS हल्ल्यात, हल्लेखोर लक्षित प्रणाली(target system) किंवा नेटवर्कला ट्रॅफिक किंवा विनंत्यांनी भरून टाकतो, ज्यामुळे उपलब्ध संसाधने जसे की बँडविड्थ(bandswidth), CPU सायकल्स, किंवा मेमरी वापरली जातात आणि योग्य वापरकर्त्यांना त्यांचा प्रवेश करता येत नाही.

डॉस हल्ल्यांचे (DOS attack) प्रकार:

- **फ्लड अटॅक(Flood Attack)**:येथे, हल्लेखोर एकूण इतक्या मोठ्या संख्येने पॅकेट्स(packet) किंवा विनंती(request) सिस्टम किंवा नेटवर्ककडे पाठवतो की ती सर्व हाताळू शकत नाही आणि प्रणाली(system) क्रॅश होते.
- **एम्प्लिफिकेशन अटॅक(Amplification attack)**: या श्रेणीत, हल्लेखोर हल्ल्याची ताकद वाढवण्यासाठी दुसऱ्या प्रणाली किंवा नेटवर्कचा(system or network) वापर करून ट्रॅफिक(traffic) वाढवतो आणि नंतर ते सर्व लक्षित प्रणालीकडे पाठवून हल्ल्याची शक्ती(power) वाढवतो.

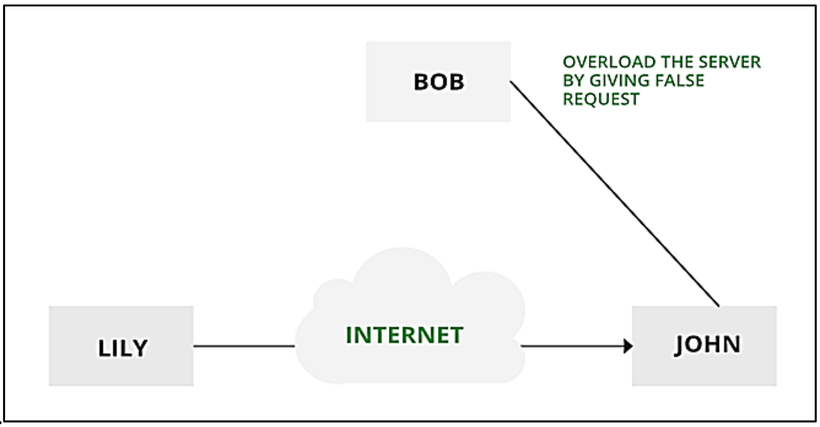


Figure.1.5 Denial of Service(Courtesey: https://www.geeksforgeeks.org)

1.4.2 पॅसीव्ह अटॅक(Passive Attack)

पॅसीव्ह अटॅकमध्ये (passive attack) हल्लेखोर(attacker), प्रणालीतील माहिती शिकण्याचा किंवा त्याचा वापर करण्याचा प्रयत्न करतो, परंतु प्रणाली संसाधनांवर(system resourcses) परिणाम करत नाही. पॅसीव्ह अटॅकमध्ये हल्लेखोर डेटा बदलू किंवा नष्ट न करता फक्त निरीक्षण करतो किंवा संकलित करतो. पॅसीव्ह अटॅकचे उदाहरणे म्हणजे ईव्हसड्रॉपिंग(evasdropping), ज्यामध्ये हल्लेखोर नेटवर्क ट्रॅफिकवर ऐकून संवेदनशील माहिती गोळा करतो, आणि स्निफिंग(sniffing), ज्यामध्ये हल्लेखोर डेटा पॅकेट्स कॅप्चर करून आणि विश्लेषण करून संवेदनशील माहिती चोरण्याचा प्रयत्न करतो.

पॅसीव्ह अटॅक(Passive Attack) चे प्रकार खालीलप्रमाणे आहेत:

1.द रीलीझ ऑफ मेसेज कन्टेन्ट (The release of message content)

2.ट्रॅफिक ॲनालिसिस (Traffic Analysis)

1.रिलीज ऑफ मेसेज कंटेंट : (The release of message content)

टेलिफोनिक संभाषण, इलेक्ट्रॉनिक मेल (electronic mail)संदेश किंवा हस्तांतरित फाइलमध्ये(file) सेन्सीटिव्ह(sensitive) किंवा गोपनीय इन्फॉरमेशन असू शकते.

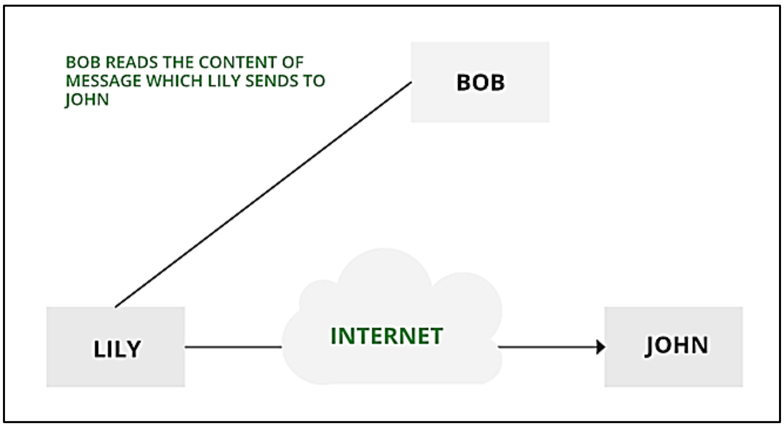


Figure1.6 Passive attack(Courtesey: https://www.geeksforgeeks.org)

2.ट्रॅफिक ॲनालिसिस(Traffic analysis)

समजा आपल्याकडे माहिती लपविण्याचा एक मार्ग आहे, ज्यामुळे हल्लेखोराला संदेश प्राप्त झाला तरीही त्याला संदेशातील कोणतीही माहिती काढून घेता येत नाही. प्रतिस्पर्धीने संप्रेषण(communicating) करणाऱ्या होस्टचे स्थान आणि ओळख निश्चित केली तरी, तो संदेशांच्या बदलांची वारंवारता आणि लांबी पाहून निरीक्षण करू शकतो. ट्रॅफिक ॲनालिसिस(Traffic analysis) एक सुरक्षा तंत्रज्ञान आहे जे नियमन करते की कोण किंवा काय संसाधनांना (resourses) पाहू किंवा वापरू शकते. हे सुरक्षा क्षेत्रातील एक मूलभूत संकल्पना आहे जी व्यवसाय किंवा संस्थेसाठी धोका कमी करते.

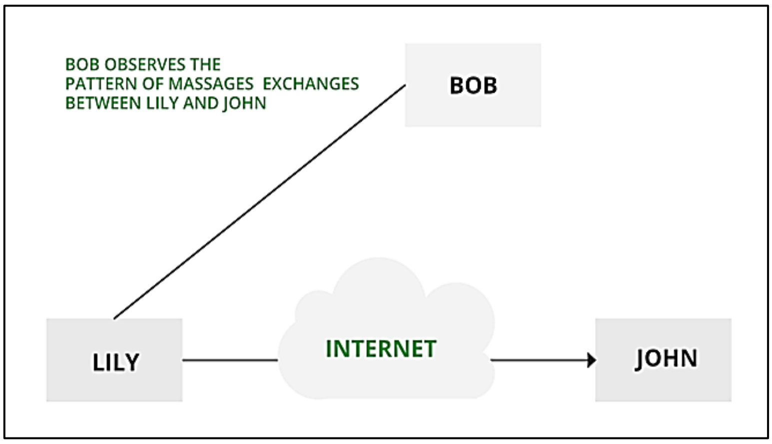


Figure1.7: Traffic Analysis(Courtesey: https://www.geeksforgeeks.org)

1.4.3 डिस्ट्रिब्युटेड डिनायलओफ सर्व्हाइस (डीडॉस) (Distributed DOS)

डिस्ट्रिब्युटेड डिनायल ऑफ सर्विस (DDoS) हल्ला हा एक सायबर हल्ला आहे जो सर्व्हर किंवा नेटवर्कवर(server and network) ट्रॅफिकने ओव्हरलोड करून त्याच्या सामान्य कार्यप्रणालीला विघटित (disrupt) करतो. DDoS हल्ले हे डिनायल ऑफ सर्विस (DoS) हल्ल्यांतील एक प्रकार आहे, परंतु ते अधिक हानिकारक आणि अडचणीचे असतात कारण ते अनेक स्त्रोतांकडून येतात आणि त्यांना थांबवणे (blog)कठीण असते.

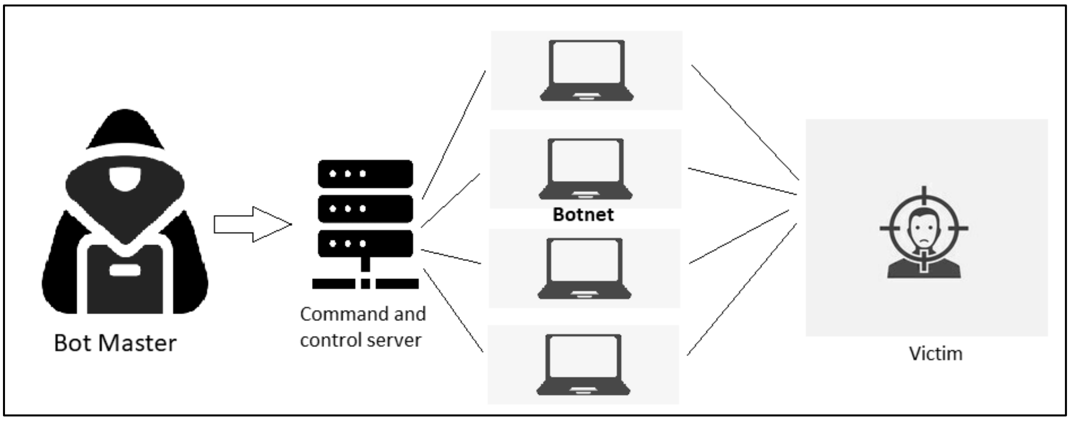


Figure1.8 DDoS Attack(Courtesey: https://www.geeksforgeeks.org)

हे कसे कार्य करते

- हल्लेखोर तडजोड केलेल्या संगणकांचा वापर करतात, ज्यांना बॉटनेट्स(botnet) म्हणतात, जे लक्ष्यावर मोठ्या प्रमाणात विनंत्या(request) पाठवतात.
- लक्ष्य (target)त्या विनंत्यांचा सामना करू शकत नाही आणि सेवा मंद होऊन किंवा कोसळून जाते.
- हल्ला (attack) लक्ष्यातील सेवा वैध(target) वापरकर्त्यांसाठी प्रवेशयोग्य नसल्यास बनवू शकतो.

प्रभाव

- DDoS हल्ल्यांमुळे व्यवसाय आणि संस्थांसाठी मोठा डाउनटाइम (downtime)होऊ शकतो.
- हे आर्थिक तोटे आणि वेबसाइटच्या प्रतिष्ठेची हानी करू शकतात.
- हे व्यवसायाची ऑनलाइन (online)सुरक्षा, विक्री आणि प्रतिष्ठा धोक्यात आणू शकतात.

संरक्षण

- फायरवॉल (firewall)आणि विशेष सेवा मॅलीशीअस ट्रॅफिक फिल्टर **(**malicious traffic filter**)** करू शकतात आणि वेबसाइट (website)प्रवेश करण्यायोग्य ठेवू शकतात
- संघटनात्मक प्रतिसाद योजना हल्ल्याचा प्रभाव कमी करण्यात मदत करू शकतात

1.4.4 बॅकडोअर आणि ट्रॅपडोअर (Backdoor and Trapdoor)

- बॅकडोअर (backdoor) हे एक मॅलीशीअस(malicious) संगणक प्रोग्राम किंवा विशेष मार्ग आहे, जो हल्लेखोराला तडजोड केलेल्या प्रणालीवर , स्थापित सॉफ्टवेअरच्या कमकुवतपणाचा(vulnerabilities) फायदा घेऊन आणि सामान्य प्रमाणीकरण चुकवून अनधिकृत रिमोट प्रवेश प्रदान करतो.
- बॅकडोअर पार्श्वभूमीत कार्य करतो आणि वापरकर्त्यापासून लपवतो. हे व्हायरससारखेच आहे आणि त्यामुळे त्याला शोधणे आणि पूर्णपणे अक्षम(disable) करणे खूप कठीण असते.
- बॅकडोअर हा एक अत्यंत धोकादायक परजीवी प्रकार आहे, कारण यामुळे एक दुष्ट व्यक्ती तडजोड केलेल्या संगणकावर कोणतीही क्रिया करण्यास सक्षम होतो. हल्लेखोर बॅकडोअर वापरून:
    - वापरकर्त्याची गुप्तपणे तपासणी करू शकतो,
    - फाइल्स व्यवस्थापित करू शकतो,
    - अतिरिक्त सॉफ्टवेअर किंवा धोकादायक धमक्यांचे संस्थापन करू शकतो,
    - संपूर्ण प्रणालीवर नियंत्रण ठेवू शकतो, ज्यामध्ये उपस्थित अनुप्रयोग (applications) किंवा हार्डवेअर उपकरणे देखील समाविष्ट आहेत,
    - संगणक बंद किंवा रिबूट करू शकतो, किंवा
    - इतर होस्ट्सवर हल्ला करू शकतो.
- बहुतेक बॅकडोअर हे स्वायत्त मॅलीशीअस प्रोग्राम असतात जे काही प्रकारे संगणकावर स्थापित करावी लागतात. काही परजीवींना स्थापित करण्याची आवश्यकता नाही, कारण त्यांचे भाग पूर्वीच विशेष सॉफ्टवेअरमध्ये समाविष्ट असतात जे

रिमोट होस्टवर चालत असते. हॅकर्स हे अनडॉक्युमेंटेड(undocumented) वैशिष्ट्ये शोधून त्यांचा वापर प्रणालीमध्ये प्रवेश करण्यासाठी करतात.

काउंटरमेजर(Countermeasure)

- **शक्तिशाली अँटीव्हायरस आणि अँटी-स्पायवेअर उत्पादने(antivirus and anti-spyware)**

क्रिप्टोग्राफीमध्ये(cryptography), ट्रॅपडोअर म्हणजे एक गुप्त बॅकडोअर जो एखाद्या अल्गोरिदम (algorithm)किंवा व्यक्तिगत डेटाच्या तुकड्यात लपवलेला असतो. याचा अर्थ असा की, लोक त्या बॅकडोअरचा शोध त्याबद्दल आधीपासून माहिती न मिळाल्यास घेऊ शकत नाहीत. हे ट्रॅपडोअर क्रिप्टोग्राफीमध्ये अत्यंत उपयुक्त असते, कारण ते माहितीला अवघड, तोडता न येणाऱ्या कोडमध्ये रूपांतरित करून ती सुरक्षित ठेवतात.
ट्रॅपडोअर हे आधुनिक क्रिप्टोग्राफीचे मुख्य आधारस्तंभ आहेत. त्यांचा उपयोग बँक खात्याच्या पासवर्ड्स(passwords) आणि सरकारी गुपिते सुरक्षित करण्यासाठी केला जातो. ट्रॅपडोअर असे काम करते ,जे वापरकर्ता किंवा प्रणाली ट्रॅपडोअरला प्रवेश करू शकते, ती व्यक्ती किंवा प्रणाली(system) जलदपणे प्रवेश करू शकते, आणि इतर लोकांना बॅकडोअर शोधणे अशक्य बनवते. यामुळे ट्रॅपडोअर तोडता येत नाहीत, जोपर्यंत डेव्हलपर (developer) त्यांना गुप्त(secret) ठेवतो.

1.4.5 स्निफिंग(sniffing)

पॅकेट स्निफिंग अटॅक(packet sniffing attack) हा एक नेटवर्क-निर्मित धोका आहे जिथे एक मॅलीशीअस नेटवर्क, पॅकेट्स कॅप्चर(capture) करते जे डेटा रहदारी रोखू किंवा चोरी करू शकत नाही.

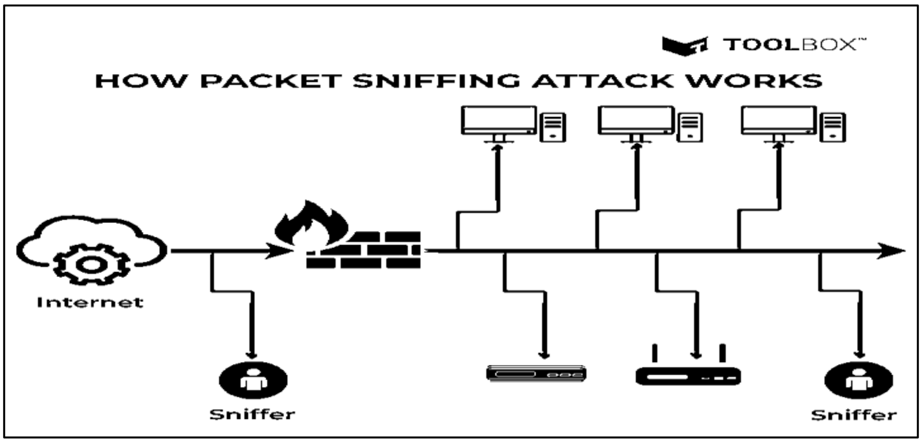


Figure. 1.9: Sniffing(Courtesey: https://www.spiceworks.com)

नेटवर्क इंटरफेस कार्ड (एनआयसी)(NIC) एक हार्डवेअर(hardware) घटक आहे ज्यामध्ये प्रत्येक संगणक नेटवर्कमध्ये सर्किट बोर्ड(circuit board) असते. एनआयसी(NIC) हे नॉन-अॅड्रेस्ड ट्रॅफिकला (non-addressed traffic)दुर्लक्ष करतात. स्निफिंग अटॅकसाठी एनआयसी प्रॉमिस्युअस(promiscuous) मोडवर सेट करणे आवश्यक आहे, जे एनआयसींना सर्व नेटवर्क रहदारी प्राप्त करण्यास अनुमती देते. स्निफर्स(sniffers) डेटा पॅकेटमधील एन्कोड(encode) केलेल्या इन्फॉरमेशनचे डीकोड(decode) करून एनआयसीमधून जाणाऱ्या सर्व रहदारीला पाहू शकतात. कमकुवतपणे एन्क्रिप्टेड डेटा पॅकेट्सद्वारे(encrypted data packets) स्निफिंग हल्ले अधिक प्रवेशयोग्य केले जातात.

1.4.5 फिशिंग(Phishing)

सायबर सिक्युरिटीमध्ये, "फिशिंग" म्हणजे एक फसवणुकीचा प्रकार आहे, ज्यामध्ये हल्लेखोर वैध संस्थेचे (जसे की बँक किंवा कंपनी) अनुकरण करतात. ईमेल्स, मजकूर संदेश, किंवा फोन कॉल्सद्वारे वापरकर्त्यांना संवेदनशील माहिती जसे की पासवर्ड्स, क्रेडिट कार्ड तपशील, किंवा व्यक्तिगत डेटा उघड करण्यासाठी फसवतात. हे हल्लेखोर वापरकर्त्यांना हानिकारक लिंक्सवर क्लिक करायला किंवा हानिकारकअटॅचमेंट्स डाउनलोड करायला प्रवृत्त करतात. मुख्यतः हे एक सामाजिक अभियांत्रिकी तंत्र आहे, जे वापरकर्त्यांना गोपनीय माहिती दिल्याने फसवण्याचे उद्दिष्ट ठरवते.

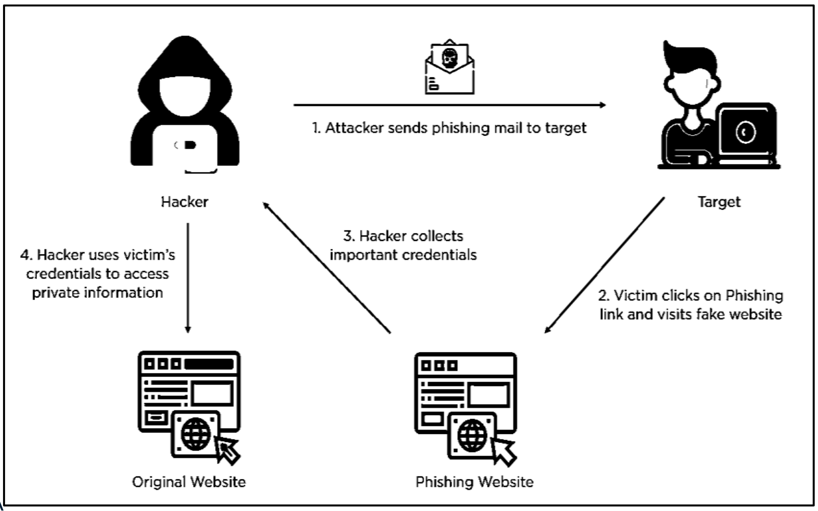


Figure1.10: Phishing(Courtesey: https://www.simplilearn.com)

स्टेप 1: एक मॅलीशीअस हॅकर (malicious hacker) टारगेट (target) ईमेल किंवा संदेश पाठवतो, ज्यामध्ये तो एक प्रतिष्ठित स्त्रोत म्हणून कार्य करत असतो. बहुतेक वेळा, तो लक्ष्याला एक तिसऱ्या पक्षाचा(thirdparty)लिंक्स अनुसरण करण्यास सांगतो, जे सुरक्षा तपासणी किंवा साध्या फिचर अपडेटसाठी असते.

स्टेप 2: टारगेट(target)ला असे वाटते की ईमेल उल्लेख केलेल्या प्रेषकाकडून आले आहे, हे बँक असो किंवा कंपनी, आणि तो लिंकमध्ये क्लिक करून बनावट वेबसाइटवर जातो, जी वास्तविक वेबसाइटसारखी दिसण्याचा प्रयत्न केलेली असते.

स्टेप 3: बनावट वेबसाइटवर, वापरकर्त्याला काही खाजगी माहिती जसे की एखाद्या विशिष्ट वेबसाइटसाठी अकाउंट क्रेडेन्शियल्स सबमिट करण्यास सांगितले जाते . एकदा माहिती सबमिट झाल्यावर, सर्व माहिती त्या हॅकरकडे(hacker) पाठवली जाते, ज्याने वेबसाइट आणि मॅलीशीअस (malicious) ईमेल डिझाइन केली होती.

स्टेप 4: अकाउंट क्रेडेन्शियल्स प्राप्त झाल्यावर, हॅकर त्यांचा वापर लॉगिन करण्यासाठी करू शकतो किंवा इंटरनेटवर मिळवलेल्या संबंधित माहितीला उच्चतम बोलीदाराला विकू शकतो.

1.4.6 स्पूफिंग(spoofing)

स्पूफिंग हा एक प्रकारचा सायबर गुन्हेगारी अॅक्टिविटी (activity) आहे जिथे एखादी व्यक्ती किंवा एखादी गोष्ट सेंडरची(sender) इन्फॉरमेशन तयार करते आणि वैयक्तिक इन्फॉरमेशनमध्ये (information)प्रवेश मिळविण्याच्या उद्देशाने कायदेशीर स्त्रोत, व्यवसाय, सहकारी किंवा इतर विश्वासार्ह संपर्क असल्याचे भासवते.

1.4.7 मॅन-इन-द-मिडल (Man in Middle)

मॅन-इन-द-मिडल (एमआयटीएम) व्यत्यय किंवा आर्थिक फायद्यासाठी डेटा(data) गोळा करणे किंवा बदलण्याच्या उद्देशाने दोन पक्षांमधील संप्रेषणास(communication) अडथळा आणते.

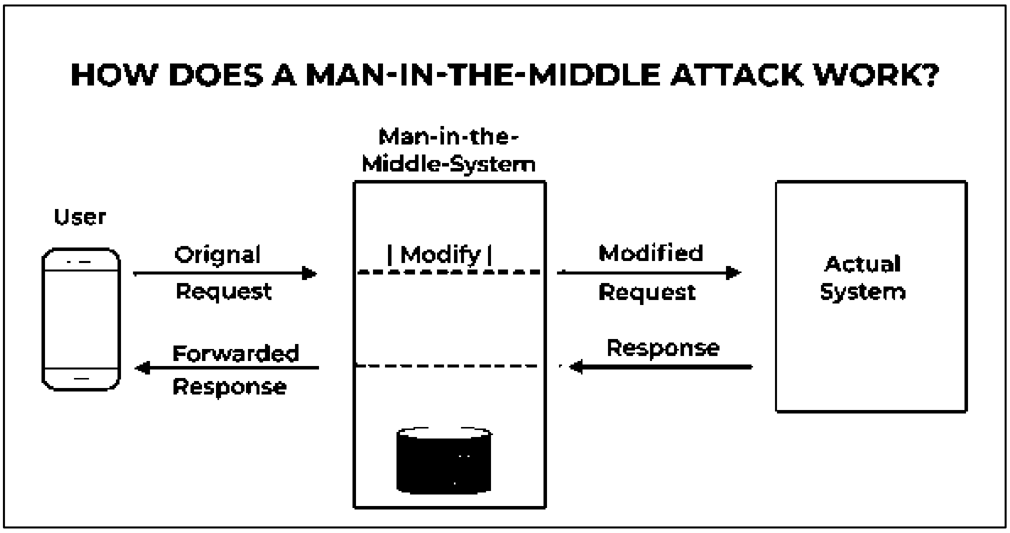


Figure.1.11: Man in Middle(Courtesey: https://www.spiceworks.com)

1.4.8 रीप्ले(Replay)

रिप्ले हल्ला हा नेटवर्क हल्ल्याचा (network attack)एक प्रकार आहे, ज्यामध्ये हल्लेखोर वैध नेटवर्क ट्रान्समिशन कॅप्चर करतो आणि नंतर त्याला पुनःप्रक्षिप्त(retransmit) करतो. मुख्य उद्देश हा असतो की, प्रणालीला डेटा पुनःप्रक्षिप्त केलेले ट्रान्समिशन वैध म्हणून स्वीकारण्यास फसवले जाऊ शकते. याव्यतिरिक्त, रिप्ले हल्ले धोकादायक असतात कारण त्यांचा शोध घेणे आव्हानात्मक असते. आणखी एक गोष्ट म्हणजे, जरी मूळ ट्रान्समिशन एन्क्रिप्ट केलेले असले तरी हा हल्ला यशस्वी होऊ शकतो. हल्लेखोर, प्रणाली किंवा नेटवर्कवर अनधिकृत प्रवेश मिळवण्यासाठी रिप्ले हल्ला सुरू करू शकतो . हल्लेखोर डेटा पॅकेट्स नेटवर्कवर इंटरसेप्ट(intercept) करून आणि पुनःप्रक्षिप्त करून हा हल्ला करण्यात यशस्वी होऊ शकतो. याव्यतिरिक्त, एक यशस्वी रिप्ले हल्ला रेकॉर्ड केलेले ऑडिओ किंवा व्हिडिओ (audio and video)ट्रान्समिशन्स पुन्हा प्ले देखील केला जाऊ शकतो.

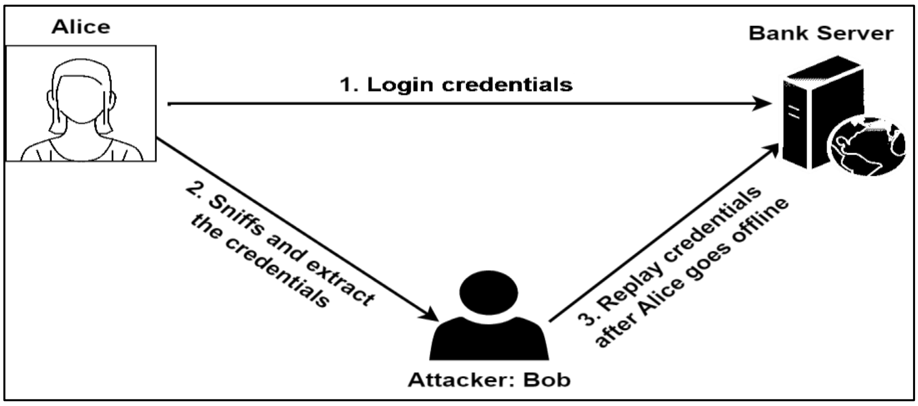


Figure.1.12: Replay attack process(Coutesey: https://www.baeldung.com/cs/replay-attacks)

कल्पना करा की ॲलिस तिच्या ऑनलाइन बँकिंग खात्यात सुरक्षित वेब कनेक्शन(web connection) वापरून लॉगिन (login)करण्याचा प्रयत्न करत आहे. जेव्हा ती तिचे लॉगिन क्रेडेन्शियल्स टाकते आणि सबमिट(submit) बटणावर क्लिक करते, तेव्हा लॉगिन विनंती इंटरनेटवरून बँकेच्या सर्व्हरकडे पाठवली जाते. बॉब नावाचा एक हल्लेखोर नेटवर्कचे निरीक्षण करत आहे आणि लॉगिन विनंती कॅप्चर करतो जशी ती प्रसारित केली जात आहे. बॉब नंतर ॲलिस तिच्या खात्यातून लॉगआउट होईपर्यंत थांबतो आणि कॅप्चर केलेली लॉगिन विनंती बँकेच्या सर्व्हरवर पुन्हा प्रसारित करतो. कारण लॉगिन विनंती वैध आहे, सर्व्हर ती स्वीकारतो आणि बॉबला ॲलिसच्या खात्यात प्रवेश मिळवून देतो.या परिस्थितीत, बॉब कॅप्चर केलेली लॉगिन विनंती पुन्हा खेळवून ॲलिसच्या खात्यात अनधिकृत प्रवेश मिळवू शकतो. तथापि, ॲलिस रिप्ले हल्ला रोखू शकते एक सुरक्षित संप्रेषण चॅनेल वापरून, ज्यामध्ये एक टाइमस्टॅम्प (timestamp)किंवा नॉनस (nonce) समाविष्ट असतो.

1.4.9 टीसीपी/आयपी हायजॅकिंग: (TCP/IP Hijacking) :टीसीपी/आयपी हायजॅकिंग(TCP/IP Hijacking) हा एक **मॅन-इन-द-मिडल(Man in middle)** नेटवर्क अटॅक आहे. ह्या अटॅक मध्ये अधिकृत वापरकर्ता दुसऱ्या वापरकर्त्याच्या किंवा क्लायंटच्या (client)अधिकृत नेटवर्क कनेक्शनमध्ये प्रवेश मिळवू शकतो. टीसीपी/आयपी (TCP/IP)सत्र अपहृत(hijack) केल्यानंतर, आक्रमणकर्ता हस्तांतरित पॅकेट (Packet)सहजपणे वाचण्यास आणि सुधारित करण्यास सक्षम असतो आणि हॅकर(hacker) वापरकर्त्यास स्वतःच्या विनंत्या पाठविण्यास सक्षम होतो. टीसीपी/आयपी हायजॅकिंगकरण्यासाठी, हल्लेखोर डॉस(DOS) हल्ले आणि आयपी स्पूफिंग (IP Spoofing)वापरतात.

टीसीपी/आयपी हायजॅकिंग प्रक्रिया: (Process of TCP/IP Hijacking)

- आक्रमणकर्त्याचे पहिले मुख्य लक्ष्य म्हणजे समान नेटवर्क किंवा कनेक्शनचा वापर करून संवाद साधणाऱ्या दोन डिव्हाइसचे(two device) आयपी(IP) प्राप्त करणे. हे करण्यासाठी, डिव्हाइसचा आयपी प्राप्त होईपर्यंत आक्रमणकर्ता नेटवर्कवरील डेटा ट्रान्समिशनचे(transmission) परीक्षण करतो.
- वापरकर्ता आयपी यशस्वीरित्या पकडल्यानंतर,हॅकर्स(hackers) सहजपणे कनेक्शनवर हल्ला करू शकतात.
- कनेक्शनमध्ये प्रवेश मिळविण्यासाठी, हॅकरने(Hackers) डॉस(DOS) हल्ल्याद्वारे दुसऱ्या वापरकर्त्याचे कनेक्शन बाजूला ठेवून वापरकर्त्याचे कनेक्शन पुन्हा कनेक्ट करण्याची प्रतीक्षा करतो.
- डिस्कनेक्ट(disconnect) केलेल्या वापरकर्त्याच्या आयपीची स्पूफ (IP spoof)करून, हॅकर्स सहजपणे पुन्हा कम्युनिकेशन (communication) करू शकतात.

प्रतिबंधात्मक उपाय:

- अनवॉन्टेड(unwanted) किंवा अननोन(unknown) लिंकवर (link) क्लिक(click) करू नका.
- सर्व एरर(error) साठी वेब अँपलिकेशन(web application) तपासा.
- अनवॉन्टेड किंवा अननोन ऍक्टीव्हीटीसाठी नेटवर्क ट्रॅफिक चे परीक्षण करण्यासाठी आणि एआरपी स्पूफिंग/पॉईझीनिंग(ARP Spoofing poisioning) शोधण्यासाठी इंट्रूयूशन डिटेक्शन सिस्टम(intrusion detection) (आयडीएस) वापरा.
- वाढीव सुरक्षेसाठी हबऐवजी(hub) स्विच वापरा.
- सुरक्षेच्या वाढीसाठी नेहमीच एसएसएलवर(SSL) सेशन आयडी पाठवा.
- प्रत्येक पृष्ठासाठी सेशन आयडीची भिन्न संख्या वापरा.
- एचटीटीपी(HTTP) सारख्या साध्या मजकूर प्रोटोकॉलऐवजी एचटीटीपीएस सारख्या सुरक्षित प्रोटोकॉलचा(protocol) वापर करा, जोपर्यंत आपल्याला काय योग्य आहे हे माहित नाही.

1.4.10 एन्क्रिप्शन अटॅक्स(Encryption attack)

"एन्क्रिप्शन अटॅक्स " माहिती सुरक्षा मध्ये हॅकऱ्याचा एक मॅलीशीअस प्रयत्न आहे, ज्यामध्ये तो एन्क्रिप्शन अल्गोरिदम किंवा की व्यवस्थापन प्रणालीतील कमकुवतनांचा (vulnerabilities) शोध घेऊन एन्क्रिप्ट केलेल्या डेटाला डिकोड करण्याचा आणि योग्य डिक्रिप्शन की(decryption key)शिवाय मूळ प्लेनटेक्स्ट माहितीवर प्रवेश मिळवण्याचा प्रयत्न करतो. साधारणपणे, एन्क्रिप्ट केलेल्या डेटाच्या सुरक्षा प्रणालीला बायपास करून अनधिकृत प्रवेश मिळवण्याचा प्रयत्न करतो.

एन्क्रिप्शन हल्ल्यांविषयी मुख्य मुद्देः

ध्येय(aim): एन्क्रिप्शन की (Encryption key)शी तडजोड करून किंवा एनक्रिप्शन अल्गोरिदममधील कमकुवतपणा शोधून एनक्रिप्टेड सायफरटेक्स्टमधून प्लेनटेक्स्ट(plaintext) डेटा पुनर्प्राप्त करण्यासाठी.

एन्क्रिप्शन हल्ले कसे कमी करावे:

- स्ट्रॉंग एन्क्रिप्शन अल्गोरिदम: (Strong Encryption Algorithm) एईएस(AES) सारख्या सुप्रसिद्ध आणि मजबूत एन्क्रिप्शन अल्गोरिदम वापरणे.
- स्ट्रॉंग की मॅनेजमेंट: (strong key management)की जनरेशन(key generation) , वितरण आणि संचयनासाठी सुरक्षित पद्धती लागू करणे.

- रेग्युलर नियमित की रोटेशन: दीर्घकाळापर्यंत संपर्क रोखण्यासाठी नियमितपणे एन्क्रिप्शन की(encryption key) बदलणे.
- व्हॅलिडेशन अँड इनपुट सॅनिटायझेशन: (validation and input sanitization) संभाव्य असुरक्षा टाळण्यासाठी मॅलीशीअस इनपुट फिल्टर(filter) करणे.

एन्क्रिप्शन हल्ल्याची काही उदाहरणे:

1. **ब्रूट फोर्स अटॅक: (Brute force attack)**डेटा डिक्रिप्ट(data decrypt) करण्यासाठी प्रत्येक संभाव्य की संयोजनाचा प्रयत्न करीत आहे, जो मजबूत एन्क्रिप्शन आणि मोठ्या कीस्पेससह कमी प्रभावी बनतो.
2. **चोझन प्लेनटेक्स्ट अटॅक:** (**Chosen Plaintext Attack)** हल्लेखोर एन्क्रिप्शन करण्यासाठी प्लेनटेक्स्ट्सची (plaintext)निवड करतो आणि संबंधित सायफरटेक्स्ट (ciphertext) प्राप्त करतो, ज्यामुळे त्यांना एन्क्रिप्शन तोडण्यासाठी नमुन्यांचे विश्लेषण करण्याची परवानगी मिळते.
3. **चोझन सायफरटेक्स्ट अटॅक Chosen Ciphertext Attack:** एक आक्रमणकर्ता सिफरटेक्स्ट्स निवडतो आणि त्यांचे संबंधित प्लेनटेक्स्ट्स प्राप्त करतो, ज्यामुळे त्यांना एन्क्रिप्शन अल्गोरिदममधील असुरक्षिततेचे शोषण करण्यास सक्षम करते.
4. **नोन -प्लेनटेक्स्ट अटॅक: (Known-Plaintext Attack)** हल्लेखोरांना प्लेन टेक्स्ट(plaintext) आणि त्याच्या संबंधित सायफरटेक्स्ट या दोघांमध्ये प्रवेश आहे, ज्यामुळे एन्क्रिप्शन की उलगडणे सोपे होते.
5. **सायफरटेक्स्ट-ओन्ली अटॅक: (Ciphertext-Only Attack)** हल्लेखोरांना केवळ कोणत्याही ज्ञात प्लेनटेक्स्टशिवाय एनक्रिप्टेड डेटामध्ये प्रवेश आहे, ज्यामुळे तो सर्वात कठीण प्रकारचा अटॅक बनतो.

1.4.11 सोशल अभियांत्रिकी(Social Engineering)

सोशल इंजिनीअरिंग म्हणजे एका पीडित(victim) व्यक्तीला फसवणूक करून, प्रभाव टाकून किंवा त्याचे मॅनुप्लेट (Manipulate) करून संगणक प्रणालीवर नियंत्रण मिळवणे किंवा वैयक्तिक आणि आर्थिक माहिती चोरली जाणे. हे वापरकर्त्यांना सुरक्षेच्या चुका करण्यासाठी किंवा सेन्सीटिव्ह इन्फॉरमेशन (sensitive information)देण्यास फसविण्यासाठी मानसिक हाताळणीचा वापर करते.

1.5 टाइप्स ओएफ मालवेअर्स आंड इम्पॅक्ट ओन सिक्युरिटी आंड प्रिव्हेंशन (Types of Malwares and their impact on security and prevention): - व्हायरस(Virus), वर्म्स (Worms), ट्रोजन हॉर्स (Trojan horse), स्पायवेअर (Spyware), अडवेअर (Adware), रॅनसम वेअर (Ransom ware), लॉजिक बॉम्ब्स (Logic Bombs), रूटकिट्स (Rootkits), बॅकडर्स (Backdoors), की -लॉगर्स(Key-loggers)

1.5.1 व्हायरस(Virus), वर्म्स (Worms)

संगणकात, आपल्याला दोन प्रकारचे मॅलीशीअस घटक सापडतील जे आपल्या संगणकाच्या डेटासह छेडछाड करू शकतात, व्यत्यय आणू शकतात, नुकसान करतात किंवा संगणक प्रणालींमध्ये अनधिकृत प्रवेश मिळवू शकतात.

हे दोन घटक वर्म्स(worms) आणि व्हायरस(virus) म्हणून ओळखले जातात. हे घटक आपल्या संगणकास लक्षणीय नुकसान करू शकतात.

व्हायरस (virus)काय आहेत?

व्हायरस(virus) हा एक मॅलीशीअस एक्झिक्युटेबल(executable) कोड आहे जो दुसऱ्या एक्झिक्युटेबल फाइलशी संलग्न(attach) आहे जो निरुपद्रवी (harmless)असू शकतो किंवा डेटा सुधारित करू शकतो किंवा हटवू शकतो. जेव्हा संगणक प्रोग्राम व्हायरससह संलग्न होतो तेव्हा संगणक प्रणालीमधून फाइल हटविण्यासारख्या काही क्रिया करतात. रिमोटद्वारे व्हायरस नियंत्रित केले जाऊ शकत नाही.

वर्म्स(worms) व्हायरससारखेच असतात परंतु त तो प्रोग्राम सुधारित करत नाही. संगणक प्रणाली कमी करण्यासाठी तो स्वत: च्या अधिकाधिक प्रतिकृती बनवतो. रिमोटद्वारे वर्म्स नियंत्रित केले जाऊ शकतात. वर्म्स चे मुख्य उद्दीष्ट म्हणजे सिस्टमची रिसोर्सेस (system resourses) वारपणे.

Table 1.1: Difference between Worms and Viruses

Basis of Comparison	वर्म्स(worms)	व्हायरस(virus)
Definition व्याख्या	वर्म्स मालवेयरचा(malware) एक प्रकार आहे जो स्वतःची प्रतिकृती बनवितो आणि नेटवर्कद्वारे वेगवेगळ्या संगणकांमध्ये पसरवू शकतो.	व्हायरस(virus) हा एक मॅलीशीअस एक्झिक्युटेबल कोड आहे जो दुसऱ्या एक्झिक्युटेबल(executable) फाइलशी संलग्न आहे जो निरुपद्रवी असू शकतो किंवा डेटा सुधारित करू शकतो किंवा हटवू शकतो.
Objective उद्दीष्ट	वर्म्सचे मुख्य उद्दीष्ट म्हणजे सिस्टमची रिसोर्सेस वापर करणे.हे मेमरी(memory) आणि बँडविड्थ (bandwidth) सारख्या सिस्टम रिसोर्सेसचा वापर करते आणि सिस्टमला इतक्या प्रमाणात वेग कमी करते की ते प्रतिसाद देणे थांबवते.	व्हायरसचे मुख्य उद्दीष्ट इन्फॉरमेशन(information) सुधारित करणे आहे
Host होस्ट	एका संगणकावरून दुसऱ्या संगणकावर प्रतिकृती तयार करण्यासाठी होस्टची आवश्यकता नाही.	एका संगणकावरून दुसऱ्या संगणकावर प्रतिकृती तयार करण्यासाठी होस्टची आवश्यकता असते.
Harmful हानिकारक	तुलनेत हे कमी हानिकारक आहे	हे अधिक हानिकारक आहे.
Detection and Protection शोध आणि संरक्षण	अँटीव्हायरस(antivirus) आणि फायरवॉलद्वारे (firewall) वर्म्स शोधले आणि काढले जाऊ शकतात.	अँटीव्हायरस(antivirus) सॉफ्टवेअरचा वापर व्हायरसपासून संरक्षणासाठी केला जातो.
Controlled by कंट्रोल बाय	रिमोटद्वारे वर्म्स नियंत्रित केले जाऊ शकतात.	रिमोटद्वारे व्हायरस नियंत्रित केले जाऊ शकत नाही.
Execution अंमलबजावणी.	सिस्टममधील कमकुवतपणाद्वारे वर्म्स अंमलात आणले जातात.	एक्झिक्युटेबल फायलींद्वारे (executable file) व्हायरस कार्यान्वित केले जातात.
Comes from कम्स फ्रॉम	वर्म्स(worms) सामान्यत: डाउनलोड केलेल्या फायलींमधून किंवा नेटवर्क कनेक्शनद्वारे येतात.	व्हायरस सामान्यत: शेअरर्ड(shared) किंवा डाउनलोड केलेल्या फायलींमधून येतात.
Symptoms लक्षणे	1. संगणकाच्या कार्यप्रदर्शनात अडथळा आणणे आणि ते हळू करणे. 2. प्रोग्राम्सचे आपोआप उघडणे आणि चालवणे. 3. तुमच्या माहितीशिवाय ईमेल्स पाठवणे.	1.पॉप-अप(pop-up) विंडोज मॅलीशीअस वेबसाइटशी लिंक साधतात 2. संगणकाच्या कार्यप्रदर्शनात अडथळा आणणे आणि ते हळू करणे 3. बूट(boot) केल्यानंतर, अननौन प्रोग्राम प्रारंभ करणे.
Examples उदाहरणे	वर्म्सच्या उदाहरणांमध्ये मॉरिस वर्म्स, स्टॉर्म वर्म्स (Morris worm , storm worm)इत्यादींचा समावेश आहे.	व्हायरसच्या उदाहरणांमध्ये क्रीपर , ब्लास्टर, स्लॅमर इ. (Creeper, Blaster, Slammer) समाविष्ट आहे.

Interface **इंटरफेस**	प्रतिकृती तयार करण्यासाठी मानवी कृतीची आवश्यकता नाही ..	प्रतिकृती तयार करण्यासाठी मानवी कृतीची आवश्यकता आहे
Speed **वेग**	त्याची पसरण्याची गती वेगवान आहे.	वर्म्सच्या तुलनेत त्याची पसरण्याची गती कमी होते

1.5.2 ट्रोजन हॉर्स (Trojan horse)

ट्रोजन हॉर्स, किंवा सोप्या शब्दात ट्रोजन, हा एक प्रकारचा मॅलवेयर आहे जो स्वतःला कायदेशीर सॉफ्टवेअर म्हणून लपवतो ज्याद्वारे तो संगणक प्रणालीवर प्रवेश मिळवतो. एकदा स्थापित झाल्यावर, ट्रोजन विविध दुष्ट ऍक्टिव्हिटीचे परीक्षण करू शकतात, जसे की संवेदनशील डेटा चोरून नेणे, वापरकर्ता क्रियाकलापाचे निरीक्षण करणे, आणि सायबर क्रिमिनल्ससाठी अनधिकृत रिमोट प्रवेश प्रदान करणे. इतर मॅलवेयर प्रकारांप्रमाणे, जसे की संगणक विषाणू(virus) किंवा वर्म्स(worms) , ट्रोजन स्वतःची पुनरावृत्ती करत नाहीत. त्याऐवजी, ते वितरणासाठी सामाजिक अभियांत्रिकी तंत्र आणि वापरकर्ता संवादावर अवलंबून असतात. उदाहरणार्थ, ते सामान्यतः निरापद(harmless) असलेल्या ईमेल अटॅचमेंट्समध्ये लपलेले असू शकतात किंवा बनावट सॉफ्टवेअर अपडेट्समध्ये एम्बेडेड(embedd) असू शकतात.

ट्रोजन हॉर्सचा इतिहास

ट्रोजन हॉर्स संकल्पना प्राचीन ग्रीक पुराणकथांमध्ये आहे, जिथे ग्रीक सैनिक एका लाकडी अश्वात लपले होते जेणेकरून ते ट्रॉय (troy)शहरात प्रवेश करू शकतील आणि ते जिंकू शकतील. सायबर सुरक्षा संदर्भात, ट्रोजन 1980 च्या दशकाच्या उत्तरार्धात पीसी-राईट(PC Write) ट्रोजनसह प्रथम समोर आले. हे मॅलवेयर, जे एक कायदेशीर प्रोग्राम म्हणून लपले होते, संक्रमित संगणकांवरील फाइल्स डिलीट करत होते.

ट्रोजन हॉर्स कसे कार्य करतात

एखाद्या व्यक्तीच्या संगणक प्रणालीमध्ये प्रवेश मिळविण्यासाठी ट्रोजन्स स्वत: ला वैध अनुप्रयोग किंवा फायली म्हणून स्वतःला दर्शवतात. एकदा स्थापित झाल्यानंतर, ते विविध प्रकारचे नुकसान करु शकतात, जसे की सेन्सीटिव्ह इन्फॉरमेशन चोरणे, सिस्टमच्या कार्यक्षमतेत व्यत्यय आणणे किंवा सायबर गुन्हेगारांद्वारे रिमोट कंट्रोलला परवानगी देणे. टारगेट प्रणालीच्या आत, ट्रोजन्स सामान्यत: त्यांच्या मॅलीशीअस ऍक्टईव्हिटी करताना दृश्यापासून लपून राहतात. ते कदाचित अनधिकृत प्रवेशासाठी बॅकडोअर(backdoor) तयार करू शकतात; अँटीव्हायरस सॉफ्टवेअरद्वारे (antivirus software)शोध टाळण्यासाठी किंवा शंका न वाढवता एक्सफिल्ट्रेट(exfiltrate) डेटा टाळण्यासाठी सुरक्षा सेटिंग्ज सुधारित करा. परिणामी, संभाव्य धोके ओळखण्यात आणि त्यांच्याविरूद्ध मजबूत सायबर सुरक्षा उपायांची अंमलबजावणी करण्यात व्यक्ती आणि संस्थांनी जागरुक राहिले पाहिजे.

ट्रोजन हॉर्स कसा ओळखावा

ट्रोजन हॉर्स शोधणे आव्हानात्मक असू शकते, कारण ते बहुतेकदा कायदेशीर सॉफ्टवेअर म्हणून स्वत:ला लपवतात. तथापि, काही चिन्हे आपल्या संगणकावर ट्रोजन हॉर्स दर्शवू शकतात. जागरूकता आणि या चेतावणीच्या चिन्हांची जाणीव ठेवून महत्त्वपूर्ण नुकसान होण्यापूर्वी आपण कारवाई करू शकतो.

- **अनपेक्षित सिस्टम वर्तन(unexpected system behaviour):** जर आपला संगणक अनियमितपणे वागू लागला असेल किंवा वारंवार क्रॅशचा(crash) अनुभव घेत असेल तर ते ट्रोजन संसर्ग दर्शवू शकेल.
- **हळू कामगिरी(slow performance**): सिस्टमच्या कामगिरीमध्ये अचानक घट झाल्याने मालवेयर सेवन करणाऱ्या रिसोर्सेस(resourses) च्या उपस्थितीचे संकेत मिळू शकतात.
- **नवीन फायली किंवा प्रोग्राम(new files and programs)** : ट्रोजन हॉर्सच्या (trojen horse) स्थापनेमुळे वापरकर्त्याच्या कृतीशिवाय आपल्या संगणकावर अपरिचित फायली किंवा प्रोग्राम दिसू शकतात.
- **संशयास्पद ईमेल आणि संलग्नक(suspicious emails and attachments)**: अज्ञात प्रेषक किंवा अनपेक्षित संलग्नकांकडून ईमेल उघडताना सावधगिरी बाळगा, या मॅलीशीअस संलग्नकांमध्ये आपल्या सिस्टममध्ये घुसखोरी करण्यासाठी प्रोग्राम केलेला मॅलीशीअस कोड असू शकतो.

- **सुरक्षा सेटिंग्जमध्ये अचानक बदलः(abrupt changes in security setting)** ट्रोजन्स फायरवॉल (trojen firewall)आणि अँटीव्हायरस(antivirus) सॉफ्टवेअर सारख्या सुरक्षा वैशिष्ट्ये अक्षम करण्याचा प्रयत्न करू शकतात. जर तुम्हाला असे बदल दिसले जे तुम्ही अधिकृत केले नाहीत, तर संभाव्य धोके(threats) तपासण्यासाठी आणखी चौकशी (investigate) करा.

ट्रोजन हॉर्स कसा काढायचा

आपल्या सिस्टममधून ट्रोजन हॉर्स काढून टाकण्यासाठी सर्वोत्तम पद्धती आणि योग्य साधनांचे संयोजन आवश्यक आहे. हा धोका दूर करण्यासाठी खालील स्टेप्स वापरा:

- **आपले अँटीव्हायरस सॉफ्टवेअर अपडेट् करा**: आपल्याकडे अँटीव्हायरस सॉफ्टवेअरची नवीनतम आवृत्ती असल्याचे सुनिश्चित करा, कारण त्यात नवीन धोके शोधण्यासाठी आणि काढण्यासाठी अद्ययावत व्याख्या आहेत.
- **इंटरनेटवरून डिस्कनेक्ट करा:** पुढील नुकसान किंवा डेटा चोरी रोखण्यासाठी, मालवेयर(malware) काढताना आपले डिव्हाइस नेटवर्कमधून डिसकनेक्ट करा.
- **सेफ मोडमध्ये सुरक्षितपणे बूट करा:** सेफ मोडमध्ये(safe mode) रीस्टार्ट(restart) केल्याने आपल्याला मॅलीशीअस प्रक्रियेत हस्तक्षेप न करता आवश्यक प्रोग्राम चालविण्याची परवानगी मिळते. विंडोज सिस्टमसाठी स्टार्टअप दरम्यान एफ 8 (F8)दाबा किंवा मॅक ओस डिव्हाइसवर (macOS devices) रीस्टार्ट दरम्यान शिफ्ट होल्ड करा.
- **टेम्पररी(Temporary) फायली काढा:** तात्पुरती फायली साफ केल्याने व्हायरस स्कॅनिंगला(virus scanning) गती मिळू शकते आणि संभाव्यत: काही मालवेयर घटक काढून टाकू शकतात. विंडोजवर डिस्क क्लीनअप(disk cleanup) वापरा किंवा मॅक ओस (macOS)वरील "रिक्त कचरा(empty trash)" वैशिष्ट्य फाइंड आऊट करा .
- **अँटीव्हायरस(Antivirus) स्कॅन(scan) करा**: एक विश्वासार्ह अँटीव्हायरस सॉफ्टवेअरचा वापर करून एक संपूर्ण सिस्टम स्कॅन आपल्या डिव्हाइसवर उपस्थित असलेल्या कोणत्याही ट्रोजन ओळखण्यात आणि त्यांना क्वारंटाइन (quarantine) करण्यात मदत करेल.

1.5.3 स्पायवेअर(spyware)

स्पायवेअर हा मालवेयरचा एक प्रकार आहे जो वापरकर्त्याच्या परवानगीशिवाय संगणकावरून वैयक्तिक इन्फॉरमेशन चोरतो. याचा उपयोग वापरकर्त्याच्या ऍक्टिव्हिटीचे परीक्षण करण्यासाठी, त्यांची क्रेडेन्शियल्स(credentials) चोरण्यासाठी आणि तृतीय पक्षाला (third party)इन्फॉरमेशन पाठविण्यासाठी वापरली जाऊ शकते.

स्पायवेअर वापरकर्त्यावर कसा परिणाम करू शकतो

1. आयडेंटिटी थेफ्ट (Identity theft): स्पायवेअर संकेतशब्द, बँक खात्याचे तपशील आणि इतर वैयक्तिक इन्फॉरमेशन चोरू शकते ज्याचा उपयोग ओळख चोरी करण्यासाठी केला जाऊ शकतो .
2. आर्थिक नुकसान: स्पायवेअरचा वापर फसव्या व्यवहार किंवा रिक्त बँक खाती करण्यासाठी केला जाऊ शकतो
3. स्लो सिस्टम कार्यक्षमता: स्पायवेअर संगणक धीमा(slow) करू शकतो, त्यास क्रॅश होऊ शकतो .
4. ब्राउझरचे इश्यूज (Browser issues**)**: स्पायवेअर ब्राउझरला नको असलेल्या (unwanted)साइटवर पुनर्निर्देशित करू शकते, मुख्यपृष्ठ (homepage)बदलू शकते किंवा वेब पेजेस अपलोड करणे कठीण करू शकते .
5. पॉप-अप जाहिराती(Pop-up ads**)**: स्पायवेअर पॉप-अप जाहिराती किंवा त्रुटी संदेश पाठवू शकते .
6. नेटवर्क समस्या: स्पायवेअर डिव्हाइसच्या फायरवॉल सेटिंग्ज सुधारित करू शकते, ज्यामुळे इतर मालवेयर सिस्टमला संक्रमित करणे सुलभ होते.

- **स्पायवेअरपासून स्वत: चे संरक्षण कसे करावे**

1. अँटीव्हायरस आणि अँटीमलवेअर सॉफ्टवेअर(antivirus and antimalware software) वापरा.
2. प्रोग्राम डाउनलोड करणे आणि ईमेल अट्चमेंट्स (email attachments) उघडणे टाळा.
3. कुकीजला(cookies) संमती देण्याबद्दल सावधगिरी बाळगा.
4. अँटी-ट्रॅकिंग ब्राउझर एक्सटेंशन (anti-tracking browser extension) वापरा.

- **स्पायवेअर कसे काढायचे**
  1. इंटरनेटवरून(internet) डिस्कनेक्ट (disconnect)करा.
  2. डिव्हाइसची प्रोग्राम्स सूची तपासा आणि कोणतेही अनवॉन्टेड(unwanted) सॉफ्टवेअर काढा.
  3. अँटीव्हायरस सॉफ्टवेअरने (antivirus software) स्कॅन करा.
  4. अँटीस्पायवेअर टूलसह स्कॅन करा.

1.5.4 ॲडवेअर(Adware)

ॲडवेअर हा मालवेयरचा एक प्रकार आहे जो वापरकर्त्याच्या डिव्हाइसवर अनवॉन्टेड जाहिराती प्रदर्शित करतो. हे ॲडवेअरच्या विकासासाठी कमाई करण्यासाठी डिझाइन केलेले आहे.

ॲडवेअर (Adware)कसे कार्य करते

- ॲडवेअर बऱ्याचदा विनामूल्य सॉफ्टवेअर किंवा ॲप्ससह एकत्रित केले जाते.
- यूझर वापरकर्त्याच्या ऑपरेटिंग सिस्टम(operating system) किंवा सॉफ्टवेअरमधील असुरक्षिततेद्वारे ॲडवेअर
- देखील स्थापित केले जाऊ शकते.
- ॲडवेअर पॉप-अप(pop-ups), ब्राउझर टॅब(browser tabs) किंवा नवीन ब्राउझर विंडोमध्ये जाहिराती प्रदर्शित करू शकते.
- ॲडवेअर वेब पृष्ठांमध्ये जाहिराती देखील इंजेक्ट(inject) करू शकते.
- ॲडवेअर वापरकर्त्याच्या ब्राउझिंगच्या सवयींचे परीक्षण करू शकते आणि वैयक्तिकृत जाहिरातींसह त्यांना टारगेट करू शकते.
- ॲडवेअर वापरकर्त्याची वैयक्तिक इन्फॉरमेशन संकलित करू शकते आणि ती तृतीय-पक्षाच्या(third party) जाहिरात नेटवर्कवर विकू शकते.

साइन ऑफ ॲडवेअर (Signs of adware)

- अनपेक्षित ठिकाणी जाहिराती दिसू लागतात.
- आपल्या परवानगीशिवाय आपल्या मुख्यपृष्ठामध्ये (homepage)बदल.
- वेब पृष्ठे योग्यप्रकारे प्रदर्शित होत नाहीत.
- वेबसाइट लिंक अनपेक्षित साइटवर पुनर्निर्देशित करीत आहेत.
- ब्राउझर स्लो होणे.
- आपल्या ब्राउझरमध्ये नवीन टूलबार(toolbar), विस्तार किंवा प्लगइन(plugin) दिसतात

ॲडवेअरपासून संरक्षण कसे करावे

- आपल्या वेब ब्राउझरमध्ये ॲडवेअर ब्लॉकर(adware blocker) स्थापित करा
- एंडपॉईंट(endpoint) सुरक्षा समाधान स्थापित करा

1.5.5 रॅन्समवेअर (Ransomware)

रॅन्समवेअर हे एक मालवेयर आहे जे वापरकर्त्यास किंवा त्यांच्या संगणकावरील फायलींमध्ये प्रवेश नाकारण्यासाठी डिझाइन केलेले आहे. या फायली एन्क्रिप्शन(encryption) करून आणि डिक्रिप्शनकी साठी(Decryption key) खंडणी देण्याची मागणी करून, सायबर हल्लेखोर संस्था अशा स्थितीत ठेवतात जिथे खंडणी देणे हा त्यांच्या फायलींमध्ये पुन्हा प्रवेश करण्याचा सर्वात सोपा आणि स्वस्त मार्ग आहे. काही प्रकारांनी अतिरिक्त कार्यक्षमता जोडली आहे-जसे की डेटा चोरीमुळे खंडणी देण्यास खंडणीच्या पीडितांना(victim) भाग पाडू शकतात.

1.5.6 लॉजिक बॉम्ब(Logic bomb)

लॉजिक बॉम्ब हा एक प्रकारचा सायबर-अटॅक आहे जो संगणक प्रणाली किंवा प्रोग्राममध्ये गुप्तपणे मॅलीशीअस कोड घालतो. जेव्हा विशिष्ट अटी पूर्ण केल्या जातात तेव्हा कोड ट्रिगर होतो, ज्यामुळे विध्वंसक कृती कार्यान्वित होते.

लॉजिक बॉम्ब कसे रोखता येईल

- अँटीव्हायरस सॉफ्टवेअर वापरा आणि ते अपडेट ठेवा.
- कॉम्प्रेस केलेल्या फायली आणि उपनिर्देशिकांसह नियमितपणे फायली स्कॅन करा.
- वापरकर्त्यांना सुरक्षा वैशिष्ट्ये सक्रिय करणे आवश्यक आहे.
- वेबसाइट सुरक्षा तपासणी करा.
- अज्ञात पाठवणाऱ्यांकडून(unknown sender) ईमेल अटॅचमेंट डाउनलोड करणे टाळा.
- ऑपरेटिंग सिस्टम आणि ॲप्लिकेशन अपडेटेड(updated) ठेवा.
- सेफ्टी पॉलिसी (safety policy)आणि सर्वोत्तम पद्धतींवर वापरकर्त्यांना प्रशिक्षण द्या.

1.5.7 रुटकिट(Rootkit)

रुटकिट हा एक प्रकारचा मालवेयर आहे जो सायबर गुन्हेगारांना शोधल्याशिवाय संगणकात प्रवेश करण्यास अनुमती देतो. रूटकिट्स चोरीसाठी डिझाइन केलेले आहेत आणि बऱ्याच काळासाठी लपून राहू शकतात. ते पाळत ठेवणे, डेटा चोरी आणि इतर मॅलीशीअस ॲक्टिव्हिटीसाठी वापरले जाऊ शकतात.

रूटकिट्स कसे कार्य करतात?

- संगणकावर रूटकिट्स स्थापित केले जातात आणि हल्लेखोरांना मूळ-स्तरीय प्रवेश प्रदान करतात.
- रूटकिट हे ओळख टाळण्यासाठी डिझाइन केलेले असतात आणि ऑपरेटिंग सिस्टम प्रमाणेच बूट होऊ शकतात.
- रूटकिट्समध्ये बॉट्स (bots), कीस्ट्रोक लॉगर(keystroke loggers) आणि सॉफ्टवेअरमध्ये मॅलीशीअस साधने असू शकतात जे सुरक्षा सॉफ्टवेअर अक्षम करतात.
- रूटकिट्सचा वापर पासवर्ड्स, क्रेडिट कार्ड इन्फॉरमेशन(credit card information) आणि इतर सेन्सीटिव्ह डेटा चोरण्यासाठी केला जाऊ शकतो.

रूटकिट्स कसे शोधायचे आणि कसे प्रतिबंधित करावे?

- आपल्या अँटीव्हायरस सॉफ्टवेअरसह रूटकिट स्कॅन करा.
- आपल्या संगणकास खाली आणा आणि स्वच्छ प्रणालीमधून स्कॅन करा.
- रुटकिट सारख्या वर्तन शोधण्यासाठी वर्तनात्मक विश्लेषण वापरा.
- ज्ञात असुरक्षिततेविरूद्ध आपली सिस्टम पॅच (system patch)करा.
- अज्ञात स्त्रोतांकडून फायली स्वीकारू नका किंवा ईमेल संलग्नक उघडू नका.
- सॉफ्टवेअर स्थापित करताना सावधगिरी बाळगा आणि अंतिम-वापरकर्ता परवाना करार वाचा.

1.5.8 की-लॉगर(keylogger)

इन्फॉरमेशन सुरक्षेतील एक "कीलॉगर" हा एक प्रकारचा सॉफ्टवेअर किंवा हार्डवेअर आहे. जो वापरकर्त्याने त्यांच्या कीबोर्डवर बनवलेल्या प्रत्येक कीस्ट्रोकची(keystroke) गुप्तपणे रेकॉर्ड करतो. ज्यामुळे हल्लेखोरांना पासवर्ड, क्रेडिट कार्ड नंबर आणि इतर गोपनीय डेटा सारख्या सेन्सीटिव्ह इन्फॉरमेशन कॅप्चर करण्याची परवानगी दिली जाते . वापरकर्ता त्यांच्या संगणकावर काय टाइप करतो याचे निरीक्षण करून; मूलतः लॉगिन क्रेडेन्शियल्स आणि वैयक्तिक माहिती चोरण्यासाठी गुप्त पाळत ठेवण्याचे साधन म्हणून काम करतो .याचे निरीक्षण करून; मूलतः लॉगिन क्रेडेन्शियल्स आणि वैयक्तिक माहिती चोरण्यासाठी गुप्त पाळत ठेवण्याचे साधन म्हणून काम करतो.हे कीबोर्डवर टाइप केलेले सर्व कीस्ट्रोक रेकॉर्ड करते, हल्लेखोरांद्वारे नियंत्रित असलेल्या दूरस्थ सर्व्हरला डेटा पाठवितो जेथे लॉगिन तपशील सारख्या मौल्यवान इन्फॉरमेशन काढण्यासाठी त्याचे विश्लेषण केले जाऊ शकते.

1.6 थ्रेट आंड रिस्क ॲनालिसिस (Threat and Risk Analysis): इंट्रोडक्शन टू असेट्स(Introduction to assets), व्हल्नरेबिलिटी(vulnerability), थ्रेट्स(threats), रिस्क्स(risks), रिलेशन बिटवीन: थ्रेट, व्हल्नरेबिलिटी, रिस्क्स(relation between: threat, vulnerability, risks)

1.6.1 असेट्सची (assets)ओळख: इन्फॉरमेशनच्या सुरक्षेमध्ये मालमत्ता म्हणजे कोणताही डेटा(data), डिव्हाइस(device) किंवा इतर घटक आहेत जे इन्फॉरमेशनशी संबंधित ऍक्टिव्हिटीना समर्थन देतात. या मालमत्ता भौतिक किंवा डिजिटल(digital) असू शकतात आणि त्यात हार्डवेअर(hardware), सॉफ्टवेअर(software) आणि गोपनीय इन्फॉरमेशन समाविष्ट असू शकते.

मालमत्तेची उदाहरणे

- हार्डवेअर (Hardware): सर्व्हर(Servers), स्विच (switches), लॅपटॉप(laptops), डेस्कटॉप(desktops), मोबाइल डिव्हाइस(mobile devices) आणि क्लाऊड सर्व्हर(cloud servers).
- सॉफ्टवेअर: मिशन गंभीर अनुप्रयोग(Mission critical applications), समर्थन प्रणाली(support systems), परवाने (licenses)आणि ऑपरेटिंग सिस्टम(operating system).
- डिजिटल इन्फॉरमेशन (digital information): डेटाबेस(database), वेबसाइट्स(websites), प्रतिमा, व्हिडिओ, ऑडिओ फायली(audio) आणि करार.
- बौद्धिक मालमत्ता: ब्रँड(brand), निष्ठा आणि इतर मालकी इन्फॉरमेशन.

असेट्स सुरक्षा

- असेट्स सुरक्षा ही मालमत्ता अनधिकृत प्रवेश, वापर, प्रकटीकरण किंवा विनाशापासून वाचविण्याची प्रक्रिया आहे.
- असेट्स सुरक्षा ही संस्थेच्या सुरक्षा धोरणाचा एक महत्त्वाचा भाग आहे.
- असेट्स सुरक्षेमध्ये फायरवॉल(firewall), प्रमाणीकरण आणि एन्क्रिप्शन(encryption) यासारख्या सुरक्षा नियंत्रणे वापरणे समाविष्ट आहे.
- असेट्स सुरक्षेमध्ये मालमत्ता व्यवस्थापनासाठी धोरणे आणि कार्यपद्धती विकसित करणे देखील समाविष्ट आहे.

1.6.2 व्हल्नरेबिलिटीज(Vulnerabilities) ही अशा प्रणालीतील कमकुवतपणा आहे जी धमक्यांना मालमत्तेत तडजोड करण्याची संधी देतात . सर्व सिस्टममध्ये व्हल्नरेबिलिटीज असतात. जरी तंत्रज्ञान सुधारत आहे परंतु व्हल्नरेबिलिटीजची संख्या वाढत आहे जसे की कोट्यवधी कोड , अनेक डेव्हलपर,, मानवी कमकुवतपणा इत्यादी हार्डवेअर, सॉफ्टवेअर, नेटवर्क आणि प्रक्रियात्मक असुरक्षिततेमुळे व्हल्नरेबिलिटीज होतात

1. हार्डवेअर(Hardware) असुरक्षा: हार्डवेअर असुरक्षा हा एक कमकुवतपणा आहे जी शारीरिक किंवा दूरस्थपणे सिस्टम हार्डवेअरवर अटॅक करण्यासाठी वापरली जाऊ शकते.

उदाहरणांसाठी:

1. सिस्टम किंवा डिव्हाइसची जुनी आवृत्ती
2. असुरक्षित स्टोरेज(storage)
3. विना -एनक्रिप्टेड डिव्हाइस इ.

2. सॉफ्टवेअर(software) असुरक्षा: सॉफ्टवेअर त्रुटी विकासात किंवा कॉन्फिगरेशनमध्ये(conFigureuration) घडते जसे की त्याची अंमलबजावणी सुरक्षा धोरणाचे उल्लंघन करू शकते. उदाहरणांसाठी:

1. इनपुट(input) प्रमाणीकरणाचा अभाव
2. पडताळणी न केलेले अपलोड(Unverified uploads)
3. क्रॉस-साइट स्क्रिप्टिंग(Cross-site scripting)
4. एन्क्रिप्ट न केलेला डेटा(Unencrypted data)

3. नेटवर्क असुरक्षितता: नेटवर्कमध्ये एक कमकुवतपणा येतो जो हार्डवेअर किंवा सॉफ्टवेअर असू शकतो.

उदाहरणांसाठी:

1. असुरक्षित संप्रेषण
2. मालवेयर(malware) किंवा मॅलीशीअस सॉफ्टवेअर (उदा. व्हायरस(virus), कीलॉगर्स(keylogger), वर्म्स(worms) इ.)
3. सामाजिक अभियांत्रिकी हल्ले
4. चुकीची कॉन्फिगर(conFigureure) केलेली फायरवॉल(firewall)

4. प्रक्रियात्मक असुरक्षा: संस्थेच्या कार्यप्रणालीमध्ये कमकुवतपणा होतो.

उदाहरणांसाठी:

1. पासवर्ड प्रक्रिया (Password procedure)- पासवर्डने पासवर्ड पॉलिसीच्या धोरणाचे पालन केले पाहिजे.
2. प्रशिक्षण प्रक्रिया - कर्मचाऱ्यांना हे माहित असणे आवश्यक आहे की सुरक्षितता हाताळण्यासाठी कोणत्या कृती केल्या पाहिजेत आणि काय करावे. कर्मचाऱ्यांना ऑनलाइन वापरकर्त्याची क्रेडेन्शियल्स(credentials) कधीही विचारू नये. कर्मचाऱ्यांना सोशल इंजिनिअरिंग आणि फिशिंगच्या धोक्यांबद्दल माहिती द्या.

1.6.3 सायबर थ्रेट (cyber threat)

थ्रेट ही अशी कोणतीही गोष्ट आहे जी एखाद्या असुरक्षिततेचा गैरफायदा घेऊ शकते आणि कॉन्फिडेन्शिअलीटी (confidentiality), अखंडता आणि मौल्यवान कोणत्याही गोष्टीची उपलब्धता अडथळा आणू शकते. धमक्या एकतर नैसर्गिक किंवा मानवी-निर्मित आणि अपघाती किंवा मुद्दाम असू शकतात. आमच्या कारच्या उदाहरणात, कारच्या मालकाने त्यांचा दरवाजा लॉक केला नाही, म्हणून एक कारजॅकर संधीचे शोषण करू शकेल. याचा अर्थ असा आहे की धोका मानवी निर्मित आणि मुद्दाम आहे.

सायबर धोका हा सायबर-धोक्यांमुळे मालमत्तेचे किंवा डेटाचे नुकसान होण्याचा संभाव्य परिणाम आहे. रिस्क(risk) कधीही पूर्णपणे काढला जाऊ शकत नाही, परंतु ती संस्थेच्या जोखीम सहनशीलतेला पूर्ण करणाऱ्या पातळीपर्यंत व्यवस्थापित केली जाऊ शकते. म्हणून, आमचे लक्ष्य रिस्क-मुक्त प्रणाली असणे नाही, तर रिस्क शक्य तितकी कमी ठेवणे आहे.

सायबर थ्रेट या सोप्या फॉर्मुल्यानें परिभाषित करता येतात.

फॉर्मुला(formula): रिस्क(Risk) = थ्रेट(Threat) + व्हल्नरेबिलिटी(Vulnerability). सायबर थ्रेट सामान्यत: थ्रेटअभिनेता आणि सिस्टमच्या असुरक्षिततेचे परीक्षण करून निर्धारित केले जातात.

रिस्क प्रकार

दोन प्रकारचे सायबर रिस्क आहेत, जे खालीलप्रमाणे आहेत:

1. एक्सटरनल (external)- एक्सटरनल सायबर रिस्क असे असतात जे एखाद्या संस्थेच्या बाहेरून येतात, जसे की सायबर-हल्ले, फिशिंग(phishing), **रॅनसम** वेअर (ransom ware), डीडीओएस हल्ले इ.

2. इंटरनल (Internal)- इंटरनल सायबर रिस्क आतील लोकांकडून येतात. या आतील व्यक्तींचा मॅलीशीअस हेतू असू शकतो किंवा योग्यरित्या प्रशिक्षण दिलेले नसते.

1.6.4 धमकी, असुरक्षा आणि रिस्क यांच्यातील संबंध:

Vulnerability x Threat = Risk

व्हल्नरेबिलिटी x **थ्रेट** = **रिस्क**

सायबर थ्रेट या सोप्या सूत्राने परिभाषित करता येतात

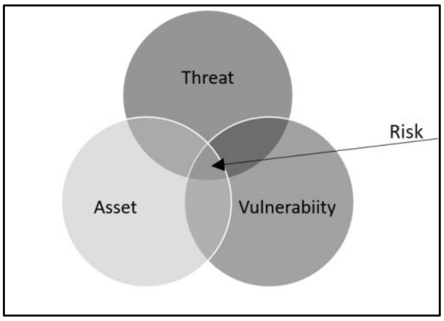


Figure. 1.13 Relationship between threat, vulnerabilities and risk (Courtesey: https://www.dionach.co)

एखादी एकच कमजोरी आणि संभाव्य धमक्यांची संख्या एकत्र केल्याने संबंधित धोका अंदाज लावला जातो. हे सूत्र जोखीमांचे(risk) योग्य मूल्यांकन आणि कमी करण्यासाठी ,असुरक्षा आणि धमक्या ओळखणे आणि नियंत्रित करणे या दोहोंचे महत्त्व अधोरेखित करते.

References:

1. Information Systems Security Second Edition By Nina Godbole (John Wiley Isbn-13: 978-8126564057)
2. Cryptography and Information Security By V.K.Pachghare – Prentice Hall India
3. Cryptography and Network security Third Edition By Atul Kahate- McGraw-Hill; Fourth edition ISBN-13: 978-9353163303
4. Computer Security Principles and Practice, Third Edition BY William Stallings, Lawrie Brown Pearson. ISBN-13: 978-0-13-377392-7

युनिट - 2
युजर ऑथेंटीकेशन अँड ॲक्सेस कंट्रोल
(User authentication and Access Control)

विषय निष्पत्ती : Course Outcome (CO):

CO2 - फाइल, फोल्डर, डिव्हाइस आणि ॲप्लिकेशनवर (File, folder, device and application) मल्टी-फॅक्टर युजर ऑथेंटिकेशन आणि ॲक्सेस कंट्रोल सिस्टीम (Multi-factor authentication and access control system) लागू करा.

घटक निष्पत्ती: (Theory Learning Outcomes)

1. वेगवेगळ्या प्रकारच्या ऑथेंटिकेशन (authentication) पद्धती वापरा.
2. विविध प्रकारच्या पासवर्ड ॲटॅक्सचे (password attacks) प्रकार ओळखा.
3. दिलेले बायोमेट्रिक पॅटर्न (biometric patterns) स्पष्ट करा.
4. ऑथोरायझेशनची (authorisation) उद्दिष्टे समजावून सांगा.
5. दिलेल्या मापदंडांच्या (parameters) आधारे डीएसी (DAC), मॅक (MAC), आरबीएसी(RBAC) आणि एबीएसीची (ABAC) तुलना करा.

2.1 आयडेंटिफिकेशन आणि ऑथेंटिकेशन (Identification and Authentication) पद्धती:

आयडेंटिफिकेशन (Identification) ही युजरला (user) ओळखण्याची प्रक्रिया आहे. हा मूलतः ओळखीचा दावा (claim of identity) आहे, म्हणजेच एक युजर (user) सांगतो "ही माझी ओळख आहे".

ऑथेंटिकेशन (authentication) म्हणजे युजरची (user) दावा (claim) केलेली ओळख पडताळण्याची प्रोसेस. ऑथेंटिकेशन (authentication) म्हणजे सिस्टिम (system) किंवा रिसोर्सेसला (resources) प्रवेश देण्यापूर्वी युजर किंवा डिव्हाइसची (user or device) पडताळणी करण्याची प्रक्रिया.

आयडेंटिफिकेशन आणि ऑथेंटिकेशन (Identification and authentication) हे डिजिटल रिसोर्सेसमध्ये (digital resources) प्रवेश मिळवण्यासाठी तीन टप्प्यांच्या प्रक्रियेचा भाग आहेत.:

1. आयडेंटिटी (Identity)-तुम्ही कोण आहात?
2. ऑथेंटिकेशन (Authentication) - तुम्ही कोण आहात आणि ते सिद्ध (prove) करा.
3. ऑथोरायझेशन (Authorisation) - तुमच्याकडे परवानगी आहे का?

1. आयडेंटिटी(Identity): " तुम्ही कोण आहात "

आयडेंटिफिकेशन (Identification) हा तो टप्पा आहे जिथे युजर (user) नाव, ईमेल ॲड्रेस (email address), फोन नंबर (phone number) किंवा युजरनेम (username) देऊन आपली ओळख (identity) सिद्ध करतात. आयडेंटिफिकेशन (Identification) हा व्यक्तीची ओळख पुष्टी (identity confirm) करण्याचा पहिला टप्पा आहे आणि ऑथेंटिकेशन आणि ऑथोरायझेशन (Authentication and Authorisation) होण्यापूर्वी ते झाले पाहिजे. हा त्या व्यक्तीने तीच व्यक्ती आहे असे सांगण्याची प्रोसेस (process) आहे.

2. ऑथेंटिकेशन(Authentication):"तुम्ही कोण आहात आणि ते सिद्ध करा"

ऑथेंटिकेशन (Authentication) ही एक प्रोसेस (process)आहे ज्याद्वारे आपण तपासू शकता की एखादी व्यक्ती तीच व्यक्ती आहे जे ती सांगते. यामध्ये सामान्यतः युजरनेम आणि पासवर्ड (username and password) असतो, परंतु ओळख सिद्ध करण्याच्या काही इतर पद्धती असू शकतात, ज्यात स्मार्ट कार्ड, रेटिना स्कॅन, व्हॉईस रेकग्निशन, किंवा फिंगरप्रिंट्स (smart card, retina scan, voice recognition or finger prints) यांचा समावेश होऊ शकतो. आयडेंटिफिकेशनसाठी (Identification) युजर आयडी (User Id) लागतो, जसे की युजरनेम (Username). परंतु ओळख प्रमाणित केल्याशिवाय, हे कसे समजून येईल की ते युजरनेम (Username) खरोखर त्यांच्याशी संबंधित आहे? तिथे ऑथेंटिकेशन (Authentication) कामात येते—युजरनेमला (Username) पासवर्ड (password) किंवा इतर प्रमाणित क्रेडेन्शियल्ससह (credentials) जोडणे. उदाहरणार्थ, ऑथेंटिकेशन (Authentication) हे विमानतळावर तिकीट काउंटरवर (counter) ड्रायव्हरचा लाइसन्स (driver license) दाखवण्यासारखे आहे.

3. ऑथोरायझेशन(Autherization): "तुमच्याकडे परवानगी आहे का?"

ऑथोरायझेशन (Authorization) ही एखाद्याला काहीतरी करण्याची परवानगी देण्याची प्रक्रिया आहे. ऑथोरायझेशन (Authorization)ही एक प्रोसेस (Process)आहे जिथे युजरला (User) ठिकाण किंवा माहिती-आधारित संसाधन (उदाहरणार्थ, एक डॉक्युमेन्ट (document), डेटाबेस (database), ॲप्लिकेशन (application), किंवा वेबसाइट(website)) प्रवेश करण्याची परवानगी दिली जाते. हे दर्शवू शकते की एक युजर (User) कोणता डेटा (data) आणि माहिती ॲक्सेस (access) करू शकतो. ऑथोरायझेशन (Authorization) सामान्यतः ऑथेंटिकेशनसोबत (Authentication) काम करते, जेणेकरून सिस्टिम (system)समजू शकेल की कोण माहिती घेत आहे.

2.1.1 आयडेंटिफिकेशन आणि ऑथेंटिकेशन पद्धती (Identification and Authentication Methods) :

आयडेंटिफिकेशन आणि ऑथेंटिकेशनच्या (Identification and Authentication) विविध पद्धती आहेत जसे की:

1. इलेक्ट्रॉनिक युजर ऑथेंटिकेशन (Electronic user authentication),
2. युजरनेम आणि पासवर्ड (Username and password),
3. मल्टी-फॅक्टर ऑथेंटिकेशन (Multi-factor authentication),
4. टोकन-बेस्ड ऑथेंटिकेशन (Token Based authentication),
5. बायोमेट्रिक्स (biometrics)

1. इलेक्ट्रॉनिक युजर ऑथेंटिकेशन (Electronic user authentication),:

माहिती प्रणालीला (information system)इलेक्ट्रॉनिक (electronic) पद्धतीने युजरच्या (User) ओळखींवर विश्वास प्रस्थापित करण्याच्या प्रक्रियेला इलेक्ट्रॉनिक ऑथेंटिकेशन (Electronic authentication) म्हणतात. इलेक्ट्रॉनिक युजर ऑथेंटिकेशन (Electronic user authentication) (ई-ऑथेंटिकेशन) ((E-authentication) ही एक प्रोसेस (process)आहे जी युजरची आयडेंटिटी (User Identity)तपासते, जेणेकरून त्यांना सिस्टिममध्ये (System) प्रवेश करण्याची परवानगी आहे की नाही हे सुनिश्चित करता येईल. हे पासवर्ड्स, बायोमेट्रिक्स, आणि मल्टी-फॅक्टर ऑथेंटिकेशन (Passwords, Biometrics and Multi-factor authentication) (एमएफए) (MFA) यांसारख्या विविध पद्धती वापरून केले जाऊ शकते.

2. युजरनेम आणि पासवर्ड (Username and password):

युजरनेम आणि पासवर्ड ऑथेंटिकेशन (Username and password authentication) ही डिजिटल सिस्टीममध्ये (digital system) ऍक्सेस (Access) करणाऱ्या युजरची (User) आयडेंटिटी (Identity)पडताळण्याची पद्धत आहे. युजर (User) एक अद्वितीय(Unique) ओळख, ज्याला युजरनेम (Username) म्हटले जाते, आणि एक गुप्त(Secrete) शब्द, ज्याला पासवर्ड (Password) म्हटले जाते. युजरनेम आणि पासवर्ड दिल्यानंतर त्याला ऍक्सेस (Access) मिळू शकेल. त्यानंतर सिस्टिम (System) युजरची (User) आयडेंटिटी (Identity)पडताळण्यासाठी या माहितीची त्याच्या संग्रहित डेटाबेसशी (Database) तुलना करते. युजरनेम आणि पासवर्ड ऑथेंटिकेशन (Username and password authentication) ही एक मूलभूत आणि व्यापकपणे वापरली जाणारी पद्धत आहे जी युजरची (User) आयडेंटिटी (Identity)प्रमाणित करण्यासाठी वापरली जाते, विशेषतः ऑनलाइन सिस्टिम, वेबसाइट्स, आणि ॲप्लिकेशन्समध्ये (Online systems, websites and applications) ऍक्सेस (Access) करताना लॉगिन क्रेडेन्शियल्स (Login credentials) हे अद्वितीय आयडेंटिटी (Identity)करणारे सेट (sets) असतात – जसे की युजरनेम आणि पासवर्ड (Username and password) – जे युजरला (User) आयडेंटिटी (Identity)प्रमाणित करण्याची आणि ऑनलाइन अकाऊंटमध्ये (Online account) लॉग इन (Login) करण्याची परवानगी देतात.

- **युजरनेम (Username):** युजरनेम(Username) हे युजर आयडेंटिटी (Identity)(User Id) आहे जे एखादी व्यक्ती त्यांच्या अद्वितीय आयडी (Unique Id) म्हणून संगणक, नेटवर्क (network), किंवा सेवेमध्ये(Service) वापरते. बहुतेक वेबसाइट्स आणि ऑनलाइन सेवा (Websites and online services), जसे की फेसबुक आणि ट्विटर (Facebook and twiter), वापरकर्त्यांना त्यांच्या युजरनेमची (Username) निवड करण्याची परवानगी देतात, जी सहसा ईमेल ऍड्रेससोबत (Email Address) किंवा फोन नंबरसह (Phone Number) जोडलेली असते. युजरनेम्स (Usernames) नेहमीच गोपनीय नसतात, म्हणून त्यांचा वापर एक व्यक्ती ओळखण्यासाठी हे एकच वापरू नये. म्हणूनच विश्वासार्ह सेवा(Service) या

युजरनेम्सला (Usernames) पासवर्डसोबत (Password) जोडतात ज्यामुळे लॉगिन क्रेडेन्शियल्स (Login credentials) तयार होतात.

- **पासवर्ड (Password):** पासवर्ड (Password) अक्षरांचा एक क्रम (अक्षरे, अंक, विशेष चिन्हे) आहे जो युजरची (User) आयडेंटिटी (Identity)प्रमाणित करण्यासाठी आणि सिस्टिम, ॲप्लिकेशन, किंवा डिव्हाइसला (System, application or device) ऍक्सेस (Access) देण्यासाठी वापरला जातो. ते सहसा युजरद्वारे (User) तयार केले जातात आणि गोपनीय ठेवले जातात. पासवर्ड (Password) हा एक नॉलेज फॅक्टर (Knowledge factor) आहे म्हणजेच असे काहीतरी जे फक्त युजरलाच (User) माहित आहे.

पासवर्ड (Password) निवडीचे निकष / स्ट्रॉंग पासवर्ड (Strong Password) कसा तयार करावा:

- त्यामध्ये कमीत कमी 8 अक्षरे असावीत
- पासवर्डमध्ये (Password) अप्पर आणि लोअरकेस (Uppercase and lowercase alphabets) अक्षरे (उदा. ए-झेड, ए-झेड Ex. A-Z, a-z) असावीत.
- पासवर्डमध्ये (Password) किमान एक संख्यात्मक अक्षर (उदा. 0-9) असावे.
- पासवर्डमध्ये (Password) कमीत कमी एक चिन्ह असावे (उदा. ~!@#$%^&*()_-+=).
- अनुक्रमिक संख्या किंवा अक्षरे वापरू नका: 1234, क्वर्टी (qwerty), जेकेएलएम (JKLM), 6789 इ. काही पहिले पासवर्ड (Password) आहेत जे हॅकर्स (hackers) तपासू शकतात. याचप्रमाणे, ब्रूट फोर्स सॉफ्टवेअर (Brute force software) सामान्यतः अनुक्रमिक अंक आणि अक्षरे तपासते कारण ती इतकी सामान्यपणे वापरली जातात.
- पासवर्डमध्ये (Password) तुमचे जन्मवर्ष किंवा जन्म महिना/दिवसचा समावेश करू नका : सायबर क्रिमिनल्स (cyber criminals) सहजपणे ही माहिती सोशल मीडिया (social media) खात्यांमध्ये(account) शोधून काढू शकतात. त्याचप्रमाणे, सहजपणे सापडणारी वैयक्तिक माहिती जसे की पाळीव प्राण्यांची नावे, पत्ते(addresses), आणि नियोक्ता(Empolyer) नावे यासाठी देखील तेच लागू आहे.
- आपल्या पासवर्डमध्ये (Password) वेगवेगळे असंबंधित शब्द एकत्र करा: या सरावामुळे सायबर (cyber) गुन्हेगारांना आपल्या पासवर्डचा (Password) अंदाज लावणे कठीण होते. लोकप्रिय गाणी, चित्रपट किंवा दूरचित्रवाणी कार्यक्रमांमधील वाक्ये वापरू नका. आपले पासफ्रेज(Pass Phrase) तयार करण्यासाठी तीन किंवा चार दीर्घ शब्द वापरा. उदाहरणार्थ, 9Sp!dErscalKetobogGaN.
- डिक्शनरीमध्ये (Dictonary) सापडलेली नावे किंवा शब्द वापरू नका: पासवर्डचा अंदाज (Password) लावणे अवघड होण्यासाठी संख्या किंवा चिन्हे असलेली अक्षरे बदलावीत. किंवा पासवर्ड किंवा पासफ्रेजमध्ये (Password or Passphrase) उद्देशपूर्ण अशुद्ध लेखनाचा वापर करा. उदाहरणार्थ, P8tty0G#5dn म्हणजे "patio garden."
- आपले पासवर्ड स्टोअर (Password store) करण्यासाठी पासवर्ड मॅनेजर (Password manager) वापरा: आपले पासवर्ड (Password) लिहू नका किंवा आपल्या संगणकावरील डॉक्युमेंटमध्ये (document) ठेवू नका. खात्री करा की आपण IT/सपोर्ट टीमने (IT support team) प्रदान केलेले पासवर्ड मॅनेजर टूल (Password manager tool) वापरत आहात ज्यामध्ये सर्व व्यावसायिक आणि वैयक्तिक पासवर्ड्स (Professional and Personal Password) साठवले जाऊ शकतात. बहुतेक पासवर्ड मॅनेजर्समध्ये (Password managers) एक उपयुक्त पासवर्ड जनरेटर (Password generator) देखील असतो, त्यामुळे तुम्हाला प्रत्येक वेळी नवीन पासवर्ड (Password) तयार करण्याची आवश्यकता नाही.
- वेगवेगळ्या डिव्हाइस (device) किंवा वेगवेगळ्या ॲप्लिकेशन्ससाठी (applcation) आपले पासवर्ड (Password) पुन्हा वापरू नका: प्रत्येक डिव्हाइस, ॲप्लिकेशन, वेबसाइट आणि सॉफ्टवेअरला (device, application, website and software) एक अद्वितीय(unique) आणि स्ट्रॉंग पासवर्ड किंवा पिन (strong password or PIN) आवश्यक आहे. फक्त एकाच पासवर्डचा (Password) पुनर्वापर सर्व खात्यांना (all accounts) धोका निर्माण करू शकतो.

पासवर्ड बेस्ड ऑथेंटिकेशन (Password based authentication) असलेली उदाहरणे:

ईमेल लॉगिन (Email Login): ईमेल खात्यांमध्ये ऍक्सेस (Access) करण्यासाठी पासवर्ड (Password)-बेस्ड (Based) ऑथेंटिकेशन (Authentication) पद्धत आवश्यक आहे.

लॉगिन तपशील (login details) प्रविष्ट करणे हे कर्मचाऱ्यांसाठी आवश्यक आहे जेणेकरून ते स्वतःला प्रमाणित करू शकतात आणि संस्थेच्या ईमेल्स किंवा सॉफ्टवेअरमध्ये (emails and software) ऍक्सेस (Access) करू शकतात. संगणक लॉगिन (login): संगणकावरील ऑपरेटिंग सिस्टिमला सामान्यत: युजर इंटरफेस आणि वैयक्तिक फायलींमध्ये ऍक्सेस (Access) करण्यासाठी पासवर्डची आवश्यकता असते. नेटवर्क ॲक्सेस (network access): कंपनी नेटवर्क किंवा वाय-फाय हॉटस्पॉटमध्ये (company network or WiFi hotspot) ऍक्सेस (Access) मिळविण्यासाठी अनेकदा पासवर्ड ऑथेंटिकेशन आवश्यक असते.

पासवर्ड बेस्ड ऑथेंटिकेशनचे (Password based authentication) फायदे :

1. ओळख(Familiarity): पासवर्ड् (Password) ही सर्वात व्यापकपणे स्वीकारलेली ऑथेंटिकेशन (Authentication) पद्धत आहे, ज्यामुळे सामान्य युजरला (user) आयडेंटिटी (identity)देतो, ज्यामुळे युजर अनुभव (user experience) अधिक सुलभ होतो आणि सपोर्ट रिक्वेस्ट्स (support requests) कमी होतात.

2. परवडणारी क्षमता(Afforadability) : काही इतर ऑथेंटिकेशन (Authentication) पद्धतींशी तुलना केली असता, ज्यांना अधिक प्रगत तंत्रज्ञान किंवा अतिरिक्त हार्डवेअर आणि सॉफ्टवेअरची (hardware and software) आवश्यकता असते, पासवर्ड बेस्ड ऑथेंटिकेशन (Password based authentication) तुलनेने साधे आणि परवडणारे आहे, तरीही मूलभूत सुरक्षा स्तर राखून ठेवते. हे छोट्या व्यवसायांमध्ये लोकप्रिय आहे ज्यांच्याकडे मर्यादित संसाधने (Resources) आहेत (जरी हा ट्रेंड (trend) बदलत आहे).

3. युजर नियंत्रण (User control): पासवर्ड (Password) बेस्ड (Based) ऑथेंटिकेशन (Authentication) युजर्सना (users) त्यांच्या पासवर्ड्सवर (Password) नियंत्रण देते, जेणेकरून ते ते कधीही बदलू किंवा रीसेट (reset) करू शकतात. हे युजर्सना (Users) त्यांचे पासवर्ड्स (Passwords) त्यांच्या योग्य वाटेल तसे व्यवस्थापित करण्याची लवचिकता देते.

पासवर्ड बेस्ड ऑथेंटिकेशनचे (Password based authentication) तोटे:

1. असुरक्षितता: पासवर्ड बेस्ड ऑथेंटिकेशनशी (Password Based Authentication) संबंधित एक प्रमुख धोका म्हणजे पासवर्ड्स (Passwords) सहजपणे चोरले जाऊ शकतात किंवा अंदाज लावला जाऊ शकतो, विशेषतः जर ते स्ट्रॉंग नसतील किंवा अनेक सिस्टम्सवर (Systems) पुनर्वापर केले जात असतील.

2. चुकता येण्याची शक्यता (फॉलबिलिटी) (Fallability) : लोक पासवर्ड्स (Passwords) विसरतात. संग्रहित क्रेडेन्शियल्स (credentials) असलेले संगणक क्रॅश (crash) होतात. इन्फॉर्मेशनच्या (Information) प्रत्यक्ष प्रती देखील हरवू किंवा चोरी होऊ शकतात.

2.1.2 मल्टी-फॅक्टर ऑथेंटिकेशन (Multi-factor Authentication):

मल्टी-फॅक्टर ऑथेंटिकेशन (Multi-factor Authentication) (एमएफए) (MFA) ही एक ऑथेंटिकेशन (Authentication) पद्धत आहे ज्यामध्ये एखाद्या व्यक्तीला सेवा किंवा नेटवर्कमध्ये (service or network) ऍक्सेस (Access) मिळविण्यासाठी अनेक घटकांमध्ये (Factors) पास होणे आवश्यक असते. हे स्टँडर्ड पासवर्ड-बेस्ड (Based) लॉगिनच्या (Standard password Based login) वर एक अतिरिक्त सुरक्षा स्तर आहे. एक सामान्य MFA घटक(fators) जो युजर्सच्या (Users) संपर्कात येतो तो म्हणजे वन-टाईम पासवर्ड्स (One Time Password) (ओटीपी) (OTP). ओटीपी हे ४-८ अंकी कोड्स असतात जे आपल्याला बर्याचदा ईमेल (Email), एसएमएस (SMS) किंवा कोणत्याही प्रकारच्या मोबाइल ॲपद्वारे (Mobile App) प्राप्त होतात. ओटीपी (OTP) मध्ये एक नवीन कोड कालांतराने किंवा प्रत्येक वेळी ऑथेंटिकेशन विनंती (Authentication request) सबमिट (submit) केल्यावर जनरेट (generate) केला जातो.

एसएमएसद्वारे ओटीपी (OTP) / टीओटीपी (TOTP), ईमेलवर (Email) ओटीपी / टीओटीपी (OTP / TOTP), पुश नोटिफिकेशन (Push Notification), हार्डवेअर टोकन (Hardware Token) आणि मोबाइल ऑथेंटिकेटर (Mobile autheticator) ही सर्व एमएफए (MFA) पद्धतींची उदाहरणे आहेत. एमएफए चे (MFA)घटक असू शकतात:

- आपण काहीतरी आहात (इनहेरेन्स) (Inherence) - जसे की फिंगरप्रिंट किंवा व्हॉइस रिकग्निशन (Fingerprint or voice recognition) सारखे बायोमेट्रिक (Biometric).
- आपल्याला माहित असलेली एखादी गोष्ट (ज्ञान) (नोलेज) (Knowledge) - जसे की पासवर्ड किंवा पिन (Password or PIN).
- आपल्या मालकीची एखादी गोष्ट (पझेशन) (Possession) - जसे की स्मार्टफोनसारखे (Smartphone) डिव्हाइस (Device).

एमएफएची (MFA) उदाहरणे :

मल्टी-फॅक्टर ऑथेंटिकेशनचे (Multi-factor Authentication) उदाहरण म्हणजे खालील घटकांचा (factors) एकत्र करून ऑथेंटिकेशन (Authentication) करणे.

ज्ञान/माहिती (नोलेज) (Knowledge):

- वैयक्तिक सुरक्षेच्या प्रश्नांची उत्तरे
- पासवर्ड (Password)
- ओटीपी (OTP)(ज्ञान/माहिती आणि ताबा दोन्ही असू शकतात - आपल्याला ओटीपी (OTP) माहित आहे आणि तो मिळविण्यासाठी आपल्या ताब्यात फोनसारखे काहीतरी असणे आवश्यक आहे)

ताबा (पझेशन)(Possession) :

- स्मार्टफोन ॲप्सद्वारे (Smartphone Apps) तयार होणारे ओटीपी (OTP)
- एसएमएसद्वारे (SMS) किंवा ईमेलद्वारे (Email) पाठविलेले ओटीपी (OTP)
- बॅज, यूएसबी डिव्हाइस, स्मार्ट कार्ड किंवा फोब्स (Badge , USB, smart card or forbes) किंवा सुरक्षा कीज(Security Keys) ॲक्सेस (access) करा
- सॉफ्टवेअर टोकन (Software Token) आणि प्रमाणपत्रे

इनहेरेंस (Inherence):

- बोटांचे ठसे, चेहऱ्याची ओळख, आवाज, रेटिना किंवा आयरिस स्कॅनिंग (Retina or IRIS scanning) किंवा इतर बायोमेट्रिक्स (Biometrics)
- वर्तणुकीचे विश्लेषण (Behaviourial Analysis)

जागा(Location) :

- लोकेशन फॅक्टर ऑथेंटिकेशन (Location factor authentication) युजरच्या (User) भौगोलिक स्थानाचा विचार करतात.
- लॉगिन (Login) चा अटेम्प्ट(attempt) युजरच्या (User) विशिष्ट किंवा अपेक्षित स्थानांशी जुळत आहे की नाही याची पडताळणी करण्यासाठी ही पद्धत युजरचा आयपी ॲड्रेस (User’s IP address) किंवा इतर भौगोलिक लोकेशन डेटा (Location data) वापरू शकते.

एमएफएची (MFA) उदाहरणे:

1.बँक खात्यात लॉगिन करणे: बँक खात्यात लॉगिन करताना, MFA वापरले जाऊ शकते जेणेकरून खाते मालकच (Account Owner) खाते ॲक्सेस (access) करू शकतो. उदाहरणार्थ, युजरला पासवर्ड प्रविष्ट(enter) करण्याची आवश्यकता असू शकते आणि दुसऱ्या प्रकारची ऑथेंटिकेशन (Authentication), जसे की त्यांच्या फोनवर पाठवलेला वन-टाईम कोड (OTP) किंवा बायोमेट्रिक स्कॅन (biometric scan), प्रदान करण्याची आवश्यकता असू शकते, जेणेकरून ते त्यांच्या बँक खात्यात लॉगिन (login) करू शकतात. हे संवेदनशील आर्थिक माहितीचा अनधिकृत ॲक्सेस (access) रोखण्यास मदत करते आणि फसवणुकीपासून संरक्षण करण्यास मदत करते.

2. कंपनी रिसोर्सेस (Company resources) साठी रिमोट ऍक्सेस (Remote Access): एमएफए (MFA) (दूरस्थ) रिमोट युजरना (Remote user) ऑथेन्टिकेट (Authenticate) करण्यासाठी वापरले जाऊ शकते जे ऑफिसच्या बाहेरून कंपनीच्या नेटवर्क किंवा सिस्टम्समध्ये (Network or systems) ऍक्सेस (access) करत आहेत. उदाहरणार्थ, जे कर्मचारी घरून काम करतात किंवा ऑन द वे (on the way) आहेत, त्यांना कंपनीचे रिसोर्सेस (company resources), जसे की ईमेल इनबॉक्स (email inbox) किंवा अंतर्गत डेटाबेस (database), ऍक्सेस (access) करण्याची आवश्यकता असू शकते. या रिसोर्सेसचे (resources) संरक्षण करण्यासाठी, कंपनी एमएफए (company MFA) लागू करू शकते, उदाहरणार्थ, कर्मचाऱ्याला पासवर्ड आणि त्यांच्या मोबाइल फोनवर पाठवलेला एक वन-टाईम कोड (OTP) प्रदान(Enter) करणे आवश्यक आहे.

एमएफएचे (MFA) फायदे :

1. मजबूत सुरक्षा(Stronger Security): एमएफए (MFA) पासवर्डच्या (password) पलीकडे जाऊन अधिक सुरक्षा स्तर प्रदान करते, ज्यामुळे हॅकर्ससाठी (hackers) युजरचे क्रेडेन्शियल्स (user credentials) मिळविल्यानंतरही ऍक्सेस (access) मिळवणे अत्यंत कठीण होते.

2. फसवणुकीची क्रिया कमी करणे : अनेक पडताळणी पद्धती वापरून , एमएफए आयडेंटिटी (identity)चोरी आणि अनधिकृत खाते प्रवेशाचा धोका लक्षणीयरीत्या कमी करते.

3. सुधारित युजर विश्वास: युजर्सना (users) त्यांचे खाते एमएफएद्वारे (MFA) संरक्षित आहे हे जाणून अधिक सुरक्षित वाटते, ज्यामुळे ऑनलाइन सेवांवरील (online services) विश्वास वाढतो.

एमएफएचे (MFA) तोटे:

1.वेळखाऊ: एक तोटा म्हणजे मल्टी-फॅक्टर ऑथेंटिकेशनला (Multi-Factor Authentication) जास्त वेळ लागतो.

2.मल्टी-फॅक्टर ऑथेंटिकेशन (Multi-Factor Authentication) कंपनी स्वत:हून सेटअप (setup) करू शकत नाही. हे थर्ड पार्टीला (third party) करावं लागतं.

3.युजर त्रुटी: पडताळणी कोड्स (Authentication Codes)किंवा एमएफए सेटिंग्ज (MFA settings) व्यवस्थापित करताना चुकांमुळे तात्पुरत्या ऍक्सेस (access) समस्या उद्भवू शकतात.

4.कमी तंत्रज्ञानासमज (टेक-सॅव्ही) (Tech-savy) असलेल्या युजर्ससाठी जटिलता (Complexity**) :** मर्यादित तांत्रिक ज्ञान असलेल्या व्यक्तींना एमएफए प्रभावीपणे सेट अप (setup) आणि वापरणे कठीण होऊ शकते.

2.1.3 टोकन-बेस्ड ऑथेंटिकेशन (Token-based authentication): टोकन (Token) म्हणजे काय?

ॲक्सेस टोकन (Access Token) हे सुरक्षा क्रेडेन्शियल (security credential) आहे जे ऑथेंटिकेशन (authentication) प्रक्रियेस सक्षम करते. ही एक टेम्पररी-की (temporary-key) आहे जी आयडेंटिटी (identity)पडताळणी करते आणि रिसोर्सेस ऍक्सेस (access) अधिकृत करते. टोकन (Token) संगणक-निर्मित किंवा हार्डवेअर बेस्ड (hardware based) असू शकते. टोकनचे (Token) दोन प्रकारांमध्ये वर्गीकरण केले जाते: फिजिकल टोकन (Physical token) आणि वेब टोकन (Web token).

1. फिजिकल टोकन (Physical token): फिजिकल टोकन (Physical token) एक फिजिकल डिव्हाइस (Physical device) वापरते जे युजरची (user) माहिती साठवते. येथे, सीक्रेट-की (secret-key) एक फिजिकल डिव्हाइस (Physical device) आहे ज्याचा वापर युजरची (user) आयडेंटिटी (identity)सिद्ध करण्यासाठी केला जाऊ शकतो. फिजिकल टोकनचे (Physical token) दोन घटक म्हणजे हार्ड टोकन (hard token) आणि सॉफ्ट टोकन (soft token). हार्ड टोकन (hard token) स्मार्ट कार्ड (smart card) आणि यूएसबीचा (USB) वापर कर्मचाऱ्यांपर्यंत पोहोचण्यासाठी कॉर्पोरेट (corporate) कार्यालयांमध्ये वापरल्या जाणार्या प्रतिबंधित नेटवर्कमध्ये (network) ऍक्सेस (access) देण्यासाठी करतात. सॉफ्ट टोकन (soft token) अधिकृत ॲप (App)किंवा एसएमएसद्वारे (SMS) एन्क्रिप्टेड कोड (encrypted code) (जसे की ओटीपी) (OTP) पाठविण्यासाठी मोबाइल (mobile) किंवा संगणकाचा वापर करतात.

2. वेब टोकन (Web token): वेब टोकनद्वारे (Web token) ऑथेंटिकेशन (authentication) ही पूर्णपणे डिजिटल (digital) प्रोसेस (process)आहे. इथे, सर्व्हर आणि क्लायंट इंटरफेस (server and client interface) युजरच्या (user) विनंतीनुसार संवाद साधतात. क्लायंट युजरचे क्रेडेन्शियल्स सर्व्हरला पाठवतो आणि सर्व्हर त्यांची पडताळणी करतो, डिजिटल सिग्नेचर तयार

करतो आणि ते क्लायंटकडे (client) परत पाठवतो. वेब टोकन (Web token) JSON जेएसओएन वेब टोकन (जेडब्ल्यूटी JWT) म्हणून प्रसिद्ध आहेत, जे डिजिटल साईन केलेले टोकन तयार करण्यासाठी एक मानक आहे.
टोकन-बेस्ड (based) ऑथेंटिकेशन (Web token based authentication) हे युजरना (user) नेटवर्कमध्ये (network) ऍक्सेस (access) करण्यासाठी सुरक्षा यंत्रणा वाढविण्यासाठी दोन- स्टेप ऑथेंटिकेशन धोरण (authentication policy) आहे. युजर (user)एकदा त्यांचे क्रेडेन्शियल्स (credentials) नोंदणी केल्यानंतर, एक अद्वितीय एन्क्रिप्टेड टोकन (unique encrypted token) प्राप्त करतात जे विशिष्ट सत्र(Session) कालावधीसाठी वैध आहे. या सत्रादरम्यान(Session), युजर (user) लॉगिनशिवाय (login) थेट वेबसाइट किंवा ॲप्लिकेशनमध्ये (website or application) ऍक्सेस (access) करू शकतात. हे पासवर्ड सिस्टिममध्ये (password system) एक सुरक्षा स्तर जोडून वेळ आणि सुरक्षितता वाचवून युजरचा एक्सपीरियन्स (user experience) वाढवते. टोकन (token) स्टेटलेस (stateless) आहे कारण ते डेटाबेसमध्ये (database) युजरची (user) माहिती सेव्ह (save) करत नाही.
हे क्रिप्टोग्राफीवर (cryptography) आधारित आहे जिथे एकदा सत्र पूर्ण झाल्यावर टोकन (token) नष्ट होते. त्यामुळे, ते हॅकर्ससाठी (hackers) पासवर्ड (password) वापरून रिसोर्सेस ॲक्सेस (resources access) करण्याच्या विरोधात फायदेशीर आहे. टोकनचे (token) एक सर्वोत्तम उदाहरण म्हणजे ओटीपी (वन-टाइम पासवर्ड) (OTP), जे योग्य युजरची (user) आयडेंटिटी (identity)पडताळण्यासाठी नेटवर्क (एन्ट्री) (network entry) ऍक्सेस (access) मिळवण्यासाठी वापरले जाते आणि ते ३०-६० सेकंदांसाठी वैध असते. सत्र कालावधीत, टोकन (token) संस्थेच्या डेटाबेसमध्ये (database) साठवले जाते आणि सत्र संपल्यावर ते अदृश्य होते.

टोकन-आधारित ऑथेंटिकेशन (Token based authentication) कसे कार्य करते?

टोकन-आधारित ऑथेंटिकेशन (Token based authentication) या पाच-स्टेप प्रक्रियेद्वारे कार्य करते:

- **विनंती**: युजर (user) त्यांच्या लॉगिन क्रेडेन्शियल्स (login credentials) वापरुन एखाद्या सेवेत (service) लॉग-इन (login) करतो, जो सर्व्हर (server) किंवा संरक्षित रिसोर्सेसला (resources) ऍक्सेस विनंती (access request) पाठवतो.
- **पडताळणी**: युजरला ऍक्सेस (user access) आहे हे निर्धारित करण्यासाठी सर्व्हर (server) लॉगिन (login) माहितीची पडताळणी करतो. यात दिलेल्या युजरनेम आणि पासवर्डची (username and password) तपासणी केली जाते.
- **टोकन सबमिशन (Token submission)**: सर्व्हर विशिष्ट कालावधीसाठी युजरसाठी (user) सुरक्षित(secure), साईन (sign) स्वाक्षरी केलेले ऑथेंटिकेशन टोकन (authentication token) तयार करतो.
- **स्टोरेज (Storage)**: टोकन (token) युजरच्या (user) ब्राउझरवर (browser) परत पाठविले जाते, जे भविष्यातील वेबसाइट (website) भेटींमध्ये ऍक्सेस (access) करण्यासाठी संग्रहित करते. जेव्हा युजर (user) नवीन वेबसाइटवर (website) ऍक्सेस (access) करण्यासाठी पुढे जातो, तेव्हा ऑथेंटिकेशन टोकन डिकोड (authentication token decode) केले जाते आणि पडताळणी केली जाते. मॅच (match) असेल तर युजरला (user) पुढे जाण्याची परवानगी दिली जाईल.
- **एक्सपायरी (Expiry):** जोपर्यंत युजर लॉग आउट (user log out) करत नाही किंवा सर्व्हर (server) बंद करत नाही तोपर्यंत टोकन (token) सक्रिय रहाते.

टोकन-आधारित ऑथेंटिकेशनचे (Token based authentication) उदाहरण:

सुरक्षा टोकनचे (Token) उदाहरण म्हणजे वायरलेस की कार्ड्स (Wireless key-cards) जे लॉक (lock) केलेल्या दरवाजांना उघडण्यासाठी वापरले जातात. की कार्ड लॉक (key-card lock) म्हणजे की कार्ड (key-card), सपाट, आयताकृती प्लास्टिक कार्डद्वारे (plastic-card) चालविले जाणारे लॉक.
हे कार्ड (card) सामान्यत: , क्रेडिट कार्ड (credit card) स्वरूपासारखेच समान आकाराचे असते. हे कार्ड (card) एक भौतिक(physical) किंवा डिजिटल पॅटर्न (digital pattern) साठवते जे (लॉक डिसइंगेज (lock disengage) करण्यापूर्वी) कुलूप उघडण्यापूर्वी दरवाजा यंत्रणा(door mechanism) स्वीकारते.

ऑनलाइन बँकिंगमध्ये (online banking) साइन इन (sign-in) करण्यासाठी किंवा वायर ट्रान्सफर (wire transfer) सारख्या व्यवहारांवर साइन (sign) करण्यासाठी डिजिटल ऑथेंटिकेटर (digital authenticator) म्हणून वापरले जाणारे बँकिंग टोकन (banking token).

वायर ट्रान्सफर (wire transfer), बँक ट्रान्सफर (bank transfer) किंवा क्रेडिट ट्रान्सफर (credit transfer), एका व्यक्तीकडून किंवा संस्थेकडून दुसऱ्या व्यक्तीकडे इलेक्ट्रॉनिक फंड (electronic fund transfer) हस्तांतरित करण्याची एक पद्धत आहे. वायर ट्रान्सफर (wire transfer) एका बँक (bank) खात्यातून दुसऱ्या बँक (bank) खात्यात किंवा कॅश ऑफिसमध्ये (cash office) रोख रकमेच्या हस्तांतरणाद्वारे केले जाऊ शकते.

टोकन-आधारित ऑथेंटिकेशनचे (Token based authentication) फायदे:

1. सुधारीत रिसोर्सेस (resources) सुरक्षा (security)): टोकन्स (tokens) युजर ऑथेंटिकेशनसाठी (user authentication) एक अधिक सुरक्षित पद्धत प्रदान करतात कारण ते स्वयंपूर्ण असतात आणि टोकन (token) तयार करणारे सर्व्हरच (server) त्याची पडताळणी करू शकतात.

2. सूक्ष्म नियंत्रण(Granular Control): टोकन (token) प्राधिकरण लवचिक आणि समायोज्य(Flexible and Adjustable) दोन्ही आहे. टोकन (tokens) कालबाह्यता आणि इतर तपशीलांवर संपूर्ण नियंत्रण ठेवत प्रशासक (ऍडमिनिस्ट्रेटर) (administrator) त्यांना सर्व ॲप्लिकेशन्स, डेटाबेस, वेबसाइट्स आणि सर्व्हर्सवर (applications, database, websites and servers) त्वरीत लागू करू शकतात.

3. सुधारित ऑथेंटिकेशन अनुभव(Modified Authentication Experience): रिसोर्सेस (resources) पुरविताना आणि ऍक्सेस (access) करताना टोकन (token) युजर (user)आणि प्रशासकांना (ऍडमिनिस्ट्रेटरना) (administrator) चांगला अनुभव देतात.

टोकन-आधारित ऑथेंटिकेशनचे (Token based authentication) तोटे:

1. जोखीम (Risk): जर टोकन-आधारित ऑथेंटिकेशन (Token based authentication) योग्यरित्या व्यवस्थापित केले गेले नाही किंवा चुकीच्या प्रकारे कॉन्फिगर (configure) केले गेले, तर व्यापक डेटा आणि ॲप्लिकेशनचे (data and application) उल्लंघन होऊ शकते.

2. सतत पुनः ऑथेंटिकेशनची (authentication) आवश्यकता: दीर्घकालीन प्रवेशासाठी टोकन-आधारित ऑथेंटिकेशन (Token based authentication) आदर्श नाही. वापरलेला प्रोटोकॉल (protocol) किंवा प्रकार काहीही असो, सर्व टोकनची (token) समाप्ती तारीख असते. म्हणून, प्रशासकांनी टोकन (token) जीवनचक्र सतत व्यवस्थापित करणे आणि आवश्यकतेनुसार क्रेडेन्शियल्सचे (credentials) नूतनीकरण करणे आवश्यक आहे.

2.1.4 बायोमेट्रिक्स (Biometrics): बायोमेट्रिक (biometric) सुरक्षा उपाय हे नाविन्यपूर्ण तंत्रज्ञान आहे जे व्यक्तींच्या युनिक फिजिकल वैशिष्ट्यांचा वापर करून त्यांची आयडेंटिटी (identity)संरक्षित आणि प्रमाणित(secure and authenticate) करतात. हे उपाय विविध उद्योगांमध्ये आणि ॲप्लिकेशनमध्ये (application) सुरक्षा वाढवण्यासाठी आणि एक सलग युजरअनुभव(user experience) प्रदान करण्यासाठी वापरले जातात. बायोमेट्रिक (biometric) सुरक्षा ही एक आधुनिक आयडेंटिटी (identity)आणि ऑथेंटिकेशन (authentication) पद्धत आहे जी एखाद्या व्यक्तीची आयडेंटिटी (identity)पडताळण्यासाठी बोटांचे ठसे, चेहऱ्याची ओळख, डोळ्याचा आयरिस किंवा रेटिना स्कॅन (IRIS or retina scan) यासारख्या युनिक फिजिकल वैशिष्ट्यांचा वापर करते.

बायोमेट्रिक (biometric) सुरक्षा प्रणाली प्रभावी आहेत कारण ही अद्वितीय वैशिष्ट्ये तयार करणे किंवा प्रतिकृती बनविणे जवळपास अशक्य आहे, ज्यामुळे एखाद्या व्यक्तीची आयडेंटिटी (identity)स्थापित करण्यासाठी ते अत्यंत विश्वसनीय ठरतात.

बायोमेट्रिक्सचे (biometrics) ढोबळमानाने खालील वर्ग (श्रेणी)(categories) आहेत:

1. जैविक बायोमेट्रिक्स (biological biometrics)
2. मॉर्फोलॉजिकल बायोमेट्रिक्स (morphological biometrics)
3. वर्तनात्मक बायोमेट्रिक्स (behavioural biometrics)

1. जैविक बायोमेट्रिक्स: यामध्ये डीएनए (DNA) किंवा तुमच्या रक्तासारख्या वैशिष्ट्यांचा समावेश असू शकतो, ज्याचे मूल्यांकन तुमच्या शरीराच्या द्रवांचा सॅम्पल (sample) घेऊन केले जाऊ शकते.
2. मॉर्फोलॉजिकल बायोमेट्रिक्स (morphological biometrics): यामध्ये तुमच्या शरीराच्या संरचनेचा समावेश आहे. तुमच्या डोळ्याची रचना, बोटांचे ठसे किंवा तुमच्या चेहऱ्याचा आकार. यासारख्या अधिक शारीरिक वैशिष्ट्यांना सुरक्षा स्कॅनरसह वापरण्यासाठी मॅप केले जाऊ शकते.
3. वर्तनात्मक बायोमेट्रिक्स (behavioural biometrics): हे प्रत्येक व्यक्तीसाठी अद्वितीय(unique) असलेल्या पॅटर्नवर (patterns)आधारित आहेत. तुम्ही कसे चालता, बोलता किंवा कीबोर्डवर (key-board) टाइप कसे करता हे पॅटर्न ट्रॅक (pattern track) केल्यास हे तुमच्या ओळखीचे संकेत असू शकतात.

बायोमेट्रिक्सची (biometrics) उदाहरणे : वरील श्रेणींवर(categories)आधारित बायोमेट्रिक्सची काही उदाहरणे खालीलप्रमाणे आहेत :

1. डीएनए मॅचिंग (DNA matching): डीएनएमधील सेगमेंटचे विश्लेषण(DNA segment analysis) करून व्यक्ती ओळखली जाऊ शकते.
2. फिंगरप्रिंट रिकग्निशन (Fingerprint recognition): फिंगरप्रिंट रिकग्निशन सिस्टिम (Fingerprint recognition system) एखाद्या व्यक्तीची आयडेंटिटी (Identity)पडताळण्यासाठी त्याच्या फिंगरप्रिंटमधील उंचवटे, दऱ्या आणि मिन्युटी याची अद्वितीय वैशिष्ट्ये पकडते आणि त्याचे विश्लेषण करते.
3. कान : कानाच्या आकाराचा वापर करून व्यक्तीची आयडेंटिटी (Identity)पटवली जाते.
4. डोळे-आयरिस (IRIS)ओळख: व्यक्तीच्या डोळ्याच्या बुभुळाच्या आसपास असलेले अद्वितीय(unique) पॅटर्न स्कॅन करून आयडेंटिटी (identity) पटविली जाते.
5. डोळे–रेटिना (Retina) ओळख: डोळ्यांच्या मागील भागातील नसांच्या पॅटर्नच्या मदतीने व्यक्तीची आयडेंटिटी (identity)पटविली जाते.
6. चेहरा ओळखणे: चेहऱ्याची आयडेंटिटी (identity)पटविणारी प्रणाली एखाद्या व्यक्तीची आयडेंटिटी (identity)पडताळण्यासाठी डोळ्यांमधील अंतर, नाकाचा आकार आणि जबडा यासारख्या चेहेऱ्याच्या वैशिष्ट्यांची नोंद घेते आणि विश्लेषण करते
7. हँड ज्योमेट्री रिकग्निशन (Hand geometry recognition): हे यूजर्सना त्यांच्या हातांच्या आकारावरून ओळखते. हँड ज्योमेट्री रीडर (Hand geometry reader) लांबी, रुंदी, डेव्हिएशन(deviation) आणि कोन यासह अनेक परिमाणांसह युजरचा तळहात आणि बोटांचे मोजमाप करतात आणि त्या मोजमापांची तुलना फाइलमध्ये साठवलेल्या मोजमापांशी करतात.
8. सिग्नेचर रिकग्निशन (signature recognition): सिग्नेचर रिकग्निशन हस्ताक्षर, गती, वेळेतील फरक आणि पेनला लागलेला दाब यांसारख्या घटकांचा वापर करून व्यक्तीची आयडेंटिटी (identity)ठरवते.
9. व्हॉइस रिकग्निशन (voice recognition) : व्यक्तीच्या आवाजाचा वापर करून बोलणाऱ्या व्यक्तीची आयडेंटिटी (identity)ठरवली जाते.

बायोमेट्रिक आधारित ऑथेंटिकेशनची (Biometric based authentication) उदाहरणे:

1. **फिंगरप्रिंट स्कॅनिंग (Fingerprint scanning):** आपल्या बोटांचे ठसे वापरून फोन अनलॉक करणे किंवा बँक खात्यात लॉग इन करणे याबद्दल आपण सर्व परिचित आहोत. भारतातील बायोमेट्रिकली व्हेरिफायबल आयडेंटिफिकेशन नंबर सिस्टीम, ज्याला आधार कार्ड म्हणून ओळखले जाते, हे बायोमेट्रिक्समध्ये केवळ लॉगिनच्या पुढे किती प्रभावी होऊ शकते याचे एक उदाहरण आहे. हि सिस्टिम - जी एखाद्या व्यक्तीचे बायोमेट्रिक्स त्यांच्या आधार नंबरशी जोडते.
2. **विमानतळावरील सुरक्षा :** विमानतळावरील सुरक्षा चेकपॉइंट्सवर (security checkpoints) प्रवाशांची तपासणी आणि क्लिअर करण्यासाठी बायोमेट्रिक्सचा वापर केला जातो. ही कॉन्टॅक्टलेस (contactless) पद्धत फास्ट ट्रॅक ट्रस्टेड-ट्रॅव्हलर लेनपासून (fast track trusted – traveller lane) बोर्डिंग पास म्हणून चेहऱ्याची आयडेंटिटी (Identity)वापरण्यापर्यंत सर्व गोष्टींसाठी आयडेंटिटी (identity)पडताळणी स्वयंचलित करू शकते.

बायोमेट्रिक आधारित ऑथेंटिकेशनचे (Biometric based authentication) फायदे :

1. **कमी प्रोसेसिंग वेळ:** बायोमेट्रिक्स प्रमाणित प्रणालींना सहसा वन-टू-वन प्रोसेस (Process)म्हणून संबोधले जाते आणि इतर आयडेंटिटी (Identity)प्रणालींच्या तुलनेत कमी प्रोसेसिंग वेळ लागतो.
2. **अचूकता :** बायोमेट्रिक प्रमाणित केलेल्या प्रणाली अधिक अचूक असतात कारण त्यांना फक्त व्यक्तीच्या डेटाची तुलना त्याच्या किंवा तिच्या संग्रहित डेटाशी करायची असते.
3. **वाढीव सुरक्षा:** पारंपारिक ऑथेंटिकेशन पद्धतींच्या तुलनेत बायोमेट्रिक तंत्रज्ञानाने प्रगत दर्जाची सुरक्षा प्रदान केली आहे.
4. **कामाची सुलभता :** आता तुम्हाला पुन्हा पुन्हा पासवर्ड टाईप करण्याची गरज नाही. किंवा हार्ड पासवर्ड लक्षात ठेवण्याची ही गरज नाही. फक्त एक फिंगरप्रिंट फोनसारखी आपली इलेक्ट्रॉनिक उपकरणे ओपन किंवा अपडेट करू शकतो.
5. **युनिक सुरक्षा वैशिष्ट्ये:** फिंगरप्रिंट किंवा रेटिनाचे वेगळेपण नॉन रेप्यूडिएशन(non repudiation) प्रदान करते. युजर असा दावा करू शकत नाही की त्यांनी एक्सेस केलेला डेटा त्यांच्याकडून हाताळला गेला नाही.

बायोमेट्रिक आधारित ऑथेंटिकेशनचे (Biometric based authentication) तोटे :

1. **क्रेडेन्शियल (Credential) चोरी:** युजरला केवळ बायोमेट्रिक डेटा वापरून फसवलेच जात नाही, तर त्याच बायोमेट्रिक डेटावर आधारित इतर खात्यांना धोका असतो. पासवर्ड हे साइट्ससाठी विशिष्ट असू शकतात आणि आवश्यकतेनुसार रीसेट केले जाऊ शकतात, परंतु बायोमेट्रिक्ससाठी हे पर्याय शक्य नाहीत. तसेच, आधुनिक ए.आय. अल्गोरिदमचा (AI algorithm) वापर फिंगरप्रिंट स्कॅनरची फसवणूक करण्याकरता बोटांचे ठसे तयार करण्यासाठी केला जाऊ शकतो.

2. **अपघात आणि वृद्धत्व:** शारीरिक जखम किंवा इजा झाल्यामुळे बायोमेट्रिक फीचर्स गमावले किंवा बदलले जाऊ शकतात. उदाहरणार्थ, गंभीर भाजल्यानंतर बोटाच्या ठशाच्या रेषांमध्ये बदल होऊ शकतो. तसेच, वय वाढल्यानंतर व्यक्तीचे शारीरिक गुणधर्म बदलतात, ज्यामुळे चुका होऊ शकतात.

3. **परिस्थितीजन्य घटक:** चेहऱ्याच्या ओळखीसाठी, प्रकाशातील बदलांमुळे ऑथेंटिकेशन अयशस्वी होऊ शकते. आयरिस स्कॅनिंग सुद्धा काम करत नाही जर युजरला लांब आयब्रोस, रंगीत कॉन्टॅक्ट लेन्सेस असतील किंवा त्याच्या डोळ्यांत रिफ्लेक्शन येईल. कोरडेपणा फिंगरप्रिंटवर परिणाम करू शकतो. आणि भावना बायोमेट्रिक वर्तनावर प्रभाव पाडू शकतात.

4. **अंमलबजावणी खर्च :** बायोमेट्रिक ऑथेंटिकेशनसाठी लागणारे हार्डवेअर आणि सॉफ्टवेअर महागात पडू शकते. त्यांची परिणामकारकता सुनिश्चित करण्यासाठी, या प्रणाली नियमितपणे अपडेट आणि मेंटेन करणे आवश्यक आहे.

5. **हार्डवेअर बिघडणे:** बायोमेट्रिक इंटरफेस कालांतराने खराब होऊ शकतात. शरीररचनेतील सूक्ष्म बदल आणि बिघडलेल्या हार्डवेअरमुळे चुका होऊ शकतात.

2.2 पासवर्डचा अंदाज लावणे आणि पासवर्ड अटॅक:

- **पासवर्डचा अंदाज लावणे :** जर पासवर्डची आवश्यकता असेल तर गुन्हेगार नेटवर्कमध्ये ऍक्सेस (access) करण्यापूर्वी पासवर्डचा अंदाज लावू शकतो किंवा वेगवेगळ्या पद्धतींनी तो शोधू शकतो. कमकुवत किंवा सहज अंदाज लावता येणारे पासवर्ड विशेषत: या प्रकारच्या हल्ल्यास (attack) असुरक्षित असतात.
- **पासवर्ड अटॅक:** पासवर्ड अटॅकच्या सर्वात सामान्य प्रकारांमध्ये ब्रुट फोर्स अटॅक (Brute-force attack) आणि डिक्शनरी अटॅक (Dictionary attack) चा समावेश आहे ज्यामध्ये हल्लेखोराकडून पासवर्डचा अंदाज लावला जातो.
- **डिक्शनरी अटॅक (Dictionary attack):** डिक्शनरी अटॅक एक प्रकारचा ब्रूट फोर्स अटॅक आहे, ज्यामध्ये हल्लेखोर(attacker) पासवर्ड-प्रोटेक्टेड सुरक्षा प्रणालीला(security system) "डिक्शनरी लिस्ट" (Dictionary list) च्या सहाय्याने क्रॅक करण्याचा प्रयत्न करतो. हल्लेखोर(attacker) सामान्य शब्द, फेमस पासवर्ड, तसेच डेटा लीक किंवा सोशल मीडिया पोस्टमधून मिळवलेले माहिती यांचा वापर करून यादी तयार करतात. या पद्धतीतून पासवर्ड शोधणे जास्त वेगवान होऊ शकते, कारण डिक्शनरीमध्ये सामान्यतः वापरण्यात येणारे शब्द असतात. शब्दकोशांच्या स्वरूपात ऑनलाइन बरेच सामान्यपणे आढळणारे पासवर्ड आहेत. या शब्दकोशात डेटा ब्रीच किंवा सामान्यपणे वापरल्या जाणार्या पासवर्डमध्ये लीक झालेल्या पासवर्डची यादी असते.

  उदाहरण: एबीसी 123, 123456789, पासवर्ड, एबीसीडीईएफ इ.

डिक्शनरी अटॅकमध्ये, हल्लेखोर (attacker) वापरकर्त्याचा पासवर्ड सामान्यपणे वापरला जाणारा शब्द (किंवा मागील साइट्समध्ये पाहिलेला पासवर्ड) आहे या आशेने वर्डलिस्ट वापरतो. वर्डलिस्ट केवळ इंग्रजी शब्दांपुरती मर्यादित नाहीत; त्यामध्ये बर्याचदा सामान्य पासवर्ड (उदा. 'पासवर्ड', 'लेटमीन', किंवा 'आयलव्ह यू', किंवा '123456') देखील समाविष्ट असतात. परंतु आधुनिक प्रणाली त्यांच्या यूजर्सना अशा सोप्या पासवर्डपासून प्रतिबंधित करतात, यूजर्सना स्ट्रॉंग पासवर्ड आणणे आवश्यक आहे जे वर्डलिस्टमध्ये सापडणार नाहीत अशी आशा आहे.

डिक्शनरी अटॅकपासून (Dictionary attack) बचाव करण्यासाठी उपाय :

- स्ट्रॉंग पासवर्ड (Strong Password) वापरणे: ज्या पासवर्डमध्ये मोठ्या आणि छोट्या अक्षरांचा, अंकांचा, आणि विशेष चिन्हांचा वापर केला जातो.
- मल्टी-फॅक्टर प्रमाणीकरण (MFA): पासवर्डच्या अतिरिक्त सुरक्षा लेयरसाठी.
- पासवर्ड मॅनेजर (Password Manager) वापरणे: बऱ्याच वेगवेगळ्या खात्यांसाठी स्ट्रॉंग आणि अद्वितीय पासवर्ड ठेवणे (strong and unique).
- पासवर्ड रीसेट पॉलिसी (Password reset policy): यूजर्सना नियमित कालांतराने पासवर्ड बदलण्याचे सूचित करणे.

ब्रूट फोर्स अटॅक (Brute-force Attack):

ब्रूट फोर्स अटॅक एक हॅकिंग पद्धत आहे, जी पासवर्ड, लॉगिन क्रेडेन्शियल्स, आणि एन्क्रिप्शन कीसाठी ट्रायल आणि एरर पद्धतीने हल्ला (attack) करते. हल्लेखोर अनेक युझरनेम आणि पासवर्ड्स टेस्ट करतो, अनेक वेळा संगणकाचा वापर करून विविध कॉम्बिनेशन्सची मोठी श्रेणी(category) तपासतो, जोपर्यंत त्याला योग्य लॉगिन माहिती मिळत नाही. ब्रूट फोर्स अटॅकमध्ये युझरनेम आणि पासवर्ड अंदाज लावून एक प्रणालीमध्ये अनधिकृत ऍक्सेस (Access) मिळवण्याचा प्रयत्न केला जातो. सामान्यत: या प्रकारच्या हल्ल्यांची प्रणाली द्वारे आयडेंटिटी (identity)केली जाऊ शकते आणि अनेक वेळा फेल्ड लॉगिन प्रयत्नांमुळे अकाउंट लॉक केले जाते, ज्यामुळे अनधिकृत ऍक्सेस (access) थांबवला जातो. तथापि, हल्लेखोर डिटेक्शन बायपास करण्याचे मार्ग शोधतात आणि पासवर्ड यशस्वीरित्या क्रॅक करतात.

ब्रुट फोर्स पासवर्ड हॅकिंग (Brute-force password hacking) कसे टाळावे?

- पासवर्ड्स साठी ऑनलाइन सापडणारी माहिती (जसे की कुटुंबातील सदस्यांची नावे) कधीही वापरू नका.
- पासवर्ड्स मध्ये जितके शक्य असेल तितके अधिक कॅरेक्टर्स असावेत.
- पासवर्ड्स मध्ये अक्षरे, संख्या आणि चिन्हे एकत्र करा.
- पासवर्ड्स मध्ये सामान्य पॅटर्न टाळा.
- पासवर्ड्स प्रत्येक युजर अकाउंटसाठी भिन्न असावे.
- आपला पासवर्ड वेळोवेळी बदलावा.
- स्ट्रॉंग आणि मोठा पासवर्ड वापरा.
- मल्टीफॅक्टर ऑथेंटिकेशन वापरा.

हल्ल्यांच्या दुसऱ्या प्रकारांमध्ये हे समाविष्ट आहे आणखी काही प्रकारचे अटॅक यामध्ये समाविष्ट आहेत :

1. पिगीबॅकिंग (Piggybacking)
2. शोल्डर सर्फिंग (Shoulder surfing)
3. डम्पस्टर डायव्हिंग (Dumpster diving)

2.2.1 पिगीबॅकिंग (Piggybacking):

पिगीबॅकिंग म्हणजे एक अधिकृत युजरचा प्रत्यक्षरित्या किंवा डिजिटलरित्या जवळून पाठलाग करणे, ज्याद्वारे ऍक्सेस (access) मिळवला जातो, बऱ्याचदा त्यांच्या संमतीशिवाय.

पिगीबॅकिंग (Piggybacking) कसे काम करते?

पिगीबॅकिंग अधिकृत युजरच्या प्रवेशाधिकारांचा वापर करून कार्य करते, ज्यामुळे अनधिकृत व्यक्तीला प्रतिबंधित प्रणाली किंवा क्षेत्रात ऍक्सेस (access) मिळवता येतो. हे प्रत्यक्षरित्या आणि डिजिटल, दोन्ही पद्धतींनी करता येऊ शकते. प्रत्यक्षरित्या, एक हल्लेखोर, कर्मचारी किंवा विझिटर्ससोबत मिसळून सुरक्षा चेकपॉइंट्सपासून बचाव करण्यासाठी अधिकृत व्यक्तीच्या

मागोमाग जाऊ शकतो. डिजिटलरित्या, हल्लेखोर (attacker) सामायिक किंवा चोरलेली लॉगिन क्रेडेन्शियल्स वापरून सुरक्षित प्रणालींमध्ये ऍक्सेस (access) मिळवू शकतो. अनेक वेळा, पिगीबॅकिंगमध्ये अधिकृत युजरच्या ऑथेंटिकेशन (user authentication) प्रक्रिये दरम्यान निरीक्षण करणे समाविष्ट असते. यामध्ये कोणीतरी आपला पासवर्ड किंवा पिन एंटर (PIN) करत असताना पाहणे किंवा की लॉगर्स आणि व्हिडिओ कॅमेरे सारख्या देखरेख साधनांचा वापर करून लॉगिन तपशील टिपणे समाविष्ट होऊ शकते. एकदा हल्लेखोराकडे(attacker) आवश्यक क्रेडेन्शियल्स असले की, ते प्रणालीमध्ये लॉगिन करू शकतात, गोपनीय डेटा ॲक्सेस करू शकतात किंवा मालवेअर सॉफ़्टवेअर (Malware software) इन्स्टॉल (install) करू शकतात.

पिगीबॅकिंगची (Piggybacking) उदाहरणे काय आहेत?

पिगीबॅकिंगची उदाहरणे प्रत्यक्ष आणि डिजिटल दोन्ही संदर्भांमध्ये आढळू शकतात. भौतिक(physical) सेटिंगमध्ये, एक अनधिकृत व्यक्ती अधिकृत व्यक्तीला दरवाजाद्वारे जवळून पाठलाग करून सुरक्षित क्षेत्रात ऍक्सेस (access) मिळवू शकते, बर्याचदा दरवाजा उघडा ठेवणार्या अधिकृत व्यक्तीच्या सौजन्याचा गैरफायदा घेऊ शकते. कार्यालयीन इमारती आणि डेटा सेंटरमध्ये ही परिस्थिती सामान्य आहे जिथे सुरक्षा प्रोटोकॉल शिथिल असू शकतात किंवा अंमलात आणले जात नाहीत.

डिजिटल क्षेत्रात वाय-फाय नेटवर्कच्या माध्यमातून पिगीबॅकिंग होऊ शकते. उदाहरणार्थ, अनधिकृत युजर एखाद्या कार्यालयाच्या वाय-फाय नेटवर्कशी कनेक्ट होऊ शकतो जर तो असुरक्षित असेल किंवा कमकुवत पासवर्ड वापरत असेल. त्याचप्रमाणे, वैयक्तिक हॉटस्पॉट(personal hotspot) आणि डिफॉल्ट किंवा सहज अंदाज येण्याजोगे पासवर्ड असलेले होम राउटर (home router) हे पिगीबॅकिंगचे मुख्य लक्ष्य आहेत, ज्यामुळे अनधिकृत युजरना नेटवर्क आणि संभाव्य संवेदनशील माहिती मिळू शकते.

पिगीबॅकिंग कसे टाळावे?

- ऍक्सेस नियंत्रण प्रणाली (Access Control System) कार्यान्वित करा.
- सर्व्हेलन्स कॅमेरे (surveillance cameras) आणि व्हिडिओ ॲनालिटिक्सचा (video analytics) वापर करा.
- कर्मचाऱ्यांना फिजिकल सेक्युरिटी बाबत(physical security) जागरुकतेचे प्रशिक्षण द्या.
- विझिटर्सचा (visitors) मागोवा घेण्यासाठी आणि अधिकृत करण्यासाठी विझिटर्स व्यवस्थापन प्रणाली वापरा.
- फिजिकल अडथळे(physical barrier) स्थापित करा.

2.2.2 शोल्डर सर्फिंग (Shoulder surfing):

शोल्डर सर्फिंग (Shoulder surfing) हल्ल्यादरम्यान, अटॅकर (attacker) अगदी जवळून एखाद्याची संवेदनशील माहिती, मग तो पासवर्ड, पर्सनल आयडेंटिफिकेशन नंबर (Personal Identification Number) (पिन) किंवा असा कोणताही डेटा असो, प्रत्यक्षरित्या पाहतो. सहसा, हा हल्ला सार्वजनिक किंवा निम -सार्वजनिक वातावरणात होतो, जिथे अटॅकर स्क्रीनवर काय आहे किंवा कीबोर्डवर काय टाईप केले जात आहे हे पाहू शकतो, आणि त्यामध्ये जास्त संशय निर्माण होत नाही. प्रायव्हसी स्क्रीन्स, जी केवळ छोट्या दृश्य कोनात डिस्प्ले दर्शवतात, त्याचा वापर युजर शोल्डर सर्फिंगपासून संरक्षण करण्यासाठी करू शकतात. शिवाय, संवेदनशील डेटा टाकताना त्यांना आजूबाजूच्या वातावरणाची जाणीव असणे आवश्यक आहे आणि संभाव्य प्रेक्षकांना ब्लॉक करता येईल अशा प्रकारे स्वत: ला ठेवणे आवश्यक आहे. ऑन-स्क्रीन कीबोर्ड (on-screen keyboard) देखील कीस्ट्रोक (keystroke) पकडण्याचा प्रयत्न करणाऱ्यांसाठी अतिरिक्त अडचण निर्माण करतील, ज्यामुळे या प्रकारच्या हल्ल्यापासून अतिरिक्त संरक्षण मिळेल.

शोल्डर सर्फर्स (Shoulder surfers) चोरी करू शकणाऱ्या माहितीमध्ये हे समाविष्ट आहे:

- युजरनेम आणि पासवर्ड (Username and Password)
- पिन नंबर (PIN Number)
- क्रेडिट आणि डेबिट कार्ड क्रमांक (Credit and Debit Card Number)
- सोशल सिक्युरिटी नंबर (Social security Number)
- बँक अकाउंटचा तपशील (Bank Account Details)
- व्हिक्टीमच्या नोकरीची माहिती

- व्हिक्टीमच्या मित्रांची आणि कुटुंबियांची माहिती

शोल्डर सर्फिंगपासून (Shoulder surfing) स्वतःचा बचाव कसा करावा?

- आपल्या सर्व डिव्हाइसवर (Device) प्रायव्हसी स्क्रीन (Privacy Screen) वापरा.
- स्क्रीनला (Screen) अशा प्रकारे झुकवा की इतर व्यक्तीला डेटा दिसणार नाही.
- संवेदनशील माहिती टाईप करताना आपल्या हाताचा शिल्ड (Shield) म्हणून वापर करा.
- आपले पासवर्ड सुरक्षित ठेवण्यासाठी पासवर्ड मॅनेजर (Password Manager) वापरा.
- लोकांपासून सुरक्षित अंतर ठेवा.
- सार्वजनिक ठिकाणी काम करताना स्वत:ला धोरणात्मक स्थितीत ठेवा.
- आपल्या स्क्रीनची ब्राइटनेस (Screen Brightness) कमी करा.
- सार्वजनिक ठिकाणी फोन कॉल्स किंवा मीटिंग्ज (Phone calls or meetings) घेऊ नका.
- जेव्हा वापरत नाही तेव्हा आपले डिव्हाइस लॉक (Device lock) करा.
- सार्वजनिक ठिकाणी संवेदनशील कामे करणे टाळा.

2.2.3 डम्पस्टर डायव्हिंग (Dumpster diving):

डंप्स्टर डायव्हिंग (Dumpster diving) म्हणजे हल्लेखोर(attacker) आपल्या कंपनीच्या ट्रॅशमधून संवेदनशील किंवा गोपनीय माहिती असलेले दस्तऐवज (document) शोधतात. इन्फॉरमेशन लीकेज (Information leakage) टाळण्यासाठी नेहमीच फाइल श्रेडर (File shredder) वापरा. डम्पस्टर डायव्हिंग ही एखाद्या व्यक्तीबद्दल / व्यवसायाबद्दल ट्रॅशमधून उपयुक्त माहिती शोधण्याची प्रोसेस (process)आहे जी नंतर हॅकिंगच्या हेतूसाठी वापरली जाऊ शकते. हा हल्ला (attack) प्रामुख्याने मोठ्या संस्था किंवा व्यवसायांना फिशिंग (Phishing) करण्यासाठी लक्ष्य करतो, (बहुतेक) पीडितांना बनावट / फसव्या ईमेल पाठवून जे वैध (अधिकृत आणि विश्वसनीय) स्त्रोतातून आलेले दिसतात. व्हिक्टीमच्या गोपनीयतेशी तडजोड करून मिळवलेली माहिती आयडेंटिटी फ्रॉडसाठी (Identity Fraud) वापरली जाते.

हॅकर (Hacker) काय शोधतो?

- ॲड्रेस / ईमेल ॲड्रेस (Address / Email Address)
- व्हिशिंग (Vishing) करण्यासाठी फोन नंबर (Phone number)
- पासवर्ड आणि इतर सोशल सिक्युरिटी नंबर (Social security number) जे आपण आपल्या सोयीसाठी स्टिकी नोट्सवर (sticky notes) लिहिले असतील.
- बँक स्टेटमेंट्स / आर्थिक स्टेटमेंट्स (Bank statements / Financial statements)
- वैद्यकीय रेकॉर्ड्स (Medical records)
- महत्त्वाची कागदपत्रे
- अकाउंट लॉग इन क्रेडेन्शियल्स (Account login credentials)
- व्यावसायिक गुपित(Business Secret)
- मार्केटिंगचे गुपित(Marketing Secret)
- कर्मचारी डेटाबेसची माहिती
- कंपनीमध्ये वापरल्या जाणाऱ्या सॉफ्टवेअर/टूल्स /टेक्नॉलॉजीची (software / tools / technology) माहिती

प्रतिबंधात्मक उपाय :

- वैयक्तिक डेटा असलेल्या कोणत्याही सीडी / डीव्हीडी (CD / DVD) नष्ट करा.
- आपल्याला यापुढे आपल्या पीसीची आवश्यकता नसल्यास, आपण सर्व डेटा डिलीट केला आहे याची खात्री करा जेणेकरून तो पुनर्प्राप्त होऊ शकणार नाही.
- फायरवॉलचा वापर संशयास्पद इंटरनेट यूजर्सना (internet users) टाकाऊ डेटामध्ये ॲक्सेस (Access) करण्यापासून रोखू शकतो.
- कागदपत्रे(documents) कायमस्वरूपी नष्ट करावीत.

- कंपन्यांनी ट्रॅश लॉक करणे आणि सुरक्षित विल्हेवाट लावावी.

2.3 बायोमेट्रिक्स (Biometrics):

बायोमेट्रिक सुरक्षा उपाय हे नाविन्यपूर्ण तंत्रज्ञान आहे, जे व्यक्तींच्या अनोख्या शारीरिक वैशिष्ट्यांचा, जसे की अंगठ्याचे ठसे, हाताचे ठसे, आवाज, आयरिस आणि रेटिना, त्यांची आयडेंटिटी (Identity) सुरक्षित / संरक्षित आणि प्रमाणित करण्यासाठी वापर करतात.

बायोमेट्रिक ऑथेंटिकेशन (Biometric authentication) एक सायबर-सुरक्षा प्रोसेस (cyber security process) आहे जी बोटांचे ठसे, आवाज, रेटिना आणि चेहऱ्याची वैशिष्ट्ये यासारख्या अद्वितीय (unique) जैविक वैशिष्ट्यांचा वापर करून युजरचीआयडेंटिटी (Identity) पडताळते. बायोमेट्रिक्स हे जैविक किंवा वर्तणुकीच्या वैशिष्ट्यांचे मोजमाप आहे जे व्यक्तींच्या ओळखीसाठी वापरले जाते. यातील बहुतेक वैशिष्ट्ये वारशाने मिळालेली आहेत आणि त्यांचा अंदाज बांधता येत नाही किंवा चोरी केली जाऊ शकत नाही. बायोमेट्रिक सिस्टिम (Biometric system) ही अशी प्रणाली आहे जी एखाद्या व्यक्तीच्या शारीरिक, वर्तनात्मक किंवा दोन्ही वैशिष्ट्यांना इनपुट (Input) म्हणून घेते, त्याचे विश्लेषण करते आणि त्या व्यक्तीला वैध किंवा हानिकारक युजर म्हणून ओळखते.

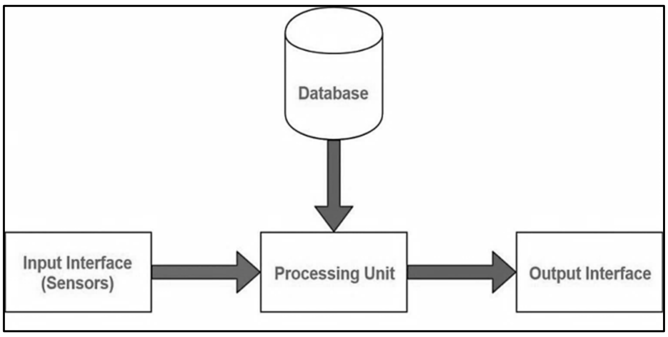


Figure 2.1: Biometric System (Courtesy: https://www.geeksforgeeks.org/what-is-biometrics/)

वापरण्यात येणारे बायोमेट्रिक वैशिष्ट्य ऑथेंटिकेशन साठी वापरण्यापूर्वी समुदायातील सर्व व्यक्तींसाठी डेटाबेसमध्ये उपलब्ध असणे आवश्यक आहे. यालाच नावनोंदणी(enrolment) म्हणतात.

ऑथेंटिकेशन खालीलपैकी एका प्रकारात असू शकते:

- **ओळख(Identification):** एखाद्या व्यक्तीच्या वैशिष्ट्यांची तुलना सर्व रेकॉर्ड्ससह केली जाते, जेणेकरून त्याचा/तिचा रेकॉर्ड डेटाबेसमध्ये आहे का हे तपासता येईल.
- **पडताळणी (Authentication)** ती व्यक्ती कोण असल्याचा दावा करीत आहे ती तीच आहे की नाही, हे तपासणे. या प्रकरणात त्या व्यक्तीचे वैशिष्ट्य केवळ त्या व्यक्तीच्या वैशिष्ट्यांशी जुळते ज्याचा तो दावा करतो.

2.3.1 बायोमेट्रिक चे प्रकार:

1. **फिंगरप्रिंट (Fingerprint) :** फिंगरप्रिंट ऑथेंटिकेशन (Fingerprint authentication) वापरले जाते कारण फिंगरप्रिंट प्रत्येक व्यक्तीसाठी अद्वितीय असतात. त्यांचे मोजमाप अनेक प्रकारे करता येते. मिन्युटी- बेस्ड मोजमाप ग्राफ वापरते जे रिड्जेस (ridges) जुळविण्यासाठी वापरले जातात, तर इमेज- बेस्ड मोजणी व्यक्तीच्या अंगठ्याच्या ठशांच्या प्रतिमेशी आणि डेटाबेसमधील अंगठ्याच्या ठशांच्या इमेजशी समानता शोधते. यामध्ये उच्च सुरक्षा स्तर आहे आणि हे आयडेंटिटी आणि प्रमाणीकरण (Identification and Authentication) दोन्हीसाठी वापरले जाते. तथापि, वयोमानानुसार किंवा आजार/दुखापतीमुळे, अंगठ्याचे ठसे बदलू शकतात. सामान्य वापर: मोबाईलमध्ये पडताळणीसाठी, कार्यालयांमध्ये ओळखण्यासाठी.गर्भाच्या अवस्थेत बोटांचे ठसे तयार होतात आणि एखाद्या व्यक्तीच्या आयुष्यभर अबाधित राहतात. दोन व्यक्तींचे, अगदी समान जुळ्या भावंडांचेही, अंगठ्याचे ठसे समान नसतात. या विशिष्टतेचा आधार आनुवंशिक आणि पर्यावरणीय घटकांमध्ये आहे, जे अंगठ्याच्या ठशांच्या विकासावर प्रभाव टाकतात.
   विश्लेषण केलेल्या बोटांच्या ठशांच्या पैलूंमध्ये हे समाविष्ट आहे:

- **पॅटर्न्स (Patterns) :** फिंगरप्रिंटचा सामान्य पॅटर्न किंवा प्रकार (आर्च, लूप किंवा व्होरल) अनुवांशिकतेद्वारे वांशिकरित्या प्राप्त होतो.

- **मिन्युटी (Minutiae):** रिड्जेसच्या अचूक तपशिलांना मिन्युटी (Minutiae) म्हटले जाते, जे अनियमित आणि अनपेक्षित घटकांद्वारे प्रभावित होतात, जसे की दबाव, रक्तप्रवाह, आणि गर्भधारणे दरम्यान गर्भाच्या स्थितीचे परिणाम.
- **रिड्जेस (Ridges):** फिंगरप्रिंटमधील प्रत्येक रिड्जमध्ये (Ridges) अनेक मिन्युटी पॉईंट्स (Minutiae points) असतात, जे बायफर्केशन्स (bifurcations) (जिथे एक रिज दोन भागात विभागली जाते) किंवा रिज एंडिंग असू शकतात.
  मिन्युटी पॉइंट्सचे वितरण आणि लेआउट (layout) प्रत्येक व्यक्तीमध्ये वेगळे असतात, जे प्रत्येक फिंगरप्रिंटच्या विशिष्ट वैशिष्ट्यांमध्ये योगदान देते. हेच वैशिष्ट्ये आहेत, बोटांच्या ठशांची तुलना आणि जुळवाजुळव करताना बायोमेट्रिक प्रणाली या वैशिष्ट्यांचे विश्लेषण करतात.

2. **हाताचे ठसे:** हाताचे ठसे बायोमेट्रिक्स माहिती सुरक्षा क्षेत्रात व्यक्तींची आयडेंटिटी (identity) पटवण्यासाठी एक पद्धत आहे, ज्यात त्यांच्या हातावर असलेल्या रेषा आणि डागांचा अद्वितीय पॅटर्न (unique pattern) स्कॅन केला जातो. संपूर्ण तळहाताचा वापर बायोमेट्रिक आयडेंटिटी (identity) म्हणून प्रमाणीकरण करण्यासाठी केला जातो. हाताची रचना पाम (palm) म्हणजे तळहात आणि बोटांच्या संरचनेवर आधारित असते, ज्यात बोटांची रुंदी, बोटांची लांबी, पाम क्षेत्राची जाडी इत्यादी समाविष्ट आहेत. ही मोजमापे लोकांमध्ये फारशी वेगळी नसली तरी आयडेंटिटी (identity) पडताळणीसाठी, म्हणजेच वैयक्तिक प्रमाणीकरणासाठी हाताची भूमिती (hand geometry) खूप उपयुक्त ठरू शकते.
3. **आयरिस आणि रेटिना (IRIS and Retina)**: डोळ्यातील पॅटर्न्स अनोखे असतात आणि त्यांचा वापर आयडेंटिटी (identity) आणि प्रमाणीकरण दोन्हीसाठी केला जाऊ शकतो. रेटिनाचे विश्लेषण करणारी उपकरणे महाग आहेत आणि म्हणूनच ते तुलनेने कमी सामान्य आहे.

   डोळे - आयरिस ओळख :

   आयरिस हा आपल्या डोळ्यांचा रंगीत भाग आहे जो डोळ्यात ऍक्सेस (access) करणार्या प्रकाशाचे प्रमाण नियंत्रित करण्यास मदत करतो. हे आजूबाजूच्या प्रकाशाच्या स्थितीनुसार आकुंचन पावते आणि आरामदायक होते. प्रत्येक व्यक्तीच्या आयरिसचा एक विशिष्ट पॅटर्न आणि आकार असतो ज्यामुळे त्याचा बायोमेट्रिक आयडेंटिटी (access) म्हणून वापर केला जाऊ शकतो. आयरिस स्कॅनरचा (IRIS scanner) वापर एखाद्या व्यक्तीचे डोळे स्कॅन करण्यासाठी केला जातो.

   डोळे - रेटिना ओळख :

   रेटिना हा आपल्या डोळ्यांचा तो भाग आहे जो प्रकाश किरणांचे इलेक्ट्रिकल सिग्नलमध्ये रूपांतर करतो जे इमेज / दृश्यांचे विश्लेषण आणि प्रदर्शन करण्यासाठी आपल्या मेंदूत पोहोचविले जातात. बायोमेट्रिक तंत्रज्ञान म्हणून रेटिना ओळख पडताळणीसाठी आपल्या डोळ्यांच्या मागील बाजूस असलेल्या रक्तवाहिन्या आणि नसांच्या अनोख्या पॅटर्नचा वापर करते.
4. **व्हॉइस रिकग्निशन (voice recognition)**: व्हॉइस रिकग्निशन व्हॉइस बायोमेट्रिक्सवर (voice biometrics) आधारित आहे. व्हॉईस बायोमेट्रिक्स (voice biometrics) हे एक तंत्रज्ञान आहे जे यूजर्सना त्यांच्या आवाजाद्वारे ओळखते आणि प्रमाणित करते. या तंत्रज्ञानाचा आधार असतो की मानवाचा आवाज अद्वितीय (unique) असतो, आणि प्रत्येक व्यक्तीचा आवाजातील वारंवारता पॅटर्न आणि वैशिष्ट्ये वेगळी असतात. हे तंत्रज्ञान सोपे आहे: आवाज रेकॉर्ड केला जातो आणि नंतर त्याचे विश्लेषण करून व्यक्तीची आयडेंटिटी (identity) पटवण्यासाठी वैशिष्ट्यांचा संच (features set) प्राप्त केला जातो. रिदम, पिच, फ्रिक्वेन्सी आणि टॅम्ब्र (Rhythm, pitch, frequency, and timbre) हे आवाज विश्लेषणात वापरले जाणारे काही वैशिष्ट्ये आहेत. व्हॉईस रिकग्निशन एखाद्या व्यक्तीसाठी अद्वितीय असलेल्या टोन, पिच आणि फ्रिक्वेन्सीचा (tone, pitch, and frequencies) वापर करून ते प्रमाणित करते. लोकांच्या आवाजात साम्य असल्यामुळे सुरक्षा स्तर (सेक्युरिटी) (security) मध्यम आहे, त्यामुळे हे मुख्यतः पडताळणीसाठी वापरले जाते. आवाजात गोंगाट, वयोमानानुसार बदल किंवा आजारपणामुळे अचूकतेवर परिणाम होऊ शकतो.

   व्हॉइस बायोमेट्रिक्स (voice biometrics) आणि व्हॉइस रिकग्निशन (voice recognition) मधील फरक

   व्हॉईस बायोमेट्रिक्स (voice biometrics):

   एक व्यक्तीच्या आवाजाच्या अनोख्या वैशिष्ट्यांचा वापर करून त्यांची विश्वसनीय आयडेंटिटी (identity) पटवते. हे सिस्टिममध्ये वापरकर्त्याचे प्रमाणीकरण (user authentication) करण्यासाठी वापरले जाते, जेणेकरून फक्त तेच

संवेदनशील माहितीपर्यंत ऍक्सेस (access) करू शकतील किंवा विशिष्ट कृती करू शकतात. याउलट, व्हॉईस रिकग्निशन (voice recognition) मुळे भाषणाला संगणक किंवा डिजिटल डिव्हाइसद्वारे (digital device) प्रोसेस (process) करण्यासाठी मजकुरात रूपांतरित केले जाते. गुगल असिस्टंट (google assistant), अॅलेक्सा किंवा सिरी (Alexa or siri) सारखे आयए असिस्टंट व्हॉइस रिकग्निशन (voice recognition) वापरतात. या प्रणाली वापरकर्त्यांना (system users) व्हॉईस कमांड वापरून कृती करण्यास आणि माहिति मिळविण्यास परवानगी देतात. थोडक्यात, व्हॉइस बायोमेट्रिक्स लोकांची आयडेंटिटी (identity) पटवते, तर व्हॉइस रिकग्निशन भाषणाचे रूपांतर करून त्याला टेक्स्टमध्ये बदलते, जे संगणक समजू शकतो. नमूद केल्याप्रमाणे, व्हॉईस बायोमेट्रिक्स सिस्टम्स (voice biometrics systems) सुरक्षा वातावरणात वापरली जाते. मुख्य अँप्लिकेशन लॉग इन (application login) करताना, आर्थिक व्यवहारांना मान्यता देताना आणि कॉल सेंटर सर्विसमध्ये (call center service) ऍक्सेस (access) करताना यूजरच्या आयडेंटिटी (identity) पडताळणीशी संबंधित आहेत. व्हॉईस बायोमेट्रिक्सच्या विरुद्ध, व्हॉईस रिकग्निशन हे मुख्यतः पर्सनल असिस्टंट अॅप्स जसे डिजिटल असिस्टंट आणि आरोग्य उद्योगात वैद्यकीय माहिती नोंदवण्याची गती वाढवण्यासाठी वापरले जाते.

सुरक्षिततेतील बायोमेट्रिक वापराची काही उदाहरणे:

- **फिंगरप्रिंट रिकग्निशन (Fingerprint recognition):** स्मार्टफोन अनलॉक, संगणक प्रणालीमध्ये ऍक्सेस (access) आणि वेळ आणि हजेरी / उपस्थिती ट्रॅकिंगसाठी मोठ्या प्रमाणात वापरले जाते.
- **चेहऱ्याची ओळख:** विमानतळावर प्रवाशांची आयडेंटिटी (identity)पटवण्यासाठी, सुरक्षा प्रणालींमध्ये आणि ऍक्सेस (access) नियंत्रण प्रणालींमध्ये वापरली जाते.
- **आयरिस (IRIS) ओळख:** अत्यंत सुरक्षित मानली जाते आणि सरकारी सुविधा किंवा डेटा सेंटरसारख्या उच्च जोखमीच्या वातावरणात वापरली जाते.
- **व्हॉईस रिकग्निशन (voice recognition) :** फोन बँकिंग (phone banking), कॉल सेंटर ऑथेंटिकेशन (call center authentication) आणि सुरक्षित लॉगिनसाठी याचा वापर केला जाऊ शकतो.
- **हाताची रचना:** काही परिस्थितींमध्ये ऍक्सेस नियंत्रणासाठी(access control) वापरले जाते, जिथे हाताची आकार रचना अद्वितीय / अनोखी असते.

बायोमेट्रिक ऑथेंटिकेशन (Biometric authentication) वापराची काही उदाहरणे :

आरोग्य सेवा : रुग्णालये बायोमेट्रिक्सचा वापर रुग्णांची अचूक ओळख पटवण्यासाठी आणि गोंधळ टाळण्यासाठी करतात. बायोमेट्रिक माहितीचा वापर आरोग्य केंद्रे आणि डॉक्टरांच्या कार्यालयांकडून त्यांच्या रुग्णांच्या डेटाची सुरक्षितता सुनिश्चित करण्यासाठी केला जातो. त्यामुळे वैद्यकीय कर्मचारी बायोमेट्रिक ऑथेंटिकेशनद्वारे पेशंट हिस्ट्री साठवू शकतात आणि प्राप्त करू शकतात.

प्रवास: इलेक्ट्रॉनिक पासपोर्टमध्ये (Electronic passport) एक मायक्रोचिप (microchip) असते ज्यामध्ये चेहऱ्याच्या फोटोसह त्या व्यक्तीचा बायोमेट्रिक डेटा असतो. हे नाव बायोमेट्रिक माहिती आणि इतर ओळखकर्त्यांशी जोडलेले आहे. पासपोर्ट प्राधिकरणाने अर्जदाराचे बोटांचे ठसे किंवा इतर बायोमेट्रिक्स तपासल्यानंतर आणि मायक्रोचिप डेटा प्रदान केलेल्या तपशीलांशी जुळतो की नाही याची खात्री केल्यानंतर ई-पासपोर्ट (E-passport) इलेक्ट्रॉनिक पद्धतीने जारी केला जातो.

कायद्याची अंमलबजावणी : पोलिस व्यक्तींची ओळख पटवण्यासाठी बोटांचे ठसे, चेहऱ्याची वैशिष्ट्ये, आयरिस स्कॅन (IRIS scan), व्हॉइस प्रिंट (voice print) आणि डीएनए (DNA) अशा अनेक प्रकारच्या बायोमेट्रिक वैशिष्ट्यांचा वापर करतात. कायद्याची अंमलबजावणी करणाऱ्या एजन्सी पूर्वीपेक्षा या प्रणालींचा वापर करून गोपनीय माहिति अधिक वेगाने मिळवू शकतात. प्रशिक्षित तज्ञ पारंपारिकपणे बोटांच्या ठशांची मॅन्युअली तुलना करीत असत, आता ऑटोमेटेड फिंगरप्रिंट आयडेंटिफिकेशन सिस्टिम (एएफआयएस) (automated fingerprint identification systems (AFIS)) काही मिनिटांत डेटाबेसमधील लक्षावधी लोकांच्या फिंगरप्रिंटची तुलना करू शकते.

2.4 ऑथोरायझेशन (Authorization):

2.4.1 ऑथोरायझेशनची आयडेंटिटी (Identity): अधिकृतता(Authorization) हे ऍक्सेस हक्क (access rights) देण्याचे काम करते. ऑथोरायझेशन म्हणजे यूजरना विशिष्ट रिसोर्सेसमध्ये ऍक्सेस (access) देण्याची परवानगी देते किंवा नाकारते,

संस्थेत त्यांची भूमिका काय असू शकते यावर अवलंबून असते. ऑथोरायझेशन म्हणजे यूजरना नेटवर्कवरील विशिष्ट फाइल्स, फोल्डर, ॲप्लिकेशन्स, नेटवर्क रिसोर्सेस आणि इतर सिस्टिम ऑब्जेक्ट्समध्ये (files, folders, applications, network resources, and other system objects) ऍक्सेस (access) करण्यास परवानगी देते किंवा नाकारते. संगणक सुरक्षेत अधिकृततेचे दोन पैलू महत्वाचे आहेत:

- काय अधिकृत केले जात आहे आणि
- कोण अधिकृत करीत आहे.

काय अधिकृत (ऑथोराइझ) (Authorise) केले जात आहे?

विशिष्ट फाइल्स, फोल्डर किंवा ॲप्लिकेशन्समध्ये ऍक्सेस (access) नियंत्रित करण्यासाठी ऑथोरायझेशनचा (अधिकृततेचा) वापर केला जाऊ शकतो. प्रिंटर किंवा डेटाबेस (printer or database) सारख्या नेटवर्कवरील विशिष्ट रिसोर्सेसमध्ये ऍक्सेस (access) नियंत्रित करण्यासाठी देखील याचा वापर केला जाऊ शकतो.

अधिकृतीकरण (ऑथोरायझेशन) कोण करतंय?

अधिकृतता (ऑथोरायझेशन) प्रशासकाद्वारे (ऍडमिनीस्ट्रेटरद्वारे) (administrator) केली जाऊ शकते किंवा ऑपरेटिंग सिस्टिमद्वारे (operating system) केली जाऊ शकते. प्रशासक (ऍडमिनीस्ट्रेटर) सामान्यत: अशी व्यक्ती असते ज्याला अधिकृत यूजर्सना विशिष्ट परवानग्या देण्यात आल्या आहेत. ऑपरेटिंग सिस्टीम हे संगणकावर नियंत्रण ठेवणारे सॉफ्टवेअर आहे. सुरक्षा धोरणांची अंमलबजावणी करण्यासाठी आणि यूजर्सना अधिकृत करण्यासाठी हे जबाबदार आहे. अधिकृतता हा संगणक सुरक्षेचा एक महत्त्वाचा भाग आहे कारण ते नेटवर्कवरील संसाधनांचे संरक्षण करण्यास मदत करते. हे देखील महत्वाचे आहे कारण हे सुनिश्चित करण्यात मदत करते की वापरकर्ते केवळ त्या कार्यांसाठी अधिकृत आहेत जे त्यांनी करणे अपेक्षित आहे. यामुळे संस्थेचे अनधिकृत प्रवेशापासून आणि दुर्भावनापूर्ण कृत्यांपासून(malicious activity) संरक्षण होण्यास मदत होते. अधिकृततेचे तीन प्रकार आहेत: अनिवार्य ऍक्सेस (access) नियंत्रण (मॅक) (MAC), विवेकाधीन ऍक्सेस (access) नियंत्रण (डीएसी)(DAC) आणि भूमिका-आधारित ऍक्सेस (access) नियंत्रण (आरबीएसी) (RBAC). मॅक म्हणजे जिथे सिस्टिम वापरकर्त्यास कोणता ऍक्सेस (access) आहे हे निर्धारित करते, डीएसी म्हणजे जिथे डेटाचा ओनर वापरकर्त्यास कोणता ऍक्सेस (access) आहे हे निर्धारित करतो आणि आरबीएसी म्हणजे जेथे ऍडमिनीस्ट्रेटर यूजर्सना वेगवेगळ्या भूमिका(roles) देतो आणि त्या यूजर्सना विशिष्ट डेटामध्ये काय ऍक्सेस (access) आहे हे निर्धारित करते. आरबीएसी आज वापरात असलेल्या अधिकृततेचा सर्वात सामान्य प्रकार आहे.

2.4.2 अधिकृततेची (ऑथोरायझेशनची) (Authorization) उद्दिष्टे: केवळ ऑथोराइज्ड यूजर्स, सिस्टिम्स किंवा सर्विसना (Authorised users, systems or services) आवश्यक रिसोर्सेसमध्ये ऍक्सेस (access) आहे याची खात्री करून सुरक्षा जोखीम कमी करणे हे प्राथमिक ध्येय आहे. अनधिकृत ऍक्सेसपासून डेटाचे संरक्षण करणे. परवानग्यांवर आधारित विशिष्ट कार्यक्षमता किंवा डेटामध्ये ऍक्सेस मर्यादित करणे. सर्व व्यावसायिक डेटा न देता, प्रत्येक कर्मचाऱ्याला त्यांचे काम करण्यासाठी आवश्यक असलेल्या सिस्टिम्सना आणि माहितीलाच ऍक्सेस देणे. यूजर्सच्या विविध ऍक्टिव्हिटीज रेकॉर्ड ठेवणे

ऑथेंटिकेशन आणि ऑथोरायझेशन मधील फरक:

- ऑथेंटिकेशन (Authentication) म्हणजे युजरला ओळखून त्याला सिस्टिम्स (system) मध्ये ऍक्सेस (access) देण्याची प्रोसेस (process)आहे, तर ऑथोरायझेशन (Authorization) ही रिसोर्सेसला ऍक्सेस देण्यासाठी परवानगी देण्याची प्रोसेस (process)आहे.
- ऑथेंटिकेशनमध्ये (Authentication) युजर किंवा क्लायंट (user or client) आणि सर्व्हरची (server) पडताळणी केली जाते. ऑथोरायझेशनमध्ये (Authorization), यूजरला ठरवलेल्या पॉलिसीज् आणि नियमांद्वारे परवानगी दिली गेली आहे की नाही याची पडताळणी केली जाते.
- ऑथेंटिकेशन सहसा ऑथोराइझ होण्यापूर्वी केले जाते. युजर यशस्वीरित्या प्रमाणित (ऑथेंटिकेट) (Authenticate) झाल्यानंतर ऑथोरायझेशन केले जाते.
- ऑथेंटिकेशनसाठी युजरचे लॉगिन (user login) तपशील, जसे की युजर नेम आणि पासवर्ड (username and password) इत्यादी आवश्यक आहेत. ऑथोरायझेशन साठी युजर चा विशेषाधिकार किंवा सुरक्षा स्तर आवश्यक आहे.

- ऑथेंटिकेशन क्रेडेन्शियल्स (Authentication credentials) युजरद्वारे आवश्यकतेनुसार अंशतः बदलले जाऊ शकतात. ऑथेंटिकेशन परवानग्या युजरद्वारे बदलल्या जाऊ शकत नाहीत. युजरला परवानग्या सिस्टिमच्या ओनर / व्यवस्थापकाद्वारे दिल्या जातात आणि केवळ तोच त्यांना बदलू शकतो.

उदाहरण:

ऑथेंटिकेशन (Authentication) : कर्मचाऱ्याना ऑर्गनायझेशनल ईमेल किंवा सॉफ्टवेअरमध्ये (organizational email or software) ऍक्सेस (access) करण्यासाठी स्वतःला ऑथेंटिकेट (authenticate) करण्यासाठी लॉगिन तपशील प्रविष्ट (enter) करणे आवश्यक आहे.

ऑथोरायझेशन (Authorization) : कर्मचाऱ्यानी स्वत: ला यशस्वीरित्या ऑथेंटिकेट (authenticate) केल्यानंतर, ते केवळ त्यांच्या भूमिका (role) आणि प्रोफाइलनुसार विशिष्ट कार्यांमध्ये ऍक्सेस (access) करू शकतात आणि काम करू शकतात.

2.5 ॲक्सेस कंट्रोल (Access control) :

ॲक्सेस कंट्रोल ही सिस्टिम्स किंवा रिसोर्सेसमध्ये (systems or resources) ॲक्सेस मर्यादित करण्याची एक पद्धत आहे. ॲक्सेस कंट्रोल ही एक प्रोसेस (process)आहे ज्यामध्ये नेटवर्कमधील कोणाला, कोणत्या रिसोर्सेसमध्ये आणि कोणत्या अटींवर ऍक्सेस (access) आहे, हे ठरवले जाते. ही सुरक्षा क्षेत्रातील एक मूलभूत संकल्पना आहे, जी व्यवसाय किंवा संस्थेसाठी जोखीम कमी करण्यास मदत करते.ॲक्सेस कंट्रोल सिस्टिम (Access control system)आवश्यक लॉगिन क्रेडेन्शियल्सचे (login credential) मूल्यांकन करून यूजर्स आणि संस्थांची ओळख, ऑथेंटिकेशन आणि ऑथोरायझेशन करतात ज्यात पासवर्ड, पिन, बायो-मेट्रिक स्कॅन किंवा इतर ऑथेंटिकेशन (password, PIN, Biometric scan or other authentication factors) घटकांचा समावेश असू शकतो. मल्टी-फॅक्टर ऑथेंटिकेशनसाठी (multifactor authentication) दोन किंवा अधिक ऑथेंटिकेशन घटकांची आवश्यकता असते, जे बर्याचदा ॲक्सेस कंट्रोल सिस्टिमचे संरक्षण करण्यासाठी स्तरीय संरक्षणाचा एक महत्त्वाचा भाग असतो.

ॲक्सेस कंट्रोल (Access control) कसे कार्य करते?

ॲक्सेस कंट्रोल मध्ये युजरची आयडेंटिटी (identity)त्यांच्या क्रेडेन्शियल्सच्या (credentials) आधारे पडताळली जाते आणि एकदा आयडेंटिटी (identity) कन्फर्म झाल्यावर त्यांना योग्य स्तरावर ऍक्सेस (access) प्रदान केला जातो. क्रेडेन्शियल्सचा वापर युजरला ओळखण्यासाठी आणि प्रमाणित करण्यासाठी केला जातो ज्यात पासवर्ड, पिन, सुरक्षा टोकन आणि अगदी बायोमेट्रिक स्कॅन यांचा देखील समावेश असतो. मल्टीफॅक्टर ऑथेंटिकेशन (एमएफए) (MFA) सुरक्षा वाढवते, कारण यामध्ये यूजर्सना एकापेक्षा जास्त पद्धती वापरून पडताळणे आवश्यक असते.

एकदा वापरकर्त्याची आयडेंटिटी (identity) पडताळल्यानंतर, ॲक्सेस कंट्रोल पॉलिसीज् विशिष्ट परवानग्या प्रदान करतात, ज्यामुळे युजरला पुढे जाण्याची परवानगी मिळते. संस्था त्यांच्या गरजेनुसार विविध ॲक्सेस कंट्रोल पद्धती वापरतात.

2.5.1 ॲक्सेस कंट्रोल (Access control) तत्त्वे (principles):ॲक्सेस कंट्रोलची तत्त्वे हे ठरवतात की कोणाला कोणते रिसोर्सेस ऍक्सेस (Resources access) करता येईल. ॲक्सेस कंट्रोल तत्त्वे ही नियमांचा एक संच आहे, जे ठरवतात की कोण रिसोर्सेसमध्ये ऍक्सेस (access) करू शकतात आणि ते कसे ऍक्सेस (access) करू शकतात. संवेदनशील माहितीचे संरक्षण करण्यासाठी आणि सुरक्षा मानकांचे पालन सुनिश्चित करण्यासाठी ही तत्त्वे महत्त्वपूर्ण आहेत.

ॲक्सेस कंट्रोल (Access control) ची मुख्य तत्त्वे (principles) येथे आहेत:

- **ऑथेंटिकेशन :** पासवर्ड, स्मार्ट कार्ड, टोकन किंवा बायोमेट्रिक डेटा (passwords, smart cards, tokens, or biometric data) वापरुन युजरचीआयडेंटिटी (identity) पडताळणे
- **ऑथोरायझेशन (Authorization):** भूमिका(role), गट किंवा इतर वैशिष्ट्यांच्या आधारे यूजर्सना ऍक्सेस (access) विशेषाधिकार प्रदान करणे
- **ऑडिटिंग (Auditing):** धोके किंवा धोरणाचे उल्लंघन शोधण्यासाठी सिस्टिम क्रियाकलापांवर (Acitivities) देखरेख ठेवणे
- **किमान विशेषाधिकाराचे तत्त्व:** एखादे कार्य पार पाडण्यासाठी आवश्यक असलेल्या गोष्टींपुरतेच रिसोर्सेसमध्ये ऍक्सेस (access) मर्यादित करणे.

- **धोरण-आधारित ॲक्सेस कंट्रोल :** कॉर्पोरेट धोरणांवर आधारित ॲक्सेस कंट्रोल आणि हक्कांचे मूल्यांकन करणे.

2.5.2 ॲक्सेस हक्क आणि परवानगी:

ॲक्सेस हक्क आणि परवानग्या म्हणजे यूजरला किंवा ॲप्लिकेशनला विशिष्ट विशेषाधिकार दिले जातात, ज्यामुळे त्यांना सिस्टिमवर काही काम करण्याची परवानगी मिळते, जसे की फाइल्स वाचणे, लिहिणे, हटविणे, सेटिंग्ज (settings) मध्ये बदल करणे किंवा विशिष्ट डेटा ॲक्सेस (data access) करणे. मूलत: युजर त्यांच्या दिलेल्या ऍक्सेस स्तराच्या आधारे सिस्टिम किंवा ॲप्लिकेशनमध्ये (system or application) काय करू शकतो आणि काय करू शकत नाही हे ठरवते ते.

ॲक्सेस हक्क आणि परवानग्यांबद्दल मुख्य मुद्दे:

कार्यप्रणाली(functionality) : परवानग्या एखाद्या रिसोर्सेसवर युजरला विशिष्ट क्रिया करण्याची परवानगी देतात, जसे की दस्तऐवजाचे " केवळ वाचन " किंवा " निर्माण आणि संपादन" प्रवेश (Read only or create and edit access).

युजरच्या भूमिका: ॲक्सेस (access) अधिकार सामान्यतः एक युजरच्या संस्थेतील भूमिकेनुसार दिले जातात, जे सुनिश्चित करतात की फक्त अधिकृत व्यक्तींना संवेदनशील माहितीला ॲक्सेस मिळू शकेल.

ग्रैन्युलर कंट्रोल (Granular control): सिस्टिम छोटया-छोटया परवानग्या लागू करू शकतात, ज्यामुळे प्रशासकांना वैयक्तिक फाइल्स, फोल्डर्स किंवा वैशिष्ट्यांवर वेगवेगळ्या यूजर्ससाठी विशिष्ट ॲक्सेस (access) स्तर सेट करण्याची परवानगी मिळते.

सुरक्षा परिणाम: डेटा सुरक्षा, अनधिकृत ॲक्सेस (access) रोखण्यासाठी आणि संवेदनशील माहितीचे संरक्षण करण्यासाठी ॲक्सेस (access) हक्कांचे योग्य व्यवस्थापन करणे महत्वाचे आहे.

2.5.3 ॲक्सेस (Access) नियंत्रण धोरणे (ॲक्सेस कंट्रोल पॉलिसीज) (Access control policies):

- विवेकाधीन ॲक्सेस (access) नियंत्रण (डिस्क्रेशनरी ॲक्सेस कंट्रोल) (डीएसी) (DAC)
- अनिवार्य ॲक्सेस (access) नियंत्रण (मँडेटरी ॲक्सेस कंट्रोल) (मॅक) (MAC)
- भूमिका-आधारित ॲक्सेस (access) नियंत्रण (रोल-बेस्ड ॲक्सेस कंट्रोल) (आरबीएसी) (RBAC)
- वैशिष्ट्य-आधारित ॲक्सेस (access) नियंत्रण (ऍट्रीबुट-बेस्ड ॲक्सेस कंट्रोल) (एबीएसी) (ABC)

2.5.3.1 विवेकाधीन ॲक्सेस (access) नियंत्रण (डिस्क्रेशनरी ॲक्सेस कंट्रोल) (डीएसी)(DAC):

डीएसी मॉडेल्स (DAC models) डेटा ओनरला (data owner) ॲक्सेस कंट्रोल (access control) ठरवण्याची परवानगी देतात, ज्यामध्ये यूजर्सनी निर्दिष्ट केलेल्या नियमांना ॲक्सेस (access) अधिकार प्रदान केले जातात. जेव्हा एखाद्या यूजरला सिस्टिममध्ये ॲक्सेस (access) दिला जातो, तेव्हा तो त्याला योग्य वाटेल तसे इतर यूजर्सना ॲक्सेस (access) देऊ शकतो. डीएसी हे ॲक्सेस कंट्रोल लिस्ट (एसीएल) (Access control list) वर आधारित आहे.

एसीएल लिस्ट (ACL List) तयार करते की कोणत्या यूजर्सना एखाद्या ऑब्जेक्टमध्ये ॲक्सेस (access) आहे आणि ते ऑब्जेक्टसह काय करू शकतात. एसीएल यूजर्स आणि परवानग्यांची लिस्ट तयार करेल. तुम्ही परवानग्या देऊ शकता किंवा विशिष्टपणे परवानग्या नाकारू शकता. नेटवर्क रिसोर्सेसमध्ये ॲक्सेस (access) नियंत्रित करण्यासाठी डीएसी मॉडेल दोन मुख्य संकल्पनांवर अवलंबून आहे.

विषय (सब्जेक्ट) (Subject): यूजर्स किंवा यूजर्स ग्रुप्स डीएसीद्वारे संरक्षित रिसोर्सेसमध्ये ॲक्सेस (access) शोधत आहेत.

ऑब्जेक्ट (Object): एक सिस्टिम रिसोर्स जसे की ॲप्लिकेशन किंवा नेटवर्कवर संग्रहित डेटा. डीएसी (DAC) हे ऑब्जेक्ट्सना ॲक्सेस देण्यासाठी सब्जेक्ट आयडेंटिफिकेशनवर (subject identification)अवलंबून असते. यूजर्सना त्यांच्या स्टेटसची आयडेंटिटी (identity)पटवणारी ऑथेंटिकेशन माहिती पुरवावी लागते, त्यानंतरच सिस्टिम ॲक्सेस देईल. त्यानंतर ॲक्सेस कंट्रोल सिस्टीम ठरवते की सब्जेक्टला विशिष्ट ऑब्जेक्टमध्ये ॲक्सेस (access) करण्यासाठी आवश्यक अधिकार आहेत की नाहीत.

डीएसी सिस्टिमचे (DAC system) मुख्य दोन प्रकार आहेत :

- **ॲक्सेस कंट्रोल लिस्ट (एसीएल) (ACL List):** ॲक्सेस कंट्रोल लिस्ट हे एक डॉक्युमेंट आहे ज्यामध्ये ऑथोराइज्ड यूजर्स बद्दल माहिती असते. हे ऍडमिनिस्ट्रेटर्सना प्रत्येक ऑब्जेक्टसाठी रुल-बेस्ड ॲक्सेस कंट्रोल सिस्टिम (Rule-based access control system) सेट करण्याची परवानगी देते. एसीएलमध्ये युजरचीआयडेंटिटी (identity)आणि प्रत्येक

युजरकडे असलेल्या विशेषाधिकारांचा समावेश आहे. रोल-बेस्ड ॲक्सेस कंट्रोल सिस्टिमचा (Role-based access control system) भाग म्हणून ते यूजर्स ग्रुप्सशी देखील जोडले जाऊ शकतात.

- **कॅपॅबिलिटी सिस्टिम्स (Capability systems):** या विकेंद्रित (डिसेन्ट्रलाइज्ड) सिस्टिम्स (Decentralised systems) एसीएलवर (ACL)अवलंबून नसतात. त्याऐवजी, ॲक्सेस हा त्या ॲक्सेस केलेल्या ऑब्जेक्टच्या आयडेंटिटीशी संबंधित असतो. उदाहरणार्थ, क्रिप्टोकरन्सी ओनर (Cryptocurrency owner) त्यांच्याकडे प्रायव्हेट-की (private-key)असल्यास त्यांच्या करन्सी ॲक्सेस करू शकतात. ईमेजर यूजर्स (Imager users)कडे प्रत्येक ईमेजसाठी हिडन यूआरएल असल्यास ते ऑब्जेक्टस एडिट करू शकतात.

दोन्ही प्रकार विवेकाधीन (डिस्क्रेशनरी)(discretionary) आहेत. ऑब्जेक्ट ओनर (object owner) यूजरच्या विशेषाधिकारांना मर्यादित करणे किंवा परवानगी देणे आणि विस्तारित करणे यासाठी एसीएल (ACL) बदलू शकतात. उदाहरणार्थ, काही ग्रुप्सना लेखनाचे विशेषाधिकार असू शकतात. इतरांना फक्त डेटाबेसमधील नोंदी वाचण्याची परवानगी असू शकते.

फायदे:

1. **युजर फ्रेंडली (User friendly) :** डेटा आणि परवानग्या व्यवस्थापित करणे डीएसीसह (DAC) सोपे आहे. युजर इंटरफेस (user interface) ऑपरेट करणे खूप सोपे आहे. त्यामुळे एकाच वेळी सर्व नियोजन करण्याची आवश्यकता नाही.
2. **फ्लेक्सिबल(Flexible) :** काम करताना अनेकदा सहकाऱ्यांसोबत डेटा शेअर (data share) करण्याची गरज भासते. डीएसी सिस्टिम (DAC system) कोणत्याही युजरला विशिष्ट माहितीचा ॲक्सेस मिळाल्यास इतरांना देखील ॲक्सेस देण्याची परवानगी देते. ज्यामुळे कार्य प्रोसेस (PROCESS)सुरळीत होते.
3. **ॲडमिनिस्ट्रेशनसाठी (Administration)कमी त्रास:** डीएसीला (DAC) नियमित देखभालीची आवश्यकता नसते आणि जास्त वेळ लागत नाही. डेटा शेअर करणे खूप सोपे आहे कारण प्रत्येक वेळी डेटा शेअर करण्याची आवश्यकता असताना ॲडमिनिस्ट्रेशनला हस्तक्षेप करण्याची आवश्यकता नसते.

तोटे:

1. **कमी सुरक्षित सिस्टिम (System):** एका व्यक्तीकडून दुसर्या व्यक्तीला ॲक्सेस दिला जाऊ शकतो, डीएसी (DAC)अंतर्गत डेटा फारसा सुरक्षित नसतो. त्यामुळे, प्रशासनासाठी एसीएल (ACL) वेळोवेळी पाहणे सोपे नाही. त्यामुळे संस्थेबाहेरील व्यक्तीला डेटा लीक (data leak) होऊ शकतो.
2. **डेटाचा ट्रॅक (Data track) ठेवणे कठीण:** डीएसी सिस्टिम (DAC system) केंद्रीकृत (centralized) नसल्यामुळे, ॲडमिनिस्ट्रेशनसाठी डेटा-फ्लो (Data flow) वर लक्ष ठेवण्याचा एकमेव मार्ग म्हणजे एसीएल (ACL) पाहणे. हे फक्त छोट्या संस्थेमध्ये सोयीस्कर आहे जिथे कर्मचारी कमी असतात.

2.5.3.2 मँडेटरी ॲक्सेस कंट्रोल (Mandatory access control) (मॅक) (MAC) :

मॅक प्रत्येक यूजर वर आणि ते ॲक्सेस करू इच्छित असलेल्या डेटा, रिसोर्सेस आणि सिस्टिम्स (data, resources and systems) वर कठोर धोरणे ठेवते. धोरणांचे व्यवस्थापन संस्थेचे ॲडमिनीस्ट्रेटर (administrator) करतात. यूजर्स परवानग्या बदलू शकत नाहीत, रद्द किंवा सेट करू शकत नाहीत. एमएसी (MAC) ही संस्थेतील खाजगी माहितीला ॲक्सेस देण्याची किंवा नाकारण्याची सिस्टिम आहे. मॅकचे इतर सिस्टिम्सपेक्षा वेगळेपण म्हणजे ते हायरारची पॅटर्नमध्ये (hierarchy pattern) काम करते. या सिस्टिमअंतर्गत, संपूर्ण टीमला त्यांच्या भूमिकांनुसार आणि जबाबदाऱ्यांनुसार आणि ते पाहू शकतात अश्या माहितीनुसार श्रेणींमध्ये विभागले पाहिजे. त्यासाठी इन्फॉर्मशन फ्लो (information flow) चे योग्य नियोजन करताना प्रशासनाने बरेच प्रयत्न करण्याची आवश्यकता आहे. सर्व काही योग्यरित्या सेट करण्याचा हा केवळ एकवेळचा प्रयत्न असेल, त्यानंतर केवळ पोझिशन / रोल (position / role) बदलानुसार अपडेट (update) आवश्यक असतील.

फायदे:

1. **उच्च-स्तरीय डेटा संरक्षण (आरबीएसी, मॅक आणि डीएसी सिस्टिम्समध्ये सर्वात सुरक्षित सिस्टिम):** मॅकसह, कोणीही खात्री करू शकते की त्यांचा सर्वात गोपनीय डेटा चांगल्या प्रकारे संरक्षित आहे आणि कोणत्याही प्रकारे डेटा लिकेज होत नाही.

2. **सेन्ट्रलाइज्ड डेटा (Centralised data) :** एकदा डेटा एखाद्या श्रेणीत सेट केल्यावर मुख्य ऍडमिनिस्ट्रेटर (administrator) शिवाय इतर कोणालाही त्याचे वर्गीकरण करता येत नाही. यामुळे संपूर्ण यंत्रणा केंद्रीकृत होऊन केवळ एका प्राधिकरणाच्या नियंत्रणाखाली येते.
3. **प्रायव्हसी (Privacy):** डेटा ऍडमिनिस्ट्रेटरद्वारे मॅन्युअली सेट केला जातो. अॅडमिनव्यतिरिक्त कोणीही कोणत्याही कॅटेगरीमध्ये यूजर अॅक्सेसच्या कॅटेगरी किंवा लिस्टमध्ये बदल करू शकत नाही. ते फक्त अॅडमिनच अपडेट करू शकतात.

तोटे:

1. **काळजीपूर्वक सेटिंग करणे:** मॅक ला चांगल्या प्रकारे सेट करणे आवश्यक आहे, अन्यथा ते कामकाजात गोंधळ निर्माण करू शकते. कारण कधी कधी एकच माहिती संस्थेतील सहकाऱ्यांमध्ये शेअर करणे आवश्यक असते, पण मॅक कोणालाही तसे करण्यापासून प्रतिबंधित करते.
2. **नियमित अपडेट आवश्यक:** जेव्हा नवीन डेटा ऍड (add) केला जातो किंवा जुना डेटा डिलीट (delete) केला जातो तेव्हा नियमित अपडेट करणे आवश्यक असते. प्रशासनाला मॅक सिस्टिम आणि एसीएलवर वेळोवेळी विचार करावा लागतो.
3. **लवचिकतेचा अभाव:** मॅक सिस्टम ऑपरेशनली फ्लेक्सिबल (flexible) नाही. सुरुवातीला सर्व डेटा इनपुट करणे आणि एसीएल तयार करणे हे सोपे काम नाही जे नंतर कोणतीही समस्या निर्माण करणार नाही.

2.5.3.3 रोल-बेस्ड अॅक्सेस कंट्रोल (Role based access control) (आरबीएसी) (RBAC) :

आरबीएसी यूजर्स ग्रुप्स, यूजर्सकडे असलेल्या भूमिका आणि यूजर्सनी केलेल्या कृतींच्या आधारे परवानग्या तयार करते. यूजर्स त्यांना दिलेल्या भूमिकेवर आधारित कोणतीही कृती करू शकतात आणि त्यांना त्यांच्या नेमून दिलेल्या अॅक्सेस कंट्रोल स्तरात बदल करण्याची परवानगी नाही. रोल-बेस्ड अॅक्सेस कंट्रोल मॅनेजमेंट (**Role based access control management**) ही एक सिस्टिम आहे ज्याद्वारे कंपनीचे व्यवस्थापन एखाद्या कंपनीतील कर्मचाऱ्याच्या स्थितीवर किंवा त्याच्या / तिच्या कामाच्या प्रोफाइलवर अवलंबून विशिष्ट क्षेत्र किंवा माहितीवर अॅक्सेस (access) नियंत्रित किंवा प्रतिबंधित करू शकते.

अॅक्सेस कंट्रोल मॅनेजमेंटच्या या प्रकाराअंतर्गत, कंपनीतील कर्मचाऱ्यांची स्थिती त्यांच्याबरोबर कोणती माहिती शेअर केली पाहिजे हे ठरवते. काही माहिती वरिष्ठ व्यवस्थापनाकडेच ठेवणे आवश्यक असल्याने आणि आरोग्य सेवा संस्था, वित्तीय संस्था अशा काही विशिष्ट क्षेत्रांमध्ये व्यवस्थापनाला डेटा रूम्स, तिजोरी, लॉकर रूम, मीटिंग रूम (data rooms, vaults, locker room, meeting room) इ. ठिकाणी अॅक्सेस मर्यादित ठेवावा लागतो, कारण असा अॅक्सेस ठराविक लोकांनाच देणे आवश्यक आहे.

रोल-बेस्ड अॅक्सेस कंट्रोल सोल्यूशन मॅनेजमेंटचे (Role based access control solution management) फायदे :

- **कामाची कार्यक्षमता सुधारते :** आरबीएसीचा वापर केल्याने कार्यालयीन कर्मचाऱ्यांच्या भूमिकेतील बदलानुसार कार्यालय व्यवस्थापनाला अॅक्सेस (access) बदलणे अधिक सोपे जाते. प्रत्येकाला अॅक्सेस (access) देण्यापेक्षा आणि बाहेर पडण्यापेक्षा आणि प्रत्येक वेळी मान्यता देण्यापेक्षा हे करणे अधिक सोयीस्कर आहे.
- **कोणत्याही इन्फॉरमेशन लिकेजपासून (Information leakage) सुरक्षा :** विशिष्ट माहिती किंवा रूमला (room) अॅक्सेस (access) केवळ जबाबदार आणि विश्वासार्ह लोकांच्या विशिष्ट ग्रुपलाच दिला जाईल, यामुळे कोणत्याही प्रकारच्या गोपनीय माहितीचे लिकेज किंवा कोणत्याही अयोग्य व्यक्तीचा अॅक्सेस (access) होण्याची शक्यता कमी होते.
- **वेळेची बचत :** आरबीएसी मॅनेजमेंट अंतर्गत कोणत्याही माहिती/ रूमला अॅक्सेस (access) मिळवण्यासाठी केवळ कार्ड किंवा पासवर्ड (सिस्टीम कार्यक्षमतेनुसार) आवश्यक असतो ज्यामुळे वेळेची बचत होते. हे पूर्वीच्या पद्धतींच्या विरूद्ध आहे ज्यात सुरक्षा अधिकारी एखाद्याची क्रेडेन्शियल्स (credentials) विचारतात आणि पडताळणी करतात आणि नंतर सर्व काही ठीक वाटल्यानंतर त्या व्यक्तीला अॅक्सेस (access) दिला जातो, जे खूप वेळखाऊ आहे.
- **रेकॉर्ड ठेवण्यास मदत करते :** आरबीएसी सिस्टिम केवळ सुरक्षितता सुनिश्चित करत नाही तर अॅक्सेस (access) आणि बाहेर पडण्याचा डेटा देखील रेकॉर्ड करते ज्यामुळे कामाच्या तासांचे विश्लेषण (तपास) करणे देखील सोपे होते.

रोल-बेस्ड ॲक्सेस कंट्रोल सोल्यूशन मॅनेजमेंटचे (Role based access control solution management) तोटे :

- **लार्ज स्केल ऑर्गनायझेशनसाठी (Large-Scale Organization) कॉम्प्लेक्स (complex) :** मोठ्या संस्थेत हजारो कर्मचारी वेगवेगळ्या भूमिकांमध्ये काम करतात. आरबीएसीसह मोठ्या संख्येने कर्मचाऱ्यांसाठी ॲक्सेस व्यवस्थापित करणे कठीण होऊ शकते.
- **व्यवस्थापन भूमिकेपुरते मर्यादित :** आरबीएसी व्यवस्थापनांतर्गत निर्बंध केवळ व्यक्तींच्या भूमिकेच्या आधारे निश्चित केले जाऊ शकतात, त्यांच्याद्वारे पार पडलेल्या क्रिया किंवा त्यांनी केलेल्या ऑपरेशनवर नव्हे.

2.5.3.4 ॲट्रीबुट-बेस्ड ॲक्सेस कंट्रोल (Attribute based access control) (एबीएसी) (ABAC) : एबीएसी एक ॲक्सेस कंट्रोल मॉडेल (Access control model) आहे जे यूजर्स, रिसोर्सेसआणि एन्व्हायरॉन्मेंटल कंडिशन्सशी (users, resources, and environmental conditions) संबंधित वैशिष्ट्यांवर आधारित अधिकृत निर्णय घेते, ज्यामुळे ॲक्सेस (access) परवानग्यांवर गतिशील आणि सूक्ष्म नियंत्रण ठेवता येते.

- **ॲट्रीबुट-बेस्ड ॲक्सेस कंट्रोल (Attribute based access control) (एबीएसी) चे ॲट्रिब्युटस (Attributes) :**

एबीएसीमध्ये ॲट्रिब्युटस हे मुख्य घटक आहेत जे ॲक्सेस कंट्रोल कोणत्या अटींखाली केले जातील हे ठरवतात. त्यांचे चार मुख्य प्रकारांमध्ये वर्गीकरण केले जाते:

1. युजर ॲट्रिब्युटस (User attribute) :

ॲक्सेस रिक्वेस्ट करणाऱ्या व्यक्तीच्या वैशिष्ट्यांशी संबंधित उदाहरणे :

- युजर आयडी
- टायपोलॉजी (उदा., व्यवस्थापन, अधीनता)
- विभाग
- सिक्युरिटी क्लिअरन्स लेव्हल
- ग्रुप मेंबरशिप

2. रिसोर्सेस ॲट्रिब्युटस (Resources Attribute):

विशिष्ट ग्रुपने त्याच्या उद्दिष्टांकरिता वापरासाठी वापरलेल्या रिसोर्सेसची वैशिष्ट्ये. उदाहरणांमध्ये हे समाविष्ट आहे:

ॲक्शन ॲट्रिब्युटस (Action Attributes):

त्या क्रियेच्या पूर्ततेशी निगडित काही ॲट्रिब्युटस (Attributes). उदाहरणांमध्ये हे समाविष्ट आहे:

- ॲक्शन टाईप (उदा.; वाचा, लिहा, डिलीट करा)
- एचटीटीपी (उदा., गेट, पोस्ट (GET, POST))
- सर्व सीआरयुडी ऑपरेशन्स (CRUD operations) – सी-क्रिएट (C - Create) करा, आर-रीड (R - Read), यु-अपडेट (U - Update) करा आणि डी-डिलीट (D - Delete).

पर्यावरण संबंधित ॲट्रिब्युटस :

ज्या नागरिकाने प्रवेशाची मागणी केली आहे, त्या नागरिकाच्या इतिहासाशी संबंधित माहिती. उदाहरणांमध्ये हे समाविष्ट आहे:

- दिवसाची वेळ
- तारीख
- डिव्हाइसचा आयपी ॲड्रेस (Device IP Address), डिव्हाइसचे भौगोलिक स्थान (Device geographical location)इ.
- डिव्हाइस प्रकार (Device type)
- नेटवर्क संरक्षणाची स्थिती (उदाहरणार्थ - व्हीपीएन, फायरवॉल (VPN, Firewall)).

ॲट्रीबुट- बेस्ड ऑथेंटिकेशनचे (Attribute-based Authentication) फायदे:

1. ग्रॅन्युलर ॲक्सेस कंट्रोल (granular access control) : पारंपारिक मॉडेल्सच्या उलट, जे व्यापक भूमिका (role) किंवा गटांवर आधारित प्रवेशास परवानगी देतात, एबीएसी विशिष्ट वैशिष्ट्यांवर आधारित ॲक्सेस हक्क निश्चित करू शकते.

तपशीलाच्या या पातळीमुळे अत्यंत ग्रॅन्युलर (granular) पातळीवर ॲक्सेस नियंत्रित करणे शक्य होते, ज्यामुळे अनधिकृत ॲक्सेस चा धोका कमी होतो.

2. यूझर्सचं फास्ट ऑनबोर्डिंग (Fast on boarding of users) : एबीएसीसह, आपण वैशिष्ट्यांवर आधारित ॲक्सेस पॉलिसिज (access policies) निश्चित करू शकता, आणि ह्या पॉलिसिज त्या गुणधर्म असलेल्या कोणत्याही यूझरवर लागू केली जाऊ शकतात. याचा अर्थ, प्रत्येक नवीन यूझरसाठी ॲक्सेस राईट्स (access rights) मॅन्युअली असाइन (manually assign) करण्याची गरज नाही, जी एक वेळखाऊ प्रोसेस (process) असू शकते.

ॲट्रीबुट- बेस्ड ऑथेंटिकेशनचे तोटे :

1. **एबीएसी मॉडेलची कॉम्प्लेक्सिटी (Complexity of the ABAC model):** एबीएसीचे पहिले आणि सर्वात प्रमुख आव्हान म्हणजे त्याची कॉम्प्लेक्सिटी. एबीएसी मॉडेलची कॉम्प्लेक्सिटी ते ऑफर करणार्या लवचिकतेमुळे उद्भवते, ज्यामुळे विविध ॲट्रिब्युट्सचे संयोजन करून ॲक्सेस कंट्रोल पॉलिसिज (access control policies) निश्चित करता येतात.
2. **पॉलिसी निर्मिती आणि व्यवस्थापन:** एबीएसी सिस्टीमसाठी पॉलिसिज तयार करण्यासाठी संस्थेच्या रिसोर्सेस, संभाव्य यूजर्स आणि ॲक्सेसची आवश्यकता असलेल्या विविध संदर्भांची सखोल माहिती असणे आवश्यक आहे. ही प्रोसेस (process) वेळखाऊ असू शकते आणि महत्त्वपूर्ण कौशल्याची आवश्यकता असते.

डीएसी, मॅक, आरबीएसी आणि एबीएसी (DAC, MAC, RBAC and ABAC) मधील मुख्य फरक:

डीएसी:

- **कंट्रोल (Control)**: यूजर्सना त्यांचा डेटा कोण ॲक्सेस करू शकेल हे ठरविण्याचा पूर्ण अधिकार आहे.
- **फ्लेक्सिबिलिटी (Flexibility)**: उच्च फ्लेक्सिबिलिटी, कारण यूजर्स ॲक्सेस परमिशन्स सहजपणे बदलू शकतात.
- **सेक्युरिटी (Security)**: अनियंत्रित शेअरींगच्या शक्यतेमुळे कमी सुरक्षित मानली जाते.

मॅक:

- **कंट्रोल (Control)** : केंद्रीय प्राधिकरणाने सेट केलेल्या पूर्वनिर्धारित पॉलिसिजद्वारे ॲक्सेस काटेकोरपणे नियंत्रित केला जातो.
- **फ्लेक्सिबिलिटी (Flexibility)** : कमी फ्लेक्सिबिलिटी, कारण यूजर्स ॲडमिनिस्ट्रेटरच्या हस्तक्षेपाशिवाय ॲक्सेस राईट्स बदलू शकत नाहीत.
- **सेक्युरिटी (Security)** : पॉलिसिजच्या काटेकोर अंमलबजावणीमुळे उच्च सुरक्षा.

आरबीएसी:

- **कंट्रोल (Control)**: यूजर्सना अशा भूमिका दिल्या जातात ज्यामुळे त्यांच्या रिसोर्सेसमध्ये ॲक्सेस (access) स्तर निश्चित होतो.
- **फ्लेक्सिबिलिटी (Flexibility)**: मध्यम फ्लेक्सिबिलिटी, कारण ॲक्सेस (access) स्तर समायोजित करण्यासाठी भूमिका बदलल्या जाऊ शकतात.
- **सेक्युरिटी (Security)**: चांगली सुरक्षा, कारण ॲक्सेस (access) पूर्वनिर्धारित भूमिकांच्या आधारे व्यवस्थापित केला जातो.

एबीएसी:

- **कंट्रोल (Control)**: यूजर्स, रिसोर्सेस आणि पर्यावरणाच्या विविध ॲट्रिब्युट्सचे मूल्यांकन करून ॲक्सेस (access) निश्चित केला जातो.
- **फ्लेक्सिबिलिटी (Flexibility)**: खूप उच्च फ्लेक्सिबिलिटी, कारण प्रवेशाचे निर्णय संदर्भाच्या आधारे गतिशीलपणे घेतले जाऊ शकतात.
- **सेक्युरिटी (Security)**: योग्यरित्या कॉन्फिगर (configure) केल्यास उच्च सुरक्षा प्रदान करू शकते, कारण ते अधिकृततेसाठी अनेक घटक विचारात घेते.

References:

1. Information Systems Security Second Edition By Nina Godbole (John Wiley Isbn-13: 978-8126564057)
2. Cryptography and Information Security By V.K.Pachghare – Prentice Hall India
3. Cryptography and Network security Third Edition By Atul Kahate- McGraw-Hill; Fourth edition ISBN-13: 978-9353163303
4. Computer Security Principles and Practice, Third Edition BY William Stallings, Lawrie Brown Pearson. ISBN-13: 978-0-13-377392-7

युनिट - 3
क्रिप्टोग्राफीची मूलतत्त्वे
(Fundamentals of Cryptography)

विषय निष्पत्ती : (Course Outcome):

CO3: दिलेल्या मजकुरासाठी मूलभूत एन्क्रिप्शन/डिक्रिप्शन (Encryption/Decryption) तंत्रे लागू करा.

घटक निष्पत्ती (Theory Learning Outcomes)

1. एन्क्रिप्शन (Encryption) आणि डिक्रिप्शनची (Decryption) प्रोसेस (Process)स्पष्ट करा
2. दिलेल्या पॅरामीटर्सच्या (Parameters) आधारे सममित (सममितीय) (Symmetric) आणि असममित (Asymmetric) क्रिप्टोग्राफीची (Cryptography) तुलना करा.
3. मजकुरावर दिलेल्या प्रतिस्थापन तंत्रांचा वापर करा.
4. मजकूरावर दिलेले ट्रान्सपोजिशन (transposition) तंत्र लागू करा.
5. स्टेग्नोग्राफीचे (Stegnography) चरण -दर -चरण स्पष्ट करा.

3.1 परिचय

क्रिप्टोग्राफी (Cryptography) म्हणजे प्रतिकुल परिस्थितीत सुरक्षित संदेशाची देवाणघेवाण करण्यासाठी वापरले जाणारे तंत्रज्ञान. सामान्यतः, क्रिप्टोग्राफी (Cryptography) म्हणजे प्रोटोकॉल (protocol) तयार करणे आणि त्यांचे विश्लेषण करणे असते. यामुळे तृतीय पक्षांना (third party) किंवा लोकांना खाजगी संदेश वाचण्यापासून प्रतिबंधित करते.

1. **साधा मजकूर (Plain Text):-** साधा मजकूर एक संदेश दर्शवितो जो प्रेषक, प्राप्तकर्ता आणि संदेशात ॲक्सेस (Access) मिळविणाऱ्या इतर कोणालाही समजू शकतो.
2. **सायफर मजकूर (Cipher Text):-**सायफर मजकूर एनक्रिप्शन अल्गोरिदम (Encryption Algorithm) वापरुन प्लेन टेक्स्टमधून (Plain text) रूपांतरित केलेला एनक्रिप्टेड (Encrypted) मजकूर आहे.
3. **क्रिप्टोग्राफी (Cryptography):** - क्रिप्टोग्राफी (Cryptography) हे साध्या मजकूरास सायफर (Cipher) मजकूरात रूपांतरित करून संप्रेषण सुरक्षित करण्याचे तंत्र आहे.
4. **क्रिप्टोॲनालिसिस (Cryptoanalysis):-** क्रिप्टॅनालिसिस (Cryptoanalysis) रिअल की (Real Key) न वापरता सायफर (Cipher), कोड आणि एनक्रिप्टेड (Encrypted) मजकूराचे विश्लेषण आणि डिक्रिप्टिंगचा (decrypting) अभ्यास आणि प्रोसेस (Process)आहे.
5. **क्रिप्टोलॉजी (Cryptology):-** क्रिप्टोलॉजी (Cryptology) म्हणजेच गुप्तलेखन किंवा गुप्तसंकेतशास्त्र. हे एक शास्त्र आहे ज्यामध्ये डेटा किंवा माहितीला गुप्त ठेवण्यासाठी विविध तंत्रज्ञानांचा वापर केला जातो.
   क्रिप्टोलॉजी मध्ये क्रिप्टोग्राफी (Cryptography) आणि क्रिप्ट (Crypt) विश्लेषण समाविष्ट आहे. ज्यामध्ये डेटा किंवा माहितीला गुप्त ठेवण्यासाठी विविध तंत्रज्ञानांचा वापर केला जातो.

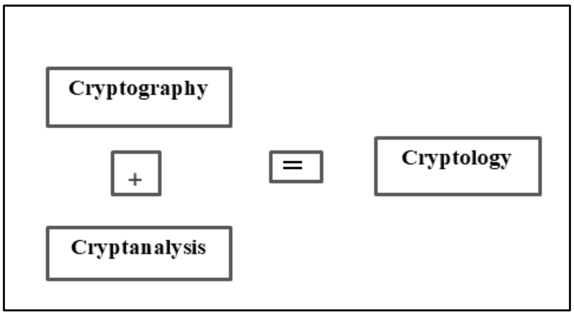


Figure. 3.1 Cryptology

6. **एन्क्रिप्शन (Encryption)**:- सायफर मजकूर संदेशामध्ये (Cipher text message) साधा मजकूर एन्कोडिंग (Plain text encoding) करण्याची प्रक्रिया एन्क्रिप्शन (encryption) म्हणून ओळखली जाते.

7. **डिक्रिप्शन (Decryption)**:- सायफर मजकूर संदेशास (Cipher text message) साध्या मजकूर (plain text) किंवा मूळ मजकूरामध्ये रूपांतरित करण्याची प्रक्रिया डिक्रिप्शन (decryption) म्हणून ओळखली जाते.

क्रिप्टोग्राफिक सिस्टम (Cryptographic System)

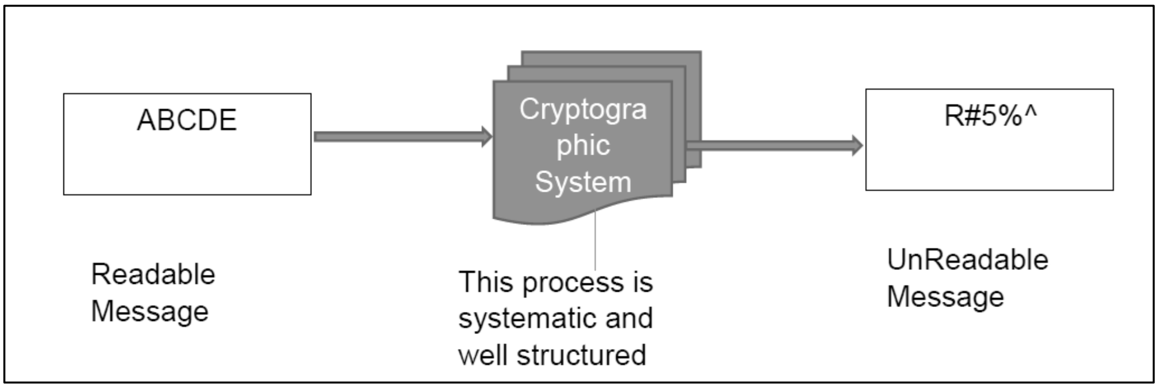


Figure. 3.2 Cryptographic System(Courtesey:Cryptography and Network security Third Edition By Atul Kahate)

क्रिप्टोऍनालिसिस सिस्टम (Cryptoanalysis System)

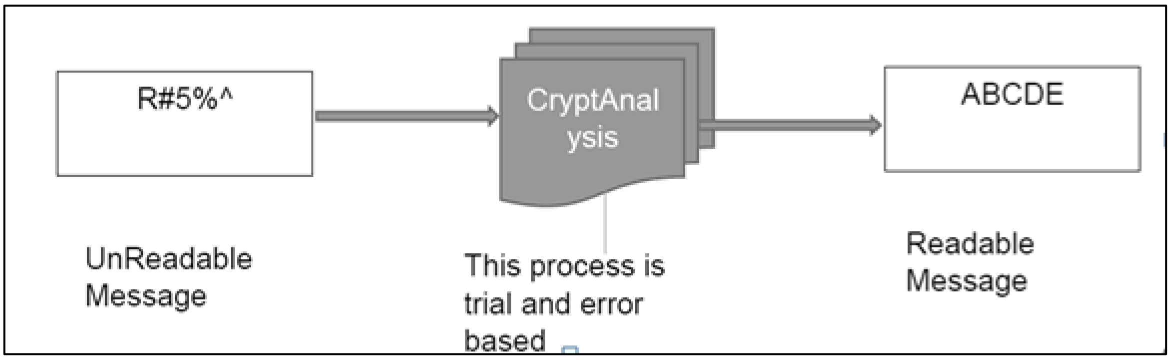


Figure. 3.3 Cryptoanalysis System(Courtesey:Cryptography and Network security Third Edition By Atul Kahate)

क्रिप्टोग्राफीचे एप्लिकेशन्स (Applications of Cryptography)**:**

1.डेटा लपविणे (data hiding)**:** क्रिप्टोग्राफीचा (cryptography) मूळ वापर म्हणजे लिहिलेले काहीतरी लपविणे.

२. डिजिटल कोड (Digital code)**:** क्रिप्टोग्राफी (Cryptography) ही सॉफ्टवेअर (software), ग्राफिक्स (graphics) किंवा व्हॉईस (voice) वर देखील लागू केली जाऊ शकते, ती डिजिटल (digital) कोड केलेल्या कोणत्याही गोष्टीवर लागू केली जाऊ शकते.

3. बँकिंगमधील इलेक्ट्रॉनिक पेमेंट्स (electronic payments banking): जेव्हा इलेक्ट्रॉनिक पेमेंट्स (electronics payment) नेटवर्कद्वारे (network)पाठविले जातात, तेव्हा सर्वात मोठा धोका म्हणजे पेमेंट मेसेजमध्ये बदल होईल किंवा बनावट मेसेज सादर केले जातील आणि कोणीतरी मेसेज वाचले जाण्याचा धोका किरकोळ महत्वाचा असू शकतो.

4. संदेश प्रमाणीकरण (Message Authentication):

एखाद्या व्यक्तीस नेटवर्कमध्ये हस्तक्षेप करून संदेश बदलण्यापासून संपूर्णपणे रोखता येणं शक्य नाही, परंतु जर असे झाले तर ते नक्कीच शोधले जाऊ शकते. प्रसारित संदेशाची अखंडता तपासण्याच्या या प्रक्रियेस बऱ्याचदा संदेश प्रमाणीकरण (Message Authentication) म्हणतात. क्रिप्टोग्राफीच्या (cryptography) वापरामधील सर्वात अलीकडील आणि उपयुक्त विकास म्हणजे डिजिटल स्वाक्षरी (digital signature).

5. मोबाइल बँकिंग (mobile banking), एटीएम (ATM),क्रेडिट कार्ड (credit card)

6. ईमेल (Email) ईकॉमर्स (Ecommerce), इलेक्ट्रॉनिक पेमेंट (electronic payment) गेटवे (gateway)

3.2 क्रिप्टोग्राफीचे (Cryptography) दोन प्रकार आहेत.

- सिमेट्रिक क्रिप्टोग्राफी (Symmetric Cryptography)
- असिमेट्रिक क्रिप्टोग्राफी (Asymmetric Cryptography)

3.2.1 सिमेट्रिक क्रिप्टोग्राफी (Symmetric Cryptography) : सिमेट्रिक क्रिप्टोग्राफी (Symmetric cryptography) मधे एकच सेम सिक्रेट की (Same secret key) मॅसेज एनक्रिप्ट (encrypt) आणि डिक्रिप्ट (decrypt) करण्यासाठी वापरतातं. म्हणूनच याला सिंगल की किंवा सीक्रेट की किंवा सामायिक की अल्गोरिदम म्हणून देखील ओळखले जाते.

सेन्डर (sender) आणि रिसिव्हर (receiver) एन्क्रिप्टेड डेटा वाचण्यासाठी सेम की(key) वापरतातं. की (key) फक्त सेन्डर (sender) आणि रिसिव्हर (receiver) लाच माहीत असते, इतर कोणालाही माहीत नसते.

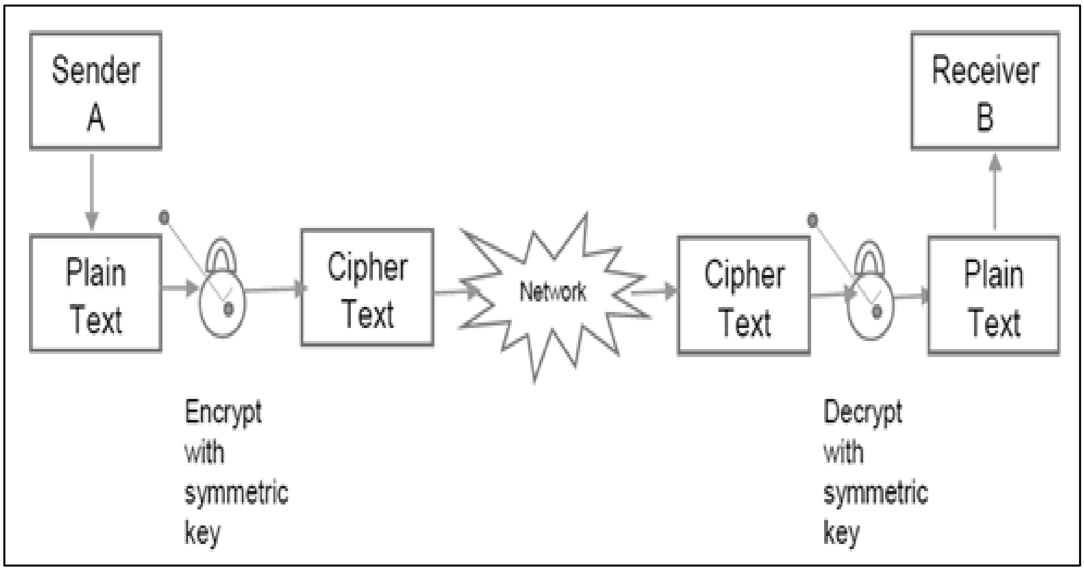


Figure. 3.4 Symmetric Cryptography(Courtesey:Cryptography and Network security Third Edition By Atul Kahate)

सिमेट्रिक की क्रिप्टोग्राफीची कार्यप्रणाली: (Symmetric Cryptography)

1. **की निर्मिती (Key Generation):**– एक गुप्त की (Secret Key) तयार केली जाते जी पाठवणारा (Sender) आणि प्राप्त करणारा (Receiver) यांच्याकडे असते.
2. **एनक्रिप्शन (Encryption):**– सेंडर (Sender) आपल्या मूळ संदेशाला (Plaintext) त्या गुप्त की च्या मदतीने एनक्रिप्ट करून सायफर टेक्स्ट (Ciphertext) स्वरूपात बदलतो.
3. **संप्रेषण (Transmission):**– हा सांकेतिक संदेश (cipher text) नेटवर्कवर पाठवला जातो.
4. **डीक्रिप्शन (Decryption):**– रिसिव्हर त्याच गुप्त की (secret key) च्या मदतीने सांकेतिक संदेशाचे (cipher text) डीक्रिप्शन (Decryption) करून मूळ संदेश (Plain Text) वाचतो.

सिमेट्रिक क्रिप्टोग्राफीचे (Symmetric Cryptography): फायदे:

1. सोपे (Easy):- या प्रकारचे क्रिप्टोग्राफी वापरण्यास सुलभ आहे. सर्व वापरकर्त्यांना सिक्रेट की (Secret key) शेयर करावी लागेल आणि नंतर संदेश एनक्रिप्ट (Encrypt) आणि डिक्रिप्ट (Decrypt) करायचा.
2. वेगवान (Fast):-हे तंत्र असिमेट्रिक की क्रिप्टोग्राफीपेक्षा (Asymmetric key Cryptography) बरेच वेगवान आहे.
3. कमी संगणक संसाधने वापरते (Uses Less Computer Resources):- सार्वजनिक की एन्क्रिप्शनच्या (Public Key Encryption) तुलनेत सिमेट्रिक की एन्क्रिप्शनला (Symmetric key Encryption) बऱ्याच संगणक संसाधनांची (Computer Resources) आवश्यकता नसते.
4. व्यापक संदेश सुरक्षा तडजोड प्रतिबंधित करते (Prevents Widespread Message Security Compromise):- प्रत्येक भिन्न पार्टीशी (Different party) संवाद साधण्यासाठी एक वेगळी सिक्रेट (Secret key) की वापरली जाते.

एखाद्या की (key) शी तडजोड केली असल्यास, केवळ सेन्डर(sender) आणि रिसिव्हर (receiver) च्या विशिष्ट जोडीमधील मेसेज (message) वर परिणाम होतो.

सिमेट्रिक (Symmetric) क्रिप्टोग्राफीचे तोटे :

1. सिक्रेट की एक्सचेंजसाठी **(**Secret Key Exchange**)**सुरक्षित कम्युनिकेशन चॅनेलची (Communication Channel) आवश्यकता**:-** सुरुवातीस सिक्रेट की (key) शेयर करणे सिमेट्रिक की एन्क्रिप्शनमध्ये मध्ये समस्या आहे. हे अशा प्रकारे एक्सचेंज करावे लागेल की ते सिक्रेट (Secret)राहील.
2. बऱ्याच कीज (Many keys) **:** प्रत्येक भिन्न पार्टीशी कम्युनिकेशन (communication) साधण्यासाठी एक नवीन सिक्रेट (Secret key)की उत्पन करावी लागेल. त्यामुळे या सर्व कीज (keys) व्यवस्थापित करणे आणि सुनिश्चित करण्यात समस्या निर्माण होते.
3. ओरिजिनल (original) आणि संदेशाच्या सत्यतेची हमी दिली जाऊ शकत नाही**:-** सेन्डर (Sender) आणि रिसिव्हर (receiver) दोघेही समान की (same key) वापरत असल्याने संदेश एखाद्या विशिष्ट वापरकर्त्याकडून आला असल्याचे सत्यापित केले जाऊ शकत नाही.

सिमेट्रिक क्रिप्टोग्राफीचे उदाहरण (Symmetric Cryptogrphy Examples**):**

1. AES (Advanced Encryption Standard) **आणि** DES (Data Encryption Standard) **हे प्रसिद्ध सिमेट्रिक** (Symmetric Encryption) **एनक्रिप्शन अल्गोरिदम** (Algorithm) **आहेत.**
2. **ही क्रिप्टोग्राफी** (Cryptogrphy) **वेगवान आणि कार्यक्षम असली तरी, मोठ्या संख्येने युजर्ससाठी** (Users) **असिमेट्रिक की क्रिप्टोग्राफी** (Asymmetric Key Cryptogrphy) **अधिक सुरक्षित मानली जाते.**

सिमेट्रिक क्रिप्टोग्राफीचे प्रकार (Symmetric Cryptogrphy Types**):**

1. ब्लॉक सायफर (Block Cipher**) :-** ह्या एन्क्रिप्शन (Encryption) तंत्रा मधे डेटाचे (data) 64 बिट ब्लॉक (block)एका वेळी एन्क्रिप्शन अल्गोरिदमसह (Encryption Algorithm) एनक्रिप्ट (Encrypt) केले जातात. (उदा. AES, DES)
2. स्ट्रीम सायफर **(**Stream Cipher**) :-** एकावेळेला साध्या मजकूर डेटाचा (data) लहान ब्लॉक (block) म्हणजेच बिट (bit) किंवा बाइट (byte) एनक्रिप्ट (Encrypt)करते. (उदा. RC4)

की वितरण (Key distribution):-

कि डिस्ट्रिब्युशन (Key distribution) सोडवण्याचे 2 मार्ग आहेत

एक मार्ग म्हणजे फिज़िकल किज (Physical Keys) ची देवाणघेवाण करणे. सिक्रेट कि (secret key) वैयक्तिकरित्या थर्ड पार्टी (Third party)कडे सोपविल्या जातात, जे मॅन्युअल (manual) आहे.

दुसरा मार्ग म्हणजे कीज वितरित (key distribution) करण्यासाठी “विश्वसनीय की वितरण केंद्र” वापरणे, एक विश्वासू नेटवर्क (network) अस्तित्व ज्याच्याशी एखाद्याने सिक्रेट की (Secret Key) शेयर केली आहे.

की मॅनेजमेंट (Key Management):- की मॅनेजमेंट **(**Key management**)**म्हणजे संवेदनशील डेटाचे (data) संरक्षण करण्यासाठी क्रिप्टोग्राफिक अल्गोरिदममध्ये (Cryptography algorithm) वापरल्या जाणाऱ्या क्रिप्टोग्राफिक की (cryptographic key) तयार करणे, संचयित करणे, वितरण करणे आणि व्यवस्थापित करण्यात गुंतलेल्या प्रक्रिया आणि प्रक्रियेचा संदर्भ आहे. हे सुनिश्चित करते की संवेदनशील डेटाचे (data) संरक्षण करण्यासाठी वापरल्या जाणाऱ्या कीज (keys)अनधिकृत प्रवेशा पासून सुरक्षित ठेवल्या आहेत.

3.2.2 असिमेट्रिक क्रिप्टोग्राफी (Asymmetric Cryptography): असिमेट्रिक क्रिप्टोग्राफी (Asymmetric Cryptography) मधे एक की सार्वजनिक (public key) एनक्रिप्ट (Encrypt)करण्यासाठी वापरतातं आणि डिक्रिप्ट (Decrypt) करण्यासाठी दुसरी(different) की (खाजगी की)(private key) वापरतातं. असिमेट्रिक क्रिप्टोग्राफीला (Asymmetric Cryptography) पब्लिक की क्रिप्टोग्राफी (Public Key Cryptography) देखील म्हणतात. रिसिव्हरच्या (Receivers) सार्वजनिक कीसह संदेश एनक्रिप्ट (Encrypt)करून रिसिव्हर (Receiver) सिक्रेट (Secret) संदेश पाठवू शकतात.

या प्रकरणात, केवळ रिसिव्हर (Receiver) संदेश डिक्रिप्ट (Decrypt) करू शकतो, कारण केवळ त्या वापरकर्त्यास आवश्यक की (Key) मध्ये ॲक्सेस (access) असणे आवश्यक आहे. असिमेट्रिक क्रिप्टोग्राफीचा (Asymmetric Cryptography) मुख्य फायदा म्हणजे कीची (Key) सुरक्षा.

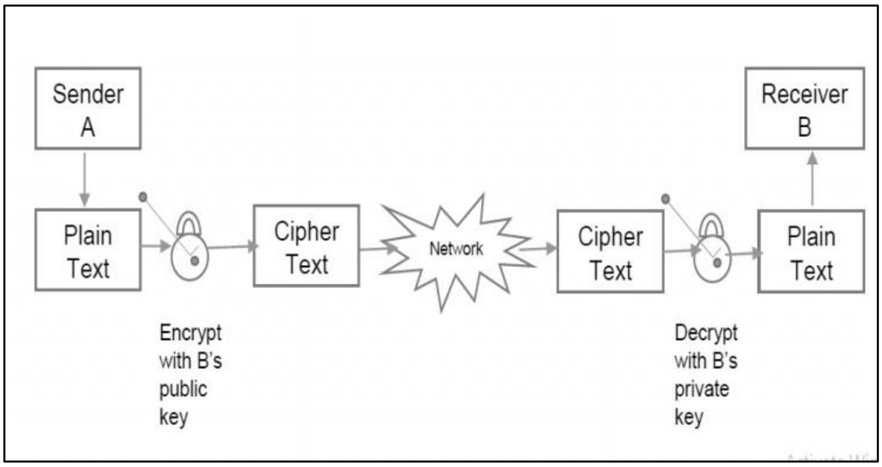


Figure. 3.5 Asymmetric Cryptography(Courtesey:Cryptography and Network security Third Edition By Atul Kahate)

असिमेट्रिक क्रिप्टोग्राफीची (Asymmetric Cryptography) कार्यप्रणाली:

1. की निर्मिती (Key Generation): प्रत्येक वापरकर्त्यासाठी दोन की (Key) तयार केल्या जातात.
   - पब्लिक की (Public Key)–जी इतरांसोबत शेअर करता येते.
   - प्रायव्हेट की (Private Key)–जी गुप्त ठेवली जाते.
2. एनक्रिप्शन (Encryption):
   - पाठवणारा (Sender) प्राप्तकर्त्याची पब्लिक की वापरून संदेश एनक्रिप्ट करतो.
   - एकदा संदेश एनक्रिप्ट (Encrypt) झाल्यावर तो फक्त त्या विशिष्ट प्राप्तकर्त्याद्वारे डीक्रिप्ट (Decrypt) केला जाऊ शकतो.
3. संप्रेषण (Transmission):एनक्रिप्टेड (Encrypted) संदेश सुरक्षितपणे नेटवर्कवर (network) पाठवला जातो.
4. डीक्रिप्शन (Decryption): प्राप्तकर्ता (Receiver) आपल्या प्रायव्हेट की (Private Key) च्या मदतीने संदेश डीक्रिप्ट (message decrypt) करतो आणि मूळ माहिती मिळवतो.

असिमेट्रिक क्रिप्टोग्राफीचे (Asymmetric Cryptography)उदाहरण:

1. RSA (Rivest-Shamir-Adleman) – सर्वात प्रसिद्ध आणि सुरक्षित असिमेट्रिक एनक्रिप्शन अल्गोरिदम (Encryption Algorithm).
2. ECC (Elliptic Curve Cryptography) – अधिक सुरक्षित आणि कार्यक्षम अल्गोरिदम, जो लहान की साइजमध्ये अधिक सुरक्षितता प्रदान करतो.
3. DSA (Digital Signature Algorithm) – डिजिटल स्वाक्षरीसाठी वापरण्यात येणारा अल्गोरिदम.

असिमेट्रिक (Asymmetric) क्रिप्टोग्राफीचे फायदे:

1. एलिमिनेट की वितरण (Eliminate key Distribution):- असिमेट्रिक (Asymmetric) क्रिप्टोग्राफी किंवा सार्वजनिक की क्रिप्टोग्राफीमध्ये की (key) ची देवाणघेवाण करण्याची आवश्यकता नाही, ज्यामुळे डिस्ट्रिब्युशनची(Distribution) मुख्य समस्या दूर होईल.

2. सुरक्षा (Security):-खाजगी की (private key) कधीही ट्रान्समीट (Transmit) करण्याची किंवा कोणालाही दाखवण्याची करण्याची आवश्यकता नाही.
3. नॉन-रिप्यूडिएशन प्रदान करा (Provide Non-Repudiation):- डिजिटल संदेशावर (Digital Signature) स्वाक्षरी करणे एखाद्या दस्तऐवजावर फिजिकली स्वाक्षरी (Physical Signature) करण्यासारखेच आहे. ही संदेशाची पावती (Receipt) आहे आणि अशा प्रकारे सेंडर (Sender) त्यास नाकारू शकत नाही.

असिमेट्रिक क्रिप्टोग्राफीचे (Asymmetric Cryptography**) तोटे:**

1. स्लो (Slow):- असिमेट्रिक की एन्क्रिपशन (Asymmetric Key Encryption) सिमेट्रिक की (Symmetric Key) एन्क्रिपशन पेक्षा स्लो (slow)आहे बिकॉज ऑफ इंटेन्सिव्ह ऑपरेशन्स (because of intensive operations).
2. एनक्रिप्शन (Encryption) आणि डीक्रिप्शन (Decryption) प्रक्रियेसाठी जास्त संगणकीय संसाधने लागतात.
3. अकार्यक्षम (Insufficient):- असिमेट्रिक की एन्क्रिपशन (Asymmetric Key Encryption) सिमेट्रिक की एन्क्रिपशन (Symmetric key Encryption) पेक्षा कमी कार्यक्षम आहे, ज्यामुळे मोठ्या प्रमाणात डेटा एन्क्रिप्टिंगसाठी अयोग्य बनते.

Table.3.1 Difference between Symmetric key Encryption and Asymmetric Key Encryption

सिमेट्रिक की एन्क्रिपशन (Symmetric key Encryption)	**असिमेट्रिक की एन्क्रिपशन** (Asymmetric Key Encryption)
एन्क्रिपशन (Encryption) आणि डिक्रिप्शन (Decryption) दोन्हीसाठी फक्त एकच सिक्रेट की (Secret key)आवश्यक आहे.	यासाठी दोन की, एक सार्वजनिक की(public key) आणि एक खाजगी की(private key), एक एन्क्रिप्ट (Encrypt)करण्यासाठी आणि दुसरे डिक्रिप्ट(Decrypt) करण्यासाठी आवश्यक आहे.
सायफर मजकूर (Cipher Text) ची साईज ओरीजनल प्लेन टेक्स्टपेक्षा (Origional Plain Text) समान किंवा लहान आहे.	सायफर मजकूर (Cipher Text) ची साईज ओरीजनल प्लेन टेक्स्टपेक्षा (Origional Plain Text) समान किंवा मोठा आहे.
एन्क्रिपशन (Encryption) प्रक्रिया खूप वेगवान आहे.	एन्क्रिपशन प्रक्रिया स्लो (Encryption Slow)आहे.
जेव्हा मोठ्या प्रमाणात डेटा (data) हस्तांतरित करणे आवश्यक असते तेव्हा हे वापरले जाते.	याचा उपयोग कमी प्रमाणात डेटा (data) हस्तांतरित करण्यासाठी केला जातो.
हे गोपनीयता प्रदान करते.	हे गोपनीयता, सत्यता आणि नॉन-रिप्यूडिएशन (non-repudiation) प्रदान करते.
वापरलेल्या कीची लेंग्थ (length) 128 किंवा 256 बिट्स (Bits)आहे.	वापरलेल्या कीची लेंग्थ (length) 2048 किंवा त्यापेक्षा जास्त आहे.
सिमेट्रिक की एन्क्रिप्शनमध्ये, असिमेट्रिक की एन्क्रिप्शनच्या तुलनेत संसाधनाचा(resources) उपयोग कमी आहे.	असिमेट्रिक की एन्क्रिप्शनमध्ये, संसाधनाचा (resources)उपयोग जास्त आहे.
हे कार्यक्षम आहे कारण ते मोठ्या प्रमाणात डेटा हाताळण्यासाठी वापरले जाते.	हे तुलनात्मकदृष्ट्या कमी कार्यक्षम आहे कारण ते कमी प्रमाणात डेटा हाताळू शकते.
एन्क्रिपशन आणि डिक्रिप्शन या दोन्ही उद्देशाने फक्त एक की वापरली जाते म्हणून सुरक्षा (security)कमी आहे.	दोन की(keys) वापरल्यामुळे सुरक्षा जास्त आहे, एक एन्क्रिप्शनसाठी आणि दुसरे डिक्रिप्शनसाठी.
गणिताचे प्रतिनिधित्व खालीलप्रमाणे आहे- P = D (K, E(K, P)) where K –> एन्क्रिपशन आणि डिक्रिप्शन की (key) P –> प्लेन टेक्स्ट (plain text)	गणिताचे प्रतिनिधित्व खालीलप्रमाणे आहे- P = D(Kd, E (Ke,P)) where Ke –> एन्क्रिपशन की (encryption key) Kd –> डिक्रिप्शन की (decryption key)

D –> डिक्रिप्शन (Decryption) E(K, P) –> एन्क्रिपशन ऑफ प्लेन टेक्स्ट युजींग K (Encryption of plain text using K)	D –> डिक्रिप्शन (Decryption) E(Ke, P) –> एन्क्रिपशन ऑफ प्लेन टेक्स्ट युजींग Ke (Encryption of plain text using Ke) P –> प्लेन टेक्स्ट (plain text)
उदाहरणे: 3 डीईएस,(3DES) ,एईएस (AES) , डीईएस आणि आरसी 4 (RC4)	उदाहरणे: डिफी-हॅलमन (Diffie-Hellman), ईसीसी (ECC), डीएसए आणि आरएसए (DSA and RSA)

3.3 सब्स्टियूशन तंत्र (Substitution Technique):

हे एक अतिशय मूलभूत तंत्र आहे जे सायफर मजकूर (Ciphet Text) उत्पन्न करण्यासाठी सोप्या अक्षराच्या सब्स्टियूशन चा वापर करते.

साध्या मजकूराचे सायफर मजकूरामध्ये रूपांतर करण्यासाठी दोन प्रकारचे तंत्र आहेत.

1. सब्स्टियूशन तंत्र (Substiution Technique) 2. ट्रान्सपोजिशन तंत्र (Transposition Technique)

3.3.1 सीझर सायफर (Caesar Cipher):

रोमचे सम्राट ज्युलियस सीझर (Julius Caesar) यांनी शत्रूंपासून गुप्त माहिती लपवण्यासाठी हा सायफर (Cipher) वापरला होता. आधुनिक काळात हा सायफर (Cipher) शिक्षण आणि मूलभूत क्रिप्टोग्राफी शिकण्यासाठी वापरला जातो. सीझर सायफर (Caesar Cipher) हे एक साधे एन्क्रिप्शन तंत्र (Encryption technique) आहे. हे प्रथम ज्युलियस सीझरने (Julius Caesar)प्रस्तावित केले होते आणि त्याला सीझर सायफर (Caesar Cipher) असे म्हणतात. हे सब्स्टियूशन सायफर (Substitution Cipher) चे पहिले उदाहरण होते. हे शिफ्ट सायफर (Shift Cipher))म्हणून देखील ओळखले जाते. हे "शिफ्ट" किंवा "की" म्हणून ओळखल्या जाणाऱ्या विशिष्ट संख्येने प्लेन टेक्स्ट (Plain text) संदेशातील अक्षरे बदलून कार्य करते. सीझर सायफरमध्ये (Caesar Cipher) वर्णमाला अक्षरे निश्चित संख्येने बदलणे समाविष्ट आहे. उदाहरणार्थ, तीन शिफ्टसह, 'ए' हे अक्षर बनते 'डी', 'बी' बनते 'ई' , वगैरे. सीझर सायफर तंत्र (Caesar Cipher technique) एन्क्रिप्शन तंत्राच्या सर्वात आधी आणि सोप्या पद्धतींपैकी एक आहे.

Table 3.2 Replacement Table

Plain	a	b	c	d	E	f	g	h	i	j	k	l	m
Cipher	d	e	f	g	H	i	j	k	l	m	n	o	p
Plain	n	o	p	q	R	s	t	u	v	w	x	y	z
Cipher	q	r	s	t	U	v	w	x	y	z	a	b	c

सीझर सायफरची कार्यपद्धती:

1. की (Key) निश्चित करणे: एक अंक निवडला जातो (उदा. Shift = 3).
2. एनक्रिप्शन (Encryption):प्रत्येक अक्षर Shift मूल्यानुसार पुढे सरकवले जाते.
   उदा. Shift = 3 असताना, 'A' → 'D', 'B' → 'E', 'C' → 'F'.
3. डीक्रिप्शन (Decryption): एनक्रिप्टेड मजकुरातील अक्षरे मागे Shift केली जातात.
   उदा. 'D' → 'A', 'E' → 'B', 'F' → 'C'.
   उदाहरण:
   एनक्रिप्शन (Encryption):
   मूळ मजकूर (Plaintext): HELLO
   Shift = 3
   एनक्रिप्टेड मजकूर (Ciphertext): KHOOR

सीझर सायफरचे (Caesar Cipher)फायदे:

1. सोपी आणि वेगवान क्रिप्टोग्राफी पद्धत.

2. हाताने किंवा संगणकाद्वारे सहज कार्यान्वित करता येते.
3. मूलभूत सायफर शिकण्यासाठी उपयुक्त.

सीझर सायफरचे (Caesar Cipher **) तोटे:**

1. सुरक्षा खूप कमी आहे, सहज क्रॅक करता येतो.
2. ब्रूट-फोर्स अटॅक (Bruit Force attack) (Shift = 1 ते 25 पर्यंत सर्व शक्यता तपासणे) ने सहज तोडता येतो.
3. मोठ्या प्रमाणावर सुरक्षित संप्रेषणासाठी योग्य नाही.

3.3.2 प्लेफेअर सायफर (Playfair Cipher): प्लेफेअर सायफर (Playfair Cipher) हा सिमेट्रिक की क्रिप्टोग्राफी (Symmetric Key Cryptography)प्रकारातील एक सुधारित सब्स्टिट्यूशन सायफर (Substitution Cipher) आहे. हा सायफर चार्ल्स व्हीटस्टोन (Charles Wheatstone) यांनी विकसित केला होता, परंतु तो लॉर्ड लायन प्लेफेअर (Lord Lyon Playfair) यांच्या नावाने प्रसिद्ध झाला.

प्लेफेअर सायफरमध्ये (Playfair Cipher)2 स्टेप्स चा समावेश आहे.

स्टेप 1: क्रिएट आणि मॅट्रिक्सची निर्मिती (Creation of matrix)

स्टेप 2: एन्क्रिपशन प्रोसेस.

स्टेप 1: मॅट्रिक्सची निर्मिती (Creation of matrix) **:-**

प्लेफेअर सायफरमध्ये "5x5 मॅट्रिक्स" चा वापर केला जातो, ज्यात गुप्त कि (Secret Key) वापरून अक्षरे भरली जातात.

1. की (Key) तयार करणे:

- एक गुप्त कि (Secret Key) निवडली जाते (उदा. "PLAYFAIR EXAMPLE").
- या किच्या मदतीने 5x5 मॅट्रिक्स तयार केला जातो, ज्यात A ते Z या अक्षरांचा समावेश असतो (I आणि J एकत्र घेतले जातात).

a. ड्रॉप डुप्लिकेट (Drop duplicate alphabets) अक्षरे

b. कीवर्डचा भाग नसलेल्या उर्वरित इंग्रजी वर्णमाला (ए-झेड) सह मॅट्रिक्समधील उर्वरित जागा भरा. असे करत असताना, टेबलच्या त्याच सेलमध्ये आय (I) आणि जे (J) एकत्र करा. आणि जर आय (I)/जे (J) कीवर्डचा एक भाग असेल तर उर्वरित स्लॉट भरताना I आणि जे(J) दोघेही दुर्लक्ष करा.

कीवर्ड(Keyword):- PLAYF<u>A</u>IR EX<u>A</u>MPLE {ए डुप्लिकेट आहे म्हणूनच मॅट्रिक्समधून सोडले गेले आहे}

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

5 x 5 Matrix

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

Generated 5 x 5 PlayFair Matrix

स्टेप 2: एन्क्रिपशन प्रोसेस (Encryption Process)

संदेशाचे दोन-दोन अक्षरांचे जोड (Digraphs) तयार केले जातात आणि खालील नियमांनुसार एनक्रिप्शन केले जाते:

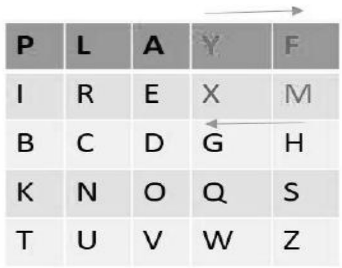
1. जर दोन्ही अक्षरे एकाच ओळीत (Same Row) असतील, तर त्यापेक्षा उजवीकडील अक्षर घेतले जाते (शेवटच्या अक्षरासाठी पहिल्या स्तंभातील अक्षर घ्यावे).).

2. जर दोन्ही अक्षरे एकाच स्तंभात (Same Column) असतील, तर त्यांच्या खालचे अक्षर घेतले जाते ((शेवटच्या अक्षरासाठी पहिल्या ओळीतील अक्षर घ्यावे).

3. जर अक्षरे भिन्न ओळी आणि स्तंभात असतील, तर त्याच ओळीतील दुसऱ्या अक्षराचा वापर करावा.

एन्क्रिप्ट टेक्स्ट (Encrypt the text):- MY NAME IS ATUL

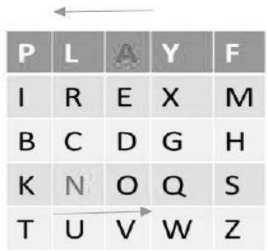
1. पहिली जोडी (First Pair) :-MY



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

Apply Step #5
Plain Text: MY
Cipher text block: XF

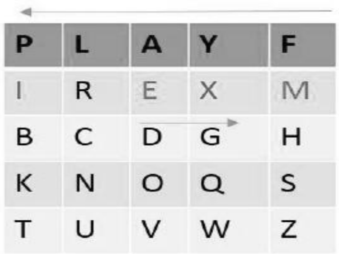
2. नेक्स्ट जोडी (Next Pair) :NA



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

Apply Step #5
Plain Text: NA
Cipher text block: OL

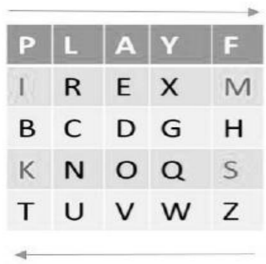
3. नेक्स्ट जोडी(Next Pair):-ME



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

Apply Step #3
Plain Text: ME
Cipher text block: IX

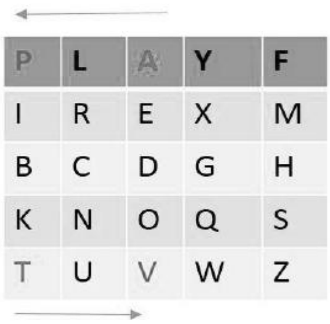
4. नेक्स्ट जोडी (Next Pair): IS



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

Apply Step #5
Plain Text: IS
Cipher text block: MK

5. नेक्स्ट जोडी (Next Pair) : AT



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

Apply Step #5
Plain Text: AT
Cipher text block: PV

6. नेक्स्ट जोडी (Next Pair) : UL

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

Apply Step #5
Plain Text: UL
Cipher text block: LR

प्लेन टेक्स्ट (Plain Text): MY NAME IS ATUL

सायफर टेक्स्ट (Cipher Text)**:** XF OL IX MK PV LR

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

प्लेफेअर सायफरचे फायदे (Advantages of Playfair Cipher)**:**
1. सीझर सायफर आणि सिंगल सब्स्टिट्यूशन सायफरपेक्षा अधिक सुरक्षित आहे.
2. ब्रूट-फोर्स हल्ल्याने सहज क्रॅक करता येत नाही.
3. संभाव्य 25x25 = 625 जोडण्यामुळे क्रिप्टोग्राफी अधिक सुरक्षित होते.

प्लेफेअर सायफरचे तोटे (Disdvantages of Playfair Cipher)**:**
1. गुप्त कि(Private Key) सुरक्षित ठेवणे आवश्यक असते.
2. संदेशाच्या लांबीवर काही प्रमाणात निर्बंध असतो.

3.3.3 विजेनर सायफर /पॉलीअल्फाबेटिक सब्स्टियूशन सायफर(Vigenere Cipher/Poly-Alphabetic Substitution Cipher)

विजेनर सायफर हा पॉली-अल्फाबेटिक सब्स्टिट्यूशन सायफर (Poly-Alphabetic Substitution Cipher) प्रकारातील एक प्रसिद्ध क्रिप्टोग्राफी अल्गोरिदम (Cryptography algorithm) आहे जो मूळ सिंगल-शिफ्ट सायफरपेक्षा (Single Shift Cipher)अधिक सुरक्षित आहे. हा सायफर 1586 मध्ये ब्लेझ डी विजेनर (Blaise de Vigenère) यांनी विकसित केला.

विजेनर सायफरची कार्यपद्धती (Process of Vigenere Cipher):
हे व्हिग्नेर टेबलवर आधारित आहे. हे टेबल 27 ओळींनी बनलेले आहे. लोअर केस लेटर्सची (Lower case) पहिली ओळ साध्या मजकूर वर्णांचे प्रतिनिधित्व करते.

कीवर्ड (Keyword) निवडणे:
- विजेनर सायफरमध्ये (Vigenere Cipher) एक गुप्त कीवर्ड (Secret Keyword) वापरला जातो, जो मजकूराच्या प्रत्येक अक्षरावर लागू होतो.
- ही कीवर्ड (Keyword)संदेशाच्या लांबी (length) इतकी वारंवार पुनरावृत्ती केली जाते.
- प्रत्येक त्यानंतरची ओळ एक सायफर टेक्स्ट प्रतिनिधित्व करते.
- प्रत्येक वर्णमाला प्रथम वर्ण मागील पंक्तीपेक्षा एक स्थान हलविले जाते.
- पहिल्या स्तंभात(column), प्रत्येक ओळीला वर्णमाला अक्षरासह लेबल केले जाते.
- सायफर प्रक्रिया सुरू करण्यासाठी की (Key)आवश्यक आहे.

उदाहरण:
Key: AYUSH
Plain Text: “GEEKSFORGEEKS”

Key	A	Y	U	S	H	A	Y	U	S	H	A	Y	U
Plain text	G	E	E	K	S	F	O	R	G	E	E	K	S

1.आता सर्व जागांसह संदेश(message) लिहा.
2.संदेशाच्या वरील की (Key) लिहा जेणेकरून की(Key) चे प्रत्येक लेटर मेसेजच्या एका अक्षराशी संबंधित असेल, खाली दर्शविल्याप्रमाणे. संपूर्ण मेसेज कव्हर करण्यासाठी आवश्यक तितक्या वेळा की(Key) रिपीट (Repeat)करा.

3. की (key)मधील लेटर शी संबंधित टेबल मधील पंक्ती(rows) ओळखा. म्हणजेच पहिल्या स्तंभात (column) अ(A), वाय (Y), यू (U), स (S), ह (H) म्हणून नियुक्त केलेल्या ओळी निवडा.
यापैकी प्रत्येक ओळी (rows) आम्ही आपला संदेश एनक्रिप्ट करण्यासाठी वापरत असलेल्या सायफर लेटर दर्शवितात.
संदेशातील(message) प्रत्येक अक्षर त्याच्या संबंधित सायफर टेक्स्ट सह पुनर्स्थित करा.
उदाहरणार्थ :प्लेन टेक्स्टमधील पहिले अक्षर, G हे की चे पहिले अक्षर A सोबत जोडलेले आहे. म्हणून Vigenère स्केअरमधील पंक्ती G आणि स्तंभ A वापरा, म्हणून सायफर लेटर "G" आहे. योग्य सायफर टेक्स्ट शोधण्यासाठी वरील स्टेप्स ची पुनरावृत्ती करा.
एन्क्रिप्टेड टेक्स्ट (Encrypted Text) : GCYCZFMLYLEIM

Table 3.3 Vignere Cipher Table

	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

विजेनर सायफरचे फायदे (Advantages of Vigenere Cipher) :
1. सीझर सायफरपेक्षा अधिक सुरक्षित, कारण एकाच वेळी एकापेक्षा जास्त शिफ्ट्स वापरले जातात.
2. ब्रूट-फोर्स अटॅकला अधिक प्रतिरोधक, कारण कीवर्डमुळे वारंवार बदल होतो.
3. मोठ्या मजकुरासाठी वापरण्यास योग्य.

विजेनर सायफरचे तोटे (Disdvantages of Vigenere Cipher)**:**
1. कीवर्ड गुप्त ठेवणे आवश्यक आहे, नाहीतर सायफर क्रॅक केला जाऊ शकतो.
2. की लांबी (Key Length) ओळखण्याचा प्रयत्न करून क्रिप्टॲनालिसिस शक्य आहे.
3. कासिस्की विश्लेषण (Kasiski Examination) तंत्राने की लांबी शोधून सायफर ब्रेक करता येतो.

3.3.4 वर्नम सायफर /एक वेळ पॅड (Vernam Cipher /One time pad):-

वर्नम सायफर, ज्याला वन टाईम पॅड (One-Time Pad) देखील म्हणतात, हा एक अत्यंत सुरक्षित आणि अनब्रेकबल (Unbreakable) क्रिप्टोग्राफी तंत्र आहे. 1917 मध्ये गिल्बर्ट वर्नम (Gilbert Vernam) यांनी हा सायफर विकसित केला. एक टाइम पॅड देखील वेरनम सायफर म्हणून ओळखला जातो, इनपुट सायफर मजकूर म्हणून नॉन-रीपिटिंग वर्णांचा याहच्छिक संच वापरून लागू केला जातो. एकदा ट्रान्सपोजिशनसाठी इनपुट सायफर मजकूर वापरला की तो इतर कोणत्याही संदेशासाठी

पुन्हा कधीही वापरला जात नाही म्हणून नाव एक-वेळ पॅड. इनपुट सायफर मजकूराची लांबी मूळ साध्या मजकूराच्या लांबीच्या समान आहे.

वर्नम सायफर / वन टाइम पॅडमध्ये (One time Pad)वापरल्या जाणाऱ्या अल्गोरिदमचे वर्णन खालीलप्रमाणे केले आहे: -

1.प्रत्येक साध्या मजकूर वर्णमाला वाढत्या अनुक्रमात एक संख्या म्हणून हाताळा, म्हणजे ए (A)= 0, बी(B) = 1,... झेड(Z) = 25.

2.हि प्रोसेस इनपुट सायफर (Input cipher) मजकूराच्या प्रत्येक वर्णासाठी करा.

3.संबंधित इनपुट सायफर मजकूर वर्णमाला संख्येशी साध्या मजकूर वर्णमाला संबंधित प्रत्येक क्रमांकाची नोंद करा.

4.जर अशा प्रकारे तयार केलेली बेरीज 26 पेक्षा जास्त असेल तर त्यापासून 26 वजा करा.

5.संबंधित वर्णमाला परत बेरीजची प्रत्येक संख्या ट्रान्सलेट करा. हे आउटपुट सायफर मजकूर देते.

उदाहरण: - साधा मजकूर = = “BEING HUMAN”

1 PLAIN TEXT	B	E	I	N	G	H	U	M	A	N
	1	4	8	13	6	7	20	12	0	13
+										
2 ONE TIME PAD	O	R	D	I	N	A	R	I	L	Y
	14	17	3	8	13	0	17	8	11	25
3. INITIAL TOTAL	15	21	11	21	19	7	**37**	20	11	**38**
4. SUBTRACT 26, IF >26	15	21	11	21	19	7	11	20	11	12
5. CIPHER TEXT	Q	V	L	V	T	H	L	V	L	M

एक-वेळ पॅड(One Time Pad) एकदा वापरल्यानंतर टाकून दिला जातो आणि म्हणूनच केवळ लहान संदेशांसाठी योग्य आहे.

वर्नम सायफरचे फायदे (Advantages of Vernam Cipher /One time pad)**:**

1.100% सुरक्षित (Unbreakable) – योग्यरित्या वापरल्यास कोणतेही क्रिप्टोग्राफिक हल्ले (Attacks) त्याला क्रॅक करू शकत नाहीत.

2.कोणतेही सांख्यिकी नमुने नसतात (No Patterns) – ब्रूट-फोर्स किंवा फ्रिक्वेन्सी ॲनालिसिस काम करत नाही.

3.परफेक्ट सिक्युरिटी (Perfect Secrecy) – क्लॉड शॅनॉन (Claude Shannon) यांनी सिद्ध केले की हा सायफर परिपूर्ण सुरक्षितता प्रदान करतो.

वर्नम सायफरचे तोटे (Advantages of Vernam Cipher /One time pad)**:**

1. की व्यवस्थापन (Key Management) कठीण आहे – की लांबी (Key Length)मोठी असल्याने ती सुरक्षित ठेवणे आणि वितरित करणे अवघड होते.

2. की (Key)पुन्हा वापरता येत नाही (One-Time Use) – की (key) एकदाच वापरली गेली पाहिजे.पुन्हा वापरल्यास सुरक्षा धोक्यात येते.

3. ट्रूली रँडम की (Truly Random Key) निर्माण करणे आवश्यक – पूर्णतः ट्रूली रँडम की (Truly Random Key)निर्माण करणे आवश्यक आहे, जी संगणकीय दृष्टिकोनातून आव्हानात्मक असते.

वर्नम सायफरचा वापर (Uses of Vernam Cipher /One time pad)**:**

1. मिलिटरी आणि गुप्तचर संस्था (Military & Intelligence Agencies) – टॉप-सीक्रेट कम्युनिकेशनसाठी (top secret Communication).

2. हाय-लेव्हल डिप्लोमॅटिक कम्युनिकेशन – पूर्णतः सुरक्षित संदेश पाठवण्यासाठी.

3. क्वांटम क्रिप्टोग्राफीमध्ये (Quantum Cryptography) – वन-टाईम पॅडच्या संकल्पनेवर आधारित अल्गोरिदम विकसित करण्यात आले आहेत.

3.4 ट्रान्सपोजिशन तंत्र (Transposition technique)**:**

ट्रान्सपोझिशन तंत्र (Transposition technique) ही मजकूरावर क्रमपरिवर्तन करून साधा मजकूर सायफर टेक्स्टमध्ये एन्क्रिप्ट करण्याची एक पद्धत आहे.ट्रान्सपोजिशन तंत्र (Transposition technique)प्रतिस्थापन तंत्रापेक्षा भिन्न आहे.ट्रान्सपोझिशन सायफर हे एक प्रकारची एन्कोडिंग तंत्र आहे ज्यामध्ये साध्या संदेशातील अक्षरे स्वतःमध्ये बदल न करता त्यांची पुनर्रचना करणे समाविष्ट आहे . ही पद्धत सामान्यतः वर्तमानपत्रे आणि कोडे(Puzzle) मासिकांमध्ये वापरली जाते, जिथे संदेश अक्षरांच्या गोंधळाच्या रूपात(jumble format) दिसतो जो क्रॅक(crack) करणे तुलनेने सोपे असू शकते.ट्रान्सपोझिशन सायफर, क्रमपरिवर्तन म्हणून ओळखल्या जाणाऱ्या नियमांच्या संचाद्वारे वर्णाचे स्थान बदलतो.

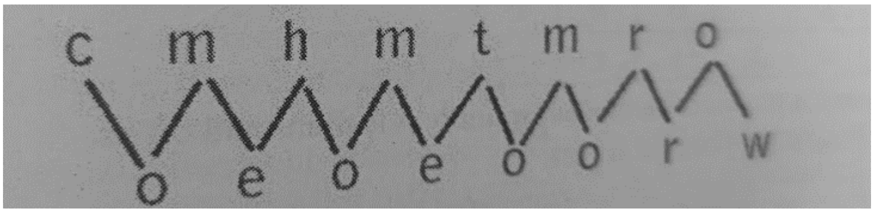
3.4.1 रेल फेन्स तंत्र (Rail Fence Cipher): याला झिगझॅग सायफर (Zigzag Cipher) देखील म्हणतात. हा एक ट्रान्सपोझिशन सायफर(Transposition cipher)आहे जो मूलभूत अल्गोरिदम वापरून संदेशाच्या अक्षरांचा क्रम जंबल (Jumble)करतो. रेल फेन्स (Rail-Fence) द्वारे एन्कोड (encode)केलेल्या संदेशामध्ये मूळ मजकुराच्या (Plain text)भाषेच्या समान योगायोगाची अनुक्रमणिका असते.

रेल फेंस (Rail-Fence) सायफरमध्ये, साधा मजकूर(Plain text) एका काल्पनिक कुंपणाच्या सलग "रेल्स" वर तिरपेपणे खाली लिहिला जातो, नंतर खालच्या रेल्सवर पोहोचल्यावर वर सरकतो, वरच्या रेल्सवर पोहोचल्यावर पुन्हा खाली सरकतो आणि संपूर्ण साधा मजकूर संपेपर्यंत असेच चालू राहते. त्यानंतर सायफरटेक्स्ट ओळींमध्ये वाचला जातो.

रेल फेन्स सायफरची कार्यपद्धती (Process of Rail-Fence) :

1. रेलफेन्स पद्धतीने मजकूर मांडणे:
   - एक विशिष्ट "की" (Key) किंवा "रेलफेन्सच्या ओळींची संख्या" निवडली जाते.
   - मजकूर झिग-झॅग (Zig-Zag) पद्धतीने ओळींमध्ये विभागला जातो.
   - नंतर या ओळी सलग वाचल्या जातात आणि त्यातून गुप्त संदेश (Ciphertext) मिळतो.

उदाहरण (example):- प्लेन टेक्स्ट (plain text) =come home tomorrow



आता पंक्तीचा क्रम म्हणून वाचा.

सायफर टेक्स्ट (Cipher text) : cmhmtmrooeoeoorw

रेल फेन्स सायफरचे फायदे (Advantages of Rail-Fence):

1. सोपे आणि जलद एन्क्रिप्शन व डीक्रिप्शन प्रक्रिया.
2. सीझर सायफरपेक्षा अधिक सुरक्षित, कारण अक्षरांचा क्रम बदलतो.
3. शिक्षण व प्राथमिक क्रिप्टोग्राफीसाठी उपयुक्त.

रेल फेन्स सायफरचे तोटे(Disdvantages of Rail-Fence):

1. ब्रूट-फोर्स हल्ल्याने सहज क्रॅक करता येतो (Rails संख्या अंदाज लावून सापडू शकते).
2. संदेशामधील अक्षरांची वारंवारता समान राहते, त्यामुळे फ्रिक्वेन्सी ॲनालिसिस शक्य आहे.

3.4.2 साधा स्तंभ ट्रान्सपोजिशन तंत्र किंवा पंक्ती ट्रान्सपोजिशन (Simple columnar Transposition technique or Row Transposition): -

अल्गोरिदम (Algorithm):

1. पूर्वनिर्धारित आकाराच्या (size) आयतात पंक्तीने साधा मजकूर संदेश पंक्ती लिहा (कीवर्ड आकार(size))
2. स्तंभानुसार (Column) संदेश स्तंभ वाचा, तथापि, ते स्तंभांच्या क्रमाने (column order)असणे आवश्यक नाही, ही कोणतीही यादृच्छिक ऑर्डर (random order)असू शकते.
3. अशा प्रकारे प्राप्त केलेला संदेश म्हणजे सायफर टेक्स्ट (Cipher text).

Example: प्लेन टेक्स्ट (Plain Text): —Come Home Tomorrow"
कीवर्ड (Keyword): ZEBRAS

सहा स्तंभ (Six Columns)असलेल्या आयताचा विचार करा आणि म्हणूनच, जेव्हा संदेश आयताच्या पंक्तीमध्ये पंक्तीने लिहिला जाईल तेव्हा ते खालीलप्रमाणे दिसेल.

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
C	O	M	E	H	O
M	E	T	O	M	O
R	R	O	W		

आता, स्तंभांच्या ऑर्डरचा काही यादृच्छिक ऑर्डर(random order) म्हणून ठरवा, म्हणा, 4, 6, 1, 2, 5, 3 नंतर या स्तंभांच्या क्रमाने मजकूर वाचा.

त्यातून प्राप्त केलेला सायफर टेक्स्ट(Cipher text) असेलः **EOW OO CMR OER HM MTO**

डिक्रिप्शन (Decryption) फेज असताना सायफर समान आकारासह समान आयतात लिहिला जातो आणि सर्व सायफर की नुसार ठेवल्या जातात.

3.5 स्टेगनोग्राफी (Steganography):

परिचय: -स्टेगॅनोग्राफी (Steganography) हा शब्द दोन ग्रीक शब्दांपासून आला आहे - 'स्टेगोस' म्हणजे 'झाकणे' आणि 'ग्रेफिया', म्हणजे 'लेखन', अशा प्रकारे 'झाकलेले लेखन' किंवा 'लपलेले लेखन' असे भाषांतरित केले आहे. स्टेगनोग्राफी (Steganography) म्हणजे गुप्त ठेवल्या जाणाऱ्या दुसऱ्या संदेशामध्ये संदेश एम्बेड (Embed) करून माहिती लपविण्याची कला आणि विज्ञान आहे. एखाद्या फाईलमध्ये, छायाचित्रात किंवा मेसेजमध्ये गुप्तपणे डेटा लपवणे याला स्टेगनोग्राफी (Steganography) असे म्हणतात.

स्टेगेनोग्राफीच्या मदतीने आम्ही माध्यमाच्या मागे पाठ्यपुस्तक, प्रतिमा, व्हिडिओटेप इत्यादी कोणतीही डिजिटल (digital) गोष्ट लपवू शकतो. हे कव्हर मेसेजमध्ये (Cover message) एक गुप्त संदेश एम्बेड (Embed) करते, ही प्रक्रिया सहसा स्टेगो की(Stego Key) द्वारे केली जाते आणि एम्बेडेड (Embeded) माहितीचे वाचन केवळ हीच की (key) वापरून शक्य आहे.

कव्हर मीडिया (Cover media) + सिक्रेट मेसेज (Secret Message)+ स्टेगो की (Stego Key)= स्टेगो माध्यम (Stego medium).

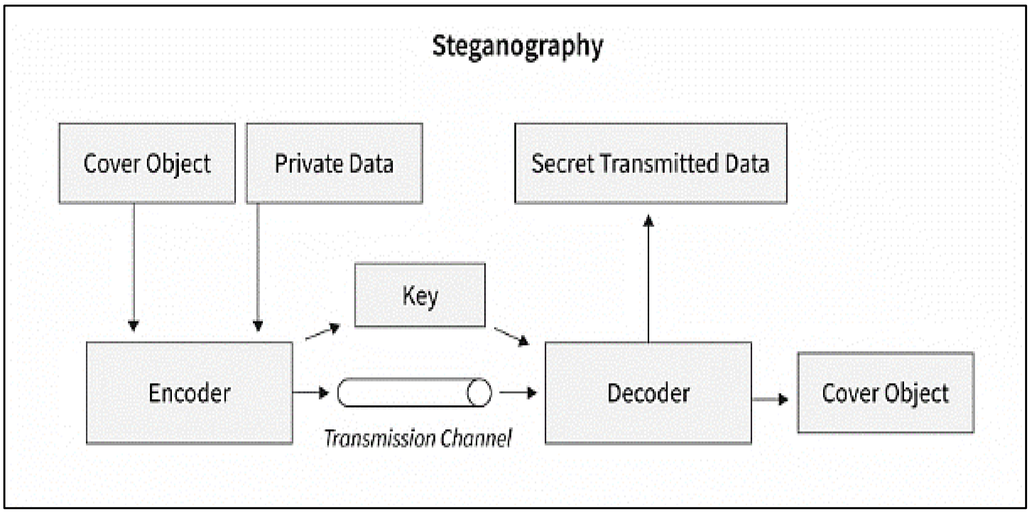


Figure 3.5.1 Stegnography

स्टेगनोग्राफीचे कार्य (Working of Stegnography)**:** स्टेगनोग्राफी नियमित संगणक फायलींमध्ये (File) (जसे की ग्राफिक्स, ध्वनी, मजकूर आणि एचटीएमएल) निरुपयोगी किंवा न वापरलेल्या डेटाचे बिट (data bits)बदलून वेगवेगळ्या अदृश्य

माहितीच्या बिट्ससह कार्य करते.ही लपलेली माहिती प्लेन टेक्स्ट(Plain Text), सायफर मजकूर (Cipher Text) किंवा अगदी प्रतिमा असू शकते.

स्टेगनोग्राफीचे स्टेपवाईज कार्य (Stepwise Working of Stegnography)**::**

1. डेटा तयार करणे – लपवायचा डेटा (मजकूर, इमेज, ऑडिओ इ.) तयार केला जातो.
2. कव्हर मीडिया निवडणे – माहिती लपवण्यासाठी योग्य मीडिया (प्रतिमा, ऑडिओ, व्हिडिओ किंवा इतर फाईल्स) निवडली जातात.
3. एन्कोडिंग (Encoding) – माहिती स्टेग्नोग्राफी अल्गोरिदमद्वारे मीडिया फाईलमध्ये एम्बेड केली जाते.
4. ट्रान्समिशन किंवा संचयन – तयार केलेली स्टेग्नोग्राफिक फाईल सुरक्षितरित्या पाठवली किंवा संग्रहित केली जाते.
5. डिकोडिंग (उघड करणे) – रिसीव्हर योग्य स्टेग्नोग्राफी तंत्रज्ञान वापरून लपवलेली माहिती परत मिळवतो.

Table No.3.4 Difference between Stegnography and Cryptography

स्टेगनोग्राफी (Stegnography)	**क्रिप्टोग्राफी (Cryptography)**
स्टेगनोग्राफीला डेटा किंवा माहिती अंडर-ज्ञात-गुप्त डेटा किंवा प्रशिक्षण लपविण्याची एक प्रणाली म्हणून परिभाषित केली जाते.	क्रिप्टोग्राफी म्हणजे प्रतिकुल परिस्थितीत सुरक्षित संदेशाची देवाणघेवाण करण्यासाठी वापरले जाणारे तंत्रज्ञान.
संप्रेषण सुरक्षा राखणे हा त्याचा मुख्य हेतू आहे.	त्याचा मुख्य हेतू डेटा संरक्षण देणे आहे.
स्टेगनोग्राफीच्या बाबतीत डेटाची रचना सुधारित केली जात नाही.	क्रिप्टोग्राफीच्या बाबतीत डेटाची रचना सुधारित केली आहे.
की(key) चा वापर अनिवार्य नाही, परंतु जर तो वापरला गेला तर तो सुरक्षा वाढवितो.	क्रिप्टोग्राफीच्या बाबतीत कीचा वापर अनिवार्य आहे.
स्टेगेनोग्राफीमध्ये, उत्कृष्ट मेटामॉर्फोसचा वापर महत्त्वपूर्णपणे गुंतलेला नाही.	क्रिप्टोग्राफीमध्ये, डेटासह खेळण्यासाठी आणि संरक्षण वाढविण्यासाठी उत्कृष्ट मेटामॉर्फोसचा वापर केला जातो.

स्टेगेनोग्राफी मधील टर्मिनॉलॉजी (Terminology in Steganography) **:**

1. कव्हर-मीडियम (Cover Medium) :- ज्या डेटामध्ये संदेश लपविला गेला आहे. उदा. प्रतिमा(Image) फाइल, ऑडिओ फाइल इ.
2. स्टेगो की (Stego Key):- डेटा एन्कोड करण्यासाठी आणि डीकोड करण्यासाठी वापरली जाणारी की(Key).
3. स्टेगो-माध्यम (Stego Medium):- डेटा ज्यामध्ये एक संदेश लपविला गेला आहे.
4. स्टेगो फंक्शन (Stego Function) :- डिकोडिंगसाठी (Decoding)एन्कोडिंग (Encoding)आणि रिव्हर्स फंक्शनसाठी कार्य.
5. संदेश (Message):- याला लपविलेले डेटा म्हणून देखील म्हटले जाते. हा संदेश आहे जो कव्हरमध्ये लपविला जाईल.
6. रिडंडंट बिट (Redund Bit):- कव्हर माध्यमातील बिट जे त्या माध्यमाच्या अखंडतेशी तडजोड न करता सुधारित केले जाऊ शकते..

विविध प्रकारचे स्टेगनोग्राफी:

1.टेक्स्ट स्टेगनोग्राफी (Text Stegnography): - मजकूर फायलींमध्ये स्टेगानोग्राफी आहे, ज्यामध्ये गुप्तपणे माहिती संग्रहित केली जाते. या पद्धतीत, लपलेला डेटा प्रत्येक शब्दाच्या अक्षरात एन्कोड (encode) केला जातो. मजकूर स्टेगनोग्राफीमध्ये मजकूर फायलींमध्ये माहिती लपविणे समाविष्ट आहे. यामध्ये विद्यमान मजकुराचे स्वरूप बदलणे, मजकुरातील शब्द बदलणे, वाचनीय मजकूर तयार करण्यासाठी संदर्भ-मुक्त व्याकरण वापरणे किंवा यादृच्छिक वर्ण(random character)क्रम तयार करणे समाविष्ट आहे.

2.ईमेज स्टेगनोग्राफी (Image Stegnography) - स्टेगनोग्राफीचा दुसरा प्रकार म्हणजे इमेज स्टेगनोग्राफी, ज्यामध्ये कव्हर म्हणून वेगळ्या ऑब्जेक्टच्या(Object) प्रतिमेचा वापर करून डेटा लपविणे आवश्यक आहे. पिक्सेलची (Pixel) तीव्रता प्रतिमा स्टेगेनोग्राफीमधील डेटा लपविण्याची गुरुकिल्ली आहे.

आपण इमेज स्टेग्नोग्राफी (Image Steganography) च्या मदतीने एक गुप्त संदेश प्रतिमेमध्ये कसा लपवू शकतो आणि तो कसा उघड करू शकतो याचे एक सोपे उदाहरण पाहू.

उदाहरण: मजकूर प्रतिमेमध्ये लपवणे (LSB Steganography)

1. गुप्त संदेश: "हा एक गुप्त संदेश आहे."
2. कव्हर इमेज (Cover Image):कोणतीही सामान्य प्रतिमा, उदा. एखादा निसर्ग फोटो (JPEG/PNG फॉर्मेटमध्ये).
3. स्टेग्नोग्राफी प्रक्रिया:

- लिस्ट सिग्निफिकन्ट बिट (LSB-Least Significant Bit) तंत्र वापरून या प्रतिमेच्या प्रत्येक पिक्सेलच्या रंग मूल्याचे (RGB) शेवटचे बिट बदलले जातात.
- गुप्त संदेशाचे आस्की (ASCII) कोडमध्ये रूपांतर केले जाते.
- आस्की (ASCII) कोडचे बायनरी मूल्य प्रतिमेच्या पिक्सेल्समध्ये इंजेक्ट केले जाते.
- परिणामी प्रतिमा दिसायला तशीच राहते, पण तिच्यात गुप्त मजकूर असतो.

स्टेगनोग्राफीचे फायदे (Advanatges of Stegnogaphy):

1. ज्या पक्षांच्या(parties) गुप्त संवादाची वस्तुस्थिती उघडकीस आली तर त्यांना गमावण्यासारखे काहीतरी आहे अशा पक्षांकडून याचा वापर केला जाऊ शकतो.
2. स्टेगनोग्राफी संदेश आणि संप्रेषण दोन्ही पक्षांचे संरक्षण करू शकते.

स्टेगनोग्राफीचे तोटे (Disdvanatges of Stegnogaphy**):**

1. माहितीचे तुलनेने काही बिट्स लपविण्यासाठी बरेच ओव्हरहेड आवश्यक आहे.
2. एकदा हल्लेखोराला सिस्टम कळली की, ती जवळजवळ निरुपयोगी होते.
3. हाइडिंग क्षमता कमी आहे.
4. परिणामी स्टेगो प्रतिमेची गुणवत्ता ही एक मोठी समस्या आहे.

स्टेगनोग्राफीचे ॲप्लिकेशन्स (Applications of Stegnography)

1.आधुनिक प्रिंटरमध्ये वापरली जाते.
2. डिजिटल वॉटरमार्किंग (Digital Watermarking)
3. कॉपी राइट्स (Copy Rights)
4. लष्करी ऑपरेशन्स
5. क्रिप्टोग्राफी की प्रसारित करण्यासाठी
6. हे ऑनलाइन प्रतिमांवर नोट्स टॅग करण्यासाठी वापरले जाऊ शकते.
7. संभाव्य तोडफोड, चोरी किंवा अनधिकृत दृश्यापासून डेटाचे संरक्षण करण्यासाठी मौल्यवान माहितीची गोपनीयता राखण्यासाठी याचा वापर केला जाऊ शकतो.

References:

1. Information Systems Security Second Edition By Nina Godbole (John Wiley Isbn-13: 978-8126564057)
2. Cryptography and Information Security By V.K.Pachghare – Prentice Hall India
3. Cryptography and Network security Third Edition By Atul Kahate- McGraw-Hill; Fourth edition ISBN-13: 978-9353163303
4. Computer Security Principles and Practice, Third Edition BY William Stallings, Lawrie Brown Pearson. ISBN-13: 978-0-13-377392-7

युनिट - 4
एन्क्रिप्शन अल्गोरिदम
(Encryption Algorithm)

विषय निष्पत्ती : Course Outcome (CO):

CO4 – इन्फॉर्मेशन सेक्युरिटीसाठी वापरलेले विविध एन्क्रिप्शन अल्गोरिदम लागू करा (Apply various encryption algorithms used for information security)

घटक निष्पत्ती : (Theory Learning Outcomes)

1. दिलेला मजकूर एनक्रिप्ट करण्यासाठी डी ई एस (DES)अल्गोरिदम लागू करा.
2. दिलेला मजकूर एनक्रिप्ट करण्यासाठी ए ई एस अल्गोरिदम(AES) लागू करा
3. मजकूरावर एनक्रिप्शन करण्यासाठी दिलेला अल्गोरिदम लागू करा.
4. दिलेल्या मजकुरासाठी हॅश व्हॅल्यू((Hash Value) मिळवण्यासाठी हॅश फंक्शन(Hash Function) अल्गोरिदम लागू करा.
5. डिजिटल स्वाक्षरीचे (Digital Signature)कार्य स्पष्ट करा
6. मोबाइल सुरक्षा धोक्यांची (Threats) नोंद करा.

4.1 डी ई एस (डेटा एन्क्रिप्शन स्टॅंडर्ड) अल्गोरिदम (DES Algorithm)

डेटा एन्क्रिप्शन स्टॅंडर्ड (DES) हे 56-बिट की लांबी(Key Length) ब्लॉक सायफर (Block Cipher)आहे. डी ई एस (DES) एक ब्लॉक सायफर (Block Cipher) आहे आणि प्रत्येकी 64 बिट्सच्या (Bits) आकाराच्या ब्लॉक्समध्ये (Blocks) डेटा एन्क्रिप्ट (Data Encrypt) करतो, म्हणजे 64 बिट्स प्लेन टेक्स्ट (64 bits Plain Text) डी ई एस मध्ये इनपुट (Input) म्हणून जातात, जे 64 बिट्स सायफर टेक्स्ट (64 bits cipher text) तयार करतात. समान अल्गोरिदम आणि की किरकोळ फरकांसह, एन्क्रिप्शन (encryption) आणि डिक्रिप्शनसाठी (decryption) वापरली जातात. या अल्गोरिथमसाठी की लांबी (key length) 56 बिट (bit) आहे.

डी ई एस अल्गोरिदम प्रक्रिया (DES Algorithm Procedure)**:**

डी ई एस 64-बिट साध्या मजकुराचे (plain text) 64-बिट सायफर मजकुरात (64 bit cipher text) रूपांतर करते. असिमेट्रिक (Asymmetric) पद्धती वापरल्यामुळे समान(same) की, मजकूर एनकोड (encode) आणि डीकोड (decode) करण्यासाठी देखील वापरली जाते.

अल्गोरिदमिक प्रक्रिया खाली दिल्याप्रमाणे आहे.

1. प्रक्रिया सुरू करण्यासाठी 64-बिट प्लेन टेक्स्ट ब्लॉक प्रथम इनिशिअल परम्युटेशन (Initial Permutation) फंक्शनला पाठविला जातो.
2. साधा मजकूर नंतर (IP) समोर येतो.
3. परम्युटेड ब्लॉकचे (Permuted block) डावे प्लेन टेक्स्ट (LPT) आणि उजवे प्लेन टेक्स्ट (RPT) भाग नंतर (IP) द्वारे तयार केले जातात.
4. प्रत्येक डावे प्लेन टेक्स्ट (LPT) आणि उजवे प्लेन टेक्स्ट (RPT) साठी एन्क्रिप्शनच्या 16 फेऱ्या आहेत.
5. शेवटी, LPT आणि RPT पुन्हा एकत्र केले जातात, आणि नव्याने एकत्रित ब्लॉकला अंतिम परम्युटेशन (FP) लागू केले जाते.
6. ही प्रक्रिया परिणामी आवश्यक 64-बिट सायफर टेक्स्ट (64 bit cipher text) तयार करते.

एन्क्रिप्शन प्रक्रियेचा टप्पा (वरील क्रमांक 4,) पुढील पाच टप्प्यांमध्ये विभागला गेला आहे:

- की ट्रान्झिशन (Key Transition)
- एक्सपान्शन परमुटेशन (Expansion permutation)
- एक्स ऑर आणि स्वॅप (XOR and swap)
- एस-बॉक्स (S-Box)
- पी-बॉक्स परमुटेशन (P-Box permutations)

आपण डिक्रिप्शनसाठी समान प्रक्रिया वापरतो आणि 16 राउंड की(Round Key) दुसऱ्या दिशेने व्यवस्थित(arrange) करतो.

अल्गोरिथमची सामान्य रचना खालील FIGURE.मध्ये दाखवल्याप्रमाणे आहे.

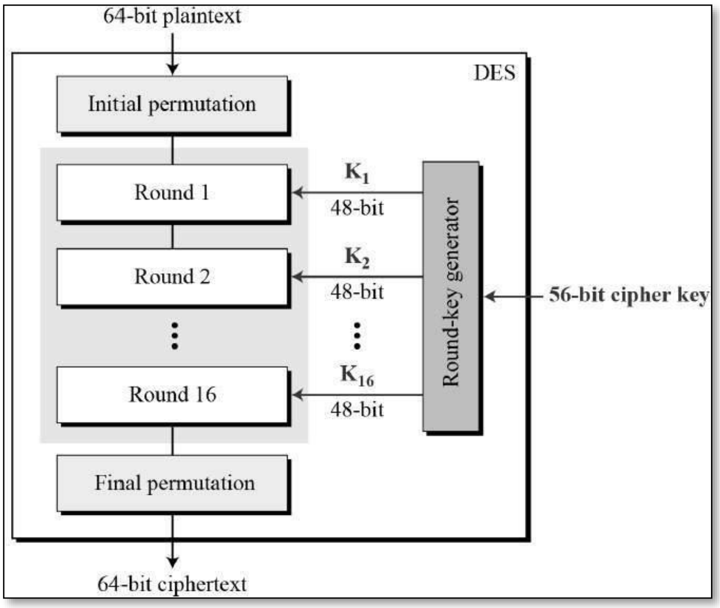


Figure4.1: DES General Structure (Courtesy: Tutorial Points)

1. इनिशिअल परम्युटेशन (Initial Permutation)

डी ई एस मधील पहिली पायरी म्हणजे इनिशिअल परम्युटेशन (IP- Initial Permutation). ही पायरी पूर्वनिर्धारित टेबल आधारे प्लेनटेक्स्टच्या बिट्सची (plain text bits) पुनर्रचना करते. उदाहरण:

प्लेनटेक्स्ट (हेक्साडेसिमलमध्ये): 0123456789ABCDEF

हेक्स ते बायनरी (hex to binary): प्लेनटेक्स्ट (बायनरीमध्ये):

00000001 00100011 01000101 01100111 10001001 10101111 11001101 11101111

Table 4.1: Initial Permutation Table

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

2. इनिशिअल परम्युटेशन करण्यासाठी, आपण टेबलनुसार प्लेनटेक्स्टच्या बिट्सची पुनर्रचना करतो. उदाहरणार्थ, मूळ

प्लेनटेक्स्टच्या स्थान 58 मधील बिट परम्युटेड मजकुराच्या स्थान 1 वर हलतो.
इनिशिअल परम्युटेशन नंतर (उदाहरण):
11001100 11110000 10101010 11001100 10101010 11001100 11110000 11001100

1. विभाजन (split)

पुढे, आपण परम्युटेड प्लेन टेक्स्टचे (permuted plain text) दोन भाग करतो. प्रत्येक अर्धा भाग ३२ बिट्सचा असतो.
डावा अर्धा भाग (L0): 11001100 11110000 10101010 11001100
उजवा अर्धा भाग (R0): 10101010 11001100 11110000 11001100

2. डावे प्लेन टेक्स्ट (LPT) आणि उजवे प्लेन टेक्स्ट (RPT) साठी एन्क्रिप्शनच्या 16 फेऱ्या की जनरेशन:

सुरुवातीची 64-बिट की(key), जी तुम्ही तुमच्या इच्छेप्रमाणे निवडू शकता, ती प्रत्येक 8 व्या बिटला काढून टाकून 56-बिट कीमध्ये रूपांतरित केली जाते. या प्रक्रियेमुळे की 56 बिट्सपर्यंत कमी होते, जी नंतर दोन 28-बिट भागांमध्ये विभागली जाते.
इनिशियल की (हेक्समध्ये): 133457799BBCDFF1
नंतर बायनरीमध्ये रूपांतरित करून प्रत्येक 8 वी बीट काढून टाका
की (बायनरीमध्ये):
00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001
प्रत्येक 8 वा बिट काढून टाकल्यानंतर
56-बिट की: 00010010 01101001 01011011 11001001 10110111 11110001
DES मध्ये, 16 राउंडपैकी प्रत्येक राउंड मूळ 56-बिट की पासून मिळवलेली वेगळी 48-बिट सब-की(sub-key) वापरतो. ही प्रक्रिया गुंतागुंत वाढवते आणि एन्क्रिप्शन सुरक्षित असल्याची खात्री करते.
प्रत्येक फेरीसाठी 48-बिट की जनरेशन प्रक्रिया
अर्ध्या भागात विभागणे:
56-बिट की दोन 28-बिट भागांमध्ये विभागली आहे:
• C0 (पहिले 28 बिट): 00010010 01101001 01011011 1100 (28 बिट)
• D0 (दुसरे 28 बिट): 1001 10110111 10110111 11110001 (28 बिट)
शिफ्टिंग (Shifting) :
16 फेऱ्यांपैकी प्रत्येकासाठी, फेरी क्रमांकानुसार, अर्धे भाग वर्तुळाकारपणे एक किंवा दोन स्थानांनी डावीकडे हलवले जातात. प्रत्येक फेरीच्या शिफ्टची संख्या खालीलप्रमाणे पूर्वनिर्धारित आहे:

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

फेरी 1 आणि 2 साठी उदाहरण:
फेरी 1: C0 आणि D0 1 स्थानाने डावीकडे हलवा.
C1: 00100100 11010010 10110111 1000
D1: 00110111 01111001 1011111 1111
फेरी 2:
C1 आणि D1 1 स्थानाने डावीकडे हलवा.
C2: 01001001 10100101 01101111 0000
D2: 01101110 11110011 0111111 1110
ही शिफ्टिंग प्रक्रिया सर्व 16 फेऱ्यांसाठी पुनरावृत्ती होते.

कॉम्प्रेशन परम्युटेशन (Compression Permutation**)**शिफ्टिंग केल्यानंतर, 56-बिट की (C आणि D भाग एकत्र करून) एका परम्युटेशन टेबलचा (Permutation Table) वापर करून 48 बिट्सपर्यंत कॉम्प्रेशन केली जाते. हे टेबल 48-बिट राउंड की तयार करण्यासाठी 56-बिट की मधून 48 विशिष्ट बिट्स निवडते.

Table 4.2: Compression Permutation Table

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

48-बिट राउंड की तयार करण्यासाठी एकत्रित 56-बिट कीमधून बिट्स निवडण्यासाठी आणि पुनर्क्रमित करण्यासाठी या टेबलचा वापर केला जातो.

उदाहरण:

राउंड 1 साठी शिफ्ट केल्यानंतर एकत्रित 56-बिट की खालील प्रमाणे गृहीत धरू:

एकत्रित C1 आणि D1:

00100100 11010010 10110111 10000011 01111001 10111111

बिट्स निवडण्यासाठी आणि पुनर्रचना करण्यासाठी कॉम्प्रेशन परम्युटेशन लागू करा:

48-बिट राउंड की (उदाहरणार्थ निवडलेले बिट्स):

111000110010001010110010000100110011010000101111

प्रत्येक राउंडसाठी ही प्रक्रिया पुनरावृत्ती करून, आपण 16 राउंडपैकी प्रत्येकासाठी एक अद्वितीय(unique) 48-बिट राउंड की तयार करतो, जी नंतर एन्क्रिप्शन प्रक्रियेत वापरली जाते.

DES मध्ये 16 फेऱ्यांमध्ये की ट्रान्सफॉर्मेशन (transformation) केले जाते. प्रत्येक फेरीसाठी, 56-बिट की मधून 48-बिट सब-की तयार केली जाते.

ब्लॉक्स (blocks) विभाजित केल्यानंतर, आपण राऊंड फंक्शन (Round function) वापरतो. प्रत्येक फेरीत, डावा अर्धा भाग जसा आहे तसाच राहतो आणि आपल्याला उजव्या अर्ध्यावर खालील ऑपरेशन्स कराव्या लागतात.

एक्सपान्शन परम्युटेशन (Expansion Permutation)

1. की मिक्सिंग (Key Mixing) ⊕

2.बस्टिट्यूशन (Substitution) (S-Boxes)(S1, S2,...,S8)

3. परम्युटेशन (Permutation)

उजव्या अर्ध्या भागातून अंतिम निकाल मिळाल्यानंतर, आपल्याला डाव्या आणि उजव्या अर्ध्या भागाचे XOR ऑपरेशन करावे लागते.

एक्सपान्शन परम्युटेशन (E): एक्सपान्शन टेबल (Expansion table) वापरून 32-बिट उजवा अर्धा भाग (विभाजन मधून)(R0) 48 बिट्सपर्यंत वाढवला जातो. येथे, प्रत्येक बिट टेबलमध्ये (Bit table) संबंधित स्थानावर दिलेल्या बिटने (Bit)बदलला जातो. एक्सपान्शन टेबल(Exapnsion Table) 32 वरून 48 बिट्सपर्यंत आकार वाढवण्यासाठी काही बिट्स डुप्लिकेट (Duplicate Bits)करते.

Table4.3:Expansion Table

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

R0 वर एक्सपान्शन परम्युटेशन (Expansion Permutation) लागू करा:

• R0 (32 बिट्स): 10101010 10101010 10101010 101010

• विस्तारित R0 (48 बिट्स): 01010101 01011010 10100101 011010 01011010 101010

1. की मिक्सिंग ⊕ (Key mixing)

विस्तारित R0 हा राउंड की (48-बिट) सह XOR केलेला आहे. मागील पायरीतील उदाहरण वापरून, राउंड 1

राउंड की (48 बिट):

111000110010001010110010000100110011010000101111

XOR ऑपरेशन करा:

10110101 00010000 00011111 01111000 01010000 00011101

सबस्टिट्यूशन (एस-बॉक्सेस (Substitution S Boxes):

एक्स ऑर (XOR) चा निकाल आठ 6-बिट ब्लॉक्समध्ये विभागला आहे आणि प्रत्येक ब्लॉक एस-बॉक्सेस वापरून बदलला आहे. येथे S1 वापर करून एक उदाहरण दिले आहे:

S1 टेबल:

प्रत्येक 6-बिट ब्लॉकचा (6 bit block) वापर एस-बॉक्समधून संबंधित 4-बिट आउटपुट (4 bit output) शोधण्यासाठी केला जातो. उदाहरणार्थ, तुम्हाला पहिल्या सब-टेबलवर एक नजर टाकावी लागेल. पहिल्या 6-बिट ब्लॉकचे उदाहरण घेऊया:

पहिला 6-बिट ब्लॉक: 101101

आडवी ओळ(row): 11 (पहिले आणि शेवटचे बिट्स)

उभी ओळ (Column): 0110 (मधले चार बिट्स)

• आउटपुट (S1[11][0110]): 0100

Table4.3: S1 Table

	S[1]															
	0	1	2	3	4	(0110) 5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
(11) 3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

सर्व 8 ब्लॉकसाठी हे करा आणि 32-बिट ब्लॉक मिळविण्यासाठी निकाल एकत्र करा.

परम्युटेशन (Permutation)

एस-बॉक्सेसचा 32-बिट निकाल एका निश्चित टेबलचा वापर करून परम्युट केला जातो:

Table 4.4: Permutation Table

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

हे परम्युटेशन लागू केल्याने राउंड फंक्शन (F) चे अंतिम 32-बिट आउटपुट मिळते.

XOR ऑपरेशन (XOR Operation)

उजव्या अर्ध्या भागाचा अंतिम निकाल मिळाल्यानंतर, आपल्याला डाव्या अर्ध्या भागाचे (L0) आणि उजव्या अर्ध्या भागाचा निकाल यांचे XOR ऑपरेशन आणि करणे आवश्यक आहे.

अंतिम 32-बिट आउटपुट F:

L0 (32 बिट्स): 11001100 00000000 11001100 11110000

XOR निकाल: L0 XOR 32-बिट निकाल F वरून

पहिल्या फेरीनंतरचा निकाल (स्वॅपिंग आवश्यक) (Swapping)

पहिल्या फेरीनंतरचा निकाल मूळ उजवा अर्धा भाग (R0) आणि XOR निकाल यांना एकत्र करून मिळतो:

• L1: <Original R0>

• R1: <XOR निकाल>

ही प्रक्रिया सर्व 16 फेऱ्यांसाठी पुनरावृत्ती केली जाते. प्रत्येक फेरीत वेगवेगळी 48-बिट सब-की (48 bit sub key)वापरली जाते आणि अंतिम निकाल 16 व्या फेरीनंतर मिळतो, त्यानंतर अंतिम क्रमपरिवर्तन (FP) होते. याचे अनुसरण करून, DES वापरून प्लेनटेक्स्टचे (plain text)सायफर टेक्स्टमध्ये (Cipher text))रूपांतर केले जाते.

4.2 एईएस (AES)(ऍडव्हान्स एन्क्रिप्शन स्टॅंडर्ड) अल्गोरिदम (Advanced Encryption Standard Algorithm)**:**

ॲडव्हान्स्ड एन्क्रिप्शन स्टँडर्ड (AES) हा एक अत्यंत विश्वासार्ह एन्क्रिप्शन अल्गोरिथम आहे जो योग्य की(Key) शिवाय डेटा वाचता न येणाऱ्या स्वरूपात रूपांतरित करून सुरक्षित करण्यासाठी वापरला जातो. ए ई एस एन्क्रिप्शन (AES Encryption) अनधिकृत प्रवेशापासून मजबूत संरक्षण प्रदान करण्यासाठी विविध की लांबी (Key length)(128, 192 किंवा 256 बिट्स) वापरते. हा डेटा सुरक्षा उपाय इंटरनेट कम्युनिकेशन (internet communication)सुरक्षित करण्यासाठी, संवेदनशील डेटाचे

संरक्षण करण्यासाठी आणि फाईल एन्क्रिप्ट (File Encrypt)करण्यासाठी व्यापकपणे अंमलात आणला जातो. आधुनिक क्रिप्टोग्राफीचा (Cryptography) आधारस्तंभ म्हणून ए ई एस, सायबर धोक्यांपासून माहिती सुरक्षित ठेवण्याच्या क्षमतेसाठी जागतिक स्तरावर ओळखला जातो. ए ई एस हा ब्लॉक सायफर आहे . की आकार (Key Length)128/192/256 बिट्स असू शकतो. प्रत्येकी 128 बिट्सच्या ब्लॉकमध्ये (128 bits block) डेटा एन्क्रिप्ट (data encrypt) केला जातो.

ए ई एस बिट्स (AES bits) ऐवजी डेटाच्या बाइट्सवर (data bytes) ऑपरेशन्स (operations) करते. ब्लॉकचा आकार 128 बिट्स(bits) असल्याने, सायफर एका वेळी इनपुट डेटाच्या 128 बिट्स (किंवा 16 बाइट्स) प्रक्रिया करतो.

राउंड्सची संख्या खालीलप्रमाणे की लांबीवर अवलंबून असते:

• 128-बिट की - 10 राउंड्स
• 192-बिट की - 12 राउंड्स
• 256-बिट की - 14 राउंड्स

राऊंड की ची निर्मिती (Creation of Round Keys):

इनिशिअल की (Initial Key)चा वापर अनेक वेगवेगळ्या राऊंड की (Round Key))तयार करण्यासाठी केला जातो ज्या एन्क्रिप्शनच्या (Encryption)संबंधित फेरीत वापरल्या जातील.

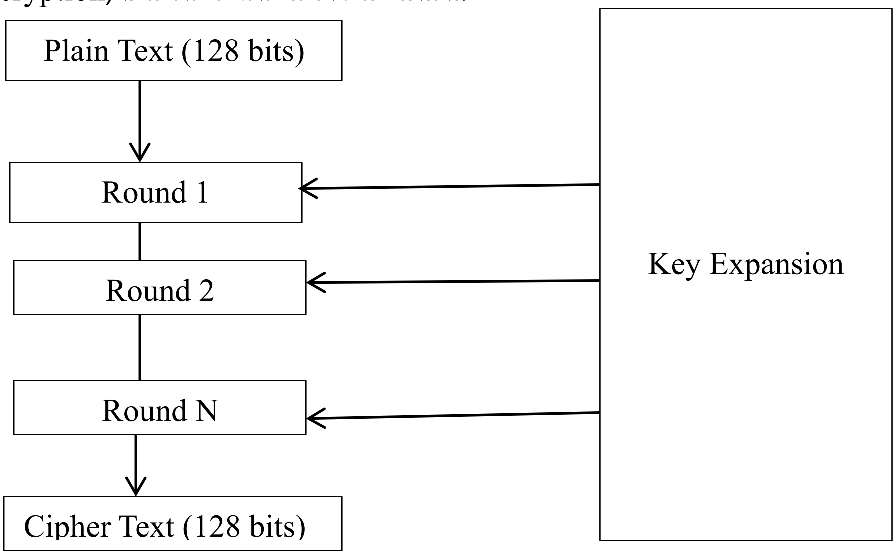


Figure4.2: Rounds Key Generation

एन्क्रिप्शन (Encryption)

ए ई एस (AES)प्रत्येक ब्लॉकला (block) कॉलम-मेजर (column major)व्यवस्थेमध्ये 16-बाइट (16 byte) (4 बाइट x 4 बाइट = 128) ग्रिड (grid) मानते.

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

प्रत्येक फेरीत 4 पायऱ्या असतात (Each round comprises of 4 steps):

• सबबाइट्स (128 बिट्स की साठी - 10 राउंड)(SubBytes For 128 bits key – 10 rounds)
• शिफ्ट रो (ShiftRows)
• मिक्स कॉलम्स (MixColumns)
• राउंड की जोडा (Add Round Key)

शेवटच्या राउंडमध्ये मिक्स कॉलम्स राउंड नाही.

128 बिट्स की साठी (for 128 bits key)

- सबबाइट्स - 10 राउंड्स (SubBytes – 10 rounds)
- शिफ्टरो ज - 10 राउंड्स (ShiftRows – 10 rounds)
- मिक्स कॉलम्स - 9 राउंड्स (MixColumns – 9 rounds)
- राउंड की जोडा - 10 राउंड्स (Add Round Key – 10 rounds)

सबबाइट्स सबस्टिट्यूशन (SubBytes Substitution) करतात आणि शिफ्ट रो (ShiftRows)आणि मिक्स कॉलम्स (mix columns)अल्गोरिदममध्ये (algorithm) परम्युटेशन (permutation) करतात.

सब बाइट्स (Sub Bytes)

ही स्टेप सबस्टिट्यूशन (Substitution) करते.

या पायरीमध्ये, प्रत्येक बाइट दुसऱ्या बाइटने बदलला(replace) जातो. हे एस-बॉक्स (S-Box) नावाच्या लुकअप (lookupTable)टेबलचा वापर करून केले जाते. हे सबस्टिट्यूशन (Substitution) अशा प्रकारे केले जाते की एक बाइट(Byte) कधीही स्वतःशी किंवा स्वतःच्या पूरक(Compliment) शी बदलला जात नाही. या स्टेप नंतर पूर्वीसारखा 16-बाइट (4 x 4) मॅट्रिक्स(matrix) मिळतो.

		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	a	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	b	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	c	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	d	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	e	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	f	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure4.3: S-Box

पुढील दोन स्टेप पेरमुटेशन करतात.

शिफ्ट रोज (Shift Rows):

ह्या स्टेप मध्ये प्रत्येक ओळ (row) विशिष्ट वेळा हलवली जाते.

- पहिली ओळ (first row) हलवली जात नाही (The first row is not shifted)
- दुसरी ओळ (second row)एकदा डावीकडे हलवली जाते. (The second row is shifted once to the left)
- तिसरी ओळ दोनदा डावीकडे हलवली जाते. (The third row is shifted twice to the left.)
- चौथी ओळ तीनदा डावीकडे हलवली जाते .(The fourth row is shifted thrice to the left.)

(डावीकडे वर्तुळाकार शिफ्ट केली जाते.)

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

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

मिक्स कॉलम्स (Mix Columns)

ह्या स्टेपमध्ये मॅट्रिक्स गुणाकार (matrix multiplication) केला जातो. प्रत्येक स्तंभ(Column) एका विशिष्ट मॅट्रिक्सने गुणाकार (matrix multiplication) केला जातो आणि त्यामुळे स्तंभातील (column) प्रत्येक बाइटची (byte)बदलते.

शेवटच्या फेरीत ही स्टेप वगळली जाते.

C0
C1
C2
C3

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

B0
B1
B2
B3

राउंड की जोडा (Add round Keys)

आता मागील टप्प्याचे आउटपुट (output) संबंधित राउंड की (Round Key)सह एक्स ऑर(XOR) केले आहे. येथे, 16 बाइट्स ग्रिड (16 bytes grid) म्हणून मानले जात नाहीत तर फक्त 128 बिट्स डेटा (128 bits data) म्हणून मानले जातात.

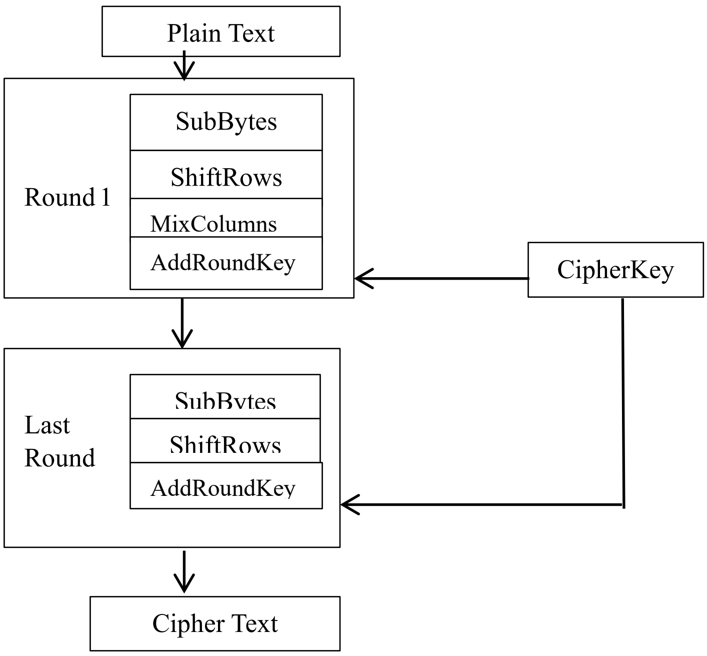


Figure 4.4 Add Round Keys in AES (Courtesy:geeksforgeeks.org)

या सर्व फेऱ्यांनंतर 128 बिट्स एन्क्रिप्टेड डेटा आउटपुट(128 bits encrypted data) म्हणून दिला जातो. जोपर्यंत सर्व एन्क्रिप्टेड डेटा (encrypted data) या प्रक्रियेतून जात नाही तोपर्यंत ही प्रक्रिया पुनरावृत्ती होते.

4.3 आरएसए अल्गोरिथम (RSA Algorithm)

आरएसए हा सर्वात सामान्य पब्लिक-की अल्गोरिथम (public key algorithm)आहे, याचे नाव त्याच्या शोधक रिव्हेस्ट, शमीर आणि एडेलमन (आरएसए) (Rivest, Shamir, and Adelman (RSA) यांच्या नावावरून ठेवण्यात आले आहे.

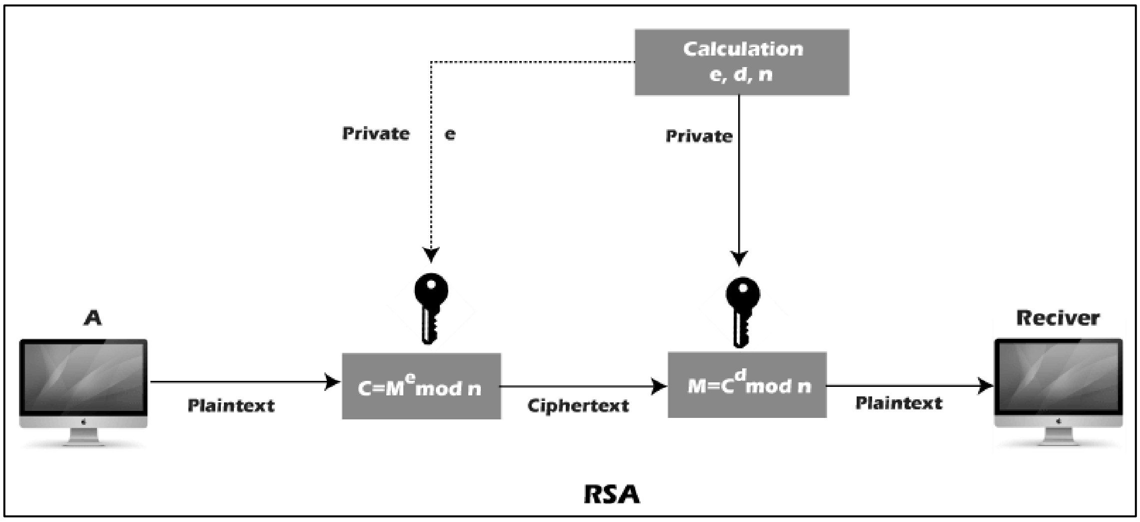


Figure 4.5 RSA Algorithm

सार्वजनिक(public) आणि खाजगी(private) की जनरेट (key generate) करण्यासाठी आरएसए अल्गोरिदम (RSA Algorithm) खालील प्रक्रिया वापरतो:

- दोन मोठ्या मूळ संख्या निवडा, p आणि q (Select two large prime numbers, p and q.)
- n = p x q शोधण्यासाठी या संख्यांचा गुणाकार (multiplication)करा, जिथे n ला एन्क्रिप्शन (Encryption) आणि डिक्रिप्शनसाठी (Decryption)मापांक(मॉड्युलस -modulus) म्हणतात.
- n पेक्षा कमी संख्या e निवडा, जेणेकरून n हा (p - 1) x (q -1) ने अविभाज्य असेल. याचा अर्थ असा की e आणि (p - 1) x (q - 1) मध्ये 1 वगळता कोणताही सामान्य घटक नाही.
  "e" असा निवडा की 1<e < φ (n), e आणि φ (n) चा अविभाज्य असेल, gcd (e,d(n)) =1
- जर n = p x q असेल, तर सार्वजनिक की < e, n> असेल. एक साधा मजकूर संदेश m सार्वजनिक की <e, n> वापरून एन्क्रिप्ट केला जातो.
  साध्या मजकुरातून (plain text)सायफर टेक्स्ट (cipher text) शोधण्यासाठी खालील सूत्र वापरले जाते जेणेकरून सायफरटेक्स्ट ((cipher text)) C मिळेल.
  $C = m^e \bmod n$
  येथे, m हा n पेक्षा कमी असणे आवश्यक आहे. मोठा संदेश (>n) हा संदेशांचा संच म्हणून मानला जातो, ज्यापैकी प्रत्येक संच स्वतंत्रपणे एन्क्रिप्ट केला जातो.
- खाजगी की (private key) निश्चित करण्यासाठी, आपण d खालील सूत्र वापरून शोधतो :
  $D_e \bmod \{(p - 1) \times (q - 1)\} = 1$ किंवा $D_e \bmod \varphi(n) = 1$
- खाजगी की <d, n> आहे. खाजगी की <d, n> वापरून एक सायफर टेक्स्ट c डिक्रिप्ट केला जातो. सायफर टेक्स्ट c मधून साधा मजकूर m मिळविण्यासाठी खालील सूत्र वापरले जाते.
  $m = c^d \bmod n$

खाली दिलेले उदाहरण दाखवते की आपण आरएसए (RSA)सार्वजनिक-की एन्क्रिप्शन अल्गोरिदम (public key Encryption Algorithm)वापरून साधा मजकूर(plain text) 9 (nine) कसा एन्क्रिप्ट करू शकतो. हे उदाहरण सार्वजनिक आणि खाजगी की (Public key and Private Key generate)जनरेट करण्यासाठी अविभाज्य संख्या(prime no) 7 आणि 11 वापरते.

स्पष्टीकरण(Explanation**):**

स्टेप 1: दोन मोठ्या मूळ संख्या निवडा, p, आणि q.

p = 7

q = 11

स्टेप 2: n = p x q शोधण्यासाठी या संख्यांचा गुणाकार करा, जिथे n ला एन्क्रिप्शन आणि डिक्रिप्शनसाठी मॉड्युलस म्हणतात. प्रथम, n शोधूया

n = p x q

n = 7 x 11

n = 77

स्टेप 3: n पेक्षा कमी e संख्या निवडा, म्हणजे n हा (p - 1) x (q -1) च्या तुलनेत मूळ असेल. याचा अर्थ असा की e आणि (p - 1) x (q - 1) मध्ये 1 व्यतिरिक्त कोणताही सामान्य घटक नाही. "e" निवडा जेणेकरून $1<e < \varphi (n)$, e हा φ (n) चा मूळ असेल, आणि gcd (e, d (n)) =1.

φ (n) = (p - 1) x (q-1)

φ (n) = (7 - 1) x (11 - 1)

φ (n) = 6 x 10

φ (n) = 60

आता आपण 60 चा सापेक्ष मूळ(relative prime) e 7 म्हणून निवडू.

अशा प्रकारे सार्वजनिक की <e, n> = (7, 77) आहे.

स्टेप 4: एक साधा संदेश m पब्लिक की <e, n> वापरून एन्क्रिप्ट केला जातो. साध्या मजकुरातून सायफर टेक्स्ट शोधण्यासाठी खालील सूत्र वापरले जाते.

$C = m^e \bmod n$

$C = 9^7 \bmod 77$

C = 37

स्टेप 5: खाजगी की (private key) <d, n> आहे. खाजगी की निश्चित करण्यासाठी, आपण खालील प्रमाणे d वापरतो :

$D_e \bmod \{(p - 1) x (q - 1)\} = 1$

7d mod 60 = 1, जे d = 43 देते

खाजगी की <d, n> = (43, 77) आहे.

स्टेप 6: खाजगी की <d, n> वापरून सायफर टेक्स्ट मेसेज c डिक्रिप्ट केला जातो सायफर टेक्स्ट c मधून साधा मजकूर m काढण्यासाठी खालील सूत्र वापरले जाते.

$m = c^d \bmod n$

$m = 37^{43} \bmod 77$

m = 9

या उदाहरणात, साधा मजकूर = 9 आणि सायफरटेक्स्ट = 37

4.4 डिफी-हेलमन की एक्सचेंज (Diffie-Hellman Key Exchange):

डिफी-हेलमन की एक्सचेंज (Diffie-Hellman Key Exchange) ज्याला एक्सपोनेन्शियल की एक्सचेंज (exponential key exchange)असेही म्हणतात, ही असुरक्षित चॅनेलवर (insecure channel) क्रिप्टोग्राफिक की (Cryptographic Key) सुरक्षितपणे एक्सचेंज (exchange)करण्याची एक पद्धत आहे. SSL/TLS आणि SSH सह अनेक सुरक्षित कम्युनिकेशन प्रोटोकॉलचा (Secure Communication Protocol)हा एक मूलभूत घटक आहे.

डिफी-हेलमन की एक्सचेंज (Diffie-Hellman Key Exchange)दोन पक्षांना (ॲलिस (Alice) आणि बॉब (Bob)) असुरक्षित चॅनेलवर सामायिक केलेल्या गुप्त कीवर (Shared private key) सहमती देण्यास परवानगी देऊन कार्य करते, इतर कोणताही पक्ष की(key) रोखू शकत नाही किंवा त्याबद्दल काहीही शिकू शकत नाही.

की(key) खालील प्रमाणे एक्सचेंज (Key Exchange) होतात -

• ॲलिस आणि बॉब दोन मोठ्या मूळ संख्या, p आणि g आणि सार्वजनिक की एक्सचेंज अल्गोरिथमवर सहमत आहेत.
• ॲलिस एक गुप्त संख्या, a निवडते आणि A = g^a mod p ची गणना करते. ती A ला बॉबला पाठवते.
• बॉब गुप्त संख्या, b निवडतो आणि B = g^b mod p ची गणना करतो. तो B ला ॲलिसला पाठवतो.

ॲलिस s = B^a mod p शोधते.
बॉब s = A^b mod p शोधते.
ॲलिस आणि बॉब दोघांकडे आता गुप्त की(private key) आहेत, ज्याचा वापर ते सुरक्षित कम्युनिकेशन (Communication) चॅनेल स्थापित करण्यासाठी करू शकतात.
डिफी-हेलमन की एक्सचेंजची (Diffie-Hellman Key Exchange) सुरक्षा, आक्रमणकर्त्याला p, g, A आणि B च्या सार्वजनिक मूल्यांमधून सामायिक गुप्त की निश्चित करणे संगणकीयदृष्ट्या अशक्य आहे या वस्तुस्थितीवर अवलंबून असते. यामुळे ॲलिस आणि बॉबला असुरक्षित चॅनेलवरून देखील सुरक्षितपणे की एक्सचेंज करण्याची परवानगी मिळते.
उदाहरण:
स्टेप 1: ॲलिस आणि बॉब यांना सार्वजनिक क्रमांक मिळतात P = 23, G = 9
स्टेप 2: ॲलिसने एक खाजगी की निवडली a = 4 आणि
बॉबने एक खाजगी की निवडली b = 3
स्टेप 3: ॲलिस आणि बॉब सार्वजनिक मूल्यांची गणना करतात
ॲलिस: x =(9^4 mod 23) = (6561 mod 23) = 6
बॉब: y = (9^3 mod 23) = (729 mod 23) = 16
स्टेप 4: ॲलिस आणि बॉब सार्वजनिक क्रमांकांची देवाणघेवाण करतात
स्टेप 5: ॲलिसला सार्वजनिक की मिळते y =16 आणि
बॉबला सार्वजनिक की मिळते x = 6
स्टेप 6: ॲलिस आणि बॉबला सिमेट्रिक कींची(Symmetric Key) गणना करतात.
ॲलिस: ka = y^a मॉड p = 65536 mod 23 = 9
बॉब: kb = x^b मॉड p = 216 mod 23 = 9
स्टेप 7: 9 हे सामायिक गुपित (Shared Secrete) आहे.

4.4.1 मॅन-इन-द-मिडल Attacks (Man-in-the-middle (MITM) Attacks) हल्ले

एमआयटीएम हल्ला(attack) हा सायबर हल्ल्याचा एक प्रकार आहे जिथे वापरकर्त्याला एका द्वेषयुक्त व्यक्तीकडून(malicious individual) दोन्ही पक्षांमधील एखाद्या प्रकारच्या बैठकीची आयडेंटिटी (Identity)करून दिली जाते, ती दोन्ही पक्षांना हाताळते आणि दोन्ही लोक एकमेकांना पोहोचवण्याचा प्रयत्न करत असलेल्या डेटामध्ये ॲक्सेस (Access) मिळवते. एमआयटीएम (MITM attack) हल्ला हा द्वेषयुक्त हल्लेखोराला(attacker), कोणत्याही सहभागीला ओळखल्याशिवाय, कोणासाठी तरी पाठवायचा असलेला आणि अजिबात पाठवायचा नसलेला डेटा हॅक (data hack) करण्यास मदत करतो. जेव्हा एखादा हल्लेखोर(attacker) स्वतःला क्लायंट (client)आणि वेबपेजच्या (webpage)मध्ये आणतो, तर मॅन-इन-द-मिडल (MITM) हल्ला होतो. या प्रकारचा हल्ला अनेक वेगवेगळ्या प्रकारे येतो.
उदाहरणार्थ, आर्थिक लॉगिन क्रेडेन्शियल्स रोखण्यासाठी, फसव्या बँकिंग वेबसाइटचा वापर केला जाऊ शकतो. वापरकर्ता आणि खऱ्या बँक वेबपेजमध्ये, बनावट साइट "मध्यभागी" असते.

एमआयटीएम कसे काम करते (How does MITM work)

हॅकर्स एमआयटीएम (hackers MITM) हल्ला वापरण्यासाठी अनेक कारणे आणि रणनीती(stratergies) आहेत. सहसा, क्रेडिट कार्ड नंबर (credit card number)किंवा वापरकर्ता लॉगिन तपशीलांसारखे (user login details), ते काहीही ॲक्सेस (access)करण्याचा प्रयत्न करतात. ते खाजगी बैठकांवर देखील हेरगिरी(spy) करतात, ज्यामध्ये कॉर्पोरेट गुपिते किंवा इतर उपयुक्त माहिती असू शकते.

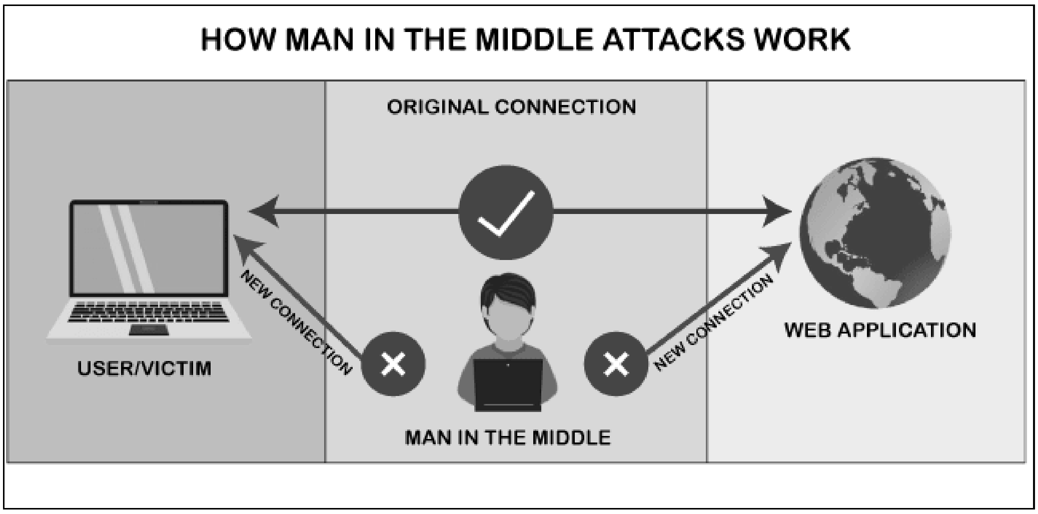


Figure 4.6 Working of MITM (Courtesy: javatpoint.com)

वर दाखविल्याप्रमाणे , तुम्ही पाहू शकता की घुसखोराने क्लायंट आणि सर्व्हरमध्ये स्वतःला उभे केले जेणेकरून गोपनीय डेटा रोखता येईल किंवा त्यांची माहिती हाताळता येईल.

एमआयटीएम हल्ल्याचे प्रकार:

- वाय-फाय इव्हसड्रॉपिंग (Wi-fi Eavesdropping)
- डीएनएस स्पूफिंग (DNS Spoofing)
- आयपी स्पूफिंग (IP Spoofing)
- एचटीटीपीएस स्पूफिंग (HTTPS Spoofing)
- एआरपी स्पूफिंग (ARP Spoofing)
- ई-मेल हॅकिंग (E-mail Hacking)
- सेशन हॅकिंग (Session Hacking)
- एसएसएल स्ट्रिपिंग (SSL Stripping)
- एमआयटीबी हल्ला (MITB attack)

• **वाय-फाय इव्हसड्रॉपिंग** (Wi-fi Eavesdropping)

जर तुम्ही कॅफेमध्ये डिव्हाइस (device) वापरले असेल तर "हे कनेक्शन सुरक्षित नाही" असे सूचित करणारी सूचना तुम्ही पाहिली असेल. सार्वजनिक वाय-फाय सामान्यतः सेवेच्या गुणवत्तेचे कोणतेही आश्वासन न देता, "जसे आहे तसे" दिले जाते. अनक्रिप्टेड वाय-फाय नेटवर्क (Uncrypted wifi network)पाहणे सोपे आहे. कोणीही त्यात सामील होऊ शकते. तुम्ही तुमचा संगणक "सार्वजनिक" वर सेट करून तुमचा ॲक्सेस (Access) मर्यादित करू शकता, जे नेटवर्क डिस्कव्हरी (network discovery)अक्षम करते. हे नेटवर्कवरील इतर वापरकर्त्यांना सिस्टमचा (system) गैरफायदा घेण्यापासून रोखते. हल्लेखोर स्वतःचा "एव्हिल ट्विन" वाय-फाय हॉटस्पॉट (Evil Twin" wi-fi hotspot)स्थापित करतो तेव्हा इतर वाय-फाय स्नूपिंग हल्ला होतो. हल्लेखोर नेटवर्क पत्ता(address) आणि पासवर्डद्वारे लिंक खऱ्या लिंकसारखीच बनवतो. वापरकर्ते अनावधानाने किंवा आपोआप "एव्हिल ट्विन" शी लिंक करतील, ज्यामुळे हल्लेखोर त्यांच्या कृतींमध्ये घुसखोरी करू शकेल.

• **डी एन एस स्पूफिंग** (DNS Spoofing)

साइट IP पत्त्यांसह कार्य करते जसे की 192.156.65.118 हा Google चा एक पत्ता (address) आहे. डी एन एस (DNS) सर्व्हर हा असा सर्व्हर आहे जो 192.156.65.118 ला google.com मध्ये रूपांतरित करतो. हल्लेखोर एक फसवा वेब सर्व्हर विकसित करू शकतो. फसवा सर्व्हर एका विशिष्ट वेब पत्त्याला एका अद्वितीय(unique) IP पत्त्यावर स्थानांतरित करतो, ज्याला "स्पूफिंग" म्हणतात.

• **आयपी स्पूफिंग** (IP Spoofing)
आपल्या सर्वांना माहित आहे की, एकाच नेटवर्कशी जोडलेल्या अनेक उपकरणांमध्ये एक आयपी ॲड्रेस असतो. आयपी स्पूफिंगमध्ये (IP Spoofing), हल्लेखोर मान्यताप्राप्त कन्सोलच्या (console) आयपी ॲड्रेसची(IP Address) नक्कल करतात. नेटवर्कसाठी, ते सिस्टम अधिकृत असल्यासारखे दिसते. मिडल-इन-द-मॅन हल्ल्यात (Middle Man In the Attack), दोन उपकरणांमध्ये ठेवून आयपी स्पूफिंग (IP Spoofing) देखील वापरले जाऊ शकते. उदाहरणार्थ, डिव्हाइस ए (Device A) आणि डिव्हाइस बी ((Device B)असे गृहीत धरतात की ते एकमेकांशी संवाद साधतात, परंतु दोन्ही अडवले जातात आणि हल्लेखोराशी संवाद साधला जातो.
डिव्हाइस ए ((Device A) = = = हल्लेखोर = = = डिव्हाइस बी ((Device B)

• **एच टी टी पी एस स्पूफिंग** (HTTPS Spoofing)
एच टी टी पी एस वेबपेजची डुप्लिकेट करणे सध्या शक्य नाही. हल्लेखोर एक अधिकृत पत्ता (authoritative address) तयार करतो. ते मानक(standard) स्क्रिप्टऐवजी आंतरराष्ट्रीय अक्षरे(Internation Letters) वापरते. हे तुम्ही वापरलेल्या असामान्य वर्णांसह (character) फिशिंग ईमेल म्हणून काम करते. उदाहरणार्थ, Rolex ला Rólex लिहिले जाऊ शकते.

• **एरपी स्पूफिंग** (ARP Spoofing)
एरपी म्हणजे ॲड्रेस रिझोल्यूशन (address resolution)वरील प्रोटोकॉल क्लायंटकडून एरपी रिक्वेस्ट(request) पाठवली जाते आणि हल्लेखोर फसवा प्रतिसाद देतो. या परिस्थितीत हल्लेखोर हा संगणक मोडेम (computer modem)सारखा असतो, जो हल्लेखोराला ट्रॅफिक फ्लोमध्ये (traffic flow) ऍक्सेस (Access) करण्यास सक्षम करतो. सहसा, ज्या स्थानिक क्षेत्र नेटवर्क (LAN) मध्ये, एरपी प्रोटोकॉल (ARP Protocol) वापरला जातो, त्यापुरते मर्यादित असते.

• **ई-मेल हॅकिंग** (E-mail Hacking)
अशा प्रकारच्या सायबरसुरक्षा घुसखोरीमध्ये हल्लेखोर वापरकर्त्याच्या ईमेल सिस्टमचा (Email system) गैरफायदा घेतो. घुसखोर देखील शांतपणे पाहतो, डेटा गोळा करतो आणि ईमेलद्वारे चर्चेवर लक्ष ठेवतो. हल्लेखोरांकडे एक स्कॅन पॅटर्न (scan pattern)असू शकतो जो "आर्थिक" किंवा "लपलेले लोकशाही धोरण"(Hidden Democratic Policies) सारखे लक्ष्यित कीवर्ड(keyword) शोधतो. सोशल इंजिनिअरिंगद्वारे, ईमेल हॅकिंग उत्तम प्रकारे कार्य करते. ऑनलाइन मित्राची नक्कल करण्यासाठी, हल्लेखोर एखाद्या प्रकारच्या हायजॅक केलेल्या ईमेल पत्त्यावरील संबंधित डेटा वापरू शकतात. वापरकर्त्याला द्वेषयुक्त ॲप्स(malicious app) डाउनलोड करण्यास फसवण्यासाठी स्पियर-फिशिंगचा वापर देखील केला जाऊ शकतो.

• **सेशन हॅकिंग** (Session Hacking)
सामान्यतः, MITM हल्ल्याचा हा प्रकार सोशल मीडिया प्लॅटफॉर्म हॅक करण्यासाठी वापरला जातो. बहुतेक सोशल मीडिया प्लॅटफॉर्मसाठी पीडिताच्या मशीनवर वेबपेजमध्ये "सेशन ब्राउझर कुकी" असते. जर ती व्यक्ती तिथून निघून गेली तर ही कुकी खोटी ठरते. परंतु जेव्हा सेशन चालू असते तेव्हा कुकी ओळख, एक्सपोजर आणि मॉनिटरिंग डेटा देते. जेव्हा सेशन हायजॅक होतो तेव्हा घुसखोर कॉन्फिगरेशन कुकी चोरतो. जोपर्यंत पीडिताचे खाते मालवेअर किंवा ॲप्लिकेशन हल्लेखोरांनी हॅक केले जात नाही तोपर्यंत ते उद्भवू शकते. जर वापरकर्ता XSS क्रॉस-स्क्रिप्टिंग घुसखोरीचा वापर करत असेल, ज्यामध्ये हॅकर सामान्यतः भेट दिलेल्या साइटमध्ये द्वेषयुक्त स्क्रिप्ट इंजेक्ट करतो, तर ते होऊ शकते.

• **एस एस एल स्ट्रिपिंग** (SSL Stripping-Secure Socket Layer Scripting)
एस एस एल म्हणजे सिक्योर सॉकेट लेयर. जर तुम्हाला वेबसाइट पत्त्याच्या पुढे http:/ ऐवजी https:/ दिसत असेल तर एस एस एल हा सुरक्षा मानक वापरला जातो . हल्लेखोर एस एस एल स्ट्रिपिंग वापरून वापरकर्त्याकडून डेटा पॅकेट ॲक्सेस करतो आणि रूट करतो:
वापरकर्ता = = = = एन्क्रिप्टेड वेबसाइट वापरकर्ता = = = = प्रमाणित वेबसाइट
वापरकर्ता सुरक्षित असलेल्या वेबसाइटशी लिंक करण्याचा प्रयत्न करतो. क्लायंटच्या खात्यात, हल्लेखोर सुरक्षित वेबसाइटशी एन्क्रिप्ट करतो आणि लिंक करतो. सहसा, हल्लेखोर ग्राहकांना सादर करण्यासाठी बनावट डिझाइन विकसित करतो. पीडिताला वाटते की त्यांनी सामान्य वेबसाइटवर साइन इन केले आहे, परंतु प्रत्यक्षात त्यांनी हॅकरच्या वेबसाइटवर साइन इन केले आहे. हल्लेखोराने पीडिताच्या डेटा कनेक्शनमधून एस एस एल प्रमाणपत्र "काढून टाकले" असते.

• **एमआयटीबी हल्ला** (MITB attack)

हा हल्ला इंटरनेट ब्राउझरच्या (internet browser)सुरक्षा त्रुटींचा फायदा घेतो. ट्रोजन (trozen), डेस्कटॉप वर्म्स (desktop worms), जावा असुरक्षा (Java vulnerabilities), एस क्यू एल (SQL) इंजेक्शन हल्ले आणि वेब ब्राउझिंग ॲड-ऑन (web browsing add-ons) हे द्वेषयुक्त हल्ले (malicious attacks) आहेत. हे सामान्यतः आर्थिक माहिती गोळा करण्यासाठी वापरले जातात. वापरकर्ता त्यांच्या बँक खात्यात साइन इन करत असताना मालवेअर त्यांचे पासवर्ड चोरतो. काही प्रकरणांमध्ये, मालवेअर स्क्रिप्ट पैसे हलवू शकतात आणि नंतर व्यवहार लपविण्यासाठी व्यवहाराची पावती बदलू शकतात.

एमआयटीएम हल्ल्यापासून बचाव करण्यासाठी (Man in the middle attack prevention**):**

• पासवर्ड संरक्षित नसलेले वायफाय कनेक्शन (wifi connection) टाळणे.
• वेबसाइट असुरक्षित असल्याचे नोंदवणाऱ्या ब्राउझर (Browser) सूचनांकडे लक्ष देणे.
• सुरक्षित ॲप वापरात नसताना त्वरित लॉग आउट (Log out) करणे.
• संवेदनशील व्यवहार करताना सार्वजनिक नेटवर्क (उदा. कॉफी शॉप, हॉटेल) न वापरणे.

4.5 हॅश फंक्शन (Hash Function)

हॅश फंक्शन (Hash Function) हे इनपुट (किंवा 'संदेश') घेते आणि निश्चित-आकाराची स्ट्रिंग बाइट्स परत करते. याचे आउटपुट, सामान्यतः एक संख्या येते, याला हॅश कोड किंवा हॅश व्हॅल्यू म्हणतात. हॅश फंक्शनचा मुख्य उद्देश म्हणजे अनियंत्रित आकाराचा डेटा निश्चित-आकाराच्या मूल्यांमध्ये (values) कार्यक्षमतेने मॅप करणे, जे बहुतेकदा हॅश टेबलमध्ये निर्देशांक(Index) म्हणून वापरले जातात.

हॅश फंक्शन्सचे प्रमुख गुणधर्म (Key Properties of Hash Functions**)**

• निर्धारक(Deterministic) हॅश फंक्शनने एकाच इनपुटसाठी सातत्याने समान आउटपुट तयार केले पाहिजे.
• निश्चित आउटपुट आकार(Fixed Output Size): हॅश फंक्शनच्या (Hash Function) इनपुटचा आकार कितीही असला तरी त्याचा आउटपुट आकार निश्चित असावा.
• कार्यक्षमता(Efficiency): हॅश फंक्शन (Hash Function) इनपुटवर जलद प्रक्रिया करण्यास सक्षम असावे.
• एकरूपता(Uniformity): हॅश फंक्शनने क्लस्टरिंग (Hash Function Clustering) टाळण्यासाठी आउटपुट स्पेसमध्ये हॅश व्हॅल्यूज (Hash Values)समान रीतीने वितरित केल्या पाहिजेत.
• प्री-इमेज रेझिस्टन्स (Pre-image Resistance): हॅश फंक्शन (Hash Function) उलट करणे संगणकीयदृष्ट्या अशक्य असावे, म्हणजेच हॅश व्हॅल्यू (Hash Values) दिलेली असताना मूळ इनपुट शोधणे अवघड आहे.
• कोलिझीन रेझिस्टन्स (Collision Resistance) समान हॅश व्हॅल्यू देणारे दोन वेगवेगळे इनपुट शोधणे कठीण असावे.
• हिमस्खलन परिणाम(Avalanch Effect): इनपुटमध्ये थोडासा बदल लक्षणीयरीत्या भिन्न हॅश व्हॅल्यू निर्माण करेल.

4.5.1 एम डी5 (MD5)

एमडी 5 हा एक क्रिप्टोग्राफिक हॅश फंक्शन अल्गोरिथम (Cryptographic Hash Function Algorithm) आहे जो कोणत्याही लांबीचा संदेश इनपुट म्हणून घेतो आणि तो 16 बाइट्सच्या (16 bytes) निश्चित-लांबीच्या संदेशात बदलतो. एमडी 5 अल्गोरिथम म्हणजे मेसेज-डायजेस्ट अल्गोरिथम. एम डी 5 हा 1991 मध्ये रोनाल्ड रिव्हेस्ट यांनी एमडी 4 मध्ये सुधारणा म्हणून प्रगत सुरक्षा हेतूंसह विकसित केला होता. एम डी5 चे आउटपुट नेहमीच 128 बिट (128 bit)असते.

एम डी 5 अल्गोरिथमचे कार्य (Working of the MD5 Algorithm**):**

1. पॅडिंग बिट्स जोडा (Append Padding Bits): पहिल्या चरणात, आपण मूळ संदेशात पॅडिंग बिट्स अशा प्रकारे जोडतो की संदेशाची एकूण लांबी 512 च्या अचूक पटापेक्षा 64 बिट्स कमी असेल.

समजा आपल्याला 1000 बिट्सचा संदेश दिला गेला आहे. आता आपल्याला मूळ संदेशात पॅडिंग बिट्स जोडावे लागतील. येथे आपण मूळ संदेशात 472 पॅडिंग बिट्स जोडू. पॅडिंग बिट्स जोडल्यानंतर पहिल्या चरणातील मूळ संदेश/आउटपुटचा आकार 1472 असेल म्हणजेच 512 च्या अचूक पटापेक्षा 64 बिट्स कमी असेल (म्हणजे 512*3 = 1536).

लांबी (मूळ संदेश + पॅडिंग बिट्स) = 512 * i – 64 जिथे i = 1,2,3 . . .

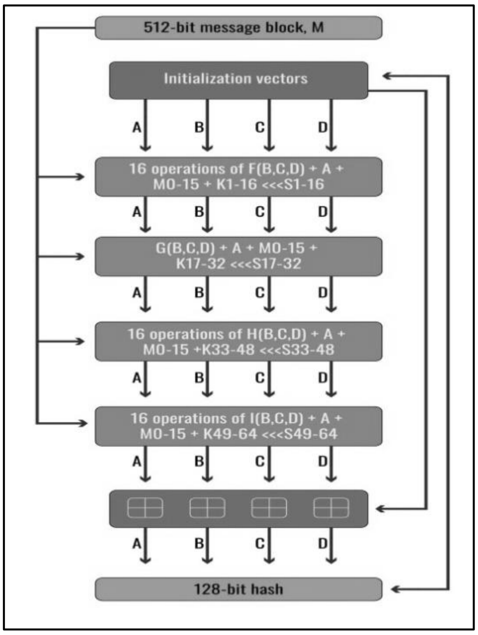


Figure 4.7 Working of MD5 Algorithm (Courtesy: comparitech.com)

2. लांबीचे बिट्स जोडा (Append Length Bits:) या स्टेप मध्ये, आपण पहिल्या स्टेप च्या आउटपुटमध्ये लांबीचा बिट (length bit) अशा प्रकारे जोडतो की बिट्सची एकूण संख्या 512 च्या परिपूर्ण गुणाकाराइतकी असेल. फक्त, येथे आपण पहिल्या स्टेप च्या आउटपुटमध्ये लांबीचा बिट म्हणून 64-बिट जोडतो.

म्हणजे पहिल्या स्टेप चे आउटपुट = 512 * n – 64

लांबीचे बिट्स (length bits) = 64.

दोन्ही जोडल्यानंतर आपल्याला 512 * n मिळेल म्हणजेच 512 चा अचूक गुणाकार.

3. एम डी बफर सुरू करा (Initialize MD buffer): येथे, आपण 4 बफर (Buffer) वापरतो म्हणजे A B, C आणि D. प्रत्येक बफरचा (Buffer) आकार ३२ बिट्स (32 bits)आहे.

- A = 0x67425301
- B = 0xEDFCBA45
- C= 0x98CBADFE
- D = 0x13DCE476

4. प्रत्येक 512-बिट ब्लॉकवर प्रक्रिया करा: एमडी 5 (MD5) अल्गोरिथमचा हा सर्वात महत्वाचा टप्पा आहे. येथे, 4 फेऱ्यांमध्ये एकूण 64 ऑपरेशन्स केल्या जातात. पहिल्या फेरीत, 16 ऑपरेशन्स केले जातात, दुसऱ्या फेरीत 16 ऑपरेशन्स केले जातात, तिसऱ्या फेरीत 16 ऑपरेशन्स केले जातात आणि चौथ्या फेरीत, 16 ऑपरेशन्स केले जातात. प्रत्येक फेरीवर एक वेगळे फंक्शन लागू केले जाते म्हणजे पहिल्या फेरीसाठी F फंक्शन, दुसऱ्या G फंक्शनसाठी, तिसऱ्या H फंक्शनसाठी आणि चौथ्या I फंक्शनसाठी वापरले जाते. फंक्शन्सची गणना करण्यासाठी OR, AND, XOR, आणि NOT (मूलतः हे लॉजिक गेट्स आहेत) करतो. प्रत्येक फंक्शनसाठी ३ बफर(buffer) वापर चा केला जातो म्हणजे B, C, D.

Table 4.5 : Round Process

Rounds	Process P
1	(b AND c) OR ((NOT b) AND (d))
2	(b AND d) OR (c AND (NOT d))
3	b OR c OR d
4	c OR (b OR (NOT d))

फंक्शन लागू केल्यानंतर आता प्रत्येक ब्लॉकवर एक ऑपरेशन केले जाते. ऑपरेशन्स करण्यासाठी आपल्याला
• मॉड्युलो (modulo)232 जोडणे आवश्यक आहे
• M[i] – ३२ बिट मेसेज.
• K[i] – ३२-बिट कॉन्स्टंट.
• <<<n – n बिट्सने लेफ्ट शिफ्ट.

आता इनिशिएलाइज MD बफर म्हणून इनपुट घ्या म्हणजे A, B, C, D. B चे आउटपुट C मध्ये दिले जाईल, C चे आउटपुट D मध्ये दिले जाईल आणि D चे आउटपुट J मध्ये दिले जाईल. हे केल्यानंतर आता आपण A साठी आउटपुट शोधण्यासाठी काही ऑपरेशन्स करावे लागतील.

• पहिल्या चरणात, B, C आणि D चे आउटपुट घेतले जातात आणि नंतर त्यांना F फंक्शन लागू केले जाते. आपण A सह याच्या आउटपुटसाठी मॉड्युलो 232 बिट्स जोडू.
• दुसऱ्या चरणात, आपण पहिल्या चरणाच्या आउटपुटसह M[i] बिट मेसेज जोडू.
• नंतर दुसऱ्या चरणाच्या आउटपुटमध्ये ३२ बिट कॉन्स्टंट म्हणजेच K[i] जोडू.
• शेवटी, आपण n ने लेफ्ट शिफ्ट ऑपरेशन करतो (n चे कोणतेही मूल्य असू शकते) आणि बेरीज २३२ ने मॉड्युलो करतो.

सर्व पायऱ्यांनंतर, A चा निकाल B ला दिला जातो. आता G, H आणि I च्या सर्व फंक्शन्ससाठी समान पायऱ्या वापरल्या जातील. सर्व 64 ऑपरेशन्स केल्यानंतर आपल्याला आपला मेसेज डायजेस्ट मिळेल.

आउटपुट:

शेवटी, राउंड्स पूर्ण झाल्यानंतर, बफर A, B, C आणि D मध्ये एम डी 5 चे आउटपुट असते खालच्या बिट A ने सुरू होते आणि उच्च बिट D ने संपते.

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

सिक्युअर हॅशिंग अल्गोरिदम (SHA) म्हणजे डेटा आणि प्रमाणपत्रे हॅश करण्यासाठी वापरला जाणारा अल्गोरिदम आहे, जो MD5 च्या सुधारित आवृत्तीवर आधारित आहे. बिटवाइज ऑपरेशन्स, मॉड्युलर ॲडिशन्स आणि कम्प्रेशन फंक्शन्सच्या मदतीने, हा हॅशिंग अल्गोरिदम इनपुट डेटा एका छोट्या आणि गुंतागुंतीच्या स्वरूपात बदलतो, जे समजून घेणे अशक्य असते.

सिक्युअर हॅश अल्गोरिदम (SHA) हे एक क्रिप्टोग्राफी तंत्रज्ञान आहे, जे नॅशनल सिक्युरिटी एजन्सी (NSA) द्वारे विकसित करण्यात आले आहे. त्यानंतर नॅशनल इन्स्टिट्यूट ऑफ स्टँडर्ड्स अँड टेक्नॉलॉजी (NIST) ने या तंत्रज्ञानाला प्रमाणित केले आणि विविध उद्देशांसाठी (प्रमाणीकरण, संदेश अखंडता तपासणी, डिजिटल स्वाक्षऱ्या आणि की डेरिव्हेशन) उपलब्ध केले.

SHA-256 हा इनपुट संदेश (कोणत्याही लांबीचा किंवा आकाराचा) घेतो आणि त्याचा 256-बिट (32-बाइट) हॅश व्हॅल्यू तयार करतो. हॅश व्हॅल्यू तयार करताना गुंतागुंतीच्या आणि प्रमाणित गणितीय अल्गोरिदम्सचा वापर केला जातो.

SHA प्रक्रिया

1. इनपुट (Input) : इनपुट म्हणजे मूळ संदेश असतो, जो प्राप्तकर्त्याला पाठवण्यापूर्वी हॅश केला जातो.
   उदाहरणार्थ, आपण "Hello, World!" हा संदेश घेतला.
2. प्री-प्रोसेसिंग (Preprocessing) :पुढील टप्प्यात, गरज नसलेली अक्षरे किंवा विरामचिन्हे काढून टाकुन इनपुट संदेशाचे बायनरी स्वरूपात रूपांतर केले जाते.

3. हॅशिंग (Hashing) : नंतर, प्रक्रिया केलेल्या इनपुट संदेशावर SHA हॅश फंक्शन लागू केले जाते. हे हॅश फंक्शन विविध गणितीय प्रक्रिया वापरून इनपुटला एक स्थिर आकाराच्या आउटपुटमध्ये (हॅश व्हॅल्यू) रूपांतरित करते.
4. आउटपुट (Output) : हॅश व्हॅल्यू इनपुट संदेशाच्या वास्तविकतेची पडताळणी करण्याचे साधन म्हणून काम करते. हा हॅश डेटा टॅम्परिंगमुळे (अनधिकृत बदल) झालेल्या कोणत्याही बदलांचा शोध घेण्यासाठी मदत करतो.

जर प्राप्तकर्त्याने त्याच हॅशिंग अल्गोरिदम आणि हॅश फंक्शनचा वापर करून वेगळी हॅश व्हॅल्यू मिळवली, तर याचा अर्थ संदेश बदलला गेला आहे. अशा परिस्थितीत तो संदेश अवैध मानला जातो आणि त्याला फेटाळले जाते.

सिक्युअर हॅश फंक्शन्सचे गुणधर्म (Secure Hash Function Properties):

- **कोलिजन हल्ले (Collision Attacks) :**कोलिजन अटॅक ही एक तंत्रनीती आहे, जी अटॅकर (attacker) वापरतात. यात, दोन वेगवेगळ्या इनपुटसाठी समान हॅश व्हॅल्यू शोधण्याचा प्रयत्न केला जातो आणि याचा वापर सायबर गुन्हे किंवा इतर अनधिकृत कृतींसाठी केला जातो. SHA फंक्शन कोलिजन अटॅक्सला प्रतिकार करू शकते आणि डेटा सुरक्षित ठेवण्यासाठी मदत करते. जर कोलिजन हल्ले (Collision Attacks) यशस्वी झाले, तर संवेदनशील माहितीचा (डेटा, वित्तीय व्यवहार इ.) गैरवापर होऊ शकतो, परिणामी मोठे आर्थिक नुकसान होऊ शकते.
- **ॲव्हलॉंच इफेक्ट (Avalanche Effect) :**सिक्युअर हॅश फंक्शन्समध्ये ॲव्हलॉंच इफेक्ट असतो, ज्यामुळे इनपुटमधे अगदी लहान बदल जरी झाला तरी आउटपुट (हॅश व्हॅल्यू) मोठ्या प्रमाणात बदलते. यामुळे डेटा टॅम्परिंग (अनधिकृत बदल) सहज शोधता येते. उदाहरणार्थ, जर इनपुटमध्ये एका अक्षराचा छोटासा बदल केला, तरी संपूर्ण हॅश व्हॅल्यू पूर्णतः वेगळी निर्माण होते. त्यामुळे हॅश फंक्शन डेटा अखंडता (data integrity) टिकवून ठेवण्यास उपयुक्त ठरते.

4.6 डिजिटल स्वाक्षरी (Digital Signature)

डिजिटल स्वाक्षरी (Digital Signature) हे एक गणितीय तंत्र आहे, जी डिजिटल दस्तऐवज, संदेश किंवा सॉफ्टवेअरच्या सत्यता आणि अखंडतेची पडताळणी करण्यासाठी वापरली जाते. ही हस्तलिखित स्वाक्षरी किंवा शिक्क्यासारखीच असते, पण ती अधिक सुरक्षित असते. डिजिटल स्वाक्षरीचा उद्देश डिजिटल संवादातील छेडछाड आणि प्रतिरूपण (impersonation) टाळणे आहे.

डिजिटल स्वाक्षरी दस्तऐवज(document), व्यवहार आणि डिजिटल संदेशांच्या मूळ स्रोत, ओळख आणि स्थितीचे पुरावे प्रदान करू शकते. स्वाक्षरी करणारे त्यांचा सुज्ञ संमतीचा दाखला देण्यासाठी याचा उपयोग करू शकतात.

डिजिटल स्वाक्षरी कशी कार्य करते?

हस्तलिखित स्वाक्षरीप्रमाणेच, डिजिटल स्वाक्षरी देखील प्रत्येक स्वाक्षरीकर्त्यासाठी वेगळी असते. DocuSign सारख्या डिजिटल स्वाक्षरी उपाय-प्रदाता पब्लिक की इन्फ्रास्टक्चर (Public Key Infrastructure (PKI)) नावाच्या विशिष्ट प्रोटोकॉलचे पालन करतात. या प्रणालीमध्ये दोन दीर्घ संख्यात्मक की (keys) तयार केल्या जातात – एक सार्वजनिक (public key) आणि एक खाजगी (private key).

जेव्हा एखादा व्यक्ती डिजिटल दस्तऐवज(digital document) स्वाक्षरी करतो, तेव्हा ती स्वाक्षरी त्याच्या खाजगी कीचा वापर करून तयार केली जाते, जी सुरक्षितपणे त्याच्याकडे राहते. गणितीय अल्गोरिदम एक सायफर (cipher) म्हणून कार्य करतो, जे दस्तऐवजाशी जुळणारा हॅश (hash) तयार करतो आणि त्या डेटाचे एन्क्रिपशन (encryption) करतो. परिणामी मिळालेली एन्क्रिपशन माहिती म्हणजे डिजिटल स्वाक्षरी असते. स्वाक्षरीसोबतच, दस्तऐवज स्वाक्षरी केल्याचा वेळही नमूद केली जाते. जर स्वाक्षरीनंतर दस्तऐवजात कोणताही बदल केला गेला, तर ती स्वाक्षरी अवैध ठरते.

उदाहरणार्थ, जेन एका टाइमशेअर (timeshare) विक्री करारावर तिच्या खाजगी की वापरून स्वाक्षरी करते. खरेदीदाराला हा दस्तऐवज प्राप्त होतो. सोबतच, त्याला जेनची सार्वजनिक की (public key) देखील मिळते. जर सार्वजनिक कीच्या साहाय्याने स्वाक्षरी डिक्रिप्ट करता आली नाही, तर याचा अर्थ ही स्वाक्षरी जेनने केली नाही किंवा स्वाक्षरीनंतर बदल करण्यात आला आहे. अशा परिस्थितीत, ती स्वाक्षरी अवैध मानली जाते.

डिजिटल स्वाक्षरीची अखंडता टिकवण्यासाठी, PKI प्रणालीमध्ये की अत्यंत सुरक्षित पद्धतीने तयार, संचालित आणि जतन केल्या जातात. तसेच, सर्टिफिकेट ऑथॉरिटी (Certificate Authority (CA)) सारख्या विश्वासार्ह संस्थेची आवश्यकता असते. डोक्युसाईन (DocuSign) सारखे डिजिटल स्वाक्षरी प्रदाते सुरक्षित डिजिटल स्वाक्षरीसाठी PKI मानकांचे पालन करतात.

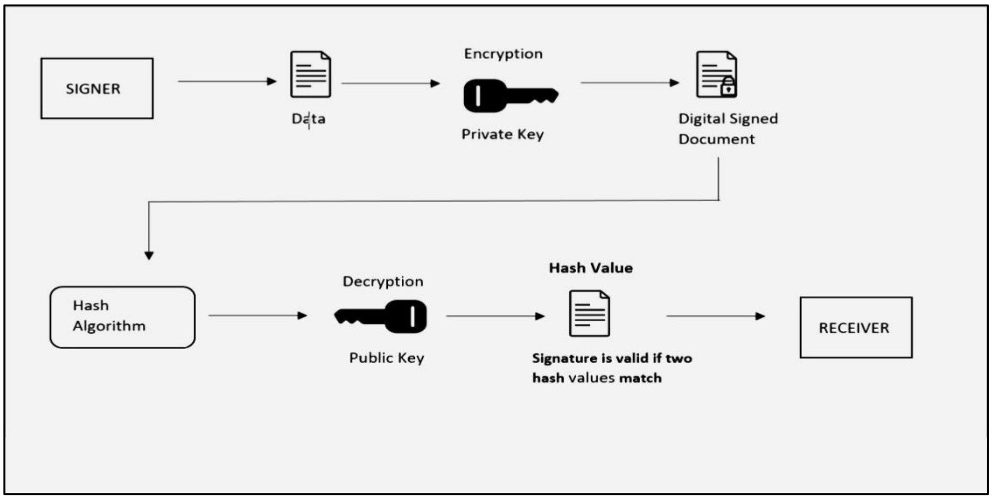


Figure. 4.8: Working of Digital Signature (Courtesy: docusign.com)

4.7 मोबाइल फोनवरील धोके आणि सुरक्षा उपाय

दैनंदिन जीवनात मोबाइल उपकरणांचा वापर वाढल्यामुळे, त्यासोबतच मोबाइल सुरक्षा देखील महत्त्वाची झाली आहे. जर तुमचा मोबाइल पुरेशा सुरक्षिततेने संरक्षित नसेल, तर हॅकर्स तुमचा डेटा चोरण्यास किंवा तुमच्या डिव्हाइसवर दूरस्थपणे नियंत्रण मिळवण्यास सक्षम होऊ शकतात. त्यामुळे, तुम्ही कोठेही प्रवास करा किंवा तुमचे डिव्हाइस कसेही वापरा, तुमचा डिजिटल डेटा खाजगी आणि सुरक्षित राहावा यासाठी योग्य सुरक्षा उपाय करणे आवश्यक आहे.

सामान्य मोबाइल सुरक्षा धोके:

1. मालवेअर आणि व्हायरस (Malware and Virus**):**

हानीकारक लिंक (links) किंवा करप्ट (corrupt) ॲप्सद्वारे तुमच्या मोबाइलमध्ये व्हायरस किंवा मालवेअर (malware) ऍक्सेस (Access) करू शकते. हे ॲप्स तुमच्या हालचालींवर लक्ष ठेवू शकतात, तुमचा डेटा चोरू शकतात, किंवा तुमच्या डिव्हाइसचे नुकसान करू शकतात. सुरक्षित स्रोतांमधूनच (Google Play Store किंवा Apple App Store) ॲप्स डाउनलोड करावेत. संशयास्पद लिंक (links) किंवा अज्ञात ॲप्स टाळावीत.

2. फिशिंग हल्ले (Fishing attacks**):**

फिशिंग (Phishing) हा एक प्रसिद्ध सायबर हल्ला(Cyber Attack) आहे, जिथे हॅकर्स बनावट ई-मेल, संदेश किंवा वेबसाइटद्वारे तुमची खाजगी माहिती (लॉगिन क्रेडेन्शियल्स, बँक खाते माहिती) चोरण्याचा प्रयत्न करतात. फिशिंग हल्ल्यापासून वाचण्यासाठी कोणत्याही संशयास्पद ई-मेल किंवा लिंक क्लिक करण्यापूर्वी त्याची पडताळणी करा आणि कधीही तुमची बँक माहिती किंवा पासवर्ड अज्ञात स्त्रोतांशी शेअर करू नका.

3. अनधिकृत ऍक्सेस (Unauthorized Access:**):**

जर तुमच्या मोबाइलला मजबूत पासवर्ड किंवा बायोमेट्रिक लॉक (फिंगरप्रिंट, फेस आयडी) नसतील, तर अनधिकृत व्यक्ती तुमच्या डिव्हाइसवर ऍक्सेस (Access) करू शकते आणि त्यावर हानीकारक सॉफ्टवेअर इंस्टॉल करू शकते. मोबाइलला नेहमी स्ट्रॉंग पासवर्ड(Strong Password) किंवा बायोमेट्रिक लॉकने सुरक्षित ठेवा. डिव्हाइस सार्वजनिक ठिकाणी अनवॉच सोडू नका.

4. हरवलेले किंवा चोरी झालेले डिव्हाइस (Lost or Stolen Devices**):**

मोबाइल डिव्हाइसेस लहान आणि पोर्टेबल असल्याने सहज हरवू शकतात किंवा चोरीला जाऊ शकतात. जर डिव्हाइसवर संरक्षित न केलेला वैयक्तिक डेटा असेल, तर मोठा सुरक्षा धोका निर्माण होऊ शकतो. मोबाइलमध्ये फाईंड माय डीवाईस (Find My Device) किंवा रिमोट लॉक/इरेझ (Remote Lock/Erase) सारखी सुरक्षा वैशिष्ट्ये कार्यान्वित करा. गहाळ झाल्यास डिव्हाइस त्वरित लॉक करा किंवा त्यातील सर्व डेटा डिलीट करा.

5. सार्वजनिक वाय-फाय धोके (Public WiFi Risks)**:**
सार्वजनिक WiFi नेटवर्क वापरताना तुमच्या डिव्हाइसवर सायबर हल्ल्याचा धोका असतो. कारण सार्वजनिक नेटवर्कमध्ये सुरक्षा वैशिष्ट्ये कमी असतात, त्यामुळे हॅकर्स तुमची वैयक्तिक माहिती सहज मिळवू शकतात. सार्वजनिक वाय-फायवर बँकिंग किंवा संवेदनशील कार्ये टाळा. व्हर्चुअल प्रायवेट नेटवर्क (VPN (Virtual Private Network)) चा वापर करा.

मोबाइल डिव्हाइस सुरक्षेसाठी सर्वोत्तम उपाय

सुरक्षा राखण्यासाठी केवळ सामान्य चुका टाळणे पुरेसे नाही; तुम्हाला संभाव्य धोके ओळखून सक्रियपणे उपाययोजना करणे आवश्यक आहे. खालील सर्वोत्तम पद्धती तुम्हाला तुमचे मोबाइल डिव्हाइस अधिक सुरक्षित ठेवण्यास मदत करू शकतात:

1. रिमोट वाइप (Remote Wipe) वैशिष्ट्य सक्रिय करा: तुमचा फोन चोरीला गेला किंवा हरवला, तर त्याला रिमोट लॉक किंवा डिलीट करण्याची सुविधा सक्षम करा. त्यामुळे, तुमच्या वैयक्तिक माहितीकडे कोणीही अनधिकृतपणे ऍक्सेस (Access) करू शकणार नाही.
2. एन्क्रिप्टेड मेसेजिंग ॲप्स वापरा: व्हॉटसॅप(WhatsApp), सिग्नल(Signal) किंवा टेलेग्राम(Telegram) सारखी एंड-टू-एंड एन्क्रिप्शन(end-to-end encryption) असलेली ॲप्स निवडा. यामुळे तुमच्या खाजगी संभाषणांमध्ये अनधिकृत ऍक्सेस (Access) होण्याचा धोका कमी होतो.
3. ब्लूटूथ न वापरताना बंद ठेवा (Turn off Bluetooth when not in use.): सतत ब्लूटूथ सुरू ठेवल्यास हॅकर्स तुमच्या डिव्हाइसवर दूरस्थपणे हल्ला करू शकतात. वापर नसताना ब्लूटूथ बंद ठेवा आणि अनोळखी डिव्हाइसेसशी कनेक्ट होणे टाळा.
4.डिव्हाइस ॲक्टिव्हिटी नोटिफिकेशन्स सक्षम करा (Set up device activity notifications): नवीन लॉगिन , अनधिकृत ऍक्सेस (Access) किंवा संशयास्पद हालचालींच्या सूचना मिळण्यासाठी ॲक्टिव्हिटी अलर्ट चालू करा. वेळेत सतर्कता बाळगल्यास मोठ्या सुरक्षा धोक्यांपासून बचाव करता येतो.
5.सुरक्षित डिव्हाइस व्यवस्थापन साधन (MDM) वापरा: मोबाइल डिव्हाइस मॅनेजमेंट (MDM) टूल्सचा उपयोग करून कंपन्या आणि वैयक्तिक वापरकर्ते सुरक्षा धोरणे लागू करू शकतात. यामुळे सर्व मोबाइल डिव्हाइसेसचे केंद्रीकृत व्यवस्थापन करणे सोपे होते.
6. ऑटो-वायफाय कनेक्शन बंद करा (Turn off auto-connect to WiFi): मोबाइल डिव्हाइस अनोळखी किंवा असुरक्षित WiFi नेटवर्कशी आपोआप कनेक्ट होऊ नये यासाठी ऑटो कनेक्ट टू वाय फाय(Auto-Connect to WiFi) बंद करा.सार्वजनिक वाय फाय (WiFi) वापरताना व्ही पी एन (VPN) वापरणे अधिक सुरक्षित पर्याय आहे.

References:

1. Information Systems Security Second Edition By Nina Godbole (John Wiley Isbn-13: 978-8126564057)
2. Cryptography and Information Security By V.K.Pachghare – Prentice Hall India
3. Cryptography and Network security Third Edition By Atul Kahate- McGraw-Hill; Fourth edition ISBN-13: 978-9353163303
4. Computer Security Principles and Practice, Third Edition BY William Stallings, Lawrie Brown Pearson. ISBN-13: 978-0-13-377392-7

युनिट - 5
इन्फॉर्मेशन सेक्युरिटी आणि सायबर कायदा
(Information Security and Cyber Law)

विषय निष्पत्ती : Course Outcome (CO):

CO5 – इंटरनेट (Internet) धोक्यांपासून संरक्षण करण्यासाठी सुरक्षा तंत्रज्ञानांची अंमलबजावणी करा.

घटक निष्पत्ती : (Theory Learning Outcomes)

1. दिलेल्या फायरवॉल(firewall)प्रकारांचे स्पष्टीकरण करा.
2. फायरवॉल(firewall) धोरणांची यादी करा.
3. नेटवर्क(network)आधारित आणि होस्ट (host)आधारित IDS ची तुलना करा.
4. ईमेल(email)सुरक्षा साठी वापरण्यात येणारे प्रोटोकॉल्स(protocol) स्पष्ट करा.
5. दिलेल्या परिस्थितीसाठी सायबरक्राइमचे (cybercrime)प्रकार ओळखा.
6. सायबर (cyber)कायद्यांच्या केटेगरीज(categories) स्पष्ट करा

5.1 फायरवॉल (Firewall)

5.1.1 फायरवॉलची आवश्यकता(Need of Firewall)

फायरवॉल(firewall) हे नेटवर्कला(network) अनधिकृत प्रवेश, हल्ले(attacks) आणि विविध धोक्यांपासून वाचविण्यासाठी अत्यंत आवश्यक आहे. हे विश्वासार्ह अंतर्गत नेटवर्क(network)आणि इंटरनेट (internet), यांच्यातील एक संरक्षक अडथळा म्हणून कार्य करते.

- हे अनधिकृत ट्रॅफिक (unauthorized traffic)प्रतिबंधित करते.
- हे येणाऱ्या ट्रॅफिकला (traffic)अधिक विश्वासार्ह अंतर्गत कंप्युटर सिस्टम्सकडे (computer systems) पाठवते.
- हे अंतर्गत कंप्युटर(computers)किंवा नेटवर्क (networks)लपवते, जे असुरक्षित असतात.
- हे अंतर्गत नेटवर्कबद्दलची(networks) माहिती लपवते, जसे कंप्युटर सिस्टम्सची नावे, नेटवर्क टोपोलॉजी(network topology) , नेटवर्क(network) उपकरणांचे प्रकार, इत्यादी.
- हे सक्षम वापरकर्ता प्रमाणिकरण (user authentication)प्रदान करते.
- हे IPSec साठी एक प्लॅटफॉर्म (platform)म्हणून कार्य करू शकते.

5.1.2 फायरवॉलचे प्रकार(Types of Firewall)

फायरवॉल्स चार प्रकारात वर्गीकृत केली जातात:: पॅकेट फिल्टरिंग फायरवॉल(Packet Filtering Firewall), स्टेटफुल पॅकेट फिल्टर(Stateful Packet Filter)एप्लिकेशन लेव्हल गेटवे(Application Level Gateway), आणि सर्किट लेव्हल (प्रॉक्सी) गेटवे(Circuit Level (Proxies) Gateways).

1. पॅकेट फिल्टरिंग फायरवॉल(Packet Filtering Firewall)

फायरवॉलची(firewall) पहिली पिढी(First Generation) म्हणजे पॅकेट फिल्टरिंग फायरवॉल(packet filtering firewall). हे नियमांवर आधारित काम करते आणि इनकमिंग आणि आउटगोइंग ट्रॅफिकसाठी आयपी पॅकेट्सना परवानगी देते IP पॅकेट्सला परवानगी देते. या नियमांचा वापर करून, पॅकेट्स(packets) पुढे पाठवली जातात किंवा नाकारली जातात. हा फायरवॉल (firewall)OSI लेयर 3 आणि 4 वर कार्य करतो. सामान्यत: हा फायरवॉल(firewall) दोन्ही दिशांनी जाणारे पॅकेट्स फिल्टर(Packet filter) करण्यासाठी डिझाइन केला जातो आणि सोर्स ॲड्रेस, डेस्टिनेशन ॲड्रेस (source address, destination address)आणि TCP/UDP पोर्ट नंबर ट्रॅक करते. या फायरवॉलद्वारे(firewall) पॅकेटच्या (packet) सामग्रीचे विश्लेषण केले जात नाही.

फायदे(Advantages):

1. त्याची कार्यक्षमता चांगली आहे.
2. ते खूप जलद आहे.

3. पॅकेट फिल्टर्स(Packet filters) तुलनेने स्वस्त आहेत.
4. ते वापरकर्त्यांसाठी पारदर्शक आहे.
5. ट्रॅफिक(traffic) व्यवस्थापन (management) चांगले आहे.
6. पॅकेट फिल्टरिंग हि सोपी पद्धत आहे.

तोटे(Disadvantages):

1. अविश्वसनीय आणि विश्वासार्ह होस्टमध्ये (untrusted and trusted hosts) थेट कनेक्शनला परवानगी आहे.
2. हे स्पुफिंग हल्ल्यांसाठी(spoofing attacks) संवेदनशील आहे.
3. त्याची स्केलेबिलिटी कमी आहे.
4. या फायरवॉल्सपैकी बहुतांश आधुनिक वापरकर्ता प्रमाणिकरण (user authentication) स्कीमला(scheme)समर्थन देत नाहीत.
5. जास्त पोर्ट रेंजेस(port ranges) उघडल्या जाऊ शकतात.
6. चुकीच्या कॉन्फिगरेशनमुळे (conFiguration), हे सुरक्षा उल्लंघनांसाठी संवेदनशील आहे.

2. स्टेटफुल पॅकेट फिल्टर (Stateful Packet Filter)

स्टेटफुल पॅकेट फिल्टर(Stateful Packet Filter) ही एक नेटवर्क सुरक्षा(Network Security)यंत्रणा आहे जी सक्रिय कनेक्शनच्या(Active connection) स्थितीचे निरीक्षण करते आणि पॅकेटना(packets) परवानगी द्यायची की ब्लॉक करायची हे ठरवण्यासाठी या संदर्भाचा वापर करते. पारंपारिक स्टेटलेस फायरवॉल्सच्या(Stateless Firewalls) तुलनेत, जे प्रत्येक पॅकेट स्वतंत्रपणे मूल्यांकन करतात, स्टेटफुल फायरवॉल(Stateful Firewall) कनेक्शनच्या स्थितीचा मागोवा घेतात आणि संपूर्ण संवाद सत्रावर(communication session) आधारित निर्णय घेतात. हा डायनॅमिक दृष्टिकोन सुरक्षा वाढवतो कारण तो परत येणाऱ्या ट्रॅफिकला परवानगी देतो, पॅकेट्सची सत्यता तपासतो आणि सेशन स्टेटसच्या(Session States) आधारे फक्त अधिकृत पॅकेट्सना ऍक्सेस (Access) देतो.

फायदे(Advantages):

1. IP स्पुफिंग आणि सेशन हायजॅकिंगसारख्या(Session Hijacking) हल्ल्यांचा शोध घेऊन आणि अडवून ते सुधारित सुरक्षा प्रदान करते.
2. स्थापित कनेक्शनसाठी परत येणारा ट्रॅफिक परवानगी देऊन आणि न मागितलेल्या ट्रॅफिकला ब्लॉक करून संदर्भ-आधारित फिल्टरिंग करते.
3. TCP आणि UDP सारख्या कॉम्प्लेक्स प्रोटोकॉल्सचे व्यवस्थापन करते, त्यांची कनेक्शन स्थिती समजून घेतो.
4. हे कनेक्शनच्या स्थितीवर आधारित नियम dynamically अपडेट करतो, ज्यामुळे ट्रॅफिक नियंत्रणात सुसंगती आणि सुधारणा साधली जाते.
5. अनावश्यक ट्रॅफिक कमी करते, ज्यामुळे संसाधनांची कार्यक्षमता सुधारते.

तोटे(Disadvantages):

1. त्याला अधिक प्रोसेसिंग पॉवर(processing power)आणि मेमरी (memory) आवश्यक असते, ज्यामुळे प्रणालीवरील(System) लोड वाढतो.
2. त्याचे कॉन्फिगरेशन स्टेटलेस फायरवॉल्सच्या(stateless firewalls) तुलनेत अधिक कठीण आहे.
3. हे पॅकेटच्या कंटेंटची(packet contents) तपासणी करत नाही, ज्यामुळे पे-लोड आधारित हल्ल्यांना (payload-based attacks)चुकवू शकते.
4. हे डिनायल ऑफ सर्व्हिस (DoS) हल्ल्यांसाठी संवेदनशील असू शकते, कारण ते उच्च संसाधनांचा (high resources) वापर करते.

3. एप्लिकेशन लेव्हल गेटवे (Application Level Gateway)

पॅकेट फिल्टरिंग फायरवॉल्स अड्रेस इन्फॉर्मेशन(address information) वर आधारित असतात आणि OSI मॉडेलच्या खालच्या स्तरांची तपासणी करतात. वाढीव सुरक्षा प्रदान करण्यासाठी, OSI मॉडेलच्या सर्व स्तरांची एकाच वेळी तपासणी केली पाहिजे.

ॲप्लिकेशन लेव्हल गेटवे फायरवॉल हे सर्व्हर-आधारित प्रोग्राम वापरून प्रदान करते, ज्यांना प्रॉक्सी सर्व्हर किंवा बेस्टन होस्ट म्हणून ओळखले जाते. हे पॅकेट्सला पुढे पाठवते किंवा नाकारते, आणि प्रोटोकॉल स्पेसिफिकेशन (protocol specification) योग्य असल्याची खात्री करते.

प्रॉक्सी (Proxies) बाह्य बाजूकडून विनंती स्वीकारते, त्यांचा तपास करते, आणि नंतर योग्य आणि विश्वासार्ह विनंती दुसऱ्या बाजूवरील इन्फॉर्मेशन(information) होस्ट कडे पाठवते. हे फायरवॉल OSI मॉडेलच्या सातही स्तरांवर निर्णय घेतो आणि विविध अनुप्रयोगांसाठी(Application), जसे की ईमेल आणि FTP, मध्यस्थ म्हणून कार्य करते. हे क्लायंटला थेट इन्फॉर्मेशन(information) नोडशी(node) कनेक्ट होण्याची परवानगी देत नाही.

फायदे(Advantages):

1. हे असे कॉन्फिगर(conFigure) केले जाते की फायरवॉल (firewall)हा एकटा होस्ट पत्ता(address) बाह्य नेटवर्कला दिसतो.
2. वेगवेगळ्या सेवांसाठी वेगळे प्रॉक्सी सर्व्हर (proxy servers) वापरले जातात.
3. एप्लिकेशन गेटवेज(Application gateways) मजबूत वापरकर्ता प्रमाणिकरणला(user authentication) समर्थन देतात.
4. हे एप्लिकेशन(Application) स्तरावर मजबूत सुरक्षा प्रदान करते.
5. हे मजबूत ऍक्सेस (access) नियंत्रण प्रदान करते.
6. हे पॅकेट फिल्टरिंग फायरवॉल्सपेक्षा (packet filtering firewalls)अधिक सुरक्षित आहे.

तोटे(Disadvantages):

1. प्रत्येक अनुप्रयोगासाठी (application)एक विशेष प्रॉक्सी (proxy)आवश्यक असतो.
2. कार्यक्षमता कमी आहे.
3. प्रत्येक कनेक्शनवर(connection) अतिरिक्त प्रोसेसिंग ओव्हरहेड(processing overhead) असतो.
4. कधी कधी वापरकर्त्यांसाठी हे असुविधाजनक होऊ शकते.
5. पारदर्शकतेची कमतरता आहे.

4. सर्किट लेव्हल गेटवेज (Circuit Level Gateways)

सर्किट-लेव्हल गेटवे (Circuit Level Gateways)हा फायरवॉलचा(firewall)एक प्रकार आहे जो एक स्वतंत्र प्रणाली म्हणून कार्य करतो. पॅकेट फिल्टरिंग(packet filtering) प्रमाणे, हे कनेक्शन प्रमाणित (validate) करते आणि पूर्वनिर्धारित नियमांवर आधारित डेटा एक्सचेंजला परवानगी देते. पॅकेट फिल्टरिंगच्या(packet filtering तुलनेत, सर्किट-लेव्हल गेटवेज (Circuit Level Gateways)पॅकेट्स रूट (route) करत नाहीत. ते पॅकेट फिल्टरिंग पेक्षा अधिक सुरक्षित असतात. हे गेटवेज राऊटर आणि बाह्य नेटवर्क (जसे की इंटरनेट) यामध्ये स्थापित केले जातात, ज्यामुळे सिस्टमचा वास्तविक पत्ता(real address) लपवला जातो आणि फक्त प्रॉक्सी (proxy)पत्ता दिसतो.

फायदे(Advantages):

1. वापरकर्त्यांसाठी(User) पारदर्शक आहे.
2. बाह्य ट्रॅफिक रिले(for relaying outbound traffic)करण्यासाठी उत्कृष्ट आहे.

तोटे(Disadvantages):

1. पॅकेट फिल्टरिंग फायरवॉल्सपेक्षा (Packet Filtering Firewall)हळू आहे.
2. इनबाउंड ट्रॅफिक(Inbound traffic) धोकादायक असू शकतो.

5.2 फायरवॉल धोरणे(Firewall Policies), फायरवॉल कॉन्फिगरेशन (Firewall configurations), फायरवॉलची मर्यादा (Limitations of a Firewall), डेमिलिटराइज्ड झोन (DMZ):

5.2.1 फायरवॉल धोरणे(Firewall Policies):

फायरवॉल धोरणे(policies) ही नियमांची एक संच असतात, जे ठरवतात की कोणता नेटवर्क ट्रॅफिक परवानगी दिला जाईल किंवा नाकारला जाईल. हे धोरणे(policies) नेटवर्क्सना अनधिकृत ऍक्सेस (Access) आणि हल्ल्यांपासून(attacks) संरक्षित करण्यासाठी अत्यंत महत्त्वाची असतात. फायरवॉल धोरणांचे मुख्य घटक खालीलप्रमाणे आहेत:

- फायरवॉल धोरणे (policies) सर्व प्रकारच्या रहदारीला परवानगी देतात परंतु टेलनेट/एसएनएमपी(TELNET/SNMP) सारख्या काही सेवा आणि हल्लेखोर वापरत असलेले पोर्ट नंबर ब्लॉक करतात.
- प्रतिबंधक धोरणे सर्व ट्रॅफिक फायरवॉलमधून पास होऊ देतात आणि फक्त HTTP, POP3, SMTP किंवा SSH सारख्या उपयुक्त ट्रॅफिकला परवानगी देतात.
- सर्वात सुरक्षित पर्याय म्हणजे सर्व संशयास्पद गोष्टी ब्लॉक करणे, आणि कोणीतरी तक्रार केल्यावर तुम्ही प्रोटोकॉल्सला परवानगी देऊ शकता.

खालीलप्रमाणे सामान्य फायरवॉल नियम संच आहेत:

1. फायरवॉल HTTP, FTP, SSH, DNS प्रोटोकॉल्सना अंतर्गत नेटवर्कपासून(internal network) इंटरनेटवर संवाद साधण्याची परवानगी देतो.
2. फायरवॉल SMTP प्रोटोकॉलला कुठूनही मेल सर्व्हरशी संवाद साधण्याची परवानगी देतो.
3. फायरवॉल SMTP आणि DNS प्रोटोकॉल्सना मेल सर्व्हरपासून इंटरनेटपर्यंत संवाद साधण्याची परवानगी देतो.
4. फायरवॉल SMTP आणि POP3 प्रोटोकॉल्सना अंतर्गत नेटवर्कपासून मेल सर्व्हरपर्यंत संवाद साधण्याची परवानगी देतो.
5. फायरवॉल फक्त प्रतिसाद पॅकेट्सना परवानगी देतो.
6. फायरवॉल इतर सर्व गोष्टी ब्लॉक करू शकतो.

5.2.2 फायरवॉल कॉन्फिगरेशन (Firewall configurations):

फायरवॉल कॉन्फिगरेशन (Firewall configurations) नेटवर्क्सना अनधिकृत प्रवेशापासून संरक्षण करण्यात आणि अंतर्गत सिस्टम्सची (internal system)सुरक्षा सुनिश्चित करण्यात महत्त्वपूर्ण भूमिका बजावतात. या कॉन्फिगरेशन्सची जटिलता(Complexity) आणि सुरक्षा नेटवर्कच्या आवश्यकतांनुसार बदलते.

फायरवॉल कॉन्फिगरेशन्सचे (Firewall conFigurations)सामान्य प्रकार:

1. स्क्रीन केलेले होस्ट फायरवॉल (सिंगल-होम्ड) Screened Host Firewall (Single-Homed Bastion)
2. स्क्रीन केलेले होस्ट फायरवॉल (ड्युअल-होम्ड बॅस्टियन) Screened Host Firewall (Dual-Homed Bastion)
3. स्क्रीन केलेली सबनेट फायरवॉल(Screened Subnet Firewall).

1. स्क्रीन्ड होस्ट फायरवॉल (सिंगल-होम्ड बॅस्टियन) Screened Host Firewall (Single-Homed Bastion)

स्क्रीन केलेला होस्ट फायरवॉल हा एक मूलभूत प्रकाराचा फायरवॉल कॉन्फिगरेशन आहे, ज्यामध्ये एकाच होस्टचे फिल्टरिंग राऊटरद्वारे संरक्षण केले जाते.

- सिंगल इंटरफेस(Single Interface): फायरवॉलमध्ये फक्त एक इंटरफेस (interface)अंतर्गत नेटवर्कशी जोडलेला असतो आणि दुसरा बाह्य नेटवर्क (सामान्यतः इंटरनेट)(external network) शी जोडलेला असतो.
- किमान सुरक्षा स्तर(Minimal Security Layer): अंतर्गत नेटवर्कची(internal network) सुरक्षा पूर्णपणे फायरवॉल होस्टवर (firewall host)अवलंबून असते, आणि सामान्यतः सॉफ्टवेअर फिल्टरिंगचा (software filtering) वापर केला जातो (उदा. IP फिल्टर्स).
- साधे कॉन्फिगरेशन(Simpler ConFiguration): हे लागू करण्यास सोपे असते, ज्यामुळे हे छोटे नेटवर्क किंवा कमी सुरक्षा आवश्यकता असलेल्या वातावरणांसाठी (environment)उपयुक्त ठरते.
- सीमित स्केलेबिलिटी(Limited Scalability): हे मोठ्या वातावरणांसाठी (environment) आदर्श नाही, जिथे जास्त उपलब्धता आणि स्केलेबिलिटी आवश्यक आहे.
- लॉग आणि मॉनिटर(Log and Monitor): बॅस्टियन होस्टमध्ये(bastion host)अनेकदा लॉगिंग आणि मॉनिटरिंग (logging and monitoring) वैशिष्ट्ये असतात, जे अनधिकृत ॲक्सेस (Access) किंवा संशयास्पद क्रियाकलाप(unauthorized access) शोधण्यासाठी उपयोगी असतात.

2. स्क्रीन केलेला होस्ट फायरवॉल (ड्युअल-होम्ड बॅस्टियन) (Screened Host Firewall (Dual-Homed Bastion))

ड्युअल-होम्ड बॅस्टियन फायरवॉल (dual-homed bastion firewall) हा एक अधिक प्रगत सेटअप आहे, ज्यामध्ये एकाच होस्टमध्ये दोन नेटवर्क इंटरफेस असतात, एक अंतर्गत नेटवर्कसाठी आणि दुसरे बाह्य नेटवर्कसाठी.

- दोन नेटवर्क इंटरफेस (Two Network Interfaces): फायरवॉल होस्ट अंतर्गत आणि बाह्य नेटवर्क(internal network and the external network) दोन्हीशी जोडलेला असतो, ज्यामुळे अधिक वेगळेपण मिळते.
- वाढवलेली सुरक्षा (Increased Security): सिंगल-होम्ड बॅस्टियनपेक्षा अधिक सुरक्षित कारण ट्रॅफिक दोन्ही नेटवर्क्समध्ये दोन्ही इंटरफेसवर फिल्टर केले जाते.
- सुधारित ऍक्सेस (Access) नियंत्रण (Improved Access Control): अंतर्गत आणि बाह्य प्रणालींमधील ट्रॅफिकवर अधिक सूक्ष्म नियंत्रण प्रदान करते.
- समर्पित फिल्टरिंग (Dedicated Filtering): या कॉन्फिगरेशनमध्ये (configuration) अधिक विस्तृत पॅकेट फिल्टरिंगची परवानगी असते आणि सिंगल-होम्ड प्रणालींपेक्षा हे दुर्बल ट्रॅफिकला(malicious traffic) अधिक प्रभावीपणे ब्लॉक करते.
- वाढलेली जटिलता (Higher Complexity): कॉन्फिगर आणि व्यवस्थापित करण्यासाठी अधिक जटिल(Complexity) आहे, ज्यासाठी अधिक प्रशासकीय प्रयत्नांची(administrative efforts) आवश्यकता आहे.
- अयशस्वीतेचा संभाव्य बिंदू (Potential Single Point of Failure): सिंगल-होम्ड बॅस्टियनपेक्षा (single-homed bastions)अधिक सुरक्षित असला तरी, जर बॅस्टियन होस्ट तडजोड झाला, तर अंतर्गत नेटवर्क अजूनही असुरक्षित होऊ शकते.

3. स्क्रीन केलेली सबनेट फायरवॉल (Screened Subnet Firewall)

स्क्रीन केलेली सबनेट फायरवॉल(Subnet Firewall) एक स्वतंत्र सबनेट(Subnet) तयार करते (ज्याला DMZ म्हणून ओळखले जाते), जे अंतर्गत नेटवर्क आणि बाह्य नेटवर्क दरम्यान असते, ज्यात बाह्य वापरकर्त्यांसाठी प्रवेशयोग्य सेवा असतात.

- DMZ झोन (DMZ Zone): स्क्रीन केलेली सबनेट फायरवॉल(Subnet Firewall) एक समर्पित DMZ वापरते, जिथे सार्वजनिकपणे प्रवेशयोग्य सेवा (उदा. वेब सर्व्हर) ठेवलेली असतात, जे अंतर्गत नेटवर्कपासून वेगळे केलेली असतात.
- दुहेरी सुरक्षा स्तर(Dual Layer of Protection): सामान्यतः दोन फायरवॉल्स असतात: एक अंतर्गत नेटवर्क आणि DMZ दरम्यान आणि दुसरा DMZ आणि बाह्य नेटवर्क दरम्यान.
- वाढवलेली सुरक्षा(Increased Security): अंतर्गत नेटवर्क दोन्ही, आंतरिक आणि बाह्य हल्ल्यांपासून संरक्षित असतो, ज्यामुळे हल्लेखोरांना अंतर्गत संसाधनांना थेट लक्ष्य करण्यासाठी अधिक कठीण बनवते.
- सार्वजनिकपणे प्रवेशयोग्य सेवा(Publicly Accessible Services): बाह्य वापरकर्त्यांना काही संसाधने (उदा. वेब सर्व्हर, मेल सर्व्हर) प्रवेश करण्याची परवानगी देते, आणि त्याच वेळी संवेदनशील अंतर्गत प्रणाली सुरक्षित ठेवते.
- DMZ मध्ये तडजोड होण्याचा धोका(Risk of Compromise in DMZ): जरी DMZ वेगळे केलेले असले तरी, जर हल्लेखोरांनी DMZ मधील एखादी सेवा तडजोड केली, तर ते अंतर्गत नेटवर्ककडे वळण्याचा प्रयत्न करू शकतात.

5.2.3 फायरवॉलची मर्यादा (Limitations of a Firewall)

- हे फायरवॉलला बायपास(bypass)करणाऱ्या हल्ल्यांपासून संरक्षण करू शकत नाही.
- हे अंतर्गत हल्ल्यांपासून नेटवर्कचे (internal attacks) संरक्षण करू शकत नाही.
- एक आंतरिक फायरवॉल नेटवर्कच्या(internal firewall) विविध भागांना विभाजित करत असला तरी, ते आंतरिक फायरवॉलच्या दोन्ही बाजूंनी असलेल्या स्थानिक संगणक प्रणालींमधील(local computer system) वायरलेस संवादांपासून संरक्षण करू शकत नाही.
- लॅपटॉप किंवा पोर्टेबल स्टोरेज डिव्हाइस (laptops or portable storage devices) यांसारखी उपकरणे फायरवॉलला बायपास करून नेटवर्कच्या बाहेर संक्रमित होऊ शकतात आणि नंतर ते आंतरिकपणे वापरण्यात येतात.

5.2.4 डेमिलिटरीझ्ड झोन (DMZ):

- नेटवर्कमधील त्यांच्या स्थानावर आधारित फायरवॉल्सचे दोन प्रकार असतात: अंतर्गत फायरवॉल आणि बाह्य फायरवॉल(internal firewall and external firewall).
- अंतर्गत फायरवॉल(Internal firewall) संपूर्ण नेटवर्कचे संरक्षण करते.

- बाह्य फायरवॉल (External firewall) स्थानिक किंवा संस्थात्मक नेटवर्कच्या सीमेवर स्थापित केले जाते, जे बाउंड्री राउटरच्या आत असते.
- दोन्ही फायरवॉल्स दरम्यान असलेला क्षेत्र(region) डेमिलिटरीझ्ड झोन(Demilitarised Zone) (DMZ) म्हणून ओळखला जातो.
- दोन्ही फायरवॉल्स दरम्यान अनेक नेटवर्क डिव्हाइसेस ठेवले जातात, ज्यामध्ये बाह्य नेटवर्क्सद्वारे प्रवेश दिलेल्या डिव्हाइसेस समाविष्ट असतात.
- या डिव्हाइसेसला बाह्यपणे प्रवेश केला जाऊ शकतो पण ते असुरक्षतेपासून संरक्षित असतात.
- DMZ मध्ये स्थित सिस्टम्स, जसे DNS सर्व्हर, ईमेल सर्व्हर किंवा वेबसाइट्स(servers, e-mail servers, or websites) , बाह्य नेटवर्कसह कनेक्टिव्हिटी आवश्यक असते.
- बाह्य फायरवॉल या सिस्टम्ससाठी सुरक्षा आणि प्रवेश नियंत्रण प्रदान करते.
- बाह्य फायरवॉल संपूर्ण नेटवर्कसाठी मूलभूत सुरक्षा प्रदान करते.
- अंतर्गत फायरवॉल बाह्य फायरवॉलपेक्षा अधिक मजबूत फिल्टरिंग क्षमता प्रदान करते, जे सर्व्हर्स आणि कार्यस्थानांवर(workstation) बाह्य हल्ल्यांपासून(attack) उच्च सुरक्षा प्रदान करते.
- अंतर्गत फायरवॉल (internal firewall) दोन-मार्गी संरक्षण देखील प्रदान करते: ते DMZ सिस्टम्सकडून (उदा. कीड, बॉट्स, हानिकारक सॉफ्टवेअर) सुरू होणाऱ्या हल्ल्यांपासून अंतर्गत नेटवर्कचे संरक्षण करते आणि अंतर्गत हल्ल्यांपासून DMZ सिस्टम्सचे संरक्षण करते.
- मोठ्या नेटवर्कच्या विविध भागांना एकमेकांपासून संरक्षण करण्यासाठी अनेक अंतर्गत फायरवॉल्स वापरले जातात.
- आंतरिक फायरवॉलमध्ये बाह्य फायरवॉलच्या तुलनेत अधिक मजबूत फिल्टरिंग क्षमता आहे, ज्यामुळे सर्व्हर्स आणि कार्यस्थानांना बाह्य हल्ल्यांपासून अधिक सुरक्षा मिळते.

5.3 इंट्रूजन डिटेक्शन सिस्टम (IDS) (Intrusion Detection System)

इंट्रूजन(Intrusion) डिटेक्शन सिस्टम (IDS) ही एक सुरक्षा यंत्रणा आहे जी नेटवर्क किंवा प्रणालीच्या क्रियाकलापांचे(system activities) निरीक्षण करण्यासाठी वापरली जाते, ज्यात कोणत्याही हानिकारक क्रियाकलाप(activities) किंवा धोरण उल्लंघनांची ओळख केली जाते. हे अनधिकृत प्रवेश, संभाव्य हल्ले (attack) आणि असामान्य वर्तन शोधते. IDS दोन प्रकारांमध्ये वर्गीकृत केली जाऊ शकते: नेटवर्क-आधारित (NIDS) आणि होस्ट-आधारित (HIDS), जे त्याच्या नेमलेल्या स्थानानुसार असतात. IDS, संभाव्य धोका ओळखण्यासाठी आणि अधिक चांगली सुरक्षा सुनिश्चित करण्यासाठी वास्तविक वेळेत निरीक्षण आणि विश्लेषण करण्यात मदत करते.

फायदे(Advantages):

1. हे वास्तविक वेळेत हानिकारक क्रियाकलाप (activities) ओळखते आणि अलर्ट करते.
2. हे गंभीर हानी होण्यापूर्वी हल्ले(attack) शोधण्यास मदत करते.
3. हे फॉरेन्सिक विश्लेषणासाठी (forensic analysis) महत्त्वाची लॉग आणि अहवाल प्रदान करते.
4. हे सिस्टम कार्यक्षमता प्रभावित न करता बॅकग्राऊंडला चालवता येते.

तोटे(Disadvantages):

1. हे खोटी चेतावणी तयार करू शकते, ज्यामुळे अनावश्यक क्रिया किंवा गोंधळ होऊ शकतो.
2. हे सिस्टम संसाधनांचा वापर करू शकते, ज्यामुळे कार्यक्षमता मंदावू शकते.
3. हे फक्त धोके शोधते; ते त्यांना थांबवत नाही.
4. कौशल्यपूर्ण हल्लेखोर IDS च्या सुरक्षेचा त्यांच्याद्वारे एनक्रिप्शन किंवा टनलिंग(encryption and tunnelling) पद्धती वापरून बायपास करू शकतात.

5.3.1 नेटवर्क इंट्रूजन डिटेक्शन सिस्टम(Network Intrusion Detection System (NIDS)):

- NIDS नेटवर्कवर कार्य करते आणि संपूर्ण सबनेटमधून जाणारी सर्व ट्रॅफिक विश्लेषण करते.

- प्रत्येक पॅकेटचे निरीक्षण केले जाते, आणि जर हल्ला(attack) किंवा असामान्य वर्तन ओळखले गेले, तर एक अलर्ट(alert) प्रशासकाला(administrator) पाठवला जातो.
- NIDS नेटवर्कवर असलेल्या पॅकेट्सचे निरीक्षण करते आणि विश्लेषणासाठी त्यांची तुलना संदर्भ डेटा सोबत करते.
- पॅकेट्सची पडताळणी केली जाते, जेणेकरून ते हानिकारक की नाही हे निश्चित करता येईल.
- NIDS नेटवर्कमधील कमकुवतपणांवर(weakness) नियंत्रण ठेवते, ज्यामुळे ते एक वितरित IDS बनते.
- NIDS नेटवर्कवर पॅकेट्स गोळा करण्यासाठी पॅकेट-स्निफिंग तंत्रांचा वापर करते.

5.3.2 होस्ट इंट्रूजन डिटेक्शन सिस्टम(Host Intrusion Detection System (HIDS)):

- HIDS होस्टवर कार्य करते, प्रणाली घटनांचे(system events) निरीक्षण करते आणि इव्हेंट लॉग्सची ऑडिटिंग करते.
- HIDS प्रणाली फाइल्सचे स्नॅपशॉट्स घेतो आणि त्यांची तुलना मागील स्नॅपशॉट्ससह करतो.
- जर कोणतीही फाईल बदलली किंवा काढून टाकली गेली, तर एक अलर्ट प्रशासकाला(administrator) पाठवला जातो.
- होस्ट-आधारित प्रणालीमध्ये, प्रत्येक स्वतंत्र संगणकावर किंवा होस्टवर घडलेल्या क्रियांचा(activities) तपास IDS करते.
- HIDS विशिष्ट प्रणालीवरील हल्ल्यांना शोधण्यासाठी स्वतंत्र संगणकांवर स्थापित केले जाते.

Table 5.1: Difference between NIDS and HIDS

नेटवर्क घुसखोरी शोध प्रणाली (NIDS) Network Intrusion Detection System	होस्ट घुसखोरी शोध प्रणाली (HIDS) Host Intrusion Detection System
1.हे संपूर्ण नेटवर्कवरील ट्रॅफिकचे (network traffic) आणि सर्व पॅकेट्सचे (packets) विश्लेषण करते.	1.हे स्वतंत्र होस्ट वर स्थापित केले जाते. प्रणालीतील घटना (System Events) व क्रियाकलापांवर(Activities) लक्ष ठेवते.
2.हे नेटवर्क ट्रॅफिकचे विश्लेषण करून संदर्भ डेटा वापरून संशयास्पद वर्तन ओळखते.	2.हे प्रणालीतील फायलींचे स्नॅपशॉट(snapshot) घेते आणि त्यांतील बदल किंवा काढून टाकलेली फाईल्स शोधते.
3.संशयास्पद किंवा हानिकारक नेटवर्क पॅकेट्स आढळल्यास अलर्ट ट्रिगर करते.	3.फायलीतील बदल, काढून टाकलेला डेटा किंवा अन्य संशयास्पद घटना आढळल्यास अलर्ट ट्रिगर करते.
4. नेटवर्क पातळीवरील असुरक्षितता शोधून त्यावर उपाययोजना करते आणि संपूर्ण नेटवर्कसाठी संरक्षित प्रणाली पुरवते.	4.संगणक प्रणालीवरील असुरक्षिततेचे निरीक्षण आणि सुरक्षा प्रदान करते.
5.हे पॅकेट-स्निफिंग तंत्रज्ञान वापरते, ज्यामुळे नेटवर्क संसाधने जास्त प्रमाणात लागतात.	5.प्रत्येक संगणकावर स्थापित केल्याने प्रशासनाचा भार वाढतो आणि सिस्टम संसाधनांचा अधिक वापर होतो.

5.3.3 हनीपॉट्स (Honeypots)

हनीपॉट ही इंटरनेटवरील एक माहिती प्रणाली आहे, जी संगणक प्रणालींमध्ये घुसखोरी करण्याचा प्रयत्न करणाऱ्या हॅकर्सना आकर्षित आणि अडकवण्यासाठी डिझाइन केली जाते. हे एक आभासी मशीन(virtual machine) असते जे हल्लेखोरांना(attackers) असे वाटायला लावते की ते एक वैध प्रणाली आहे. हल्लेखोर हनीपॉटला लक्ष्य करतो आणि त्याचे सर्व व्यवहार निरीक्षण केले जातात, त्याला कळतही नाही. यासोबतच, प्रणाली हल्ल्याविषयी महत्त्वाची माहिती गोळा करते, जसे की हल्लेखोराचा IP पत्ता(address), जो हल्लेखोराचा मागोवा घेण्यासाठी उपयुक्त ठरतो. जेव्हा एकाच सब नेटमध्ये(subnet) अनेक हनीपॉट्स जोडले जातात, तेव्हा त्याला हनीनेट(honeynet) म्हणतात. हनीपॉट्सचा वापर शोध, प्रतिबंध आणि माहिती गोळा करण्यासाठी केला जातो.

हनीपॉट डिझाइनचे उद्दीष्टे (Honeypot Design's Objectives):

1. हल्लेखोराला(attacker) विशिष्ट प्रणालींमध्ये प्रवेश मिळण्यापासून रोखते.
2. हल्ल्याविषयी माहिती गोळा करते.
3. हल्लेखोराला दीर्घकाळ सिस्टममध्ये गुंतवते, त्यामुळे प्रशासकांना(administrator) हल्लेखोराची माहिती गोळा करण्यास अधिक वेळ मिळतो.

हनीपॉट्सचे प्रकार(Types of Honeypots):

1. उत्पादन हनीपॉट्स (Production Honeypots):

- वापरण्यास सोपे आणि मर्यादित माहिती गोळा करतात, प्रामुख्याने जोखीम कमी करण्यासाठी वापरले जातात.
- हे प्रामुख्याने विशिष्ट ऑपरेटिंग सिस्टमचे अनुकरण करतात.
- हे स्वयंचलित साधनांद्वारे केले जाणारे हल्ले शोधू शकतात आणि हल्लेखोराची गती मंदावण्यासाठी शून्य-आकाराची मान्यता (zero-size acknowledgment) पाठवू शकतात, ज्यामुळे हल्लेखोर पुढील डेटा पाठवण्यासाठी मोठ्या विंडो साईझची वाट पाहतो.

2. संशोधन हनीपॉट्स (Research Honeypots):

- हे वास्तविक ऑपरेटिंग सिस्टम आणि सेवा वापरतात, त्यामुळे अधिक जोखीम असते.
- नवीन हल्ल्याच्या(attacks) पद्धती आणि तंत्रांची माहिती गोळा करण्यासाठी वापरले जातात.
- संशोधन हनीपॉट्स विविध प्रकारच्या हल्ल्यांचा अचूक अभ्यास करतात आणि घुसखोरी शोध व प्रतिबंधासाठी तपशीलवार लॉग पुरवतात.

हनीपॉट्सचे फायदे(Advantages of Honeypots):

1. हनीपॉट्स हल्लेखोरांना(attackers) आकर्षित करून त्यांना अशा ठिकाणी अडकवतात जिथे ते नुकसान करू शकत नाहीत.
2. प्रशासकांना(administrator) हल्लेखोरांचा सामना करण्यासाठी पुरेसा वेळ मिळतो.
3. हल्लेखोरांची क्रियाकलाप(activities) तपासता येतात आणि त्यांच्याकडून मिळालेल्या डेटाचा वापर हल्ल्याच्या पद्धती समजून घेण्यासाठी केला जाऊ शकतो.
4. हे अंतर्गत हल्ले अचूकपणे शोधून अंतर्गत हल्लेखोरांविषयी माहिती देऊ शकतात.
5. हे नेटवर्कच्या बँडविड्थवर अतिरिक्त भार वाढवत नाहीत.

हनीपॉट्सचे तोटे(Disadvantages of Honeypots):

1. हनीपॉट्स फक्त त्यांच्याशी थेट संवाद साधणाऱ्या हल्ल्यांचे निरीक्षण करतात; ते संपूर्ण नेटवर्कवरील हल्ले शोधू शकत नाहीत.
2. जर योग्य प्रकारे नियोजन केले गेले नाही , तर हनीपॉट्स नेटवर्कसाठी धोका निर्माण करू शकतात.

5.4 ई-मेल सुरक्षा(E-mail Security):

ई-मेल सुरक्षेची ओळख (Introduction to E-mail Security)

ई-मेल हा आजच्या जगात सर्वाधिक वापरला जाणारा संवाद साधण्याचा एक मार्ग बनला आहे. मात्र, इलेक्ट्रॉनिक मेलच्या सोयीसह सायबर हल्ल्यांचा धोका देखील मोठ्या प्रमाणात वाढतो. यामध्ये संदेशांचा इंटरसेप्शन, अनधिकृत प्रवेश आणि फेरफार करण्याचा धोका असतो. ई-मेल संप्रेषणाची गोपनीयता, अखंडता आणि प्रामाणिकता सुरक्षित ठेवण्यासाठी विविध प्रोटोकॉल आणि तंत्रज्ञान वापरले जाते. यामध्ये सिंपल मेल ट्रान्सफर प्रोटोकॉल (SMTP), प्रिटी गुड प्रायव्हसी (PGP), आणि सिक्युअर/मल्टीपर्पज इंटरनेट मेल एक्स्टेंशन्स (S/MIME) यांचा समावेश आहे.

5.4.1 सिंपल मेल ट्रान्सफर प्रोटोकॉल Simple Mail Transfer Protocol (SMTP)

- **SMTP ची संकल्पना आणि उद्देश(Definition and Purpose of SMTP):**

  सिंपल मेल ट्रान्सफर प्रोटोकॉल (SMTP) हा इंटरनेटवर ई-मेल पाठवण्यासाठी वापरला जाणारा प्रोटोकॉल आहे. तो प्रेषकाच्या(sender) ई-मेल क्लायंट किंवा सर्व्हरवरून ई-मेल प्राप्तकर्त्याच्या मेल सर्व्हरपर्यंत पोहोचवण्याचे कार्य करतो. SMTP हा इंटरनेट प्रोटोकॉल सूटच्या अप्लिकेशन लेयरवर कार्य करतो आणि TCP (ट्रान्समिशन कंट्रोल प्रोटोकॉल) चा वापर सुरक्षित ई-मेल पाठवण्यासाठी करतो. ई-मेल पाठवण्यासाठी SMTP वापरला जातो, तर IMAP (Internet Message Access Protocol) किंवा POP (Post Office Protocol) हे प्रोटोकॉल ई-मेल प्राप्त करण्यासाठी वापरले जातात.

SMTP कसे कार्य करते? (How SMTP Works ?)

1. **प्रेषकाचा ई-मेल क्लायंट ते सर्व्हर (Sender's Email Client to Server):** जेव्हा एखादा ई-मेल पाठवला जातो, तेव्हा ई-मेल क्लायंट (उदाहरणार्थ: Gmail, Outlook) पोर्ट 25, 465 किंवा 587 द्वारे आउटगोईंग मेल सर्व्हरशी जोडला जातो.
2. **सर्व्हर ते सर्व्हर संप्रेषण(Server to Server Communication):** SMTP क्लायंट-सर्व्हर मॉडेल वापरतो. प्रेषकाचा सर्व्हर (sender's server) हा ई-मेल प्राप्तकर्त्याच्या सर्व्हरपर्यंत पोहोचवण्यासाठी मध्यस्थ सर्व्हर (Intermediary Servers) चा वापर करू शकतो.
3. **प्राप्तकर्त्याच्या मेल सर्व्हरकडून ई-मेल क्लायंटपर्यंत(Recipient's Email Server to Client):**एकदा ईमेल प्राप्तकर्त्याच्या मेल सर्व्हरवर पोहोचला की, IMAP किंवा POP सारखे प्रोटोकॉल संदेश प्राप्तकर्त्याच्या क्लायंटकडे आणतात.

- **SMTP ची मर्यादा (SMTP Limitations)**

1. **एनक्रिप्शनचा अभाव(Lack of Encryption) :** SMTP ई-मेल एनक्रिप्ट करत नाही, त्यामुळे संदेश पाठवताना तो इंटरसेप्ट करून तिसऱ्या व्यक्तीला वाचता येऊ शकतो.
2. **स्पूफिंग आणि फिशिंगला धोका(Vulnerable to Spoofing and Phishing):** SMTP मध्ये अंतर्गत प्रमाणीकरण प्रणाली(authorization system) नाही, त्यामुळे हल्लेखोर(attacker) स्पूफिंग (फसवे ई-मेल पाठवणे) आणि फिशिंग (भ्रामक ई-मेलद्वारे माहिती चोरणे) सहज करू शकतात.

- **SMTP सुरक्षित करण्याचे उपाय:**

1. **STARTTLS:** STARTTLS हे SMTP साठी एक एनक्रिप्शन एक्सटेंशन (extension to SMTP)आहे, जे TLS (Transport Layer Security) वापरून असुरक्षित कनेक्शनला सुरक्षित कनेक्शनमध्ये बदलते.
2. **SMTP प्रमाणीकरण (SMTP Authentication):** SMTP प्रमाणीकरण (Authentication) च्या मदतीने, केवळ अधिकृत वापरकर्त्यांनाच ई-मेल पाठवण्याची परवानगी दिली जाते, ज्यामुळे अनधिकृत व्यक्ती स्पॅम ई-मेल पाठवू शकत नाहीत.

5.4.2 प्रिटी गुड प्रायव्हसी Pretty Good Privacy (PGP)

PGP ची ओळख (Overview of PGP): प्रिटी गुड प्रायव्हसी (PGP) हे ई-मेल संप्रेषण (email communication) सुरक्षित करण्यासाठी डेटा एनक्रिप्शन आणि डिक्रिप्शन तंत्रज्ञान आहे. PGP द्वारे एनक्रिप्शन आणि डिजिटल स्वाक्षरी (डिजिटल सिग्नेचर) वापरली जाते, ज्यामुळे प्राप्तकर्त्याला संदेशाची सत्यता आणि अखंडता सुनिश्चित करता येते.

- **PGP ची वैशिष्ट्ये(Features of PGP):**

1. ई-मेल एनक्रिप्शन(Email Encryption): PGP असिमॅट्रिक एनक्रिप्शन (public आणि private key) चा वापर करून संदेशाचे एन्क्रिप्शन करते. केवळ प्राप्तकर्ताच प्रायव्हेट की(private key) चा वापर करून संदेश वाचू शकतो.
2. डिजिटल स्वाक्षऱ्या(Digital Signatures):पीजीपी पाठवणाऱ्याला त्यांच्या खाजगी की वापरून संदेशावर डिजिटल स्वाक्षरी करण्याची परवानगी देते. ही स्वाक्षरी प्राप्तकर्त्याद्वारे प्रेषकाच्या सार्वजनिक की वापरून सत्यापित (verifiied)केली जाऊ शकते, ज्यामुळे संदेशाची सत्यता आणि अखंडता सुनिश्चित होते.
3. वेब ऑफ ट्रस्ट(Web Of Trust): PGP मध्ये वेब ऑफ ट्रस्ट (Web of Trust) नावाची पद्धत वापरली जाते, जिथे वापरकर्ते स्वतःच एकमेकांचे public keys सत्यापित करतात.

- **PGP कसे कार्य करते? (How PGP Works):**

1. की जनरेशन(Key Generation): PGP दोन प्रकारच्या क्रिप्टोग्राफिक की वापरते - public key आणि private key.
2. संदेश एन्क्रिप्शन(Encrypting the Message): प्रेषक(Sender) हा संदेश प्राप्तकर्त्याच्या public key चा वापर करून एनक्रिप्ट(encrypt) करतो.
3. संदेश स्वाक्षरी(Signing the Message): प्रेषक हा संदेश private key ने स्वाक्षरी करतो, ज्यामुळे प्राप्तकर्त्याला त्याची सत्यता तपासता येते.

- **PGP चे फायदे (Advantages of PGP):**

1. मजबूत सुरक्षा(Strong Security)**:** PGP मजबूत एन्क्रिप्शन आणि साइनिंग तंत्रांचा वापर करते, ज्यामुळे ई-मेल संवादांची गोपनीयता आणि प्रामाणिकता सुनिश्चित होते.
2. एंड-टू-एंड एन्क्रिप्शन(End-to-End Encryption)**:** PGP एंड-टू-एंड एन्क्रिप्शन प्रदान करते, म्हणजेच केवळ पाठवणारा आणि प्राप्त करणारा व्यक्तीच संदेश डिक्रिप्ट करून वाचू शकतो, ज्यामुळे तो तृतीय पक्षांच्या हस्तक्षेपापासून सुरक्षित राहतो.

- **PGP च्या मर्यादा (Limitations of PGP):**

1. सेटअप क्लिष्ट असतो**:** PGP चे की व्यवस्थापन (Key Management) आणि सेटअप जटिल (complex)असू शकतो.
2. सुसंगततेचा अभाव**:** सर्व ई-मेल सेवा PGP ला मूळतः (नॅटिव्हली) सपोर्ट करत नाहीत.

5.4.3 सिक्युअर/मल्टीपर्पज इंटरनेट मेल एक्स्टेंशन्स (S/MIME)

S/MIME ची ओळख(Overview of S/MIME):

S/MIME हे ई-मेल एनक्रिप्शन आणि डिजिटल स्वाक्षरी करण्यासाठी एक मानक आहे. PGP प्रमाणेच, S/MIME देखील ई-मेल सुरक्षित करण्यासाठी सार्वजनिक(Public) आणि खाजगी की(Private Key) प्रणालीचा वापर करते, परंतु हे सेंट्रलाइज्ड ट्रस्ट मॉडेलवर (Certificate Authorities - CAs) अवलंबून असते.

- **S/MIME ची वैशिष्ट्ये(Features of S/MIME):**

1. ई-मेल एनक्रिप्शन (Email Encryption): S/MIME मध्ये सिमेट्रिक आणि असिमॅट्रिक एनक्रिप्शन चा वापर केला जातो, ज्यामुळे संदेश संपूर्ण सुरक्षित राहतो.
2. डिजिटल स्वाक्षरी(Digital Signature): S/MIME डिजिटल स्वाक्षरींना समर्थन देते, ज्यामुळे प्राप्तकर्त्याला पाठवणाऱ्याची ओळख पडताळता येते आणि संदेशाची अखंडता पडताळता येते.
3. सर्टिफिकेट अथॉरिटीज (CAs) (Certificate Authorities (CAs)): S/MIME मध्ये वापरकर्त्याच्या public key ला प्रमाणित करण्यासाठी अधिकृत Certificate Authority (CA) आवश्यक असते.

- **S/MIME चे फायदे: (Advantages of S/MIME)**

1. सोपे एकत्रीकरण (Seamless Integration): S/MIME Microsoft Outlook आणि Apple Mail यासारख्या ई-मेल सेवांमध्ये सहज एकत्रित होते.
2. सेंट्रलाइज्ड ट्रस्ट मॉडेल(Centralized Trust Model) **:** Certificate Authorities (CAs) मुळे की व्यवस्थापन PGP पेक्षा सोपे होते.

- **S/MIME च्या मर्यादा(Limitations of S/MIME):**

1. सर्टिफिकेट खर्च(Cost of Certificates) **:** CA कडून प्रमाणपत्र मिळवण्यासाठी खर्च येतो.
2. CA वर अवलंबित्व(Dependence on CAs)**:** CA हॅक झाल्यास, त्या प्रमाणपत्रांवर अवलंबून असलेले सर्व ई-मेल असुरक्षित ठरू शकतात.

5.5 सायबर क्राईम (Cyber Crime):

5.5.1 सायबर क्राईमची ओळख (Introduction to Cyber Crime):

सायबर क्राईम (Cyber Crime)म्हणजे संगणक किंवा इंटरनेट वापरून केली जाणारी बेकायदेशीर क्रियाकलाप(Activities). या शब्दाचा अर्थ ओळख चोरीपासून हॅकिंगपर्यंत असलेल्या गुन्ह्यांचा समावेश करतो, आणि सायबर क्राईम (Cyber Crime) व्यक्ती, व्यवसाय आणि सरकारांसाठी जागतिक स्तरावर एक महत्त्वाचा धोका आहे.

परिभाषा (Definition): सायबर क्राईम म्हणजे अशी क्रिमिनल क्रियाकलाप (criminal activity) जी संगणक आणि नेटवर्कशी संबंधित असते. सायबर क्राईम हा संगणकावर किंवा त्याचा वापर करून दुसऱ्या कोणावर हल्ला करण्यास उद्दिष्ट असू शकतो.

सायबर क्राईमची मुख्य वैशिष्ट्ये (Key Characteristics of Cybercrime):

1. गोपनीयता(Anonymity): इंटरनेट गुन्हेगारांना त्यांची ओळख लपवण्याची संधी देते.

2. जागतिक पोहोच(Global Reach): सायबर क्राईम सीमा ओलांडून केली जाऊ शकतात.
3. डिजिटल पुरावे(Digital Evidence): गुन्ह्यांमुळे डिजिटल ठसा तयार होतो ज्याचा मागोवा घेतला जाऊ शकतो.
4. कुशलता(Sophistication): सायबर क्राईम (Cyber Crime) करणारे गुन्हेगार अत्याधुनिक तंत्रज्ञानाचा वापर करून प्रणालीतील कमकुवतता शोधतात.

5.5.2 हॅकिंग(Hacking)

हॅकिंग म्हणजे संगणक प्रणाली, नेटवर्क किंवा उपकरणांवर अनधिकृत प्रवेश किंवा नियंत्रण मिळविणे, ज्याचा उद्देश डेटा चोरी करणे, बदल करणे किंवा नष्ट करणे असतो.

परिभाषा (Definition): संगणक प्रणाली किंवा नेटवर्कमध्ये अनधिकृत प्रवेश मिळवून डेटा चोरणे किंवा त्यात फेरफार करणे.

हॅकिंगच्या पद्धती (Methods of Hacking):

1. फिशिंग (Phishing): वैयक्तिक माहिती चोरण्यासाठी डिझाइन केलेले फसवे ईमेल.
2. मालवेयर (Malware): हानीकारक सॉफ्टवेअर जसे की व्हायरस, वर्म्स आणि ट्रोजन्स (viruses, worms, and Trojans) जे कमकुवतता शोषण करण्यासाठी वापरले जातात.
3. डिनायल ऑफ सर्व्हिस हल्ले (Denial of Service Attacks): प्रणालीवर ट्रॅफिक लादून ते अनुपलब्ध करणे.
4. SQL इंजेक्शन (SQL Injection): वेबसाइटच्या डेटाबेसवर (website's database) हल्ला करून हानीकारक SQL कोड इंजेक्ट करणे.
5. सोशल इंजिनिअरिंग(Social Engineering): गोपनीय माहिती उघड करण्यासाठी व्यक्तींना हाताळणे.

हॅकिंगसाठी शिक्षा (Penalties for Hacking):काही न्यायक्षेत्रांमध्ये, हॅकिंगसाठी कठोर कायदेशीर शिक्षांची शिफारस केली जाते, ज्यामध्ये कारावास आणि मोठा दंड यांचा समावेश असतो.

5.5.3 डिजिटल बनावट (Digital Forgery)

डिजिटल बनावट म्हणजे डिजिटल कागदपत्रे आणि नोंदी तयार करणे, बदल करणे किंवा हाताळणे, ज्याचा उद्देश इतरांना फसवणे असतो.

परिभाषा (Definition): डिजिटल सामग्रीत फेरफार किंवा बनावट करणे, ज्यामुळे लोकांना भुलवले किंवा फसवले जाते.

उदाहरणे (Examples):

1. बनावट कागदपत्रे: करार, प्रमाणपत्रे आणि ईमेल यासारख्या बदललेल्या किंवा बनावट डिजिटल फायली.
2. तोतयागिरी: ईमेल्स किंवा सोशल मीडियावर बनावट ओळख वापरणे.
3. फोटो मॅनिप्युलेशन(Photo Manipulation): फसवणूक करणारे उद्देश असलेली प्रतिमा संपादन करणे.

कायदेशीर परिणाम: डिजिटल बनावट (Digital Forgery)हे बेकायदेशीर आहे आणि गुन्हेगारी आरोपांची शिफारस केली जाऊ शकते, ज्यामध्ये फसवणूक किंवा ओळख चोरी यांचा समावेश होऊ शकतो.

5.5.4 सायबर स्टॉकिंग आणि त्रासदायक वर्तन (Cyber Stalking and Harassment)

सायबर स्टॉकिंग (Cyber stalking)म्हणजे इंटरनेटचा वापर करून व्यक्तींना त्रास देणे किंवा त्यांचे मागोवा घेणे, जे सामान्यतः द्वेषपूर्ण उद्देशाने केले जाते.

परिभाषा (Definition) : इंटरनेटवर कोणाचाही सतत मागोवा घेणे, त्रास देणे किंवा धमकी देणे, जे प्रामुख्याने मानसिक किंवा मानसिक त्रासाला कारणीभूत ठरते.

सामान्य पद्धती(Common Methods):

1. त्रासदायक ईमेल्स(Harassing Emails): वारंवार धमकी किंवा अपमानकारक संदेश पाठवणे.
2. सोशल मीडिया हल्ले(Social Media Attacks): फेसबुक किंवा ट्विटरसारख्या प्लॅटफॉर्मवर खोटी माहिती किंवा धमक्या पसरवणे.
3. डॉक्सिंग(Doxxing): एखाद्या व्यक्तीला धमकावण्यासाठी किंवा हानी पोहोचवण्यासाठी त्याची खाजगी माहिती ऑनलाइन पोस्ट करणे.

मानसिक परिणाम(Psychological Impact):
पीडित व्यक्तींना सामान्यतः चिंता, नैराश्य आणि त्यांच्या सुरक्षिततेबद्दल भीती वाटते.

कायदेशीर कारवाई:
सायबर स्टॉकिंग (Cyber stalking): हे सायबर सुरक्षा कायदा आणि विविध राष्ट्रीय अँटी-स्टॉकिंग कायद्यांनुसार दंडनीय आहे.

5.5.5 सायबर पोर्नोग्राफी (Cyber Pornography): साइबर अश्लीलता(pornography) म्हणजे इंटरनेटवर अश्लील सामग्रीचे प्रसारण, पाहाणे किंवा तयार करणे. यामुळे व्यक्तींच्या मानसिक आणि शारीरिक स्वास्थ्यावर वाईट परिणाम होऊ शकतात आणि समाजावर नकारात्मक परिणाम होऊ शकतो.

परिभाषा (Definition): इंटरनेटद्वारे लैंगिकदृष्ट्या अश्लील सामग्री तयार करणे, वितरण करणे किंवा वापरणे.

मुख्य समस्या (Key Issues):
1. बाल पोर्नोग्राफी **(**Child Pornography**)**: अल्पवयीन मुलांशी संबंधित बेकायदेशीर सामग्री, जी कठोर कायद्यांअंतर्गत शिक्षेची पात्र आहे.
2. सहमती नसलेली पोर्नोग्राफी **(**Non-consensual Pornography**)**: जेव्हा कोणाच्याही संमतीशिवाय स्पष्ट सामग्री सामायिक केली जाते.

5.5.6 ओळख चोरी आणि फसवणूक (Identity Theft and Fraud)
ओळख चोरी म्हणजे दुसऱ्या व्यक्तींच्या वैयक्तिक माहितीचा अवैध वापर, जो मुख्यतः आर्थिक फायदेशीर उद्देशांसाठी केला जातो.

परिभाषा (Definition)**:** दुसऱ्या व्यक्तींची वैयक्तिक माहिती जसे की सोशल सेक्युरिटी नंबर, बँक तपशील, आणि क्रेडिट कार्ड माहिती चोरून त्याचा गैरवापर करणे.

ओळख चोरीचे प्रकार(Methods of Identity Theft):
1. फिशिंग(Phishing)**:** खोटी माहिती किंवा ईमेल्स पाठवून व्यक्तीची वैयक्तिक माहिती गोळा करणे.
2. डेटा ब्रिचेस(Data Breaches): कॉर्पोरेट सिस्टममधून मोठ्या प्रमाणावर वैयक्तिक माहितीची चोरी.
3. स्किमिंग(Skimming): क्रेडिट कार्डवरून डेटा चोरण्यासाठी उपकरणांचा वापर.

परिणाम (Consequences):
आर्थिक नुकसान, खराब क्रेडिट स्कोअर(credit scores), आणि पीडितांसाठी कायदेशीर अडचणी.

5.5.7 सायबर दहशतवाद (Cyber Terrorism)
सायबर दहशतवाद म्हणजे इंटरनेटचा वापर करून राजकीय हेतूंनी दहशतवादी क्रिया करणे, ज्याचा उद्देश महत्त्वाच्या माहिती प्रणालींना लक्ष्य करून व्यापक गोंधळ किंवा भीती निर्माण करणे आहे.

परिभाषा (Definition):इंटरनेटचा वापर करून दहशतवादी कारवाया करणे, जसे की महत्त्वपूर्ण पायाभूत संरचना ठप्प करणे किंवा प्रचार साधणे.

सायबर दहशतवादाच्या पद्धती (Methods of Cyber Terrorism):
1.शासन प्रणालींमध्ये हॅकिंग: राष्ट्रीय सुरक्षा किंवा सार्वजनिक सेवांना खंडित करणे.
2. महत्त्वपूर्ण पायाभूत संरचनांवर हल्ले: वीज ग्रिड्स, जलवाहन प्रणाली, किंवा वाहतूक व्यवस्था यावर हल्ले करणे.
3. डेटा हेरफेर आणि खोटी माहिती पसरवणे: समाजातील अस्थिरता निर्माण करण्यासाठी चुकीची माहिती पसरवणे.

जागतिक धोका(Global Threat): सायबर दहशतवाद हा एक अत्यंत गंभीर जागतिक सुरक्षा धोका मानला जातो आणि आंतरराष्ट्रीय करार आणि संधिपत्रांद्वारे यावर नियंत्रण ठेवले जाते.

5.5.8 सायबर बदनामी (Cyber Defamation)
सायबर बदनामी म्हणजे ऑनलाइन खोटी माहिती पसरवणे, ज्यामुळे एखाद्या व्यक्तीची किंवा संस्थेची प्रतिष्ठा धूसर होते.

परिभाषा (Definition):ऑनलाइन प्लॅटफॉर्म्स, जसे की सोशल मीडिया, ब्लॉग्स, किंवा फोरम्सवर खोटी माहिती प्रकाशित करणे, ज्यामुळे कोणाच्या प्रतिष्ठेला इजा होईल.

सायबर बदनामीचे प्रकार (Forms of Cyber Defamation)

1. खोटे आरोप: एखाद्याची प्रतिष्ठा खराब करण्यासाठी खोट्या गोष्टी पसरवणे.
2. नकारात्मक पुनरावलोकने (Negative Reviews): प्रामाणिक पुनरावलोकन (review)म्हणून बदनामी करणाऱ्या टिप्पणी पोस्ट करणे.
3. सोशल मीडिया हल्ले: प्लॅटफॉर्म्सचा वापर करून हानीकारक अफवा किंवा खोटी माहिती पसरवणे.

5.5.9 OS फिंगरप्रिंटिंग (OS Fingerprinting)

OS फिंगरप्रिंटिंग हे एक तंत्र आहे ,ज्याचा वापर हॅकर्स लक्ष्य डिव्हाइसच्या नेटवर्क प्रतिसादांवर आधारित त्याच्या ऑपरेटिंग सिस्टीमची ओळख पटवण्यासाठी करतात.

परिभाषा (Definition):दूरस्थ डिव्हाइस(remote device) किंवा सर्व्हरच्या ऑपरेटिंग सिस्टीमची ओळख पटविण्याची प्रक्रिया, ज्याचा उपयोग सिस्टममधील कमतरतांचा फायदा उठवण्यासाठी केला जातो.

फिंगरप्रिंटिंगचे प्रकार(Types of Fingerprinting):

1. सक्रिय फिंगरप्रिंटिंग: लक्ष्य डिव्हाइसला विशेषतः तयार केलेल्या पॅकेट्स पाठवणे आणि प्रतिसादाचे विश्लेषण करणे.
2. निष्क्रिय फिंगरप्रिंटिंग: ट्रॅफिक पॅटर्न्स निरीक्षण करून आणि थेट संवाद न करता ऑपरेटिंग सिस्टीमची ओळख पटवणे.

सुरक्षा परिणाम(Security Implications):

हॅकर्स OS फिंगरप्रिंटिंगचा वापर विशिष्ट ऑपरेटिंग सिस्टीमच्या कमतरतांना लक्ष्य करून हल्ले करणे, ज्यामुळे अनधिकृत प्रवेश किंवा डेटा चोरी होऊ शकते.

5.6 सायबर कायदे(Cyber Laws):

5.6.1 सायबर कायद्यांची ओळख (Introduction to Cyber Laws):सायबर कायदे (किंवा इंटरनेट कायदे) ही एक कायदेशीर चौकट आहे जी डिजिटल किंवा ऑनलाइन जगात होणाऱ्या क्रियाकलापांचे नियमन करण्यासाठी तयार केली आहे. या कायद्यांचा उद्देश व्यक्ती, संस्था आणि सरकारला सायबर अपराधापासून संरक्षण करणे आणि गोपनीयता, बौद्धिक संपत्ती, सायबर सुरक्षा आणि ऑनलाइन व्यवहारांसारख्या मुद्द्यांसाठी एक चौकट तयार करणे आहे.

परिभाषा (Definition): सायबर स्पेसमधील क्रियाकलापांचा(Activities), ज्यामध्ये इंटरनेट, संगणक आणि डिजिटल प्लॅटफॉर्मचा (digital platform) वापर समाविष्ट आहे.

उद्देश: इंटरनेटचा(internet) सुरक्षित आणि नैतिक वापर सुनिश्चित करणे, ऑनलाइन क्रियाकलापांसाठी(Activities) कायदेशीर संरक्षण प्रदान करणे आणि डिजिटल वातावरणात हक्क आणि जबाबदाऱ्यांची अंमलबजावणी करणे.

5.6.2 सायबर कायद्यांची आवश्यकता (Need of Cyber Laws)

सायबर कायदे डिजिटल पर्यावरणामध्ये विविध सायबर धोक्यांपासून संरक्षण करण्यासाठी महत्त्वपूर्ण भूमिका बजावतात. या कायद्यांचा रोल अत्यंत महत्वाचा आहे.

1. **वैयक्तिक आणि संवेदनशील माहितीचे संरक्षण (**Protecting Personal and Sensitive Information**)**: ऑनलाइन शॉपिंग(online shopping), बँकिंग आणि सोशल नेटवर्किंगमधील वाढीमुळे वैयक्तिक डेटा सायबर गुन्हेगारांसाठी एक प्रमुख लक्ष्य बनले आहे.
   उदाहरण: ओळख चोरी आणि क्रेडिट कार्ड(credit card) फसवणूक हे ऑनलाइन गुन्ह्यांचे सामान्य प्रकार आहेत ज्यामुळे लाखो व्यक्तींना वारंवार त्रास होतो. सायबर कायदे वैयक्तिक डेटाचे कसे संकलित, संग्रहित आणि शेअर केले जाते यावर कठोर नियम लागू करतात.
2. **डिजिटल सुरक्षा सुनिश्चित करणे (**Ensuring Digital Security**)**: सायबर सुरक्षा कायदे हे व्यक्ती, व्यवसाय आणि सरकारांना सायबर हल्ल्यांपासून बचाव करण्यासाठी सुरक्षा प्रोटोकॉलचे (protocol)पालन करण्यास भाग पाडतात.
   उदाहरण: रॅन्समवेअर (Ransom ware) हल्ले, जे डेटा लॉक करतात आणि खंडणीची मागणी करतात, यापासून बचाव करण्यासाठी या कायद्यांनी विशिष्ट सुरक्षा मार्गदर्शक तत्त्वे लागू केली आहेत.

3. **सायबर क्राइम आणि फसवणूक प्रतिबंधित करणे** (Preventing Cybercrime and Fraud)**:**सायबर कायदे फिशिंग, हॅकिंग आणि ऑनलाइन (phishing, hacking, and online harassment) त्रासदायक वर्तन यासारख्या क्रियाकलापांना(Activities) गुन्हा ठरवतात.
   उदाहरण: माहिती तंत्रज्ञान कायदा, 2000 (भारत) डेटा चोरी, सायबर दहशतवाद आणि बदनामी यांसारख्या अपराधांना शिक्षा करतो.
4. **ई-कॉमर्स आणि सुरक्षित व्यवहार सक्षम करणे** (Enabling E-commerce and Secure Transactions): सायबर कायदे ऑनलाइन करार आणि डिजिटल व्यवहारांसाठी कायदेशीर चौकट प्रदान करतात, ज्यामुळे त्यांची वैधता सुनिश्चित केली जाते.
   उदाहरण: ई-स्वाक्षरी अनेक देशांमध्ये कायदेशीर मान्यताप्राप्त आहे, ज्यामुळे डिजिटल(digital) व्यवसाय व्यवहार अधिक विश्वासार्ह बनतात.
5. **डिजिटल जगात इंटेलेक्टच्युअल प्रॉपर्टी(Intellectual Property) संरक्षण** (Protecting Intellectual Property in the Digital World)**:**सायबर कायदे डिजिटल सामग्रीचे, जसे की सॉफ्टवेअर(software), ऑनलाइन प्रकाशने, संगीत इत्यादीचे, अनधिकृत प्रती आणि चोरीपासून संरक्षण करतात.
   उदाहरण: कॉपीराइट(copyright) उल्लंघन हे आर्टिस्ट(artist) आणि सॉफ्टवेअर डेव्हलपर्ससाठी(software developers) एक मोठी चिंता आहे, आणि सायबर कायदे त्यांच्या कामाचे संरक्षण करतात.

5.6.3 साइबर कायदे – प्रकार (Categories of Cyber Laws)

साइबर कायद्यास विविध प्रकारांमध्ये वर्गीकृत केले जाऊ शकते:

1. **व्यक्तींविरुद्ध साइबर गुन्हे (Cybercrimes against Individuals)**

व्यक्तींविरुद्धचे साइबर गुन्हे महत्त्वपूर्ण हानी करतात, ज्यामध्ये आर्थिक हानीपासून वैयक्तिक त्रासापर्यंत समाविष्ट आहे. व्यक्तींविरुद्धचे मुख्य गुन्हे खालीलप्रमाणे आहेत:

a. **ओळख चोरी** (Identity Theft): एखाद्याची वैयक्तिक माहिती चोरून फसवणूक करण्यासाठी, जसे की बँक खाते उघडणे किंवा त्यांच्या नावावर खरेदी करणे.

b. **साइबर छळ** (Cyber bullying): इंटरनेटचा वापर करून एखाद्या व्यक्तीला त्रास देणे, अपमानित करणे किंवा धमकावणे.

c. **फिशिंग आणि ऑनलाइन फसवणूक** (Phishing and Online Fraud) फसवणूक करणारे ईमेल किंवा वेबसाइट्स, जे व्यक्तींना त्यांच्या संवेदनशील माहिती जसे पासवर्ड(password) किंवा आर्थिक तपशील सामायिक करण्यास प्रवृत्त करतात.

d. **हॅकिंग आणि डेटा चोरी** (Hacking and Data Theft) : एखाद्या व्यक्तीच्या संगणकावर किंवा खात्यावर अनधिकृत प्रवेश करून डेटा(data) चोरी करणे, जसे की आर्थिक माहिती किंवा वैयक्तिक फोटोज.

e. **ऑनलाइन छळ आणि स्टॉकिंग** (Online Harassment and Stalking): एखाद्या व्यक्तीला त्रास देण्यासाठी, लाजिरवाणे करण्यासाठी किंवा धमकी देण्यासाठी इंटरनेटचा वापर करणे.

2. सरकारविरुद्धचे साइबर गुन्हे (Cybercrimes against Governments)

सरकार ही साइबर हल्ल्यांसाठी प्रमुख लक्ष्य असतात, आणि साइबर कायदे राष्ट्रीय सुरक्षा आणि सार्वजनिक सुरक्षा यांना अशा गुन्ह्यांपासून वाचवतात.

a. **साइबर दहशतवाद** (Cyber terrorism) :डिजिटल प्लॅटफॉर्मचा(digital platform) वापर करून असे हल्ले करणे जे भिती, विध्वंस, किंवा महत्त्वाच्या इन्फ्रास्ट्रक्चरमध्ये(infrastructure) विघटन करण्यासाठी डिझाइन केले जातात.

b. **साइबर गुप्तचरता** (Cyber Espionage): सरकारी नेटवर्कमध्ये प्रवेश करून गुप्त माहिती चोरणे, बहुतेक वेळा गुप्तचर किंवा राष्ट्रीय सुरक्षा उद्देशांसाठी.

c. **डेटा उल्लंघन आणि अनधिकृत प्रवेश** (Data Breaches and Unauthorized Access)**:** सरकारी प्रणालींमध्ये अनधिकृत प्रवेश करून महत्त्वाच्या डेटाची चोरी, बदल किंवा नष्ट करणे.

3. संपत्तीविरुद्धचे साइबर गुन्हे (Cybercrimes against Property)

संपत्तीविरुद्धचे साइबर(cyber) गुन्हे व्यक्ती आणि व्यवसाय दोन्हीना प्रभावित करतात, ज्यामुळे आर्थिक आणि प्रतिष्ठेच्या दृष्टीने हानी होऊ शकते.

a. **बौद्धिक संपत्ती चोरी (**Intellectual Property Theft**)**: डिजिटल सामग्री किंवा सॉफ्टवेअर चोरणे किंवा पायरेटिंग(pirating) करणे.

b. **डेटा चोरी आणि कॉर्पोरेट गुप्तचरता** (Data Theft and Corporate Espionage): संवेदनशील कंपनी माहिती चोरी करणे, जसे की व्यापार रहस्ये, संशोधन डेटा, किंवा क्लायंट यादी..

c. **साइबर तोडफोड (Cyber Vandalism)**: साइबर तोडफोड (Cyber Vandalism) म्हणजे इंटरनेट (internet) वापरून वेबसाईट्स किंवा डिजिटल (websites and digital) सामग्रीला नुकसान पोहोचवणे किंवा त्याचा दुरुपयोग करणे.

References:

1. Information Systems Security Second Edition By Nina Godbole (John Wiley Isbn-13: 978-8126564057)
2. Cryptography and Information Security By V.K.Pachghare – Prentice Hall India
3. Cryptography and Network security Third Edition By Atul Kahate- McGraw-Hill; Fourth edition ISBN-13: 978-9353163303
4. Computer Security Principles and Practice, Third Edition BY William Stallings, Lawrie Brown Pearson. ISBN-13: 978-0-13-377392-7