Cyber Security Essentials

Jake Cho

Dristi Pande

Sivani

Aman Fatima

Information technology and Internet services both need to take cybersecurity into account. We must be aware of the significance of the various threats that might be found in the online world. Improving cyber security and safeguarding sensitive data are crucial for the security and well-being of the country. When we consider cyber security, we also include cybercrime, which is on the rise.

The concept of software security is to design Software so it can still operate as intended in the face of direct assault. Most technologists recognize this endeavor’s significance but require some assistance in comprehending how to approach it. The essay seeks to offer that assistance by examining software security best practices. A software issue is a key and crucial component of the computer security issue. Software bugs with security implications, such as implementation bugs like buffer overflows and design flaws like inconsistent error handling, are predicted to stay there for a long time.

This paper includes an Overview of Cyber Security, Cyber Security concepts, security requirements, CIA triad, Hashing, types of hashing, System & Network Security, Intrusion Detection & Prevention, Software security, etc.

**Intrusion Detection System and Types**

**Intrusions Detection System?**

An intrusion detection system (IDS) is a technological tool that scans your network’s incoming and outgoing traffic for unauthorized activity and policy violations. As the name implies, the main function of an IDS is to identify and stop intrusions into your IT infrastructure, then notify the appropriate parties. These remedies may come in the form of hardware or software.

**Five different type of Intrusion detection system:**

**Network Intrusion Detection System:**

Using one or more touchpoints, a network intrusion detection system (NIDS) keeps an eye on your whole network. A NIDS often must be installed on some hardware as part of your network architecture in order to be used. Your NIDS will begin sampling each packet (a grouping of data) that passes through it as soon as it is deployed.

**Network Node Intrusion Detection System:**

The packets that pass through a NNIDS are also examined. Instead of depending on a single device to keep an eye on all network activity, the system keeps an eye on every node linked to your network. Multiple installations are required, which is the biggest disadvantage of choosing an NNIDS. A NNIDS needs multiple devices, one for each server you want to monitor, as opposed to a NIDS which only needs one.

**Host Intrusion Detection System:**

Device independence of NNIDS is furthered by a host intrusion detection system (HIDS). You can install IDS software on each device linked to your network via a HIDS. By “snapping” pictures of the gadget they are given, HIDSs function. The HIDS can find the discrepancies that can point to an intrusion by comparing the most recent snapshot to earlier records.

**Protocol Based Intrusion Detection System:**

A particular IDS that keeps an eye on the protocol in use is known as a “Protocol-Based Intrusion Detection System” (PIDS). The HTTP or HTTPS protocol stream between your devices and the server is often examined by this system in practice. A PIDS will typically be installed at the server’s front end. Technology can safeguard your web server by keeping track of both incoming and outgoing traffic.

**Application Protocol Based Intrusion Detection System:**

IDSs that focus on software app security are called Application Protocol-Based Intrusion Detection Systems (APIDS). APIDSs keep track of communications between apps and the server and are frequently linked to host-based intrusion detection systems (HIDS). Typically, a group of servers will have an APIDS installed.

**Reference:** [**https://www.helixstorm.com/blog/types-of-intrusion-detection-systems/**](https://www.helixstorm.com/blog/types-of-intrusion-detection-systems/)

**Overview Symmetric vs. Asymmetric Key Cryptography**

**Symmetric Key Cryptography:**

Symmetric key cryptographyuses an individual key for both encryption and decryption. The sender needs the key to encrypt the plaintext and sends the encrypted document to the recipient**.** The recipient used the same key (or setofrules**)** to decrypt the message and restore the plaintext. Sinceasingle key is used for both functions, symmetric key cryptography is also known as symmetric cryptography**.**

**Asymmetric cryptography**

Asymmetric cryptography uses two keys for encryption and decryption. It depends on the public and private key techniques**.**A publickey is shared between multipleusers**.**Thedata is decrypted by a private key which is not transformed. It’s slower but safer**.** The public key used in this encryption technique applies to everyone, but the private key used is not disclosed**.**

**Differences between symmetric and asymmetric**

**Symmetric cryptography**

1. Only one key (symmetric key) is used, and a similar key can be used to encrypt and decrypt the message.
2. It’s effective because this technique is recommended for large amounts of text.   symmetric encryption is generally used to transmit bulk information.
3. Symmetric key cryptography is also known as secret key cryptography or private key cryptography.
4. Symmetric key cryptography uses fewer resources than asymmetric key cryptography. The length of the keys used is often 128 or 256 bits, depending on your security requirements.

## 

## Asymmetric cryptography

1. Two different cryptographic keys (asymmetric keys) called public and private keys are used for encryption and decryption.
2. It is inefficient because this approach is only used for short messages.
3. It is generally used in small transactions. It is used to create a secure connection channel before the actual information is transmitted.
4. Asymmetric key cryptography is also called public key cryptography or traditional cryptosystem.
5. Asymmetric key cryptography uses more resources than symmetric key cryptography.
6. The length of the keys is much longer since the recommended RSA key size is 2048 bits or higher.

**References**

**https://www.tutorialspoint.com/what-is-the-difference-between-symmetric-key-cryptographic-and-asymmetric-key-cryptography**

# 

# User Authentication & Types

## User Authentication:

Identification of users who request access to a system, network, or device is the process of authentication. The methods below are commonly used for user authenticate process.

1. Password based Authentication
2. Multi Factor Authentication
3. Certificate based Authentication
4. Biometric Authentication
5. Token based Authentication

## 

## Password Based Authentication:

The most used form of authentication is password based authentication. A string of letters, numbers, or special characters can be used as a password. It can mainly be used in login the website and applications with proper user I’d and password. Make sure your password are strong enough and incorporate a variety of characters in order to protect yourself.

## Multi Factor Authentication:

Identifying the user by two or more methods is called Multi Factor Authentication like the user’s smartphone’s generated codes, Captcha puzzles, fingerprints, voice biometrics, or facial recognition. users’ trust is increased by MFA authentication methods and technologies since they add several layers of protection.

## Certificate based Authentication:

Digital certificates are used in certificate-based authentication solutions to identify individuals, machines, or devices. A digital certificate is electronic documents that is modeled like passport or Driver’s license.

**Biometric Authentication:**

Biometric authentication is mainly authenticated on unique biological characteristics of an individual. It can offer a high level of security without causing the user any inconvenience, the technology is being used more and more. Common biometric authentication methods include

1. Facial Recognition
2. Fingerprint scanners
3. Speaker recognition
4. Eye Scanners

## 

## Token Based Authentication:

Users who utilize token-based authentication systems can exchange a unique encrypted string of random characters for their credentials once and receive it back. Instead of typing your credentials again, you can utilize the token to access protected systems. Your access authorization is demonstrated by the digital token. RESTful APIs used by numerous frameworks and clients are an example of a use case for token-based authentication.

**Reference:** <https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/>

# Cloud based SCADA Systems

SCADA is an acronym for “Supervised Control and Data Acquisition” SCADA is an example of an ICS used for the automation and control of processes. SCADA systems can be utilised for a variety of reasons in the modern era (oil and gas, transportation, and water and wastewater). Therefore, devices with components situated in different regions of the world must be centrally monitored and maintained. SCADA systems cannot carry out their monitoring and control activities without a vast network of field stations in several locations. Each active location contains a minimum of one remote terminal unit, programmable logic controller, and improvised explosive device (IED). Through real-time communication with the plant’s sensors and/or actuators, these nodes collect plant operation data, execute limited field control orders, and transfer site data to command centres known as Master Stations (MS). The Human Machine Interface displays the system’s analysis of data collected from all disciplinary locations via a robust communication network on a graphical terminal.

The SCADA supervisory layer (or control centre) is responsible for monitoring system health by gathering data from field sensors, visualising control and administrative activities, and transmitting commands to field controllers via data connections. A typical SCADA system’s nerve centre consists of SCADA servers, builder servers, communication servers, database servers, diagnostic servers, application servers, a human-machine interface, and a system operator. For example, database servers compile and store information about an organization, including process control analysis and macro-level corporate strategy.

**Cloud Security Analysis**

Currently, the possible risks and weaknesses of cloud computing are being carefully investigated. We outline the cloud service model vulnerabilities for every known security issue. The paper details the vulnerabilities and identifies the cloud service architectures vulnerable to them (SPI).

Despite the fact that this study focuses on technological difficulties, it is crucial to realise that organizational issues may equally impact the security of cloud and platform services. Listed below are some instances in which you may be susceptible to attack:

Due to inadequate hiring and screening processes, certain cloud service providers may not complete background checks on their employees. If we take cloud administrators as an example, they can frequently see all cloud-stored data without restriction.

The lack of cybersecurity knowledge among most individuals is one of the greatest obstacles to developing a safe online environment. This is true for all businesses, but the cloud’s many moving pieces magnify the effect (cloud service providers, third-party providers, suppliers, corporate clients, and end-users).

Cloud computing uses a variety of cutting-edge technologies, such as web-based services, web browsers, and virtualization, to facilitate the development of cloud-based infrastructures. Consequently, every flaw in these systems might have a substantial effect on the cloud.

An attack on data storage and virtualization could have the most catastrophic implications. Lower-level strikes have a stronger effect on those at higher levels. Our primary focus is on security concerns associated with virtualization, shared resources, and remote data storage and processing. An attack that exploits a known vulnerability is demonstrated. We anticipate that this investigation will lead us to existing safeguards against these threats. This information can be described more clearly by highlighting incorrect usage habits. Misuse patterns highlight the steps that an attacker takes to commit misuse.

In concluding this topic we can say that SCADA systems are strongly reliant on safety-critical infrastructures such as transportation networks, electricity grids, gas pipelines, and water distribution systems. Frequent vulnerability evaluations are vital to the cyber security of vital infrastructure such as power plants. Recent improvements in information and communication technologies have left current SCADA networks more vulnerable to cyber and physical layer attacks that don’t necessitate the usage of a physical device. Due to the vital importance of SCADA systems, security solutions for these systems have received significant attention in recent years. The proposed analytical framework offers a metric for measuring the system’s susceptibility to assault. As they permit a connection between the cyber layer and the physical world, data- and model-based threat detection technologies can be viewed as complementary solutions to an information security strategy.

Reference:

Ferrag, M. A., Babaghayou, M., &Yazici, M. A. (2020). Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *Journal of Information Security and Applications*, *52*, 102500.

Upadhyay, D., &Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, 101666.

Khan, M., Rehman, O., Rahman, I. M., & Ali, S. (2020, September). Lightweight Testbed for Cybersecurity Experiments in SCADA-based Systems. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1-5). IEEE.

Reuter, L., Jung, O., &Magin, J. (2020, February). Neural network based anomaly detection for SCADA systems. In *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)* (pp. 194-201). IEEE.

Selvarajan, S., Shaik, M., Ameerjohn, S., & Kannan, S. (2019). Mining of intrusion attack in SCADA network using clustering and genetically seeded flora-based optimal classification algorithm. *IET Information Security*, *14*(1), 1-11.

A single negligent breach can close your business forever because your liability insurance may not cover professional negligence if you are unable to provide evidence that you took reasonable steps to prevent a breach or other cybersecurity-related incident. Without the ability to prove steps were taken to ensure due care and due diligence were applied to your business operations, you may be considered negligent in a lawsuit and be fully exposed to fines, penalties, and damages.

This is where Compliance Forge can help, since we have the information security solutions that your company needs to be able to prove evidence of due care and due diligence with industry-accepted best practices for IT security. From IT security policies to risk assessments, to vendor management solutions, we can help you keep your company secure! Documentation serves as the foundational building blocks for your cybersecurity and privacy program.

Without properly scoped policies to address your applicable statutory, regulatory, and contractual obligations, your associated standards and 4procedures will likely be inadequate to meet your compliance needs. The requires a holistic approach to right-sizing your cybersecurity program to meet your organization’s specific compliance and security requirements. We offer a wide assortment of cybersecurity policies, standards, procedures and more, since we understand that businesses have unique needs that cannot be met by just one product. While companies want to align with a single cybersecurity framework such as NIST 800-53, ISO 27002 or NIST Cybersecurity Framework, it is getting much more common for companies to have to juggle multiple frameworks and that requires scalable documentation.

We leverage the Hierarchical Cybersecurity Governance Framework to take a comprehensive view towards the necessary documentation components that are key to being able to demonstrate evidence of due diligence and due care.

This framework addresses the interconnectivity of policies, control objectives, standards, guidelines, controls, risks, procedures & metrics. This approach works well with any cybersecurity framework to help any organization, regardless of industry, to get and stay both secure and compliant.

Compliance Forge has simplified the concept of the hierarchical nature of cybersecurity and privacy documentation in the following downloadable diagram that demonstrates the unique nature of each documentation component that is expected to exist as part of a cybersecurity and privacy program. You can click on the image below to better understand how we write our documentation to link from policies all the way down to metrics. Concept of Operations (CONOPS) is a user-oriented guidance document that describes the mission, operational objectives, and overall expectations from an integrated systems point of view, without being overly technical or formal. A CONOPS is meant to:

* Benefit stakeholders by establishing a baseline “operational concept” to establish a conceptual, clearly understood view for everyone involved in the scope of operations described by the CONOPS.
* Record design constraints, the rationale for those constraints and to indicate the range of acceptable solution strategies to accomplish the mission and any stated objectives.
* Contain a conceptual view that illustrates the top-level functionality in the proposed process or system.
* We leverage the Operationalizing Cybersecurity Planning Model in creating a practical view towards implementing cybersecurity requirements.

# Information Security Documentation

# 

Organizations are often not at a loss for a set of policies, but executing those requirements often fall short due to several reasons.

Standardized Operating Procedures (SOPs) are where the rubber meets the road for Individual Contributors (ICs), since these key players need to know how they fit into day-to-day operations,  what their priorities are and what is expected from them in their duties.

When looking at it from an auditability perspective, the evidence of due diligence and due care should match what the organization’s cybersecurity business plan is attempting to achieve.

The central focus of any procedures should be a Capability Maturity Model (CMM) target that provides quantifiable expectations for People, Processes and Technologies (PPT), since this helps prevent a “moving target” by establishing an attainable expectation for “what right looks like” in terms of PPT.

Generally, cybersecurity business plans take a phased, multi-year approach to meet these CMM-based cybersecurity objectives. Those objectives, in conjunction with the business plan, demonstrate evidence of due diligence on behalf of the CISO and his/her leadership team.

The objectives prioritize the organization’s service catalog through influencing procedures at the IC-level for how PPT are implemented at the tactical level. SOPs not only direct the workflow of staff personnel, but the output from those procedures provides evidence of due care.

Cybercrime is a global issue faced nowadays that poses a threat to individual security and to large organizations, banks, hospitals, and so on. It is a bitter truth that today’s generation lives on the internet irrespective of age. And so this generation has been considered a golden age for hackers. The hackers become smarter, more innovative, and more creative day by day and they continue with illegal activities. (Paul, 2022). Along with the growth in the cyber security, the hacking world also grows faster. Cyber attacks are usually focused at accessing, altering and destroying the sensitive information and get money from others or destroy the business organizations. Therefore, to overcome these security challenges, it is important to implement cyber security measures. Cyber security is an approach that is used to protect network integrity and prevents digital attacks and unauthorized access. The implementation of effective cyber security measures is a challenging factor today as there exists a lot of devices than people, and moreover the attackers are also becoming more innovative and creative. Cyber security strategy has a protective layer that would defend the cyber-attacks from gaining access to the data (Seemma P.S, 2018).

# 

# Network Security

A network security in cyber world is used to protect the data or any kind of information

from threats, malware or breaches. It is basically the overall protection of network and

saves the information from hackers. It also involves the control of the virus and antivirus

from the software’s for the application and network security to give few examples are VPN

and firewalls. Network security is designed to safeguard any organizations from large and

costly loss of data and information. Firewall is the security that is used for the protection it

is used to control the incoming and outgoing traffic on the network The complete cyber

security relies mainly on the firewalls and advance firewalls as they play an important role in

the cyber world.

Security components -The three main security components here in cyber security are CIS-

confidentiality, Integrity and Availability where confidentiality is defined as the assurance

that no information is leaked or passed to any unauthorized users or any devices, it protects

the data from any kind of attack and keeps the information confidential. Protection of

organizations information is the responsibility of every person working for that company.

On the other hand, integrity is defined as any information that is maintained and not

modified, changed or deleted by any unauthorized users. Integrity must maintain the

consistency and accuracy. The final part is the availability which makes sures that

information or data is available from the right source to the user when needed under any

circumstances.

# Malwares

Let us talk about the malwares in cybersecurity, few of the common malwares are viruses,

worms, trojan horses, spyware, hoax. Malware is a code that is delivered over a network,

this malware behaves exactly what the attacker wants it can steal all the sensitive data, can

attack the data in the local network. Polymorphic malware, this one can alter the

appearance of the code without changing the algorithm. Ransomware is another dangerous

malware that attacks a business organization by attacking the files, data and information.

This can completely shut down the operations. The attachments in the emails files, peer to

peer sharing of files all of them contain the malware, once opened can destroy the system

or the network by attacking.

To prevent a malware there are many security solutions like firewall, IPS-intrusion

prevention system, anti-virus, deep packet inspection capabilities. To ensure there is no

malware all security solutions must be tested. To protect the organization from the malware

good strategies must be applied like enterprise-wide malware protection strategy here the

combinations of anti-virus, spywares are used for protection.

**Reference**

What is Malware & How to Stay Protected from Malware Attacks. (2001, March 1). Palo Alto Networks. Retrieved December 8, 2022,

<https://www.paloaltonetworks.com/cyberpedia/what-is-malware>

## Different types of Malwares

### Ransomware

Software known as ransomware employs encryption to prevent a target from accessing its data unless a ransom is paid. There is no certainty that the victim group will be completely or partially unable to operate until it pays. Payment will yield the required decryption key, or the given decryption key will work as intended.

### Fileless Malware

Malware that is “fileless” doesn’t initially install anything; instead, it modifies files that are inherent to the operating system, such PowerShell or WMI. A fileless assault is not detected by antivirus software because the operating system perceives the modified files as genuine. These attacks are stealthy and up to 10 times more effective than conventional malware attacks.

### Keyloggers

A sort of spyware that keeps track on user activities is a keylogger. Keyloggers may be used in acceptable ways by businesses to keep an eye on employee conduct and by families to monitor their children’s internet activities.However, keyloggers may be used to steal financial information, sensitive information, and password data when installed for nefarious purposes. Through phishing, social engineering, or malicious downloads, keyloggers can be installed on a machine.

### Rootkits

A root kit is software that allows malevolent users to take complete administrative control of a victim’s computer from a distance. Applications, kernels, hypervisors, and firmware may all be compromised to introduce rootkits. Phishing, malicious attachments, malicious downloads, and infected shared folders are some of the ways they propagate. Keyloggers and other types of malwares can be hidden using rootkits.

### Worms

Worms use operating system flaws as their entry points into networks. They could get in via flash drives, inadvertent programme flaws, or backdoors integrated into the software, among other methods. Worms can be used by hostile actors to execute DDoS assaults, steal confidential information, or carry out ransomware operations once they have been installed.

### Trojan

A Trojan cloak itself as desired software or code. The Trojan can take control of victims’ systems for harmful reasons after being downloaded by unwary users. Trojans can conceal themselves in software patches, games, apps, and even applications themselves, or they can be found in the attachments of phishing emails.

### Adware

Adware monitors a user’s browsing habits to decide which advertisements to show them. Adware is similar to spyware, except it doesn’t install any programmes or record keystrokes on a user’s computer. Adware poses a threat to user privacy because it gathers information about a user’s online activities, whether overtly or covertly, and uses that information to build a profile of that person that includes information about their friends, purchases they’ve made, travels they’ve taken, and other things. Without the user’s permission, this information may be sold or shared with advertising.

**Reference:**

Tathagat (2021) Essential Cyber Security Concepts, CYBERVIE. Available at: https://www.cybervie.com/blog/essential-cyber-security-concepts/ (Accessed: December 8, 2022).

# 

# Software security

Software security is a theory used to secure Software against malicious attacks and other hacker threats so that the Software can continue to operate as intended in the face of these potential threats. Integrity, authentication, and accessibility can only be offered with security.

Any software that ensures that a computer or network is secure from outside threats is sometimes referred to as security software. So that security risks may be anticipated, software security engineers should be able to view the incident from a security perspective.

In this aspect, the cyber-security community has been particularly outspoken in recent years about identifying various techniques for strengthening Software, given most susceptibilities consist of compatible flaws caused by subpar coding. Modern cyber-security experts have found that software security has advanced significantly and identified areas for future enhancements in safe application delivery.

In Software Security, each product management organization needs to ensure that their product security criteria are the first rate. However, in the present sophisticated IT world, with organizations utilizing increasingly more programming than any time in recent memory and cyberattacks spinning out of control, ensuring programming is secure can get precarious.

PC security programming is generally accessible today and helps organizations, and end-clients, in ensuring that they are utilizing the right programming tools with the right devices to secure information. That’s where software security comes into the picture.

Generally, software security is the idea of executing systems in the development of safety to assist them with staying useful and resistant to assaults. This implies that a piece of programming goes through a required amount of programming security testing prior to going to market in order to really look at its capacity to endure obnoxious assaults.

The basic concept behind software security is building programming components that are secure every step of the way without adding extra security components to add extra layers of safety (albeit, as a rule, this occurs). The subsequent stage is training clients to involve the product in the possible ethical way, in short, to try not to be inclined or open to assaults. Software security is the basic idea that a malware assault can cause outrageous harm to any piece of programming while at the same time compromising respectability, validation, and accessibility simultaneously.

# Conclusion

In summary, Hence, the overall aim of using software security is to ensure the safety of the Software. However, collective cyber-security has introduced various feasible options to enhance the quality of the code and ensure safety in the absence of any manual involvement. Practically Software security-related professionals must be optimistic in their attempts to prevent software threats.

# Overview Cyber Security

    Cybersecurity is the defense against cyber threats for systems linked to the internet, including their hardware, software, and data. Individuals and businesses both utilize this technique to prevent illegal access to data centers and other digital systems. A solid cybersecurity plan can offer a decent security posture against hostile assaults intended to gain access to, change, delete, destroy, or extort sensitive data and systems belonging to a business or user. Security measures are essential in preventing attacks that try to take down or impair a system or device’s functionality.

       The importance of cybersecurity is only going to expand as there are more people, devices, and programs in the contemporary company, along with an influx of more data, most of it sensitive or secret. The issue is made much worse by the increase in the quantity and level of sophistication of cyber attackers and attack methodologies.

    Sensitive information, such as intellectual property, financial data, personal information, or other sorts of data for which illegal access or disclosure might have unfavorable effects, can make up a sizeable amount of that data. In the course of conducting business, organizations transfer sensitive data over networks and to other devices; cyber security refers to the field devoted to safeguarding such data as well as the technology used to handle or store it. Companies and organizations, especially those responsible for protecting data related to national security, health, or financial records, must take action to defend their sensitive business and people information as the frequency and complexity of cyber assaults increase.

## Cybersecurity Threats:

It can be difficult to stay on top of emerging technology, security trends, and threat information. It is required to safeguard data and other assets from many types of cyber threats. Some examples of cyber threats are:

## Malware:

Malicious software, or malware as it is more widely called, is the most frequent type of cyberattack. Spyware, ransomware, backdoors, trojans, viruses, and worms are all examples of malware.

## Spyware:

Computer software enables hackers to gather details about your computer usage by secretly sending data from your hard drive.

The goal of ransomware is to encrypt files on a device, making them (and the systems that depend on them) useless. Malicious actors frequently demand a monetary ransom in return for decryption.

A backdoor bypasses common authentication steps to gain access to a system. This enables malicious actors to remotely execute system instructions and update malware while also providing the attacker with remote access to resources within an application, such as databases and file servers.

A harmful piece of computer code created to transfer from one device to another is known as a computer virus. Typically, these self-copying malware aim to harm a machine or steal data.

Worms are a type of malware that transmits copies of itself from computer to computer without a person’s involvement and does not require an attachment to a software application to do harm.

When a user clicks on a fraudulent link or email, malware is often injected into the system. Malware can harm your system after installation, limit access to important network components, and export private data to unidentified locations.

## Phishing and Spear Phishing :

The goal of phishing, a sort of social engineering, is to get people to divulge private information, including usernames, passwords, bank account information, Social Security numbers, and credit card numbers.

Hackers frequently distribute phishing emails that appear to be sent from reputable companies like PayPal, eBay, financial institutions, or friends and coworkers. The fake emails are designed to entice recipients to click on links, which would take them to phony websites that solicit their personal information or download malware onto their computers.

Opening attachments from phishing emails can potentially lead to the installation of malware or the remote control of your devices by hackers.

An advanced type of phishing assault known as spear phishing targets exclusively privileged people like system administrators and C-suite executives. The attackers may exploit information from the target’s social media profiles to make themselves look even more trustworthy.

Smishing, vishing, clone phishing, domain spoofing, URL phishing, watering hole phishing, and evil twin phishing are examples of other phishing techniques. Costly in all cases.

**Man-in-the-Middle (MITM) Attacks :**

When malevolent actors interject themselves into a two-party dialogue, assaults like these take place. The assailant intercepts the incoming communication, filters and takes sensitive data, and then sends the original user an alternative reply.

Malicious actors occasionally create false wi-fi networks or place malware on consumers’ networks or machines. The goal of MITM attacks, also known as eavesdropping assaults, is to access consumer or corporate data

**Distributed Denial of Service (DDoS) :**

A DDoS attack seeks to bring down a company’s website by sending too many requests to the server. It’s comparable to dialing a company’s phone number repeatedly in order to prevent genuine callers from ever getting through and only receiving a busy signal.

Hundreds of thousands of IP addresses that have likely also been hijacked and duped into repeatedly requesting a website belong to a firm are the source of requests in this assault.

Your servers may be severely slowed down or perhaps taken down by a DDoS assault. Customers are unable to visit your website or place orders during these outages.

**Structured Query Language (SQL) injection :**

When online criminals upload dangerous SQL scripts in an effort to access databases, SQL injection assaults happen. Once successful, the malicious actor has access to the data kept in the SQL database and may read, modify, or remove it.

**Domain Name System (DNS) attack:**

A DNS assault is a cyberattack in which cybercriminals take advantage of DNS flaws. The attackers take use of DNS flaws to direct site visitors to malicious websites and steal data from infected PCs (DNS tunneling).

Cyber Security focuses on preventing illegal access to computer systems, networks, and data. Cyber Security can be categorized into Application security, Infrastructure security, cloud security, Network security, and IoT security.

Practically, there will always be some vulnerability in a system because no system can be perfect. Hence, security is a way to minimize that vulnerability and avoid risks and possible threats.

1. Security concepts

     Security Triad consists of Confidentiality, Integrity and Availability whereas AAA is a set of features of Access Control which includes Identification, Authentication, Authorization and Accountability.

Confidentiality refers to secrecy. It is not only applicable in information security but also implies a different level of security such as physical, network, operational etc. Keeping any data confidential is important if that data consists of personal or sensitive information. The best-known example of keeping data confidential is the encryption of data in both storage and transmission. If somehow the security is breached, the encrypted data will still be safe from harmful actions and therefore maintains the confidentiality of data.(*Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability.*, 2016)

Integrity refers to the consistency of data and restricting editing access to the data from unauthorized access. In addition to this, integrity also checks if the confidentiality of data has been compromised at some point. Practically, this is done through the Authorization and Accountability of AAA technique. Some data to an enterprise may have a huge impact if they are changed. In such cases, Integrity is very important. The use of anti-malware software or hashing helps to achieve integrity.

Availability refers to the easy accessibility of information to the user at his/her desired time. Though information is kept safe through the process of encryption, hashing, etc. It is equally important that required information should be accessible by genuine users.

# 

# Concept on cyber security

    Confidentiality, Integrity, and Availability are the three key concepts in Cyber Security. We call this the CIA triad.

More midsize businesses are being impacted as cyber threats continue to become more sophisticated. To ensure protection, organisations must be vigilant and proactive. However, given our limited understanding of the evolving threats and the expanding digital threat landscape, this is challenging to accomplish. As the Internet has evolved, so have the connections between gadgets of various types. Anything with the title “smart” may be hacked. So then, it becomes a difficult balance between adopting technologies to make labour more efficient and guaranteeing cyber security. The time when a complicated password sufficed to secure digital data is long gone.

The procedures and strategies used to safeguard computer networks, applications, sensitive data, and systems from cyber threats are known as cyber security. The following are some of the most common ways that cybercriminals have gained access:

* System manipulation
* Unauthorized access
* Exploitation of resources
* Ransomware

     As a cyber security managed service provider who is based in the U.S. fully understands, cyber security is a field that is constantly changing. National Institute of Standards and Technology (NIST) framework guides the five critical aspects of the field:

* Determine threats
* Find intrusions
* Protect data
* Respond to attacks
* Recover databases and systems and rebuild cyber security defences

**References:**

What are the basic concepts of cyber security? (no date) SSi. Available at: <https://insider.ssi-net.com/insights/what-are-the-basic-concepts-of-cyber-security> (accessed :December 8,2022).

# CIA Traid and its principle

The three main concepts of information security are confidentiality, integrity, and availability (CIA). One of these principles may be more significant than the others depending on the circumstances, environment, application, context, or use case. For instance, a financial agency would certainly encrypt any classified document being shared electronically in order to prevent unauthorized individuals from viewing its contents because the confidentiality of information is of the utmost importance to that organization. On the other hand, businesses like online marketplaces might prioritize tactics for assuring high availability over worries over encrypted data because a prolonged network outage would be extremely damaging to them.

The CIA Triad is a foundational cybersecurity paradigm that serves as a basis for the creation of security regulations intended to safeguard data. CIA Triad’s three initials stand for availability, confidentiality, and integrity.

The CIA Triad is a paradigm for data security that incorporates three different ways of dealing with data. First, the confidentiality principle dictates that only authorized users should have access to the data in a system.

The second tenet of integrity emphasizes the importance of the reliability and accuracy of data. Data must be accessible when and where users need it, according to the ultimate requirement of availability. These three ideas come together to establish a framework for safeguarding digital information.

The CIA Triad’s guiding principles provide the foundation for efficient digital asset security. Data protection requires adherence to all three principles, and problems with one of them may impact the other two. Even though in cybersecurity confidentiality and integrity are sometimes perceived as antagonistic (i.e., encryption can undermine integrity), they should be weighed against risks when creating a security plan.When creating a security program to guard against contemporary data loss due to cyber attacks, human error, natural catastrophes, and other potential risks, the CIA Triad obliges system designers and security specialists to take into account all three principles. It serves as a jumping off point for developing ideas about how information should be safeguarded and for figuring out the best approach to put those ideas into practice in a particular setting.

The three main principles of CIA Triad are confidentiality, availability and integrity.

**Best ways to implement CIA Triad are:**

- Finding the best method to enforce authentication and authorization procedures is just one of the many uses for the CIA triad model.

- Helps in recognizing the importance of protecting customer, employee, and corporate data

- Also can be used in assuring the security of whatever extra devices a business adds without raising risks.

## Confidentiality

Information must be protected so that only those with permission to view it may do so. This is referred to as confidentiality. To avoid fraudulent activity, access control for data users is critical. It follows that only those who are permitted can access particular resources. Access is actively restricted to authorized individuals, maintaining confidentiality.

The goal of confidentiality is to restrict unauthorized access to private information. The access could be willful, such as when a hacker breaks into the network and reads the data, or it could be accidental owing to the negligence or incompetence of those in charge of handling the data.

Access control and cryptography are the two primary methods for ensuring confidentiality.

- Cryptography: Encryption aids organizations in securing information against accidental disclosure as well as internal and external hacking attempts. It is challenging to break into a robust cryptographic system. Strength can also be quantified using the concept of labor factor, which is an estimation of the time and effort required to destroy a system. A system is deemed weak if it permits weak keys, has design flaws, or is simple to decrypt. A lot of the systems on the market right now are more than sufficient for personal and professional use, but they are insufficient for sensitive military or governmental applications.

- Access Control: One technique to guarantee confidentiality is through encryption, and another is through access restriction. There are numerous access control strategies that support confidentiality

**Integrity** :Data veracity and dependability are related to integrity. Data must be accurate, and any alterations must be visible. In general, maintaining data integrity entails keeping it safe at all times, including whether it is being used, being transferred (such as when sending an email or downloading a file), and being stored in a storage device, data center, or cloud. Integrity is susceptible to several threats, just as confidentiality. It may occur directly as a result of human error, system intrusion, configuration file manipulation, or system log modification (all of which are ways to escape discovery). Countermeasures including encryption, digital signatures, hashing, and digital certificates can aid in maintaining data integrity. Along with this, intrusion detection systems, reliable authentication protocols, version control, auditing, and access controls can all help to guarantee integrity. File integrity monitoring is a significant best practice for maintaining data accuracy (FIM). By auditing all attempts to access or alter files and folders containing sensitive information and determining if such actions are authorized, FIM assists companies in identifying unauthorized changes to vital data on their systems.

It is obvious that integrity is strongly related to the idea of non-repudiation, which indicates that one will be unable to dispute the veracity of specific activities. The integrity of these kinds of online transactions will be preserved, for instance, if an email with a digital signature was sent or received.

Three objectives of integrity contribute to data security:

- Preventing unauthorized users from changing information

- Preventing authorized users from unintentionally or deliberately altering information

- Maintaining both internal and external coherence

**Availability** :Data is only helpful if it is accessible, hence availability is a key factor. Data availability guarantees that it may be accessible when necessary and that it will keep working as needed. Availability ensures that a system’s authorized users may access its data and network at all times. If authorized users cannot access systems, programs, and data anytime they need it, they will become worthless. Networks, systems, applications, and data must be timely accessible to authorized users whenever resources are needed, which meant by availability.

If there is a hardware or software malfunction, a natural disaster, a power outage, or a human error, availability may be in endanger. DDoS attacks are one of the more frequent causes of availability violations.

Network, server, application, and service redundancy can ensure availability. A good defense to prevent availability violations is hardware fault tolerance in servers and storage. Systems updates, routine software patches, thorough disaster recovery plans, backups, and other measures can all be taken to assure availability. A thorough disaster recovery strategy must be created and tested as well to preserve availability.

## Importance of the CIA Triad:

The many security methods, tools, and services are somewhat made sense of by the CIA Triad. It is helpful to clearly depict what is necessary to address the security problems rather than taking a wild guess.

When a trio is used, the three ideas are in conflict with one another. For instance, demanding complex authentication increases confidentiality but also increases the risk that some individuals with access rights won’t be able to access the data, decreasing availability.

The CIA Triad can be used to more effectively decide which of the three principles will be most beneficial for a certain type of data as well as the business as a whole when developing information security policies.

**Integrity:**

   ATM system satisfies all the CIA triad concepts.

* **Confidentiality**: Confidentiality ensures that data should be accessible to authorized users only.By having the two authentications (a physical card and a PIN code) before granting access to data, ATMs ensure confidentiality.
* **Integrity**: Integrity means making sure your data is reliable and unaltered.Data integrity is enforced by the ATM and bank software, which makes sure that any transfers or withdrawals performed through the device are represented in the accounting for the user’s bank account.
* **Availability**: Availability guarantees that information will be accessible to authorized users when they need it.Due to its location in a public area and accessibility even when the bank branch is closed, the machine offers availability.

The fundamental concept of cyber security is to defend the computers, servers, mobile device and all interconnected devices and networks from security attacks. While dealing with network security, the focus is given to secure the entire network of the organization from intruders and malwares. While dealing with application level of security, the focus is in ensuring whether the soft wares and the devices are free from threats and they are secured enough to detect and protect the attacks. While dealing with this kind of security, the security practices have to be done from the designing stage itself.

While dealing with cyber security, the main three pillars of cyber security are people, technology and process. While dealing with people, they should be given training and awareness on how to identify the threats and take security measures to counteract the same (Github, 2022).

With the help of right technology, like antivirus, firewall, software updates etc., the security threats can be overcome. By choosing the right process, policies and procedures and security audits, the extend of cyber threats can be controlled.

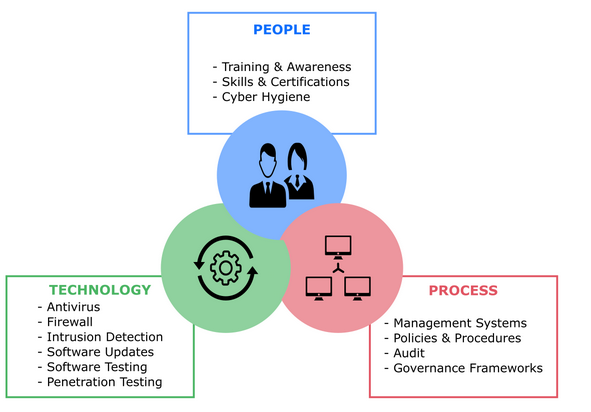


Figure 1: Cyber security concepts –three main pillars (Github, 2022).

Another important concept of security lays in preserving the data confidentially and in maintaining the data integrity. This is termed as information security where the user data, financial data, organization data etc. are well protected both in storage as well as in transit.

There is an another kind of security called the operational security where the focus will be given to ensure that the data processing, data transactions, assets dealing etc. are secured and devoid of threats. In this stage the focus will be given on user permissions while accessing the network and how the data communication is securely enabled.

While dealing with security, though several measures are taken, there is always a chance for cyber-attacks. Hence while designing the security system; it is essential that there should be a good disaster recovery plan that supports business continuity. A good security system will be able to recoup from the threats within a short span of time and proceed with the business by maintaining minimal loss and impact.

  The protection of the network which is connected to the internet such as software, hardware, and data from security issues, and cyber threats. Three fundamental concepts of cyber security are “The CIA Triad.” Confidentiality, Integrity, and Availability are basic concepts to ensure information security in the organization.

**Confidentiality** – Limit access to confidential information and it helps to restrict the access of sensitive information from cyber attackers and hackers. People are given or denied access to information in an organization based on its category by approving the authorized individuals in a department. Employees in organizations are provided with proper training to access secured information with strong passwords.

**Integrity** – Data is ensured with its accuracy and consistency. It focuses on data changes, altering, deletion, or illegal changes during the transition, and its focus is to ensure its safety. A checksum or even a cryptographic checksum is used by various organizations to confirm data integrity.

**Availability** - It is important to maintain and upgrade availability in terms of all required elements, including hardware, software, networks, devices, and security apparatus.

# CIA Traid

## Confidentiality

The actions taken by an organisation to ensure the confidentiality of its members’ information are referred to as privacy. Access to information has to be dealt properly in order to avoid unwanted data sharing of any kind, whether it be intentional or unintentional. To maintain an atmosphere of secrecy, it is necessary to take precautions to ensure that those who do not possess the necessary authorization do not get access to resources that are vital to your organisation. To reiterate, a convincing framework guarantees that the individuals who need access are in possession of the necessary consents.

Calculation sheets, ledgers, and other types of financial data should be approached by persons who engage with monetary matters, such as those who manage an organization’s cash. However, the vast majority of other employees and maybe even some bosses might not be allowed in. This is a possibility. It is necessary to establish stringent cutoff points on who may see what in order to make certain that these criteria are followed. According to the guiding concept, only the sender and receiver will have access to the data sent between them. If a communication may be accessed by someone who is not authorized, confidentiality is compromised.

## Integrity

Respectability, also known as dependability, requires you to ensure that the information you provide is accurate and unaltered. It is essential to maintain the dependability of the information you possess by acknowledging that it is genuine, accurate, and trustworthy. For instance, if your company posts information on its website regarding senior management, then that information has to be accurate. In the event that anything is wrong, visitors to your website looking for information can get the impression that your organization is dishonest. Someone who has a strong desire to ruin the reputation of your organization can try to hack into your website and change the biographies, images, or titles of the people who founded the organization in order to bring down either their reputation or the reputation of the organization as a whole.

Integrity provides the guarantee that the data obtained is precise and correct. The integrity of the communication is considered to be lost if it is altered after the sender sends it but before it reaches the intended recipient.

**Availability:**

No matter how well the information is guarded and how perfect it may be, it will in most cases be useless unless it can be accessed by individuals working inside the business as well as the customers it serves. This necessitates that structures, organisations, and applications all function appropriately and according to their own timetables. People who access certain data should also have the option to consume it whenever it is necessary, and it should not take an unnecessarily long time to access the data.

Accessibility will be impacted in the event that there is a power outage, and there is no disaster recovery strategy in place to assist customers in regaining access to fundamental frameworks, for example. In the case of a catastrophic catastrophe, such as a flood or a particularly harsh winter, customers may be prevented from reaching to their places of employment, which disrupts the accessibility of their workstations and any other devices that provide business-critical data or applications. Accessibility may also be put at risk by deliberate acts of sabotage, such as distributed denial of service (DoS) attacks or ransomware.

## 2. Security requirements

### 

### Identification and authentication:

Authentication is the process of verifying a genuine user of an organization. Even if someone bypasses entering the system who is not a part of an organization, ‘Authentication’ is another level of security that cross-checks the user’s identification through the information the user gathered during registering process. Password, security questions, biometrics, verified location, token cards, QR code, and Bar codes are a few examples of Authentication.

Basically, it works on the principle of where you are, what you know, what you are, what you have, etc. This level of security prevents data loss/leaks in an organization and hence lowers the impact and probability of risk.

### Authorization:

‘Authorization’ is the process of defining the power of accessibility over the resources of an organization. Threats and vulnerability don’t always come from outside the organization. Assigning the level of authorization in an organization builds a safe wall between the departments from the ground level.

For example, if a user from one department gets access to other departments, an organization will put itself at risk of data loss or data leak. Authorization plays a huge role in keeping data private and secure.

### Auditing:

Auditing must be done in every organization as it has a checklist to assess cyber policies and ensure that control mechanisms to implement them are in place. In most cases, that third-party must be certified in order to conduct an audit. An organization can utilize an internal audit team, but it should operate independently while a third-party auditing business may charge a high fee to visit on-site, conduct interviews, and review your procedures. The most significance part of auditing is to analyze the system’s records and activities to verify the sufficiency of system controls, check compliance with defined security policy and procedures, discover breaches in security services, and propose improvements for countermeasures.

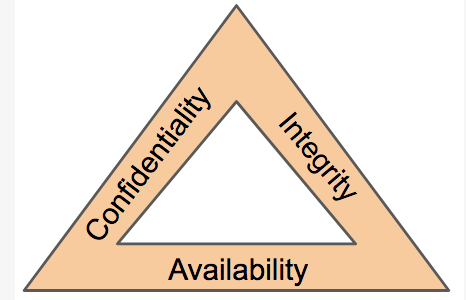
### Confidentiality:

It applies not just to cybersecurity but also to multiple levels of security such as operational, physical, network, and so on. It is critical to keep any data secret if it contains personal or sensitive information. The encryption of data in both storage and transmission is the most well-known example of data confidentiality. If the security is violated, the encrypted data is still secure from damaging operations

### Data Integrity:

Data stored on computers, as well as data exchanged between systems, such as email, must be safeguarded. Maintaining integrity requires not just controlling access at the system level, but also ensuring that system users may only change information that they are officially permitted to change.

The main security requirements that have to be taken into consideration while dealing with cyber security are Confidentiality, Integrity and Availability.



A triangle of CIA traid.

The major requirement of any security system is in maintaining the confidentiality of the data, resource and all business aspects. Utmost care has to be taken that the resources to be protected from unauthorized control in a view to avoid misuses and to ensure data protection. In any business system, the data is more prone to attack and in general the data will be collective information from various business domains. Under this situation, there will be sensitive as well as private data and hence the security system should take care in ensuring the data confidentiality and in assuring data protection.

The integrity refers to protecting the information from the unauthorized alteration. All the business operations will be done on the basis of data and hence it is essential that always the data should be accurate and complete. The integrity focuses on ensuring these factors and it can be achieved when the data is well protected from external as well as internal attacks. In general data communication happens between the two parties and there is a high probability of attack, if the network security strength is poor, the data may get lost or misused. This affects the integrity and hence the complete data communication, storage etc. has to be securely protected.

Availability is an essential requirement while dealing with security. This is because always the secured system should ensure that the data is available to the authorized users. Also it is essential that the data has to be well protected to avoid uninterrupted access to the system. It is to be noted that while dealing with financial processing or while dealing with high commercial volume of business, if the data is not made available to the intended users, it will reflect in the business financials and in turn will create bad reputation. The cyber attacker’s focuses on creating harm to the business and they will be focused to make the data unavailable to the authenticated users. Hence availability factor has to be highly considered as the important aspect of security requirements.

Every organization focuses on protecting its information assets and other network assets from attackers. Some of the security requirements are detailed below,

·       Be aware of cyber security issues and standards

·       Understand and learn about more and different cyber-attacks.

·       Keep software updated and focus on device security mechanisms up to date.

·       Be aware of cyber prevention practices.

·       Implement anti-virus software and focus on firewall protections

·       Improve password strengths and focus on password standards

·       Concentrate on data backup.

·        Avoid security risks by limit to connect with public Wi-Fi

## 3. Security Strategy

A cybersecurity strategy is a plan of action designed to improve a company’s computer network security and resilience. The security strategy document specifies and prioritizes information assurance and security actions that the company must implement to improve information and related technology security. To successfully secure a company with a strategic security strategy the critical mission enabler must be recognized as a vital component of the organization. Innovative and efficient information security initiatives need collaboration from organizational leaders and workers, as well as clear direction and commitment from top management and administration(DL, n.d.).

The cyber security strategy is actually a plan that describes the implementation of best practices that has to be followed to ensure that the business computer system is free from threats both internal as well as external. The main purpose of the security strategy is to establish a baseline for the security program that the companies can follow easily and quickly to meet emerging threats and risks. When the security strategy is rightly implemented, it increases the organizations’  ability to minimize and limit the damages that are caused by cybercriminals.

There are several security strategies in practice like zero trust security where there will be several layers of tools to create the defense in depth thus creating a sound security strategy. The security strategy has three main components they are Automation, Interoperability, and Authentication.

Automation in security strategy ensures that the strategic plans have been easily implemented and it should help to optimize the decision-making process. The interoperability clearly defines that the security plans have to go well with the business operations and it should support collaborative actions. The interoperability should be providing improved awareness and it should accelerate the learning process. It should be on the basis of technical as well as numerous security policies.

Finally, authentication is important in any strategic approach where the system should focus on improving the identification and verification of technologies that support security, affordability, feasibility, scalability, and interoperability.

The security strategies include creating an assurance-based framework to enable the actions taken by the companies to enforce the IT security guidelines and to adhere to compliance. Several endorsing actions are involved in the strategic approach to meet the security standards

It is necessary to implement best security practices and standards to protect the network from attackers. Every organization focus on developing security strategies by considering their data and possible attacks.

# 

# Cryptography and the principles

The ancient art of cryptography is the science of writing secret codes. Therefore, it is not surprising that significant developments in cryptography appeared not long after popular computer communications technology. When interacting via any untrusted medium, such as any network, notably the Internet, in the fields of data and telecommunications, cryptography is required. There are several particular security criteria that must be met in the context of any application-to-application connection, including.

## Authentication:

The method of establishing one’s identity. Today, name-based or address-based host-to-host authentication is the two most common methods, both of which are infamously insecure.

## Confidentiality:

The essential security function that cryptography offers is confidentiality. It is a security service that protects the data from being accessed by unauthorized parties. It is sometimes referred to as secrecy or privacy. There are several ways to maintain confidentiality, from physical security to using mathematical techniques for data encryption.

## Integrity:

Assuring the recipient that the message they have received hasn’t been changed in any manner from what it originally said.

## Non-repudiation:

An organization cannot deny ownership of a prior promise or activity, thanks to its security service. It is a guarantee that the person who originally created the data cannot contest its production or transfer to a receiver or third party. When there is a risk that there will be a disagreement over the sharing of data, non-repudiation is a quality that is most desired. For instance, if non-repudiation service was enabled in this transaction, a buyer cannot retract a purchase order once it has been made electronically.

Therefore, cryptography may be used for user authentication in addition to protecting data from theft or modification. Hash functions, public-key cryptography, and secret-key cryptography each of which is explained below are the three main types of cryptographic systems that are commonly employed to achieve these objectives. The original unencrypted data is always referred to as plaintext. It is converted to cipher text and then (typically) decrypted to useful plaintext. The essential security function that cryptography offers is confidentiality. It is a security service that protects the data from being accessed by unauthorized parties. It is sometimes referred to as secrecy or privacy. There are several ways to maintain confidentiality, from physical security to using mathematical techniques for data encryption.

# Types of  Cryptographic Algorithms:

There are several categories in which to put cryptographic algorithms. They will be classed for the purposes of this study depending on the number of keys used for encryption and decryption, and further classified by their application and use.

## Secret Key Cryptography (SKC):

Utilizes a single key for both encryption and decryption.

## Public Key Cryptography (PKC):

One key is used for encryption and another for decryption.

## Hash Functions:

Uses a mathematical process to permanently “encrypt” data using hash functions.

**Secret key cryptography**

A single key is utilized in secret key cryptography for both encryption and decryption. The sender encrypts the plaintext using the key (or a set of rules) before sending the ciphertext to the recipient. The same key (or ruleset) is used by the recipient to decode the message and get the plaintext. Secret key cryptography is also known as symmetric encryption since only one key is required for both purposes.

The key, which is the secret in this type of encryption, must be known by both the sender and the recipient. Of course, this strategy’s main challenge is how to distribute the key. Algorithms for secret key cryptography that are currently in use include:

**Data Encryption Standard (DES):**

The most popular SKC scheme in use today. IBM’s 1970s-era design was taken by the NBS (formerly the National Bureau of Standards) American National Standards Institute (NIST)] for non-classified commercial and government applications in 1977. A block cipher is DES. using a 56-bit key that works with 64-bit blocks. The regulations for DES are intricate, and changes were particularly intended Between sluggish software implementations and quick hardware implementations of software, however, this latter point is less important today because computer processors operate at multiple orders quicker now than it was 20 years ago. Additionally, IBM suggested a 112-bit key for DES, which the government at the time rejected. In the 1990s, using 112-bit keys was proposed. But conversion was never taken seriously.

**Advanced Encryption Standard(AES):**

NIST launched a very visible, 4-1/2a multi-year project to create a new, reliable cryptosystem for use by the American government. the outcome, Advanced Encryption Standard (AES) was adopted as the official DES replacement as of December 2001. AES uses the block-based Rijndael SKC algorithm. cipher created by Joan and Jean-Pierre of Belgium Vincent Rijmen and Daemen. The program can utilize changeable block and key lengths; the most recent specification permitted any combination of blocks of keys with lengths of 128, 192, or 256 bits128, 192, or 256 bits in length. NIST first formally chose Rijndael in October 2000. The AES standard was adopted in December.2001. A 128-bit block is described in FIPS PUB 197. Using a key that is 128, 192, or 256 bits long.

## CAST-128/256:

As stated in the Request, CAST-128 is a DES-like protocol for Comments (RFC) 2144. The cryptographic substitution-permutation algorithm uses a 64-bit operating system and a 128-bit key block. RFC 2612 is an expansion to CAST-256.CAST-128 has a block size of 128 bits and different lengths (128, 160, 192, 224, or 256-bit) keys. CAST takes its name after its creators, Carlisle Adams, and Stafford Tavares, and are offered internationally. CAST-256 was a Round 1 candidate. The AES process’s algorithms.

## International Data Encryption Algorithm (IDEA):

A 64-bit SKC block cipher employing a 128-bit key was created by Xuejia Lai and James Massey in 1992 and patented by Ascom. available abroad as well.

**Rivest Ciphers (aka Ron’s Code):**

An assortment of SKC algorithms with Ron Rivest’s name.

* RC1  Conceptualized but never carried out.
* RC2 is a 64-bit block cipher with variable-sized keys that was created to take the role of DES. Even though numerous businesses have licensed RC2 for use in their products, the source code has not been made available. found in RFC 2268.
* RC3 was discovered to be brittle during development.
* RC4 is a stream cipher with variable-sized keys that are frequently used in products for commercial cryptography. Rivest and Jacob Schuldt created an RC4 upgrade named Spritz.
* RC5 is a block cipher that supports several key sizes, encryption passes, and block sizes (32, 64, or 128) over DRFC 2040RC6.

## Blowfish:

It is a symmetric 64-bit block cipher created by Bruce Schneier that is substantially quicker than DES on a Pentium/PowerPC-class computer. It is intended for 32-bit processors with big data caches. The size of keys can range from 32 to 448 bits. Blowfish is used in a wide range of goods and is an openly available alternative to DES or IDEA.

## Twofish:

A 128-bit block cipher with keys of 128 bits, 192 bits, or 256 bits. High security and flexibility were designed into the system, which works well with big microprocessors, 8-bit smart card microprocessors, and specialized hardware. was one of the Round 2 algorithms in the AES process and was created by a team under the direction of Bruce Schneier.

## Public-key cryptography:

According to some, the most important new advancement in cryptography in the previous 300–400 years is public-key cryptography. In 1976, graduate student Whitfield Diffie and Stanford University professor Martin Hellman published the first public description of modern PKC. In their article, they presented a two-key crypto scheme that allowed two people to communicate securely across an insecure channel without disclosing a secret key.

PKC relies on the presence of so-called one-way functions, or mathematical functions that are simple to compute but difficult to compute in reverse. I’ll offer you two straightforward examples:

* Factorization vs multiplication
* Logarithms vs exponentiation

For key exchange or digital signatures, public-key cryptography methods in use today include:

## RSA:

Named after the three MIT mathematicians who created it, Ronald Rivest, Adi Shamir, and Leonard Adleman, this was the original and is still the most used PKC implementation. RSA may be used for key exchange, digital signatures, or the encryption of tiny blocks of data nowadays and is included in hundreds of software applications. A variable-size key and an adjustable encryption block are used by RSA. The key pair is formed from a very big integer, n, which is the product of two prime numbers selected in accordance with specific principles. These prime numbers may each have 100 digits or more, resulting in an n that is nearly twice as large as the prime factors. The RSA technique is so safe because an attacker cannot deduce the prime factors of n (and, consequently, the private key) from the public key information alone. The public key information consists of n and a derivative of one of n’s factors. (Some explanations of PKC make the incorrect claim that the in-factorability of huge prime integers is what makes RSA secure. Large prime numbers only have two elements, much like tiny prime numbers. Systems now can determine the prime factors of numbers with more than 200 digits, demonstrating how quickly computers are becoming more capable of attacking large-number attack techniques like RSA.

However, no factorization technique can solve the issue in an acceptable length of time if a huge number is produced from two nearly equal-sized prime factors; a 2005 test to factor a 200-digit number required 1.5 years and more than 50 years of computing time. Despite this, one alleged security feature of RSA is that users may simply raise the key size to consistently outpace computer processing. As a side note, RSA’s patent expired in September 2000, yet this doesn’t seem to have had any impact on how ubiquitous it is now.

**DIFFIE-HELLMAN:** Developed their own algorithm following the release of the RSA method. D-H is solely used for secret-key key exchange; it is not utilized for digital signatures or authentication.

**Digital Signature Algorithm(DSA):** The algorithm provided by the Digital Signature Standard (DSS) of NIST allows for the authentication of messages using digital signatures.

**ElGamal:** A PKC mechanism for exchanging keys that is comparable to Diffie-Hellman and was created by Taher Elgamal.

**Elliptic Curve Cryptography (ECC):** ECC is a PKC technique that uses elliptic curves as its foundation. ECC can provide security levels with tiny keys that are on par with RSA and other PKC techniques. It was created for computing and/or memory-constrained devices, including smartcards and PDAs. Other resources include the Certicom Web pages “The Importance of ECC” and “Online Elliptic Curve Cryptography Tutorial.” For more information on the use of ECC for digital signatures, see The Elliptic Curve Digital Signature Algorithm (ECDSA) and RFC 6090, which also provide an overview of the basic ECC algorithms.

## Public-Key Cryptography Standards (PKCS):

A collection of public-key cryptography rules and specifications developed by RSA Data Security Inc.

  PKCS #1: RSA Cryptography Standard (Also RFC 3447)

  PKCS #2: Incorporated into PKCS #1

Cramer-Shoup: a public-key cryptosystem proposed in 1998 by IBM’s R. Cramer and V. Shoup.

Key Exchange Algorithm (KEA): An adaptation of Diffie-Hellman; suggested as the Capstone key exchange technique.

LUC: The Lucas sequence-based public-key cryptosystem created by P.J. Smith. use integer factoring for encryption and signatures.

**Access control:**

Role management and rule management set the foundation for access control. While rule management regulates how far one may access the data, role management establishes who should have access to the data. The information that appears depends on who is accessing it.

Availability:

According to the availability principle, the authorised party will always have access to the resources. If information cannot be accessible, it will be of no use. Systems should have enough information readily available to fulfil user requests.

**Reference:**

Cryptography and network security principles (2022) GeeksforGeeks. Available at: <https://www.geeksforgeeks.org/cryptography-and-network-security-principles/> (Accessed: December 8, 2022).

Hash functions:

Most information security applications employ hash functions because they are so helpful. A mathematical operation known as a hash function compresses one input numerical value into another. Although the hash function’s output is always a defined length, its input can be of any length. Message digests or just hash values are terms used to describe values that a hash function returns.

Features of Hash Functions:

⦁ Fixed Length Output

⦁ Efficiency of Operation

Properties of Hash Functions:

Pre-Image Resistance

Second Pre-Image Resistance

Collision Resistance

Reference:

Cryptography hash functions (no date) Tutorials Point. Available at: <https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm> (Accessed: December 9, 2022).

**B)** **HASH FUNCTIONS :**

In a sense, techniques that employ hash functions—also known as message digests and one-way encryption—require no key. Instead, a fixed-length hash value based on the plaintext is created, making it impossible to determine the plaintext’s length or contents. To confirm that a file has not been changed by a virus or intruder, hash algorithms are often employed to give a digital fingerprint of the contents of a file. Many operating systems frequently use hash methods to secure passwords. Therefore, hash functions give an indication of a file’s integrity.

There are several hash algorithms in use right now, including:

Message Digest (MD) algorithms: A set of byte-oriented algorithms that transform an arbitrary-length message into a 128-bit hash value.

 MD2 (RFC 1319): Designed for memory-constrained devices, such as smart cards. (According to RFC 6149, MD2 has been demoted to historical status.)

  MD4 (RFC 1320): Similar to MD2 but created by Rivest, particularly for quick processing in software. (According to RFC 6150, MD4 has been demoted to historical status.)

   MD5 (RFC 1321): This method, which was also created by Rivest in response to suspected MD4 flaws, is similar to MD4 but slower since more changes are done to the original data. Despite various flaws in the method shown by German cryptographer Hans Dobbertin in 1996 (“Cryptanalysis of MD5 Compress”), MD5 has been used in a wide range of products.

Most information security applications employ hash functions because they are so helpful. A mathematical operation known as a hash function compresses one input numerical value into another. Although the hash function’s output is always a defined length, its input can be of any length. Message digests or just hash values are terms used to describe values that a hash function returns.

Features of Hash Functions:

⦁ Fixed Length Output

⦁ Efficiency of Operation

Properties of Hash Functions:

Pre-Image Resistance

Second Pre-Image Resistance

Collision Resistance

Reference:

Cryptography hash functions (no date) Tutorials Point. Available at: <https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm> (Accessed: December 8 2022).

**Secure Hash Algorithm (SHA):** NIST’s Secure Hash Standard algorithm (SHS).

SHA-1 generates a hash value of 160 bits and was first presented in FIPS PUB 180-1 and RFC 3174.

SHA-2, which was first introduced in FIPS PUB 180-2 and subsequently superseded by FIPS PUB 180-3 and FIPS PUB 180-4, consists of five algorithms in the SHS: SHA-1 plus SHA-224, SHA-256, SHA384, and SHA-512, which can generate hash values that are 224, 256, 384, or 512 bits in length, respectively. For messages that are fewer than 264 bits in length and use a 512-bit block size, SHA-2 advises using SHA-1, SHA-224, and SHA-256; for messages that are less than 2128 bits in length and use a 1,024-bit block size, SHA-384 and SHA-512 are advised. The term “truncated hash” is also introduced in FIPS PUB 180-4; it refers to a hash value based on the SHA-512 algorithm that has been reduced to t bits. SHA-512/224 and SHA-512/256 are especially discussed. In RFC 4634, SHA-224, -256, -384, and -512 are also covered.

A new suggested SHS algorithm is SHA-3. Despite the fact that SHA-2 has not been successfully attacked, NIST felt it would be wise to have a backup employing a different algorithm. To discover that substitute, they started the SHA-3 Competition in 2007. NIST stated in 2012 that Keccak had won after examining 64 entries (pronounced “catchack”). The hash lengths used by SHA-3 will be the same as those used by SHA-2 and are based on a sponge function, a different algorithm from those of SHA-1 and SHA-2. NIST should release SHA-3 by the middle of 2014.

**RIPEMD:** A collection of digests of messages that were originally produced by the RIPE (RACE Integrity Primitives Evaluation) project. To replace the then-current 128-bit hash algorithms, Hans Dobbertin, Antoon Bosselaers, and Bart Preneel created RIPEMD-160, which was optimized for 32-bit CPUs. RIPEMD-128, RIPEMD-256, and RIPEMD-320 are further variants.

**Whirlpool:** Y. Zheng, J. Pieprzyk, and J. Seberry created a hash algorithm that provides several layers of security. Hash values of 128, 160, 192, 224, or 256 bits in length can be produced using HAVAL.

**HAVAL (HAsh of VAriable Length):** a recently developed hash function, designed by P.S.L.M. Barreto and V. Rijmen. Whirlpool uses messages with fewer than 2256 bits.in length and generates 512-byte message digest bits. This item’s design is quite functional. Unlike that of SHA-1 and MD5, making it similar attacks on certain hashes are not effective against it.

**Tiger:** Tiger created by Ross Anderson and Eli Biham, is intended to readily replace MD4, MD5, SHA, and SHA-1 in other applications while still being safe and operating well on 64-bit CPUs. Tiger/128 and Tiger/160 provide hashes of lengths of 128 and 160 bits, respectively, to offer compatibility with the other hash algorithms stated above. Tiger/192 produces a 192-bit output and is compatible with 64-bit architectures.

REFERENCES:

<https://en.wikipedia.org/wiki/Cryptography#>

https://www.sciencedirect.com/topics/computer-science/cryptographic-algorithm#

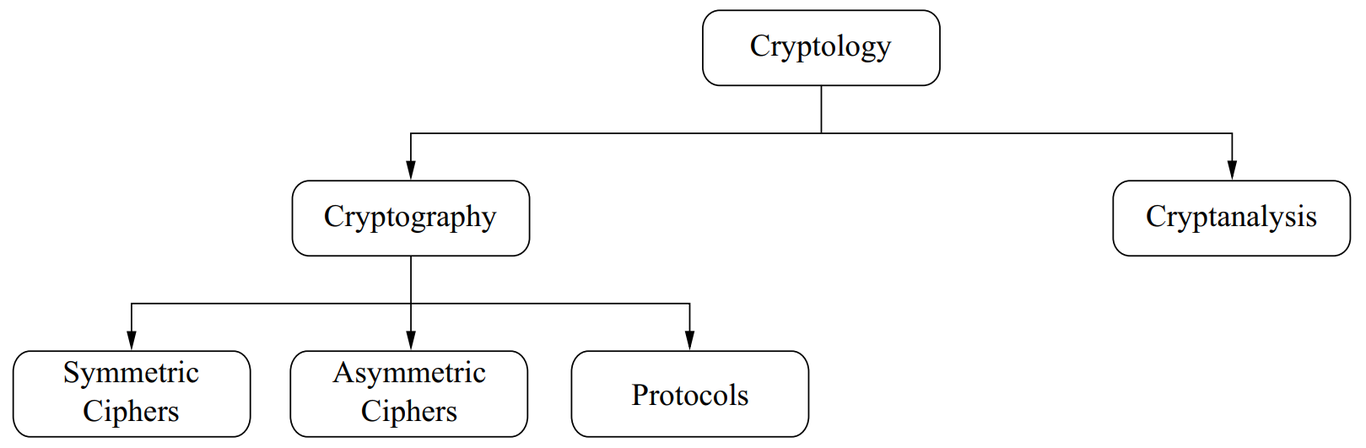
https://en.wikipedia.org/wiki/Public-key\_cryptography

https://en.wikipedia.org/wiki/Digital\_Signature\_Algorithm

Cryptography is the study of secure communication systems, such as encryption, that only the message’s author and intended receiver can access. Cryptography is no longer restricted to the art of writing; it is increasingly used to ensure the secrecy of data across networks and systems.

Security cannot be defined by just one sentence and it is never to be mistaken as a simple factor. Cryptography sets a new level to foresee how security keeps the core system of any business intact from collapsing. Without the knowledge of the importance of information, security can never be achieved and while cryptography may not be able to make one realize the importance of information, it assists in keeping it safe from anything on many levels(*Handbook of Applied Cryptography.*, 1996).

Cryptography is the art and science of secret writing to obscure the meaning of a message. It allows the authenticity of both parties exchanging the data and protects their privacy. For example, cryptography is heavily used in government communications, the financial industry, multiplayer games, etc. It employs secrecy to sensitive data; it is a complex application of sophisticated mathematical algorithms and their encryption/decryption keys, as depicted in Fig. 2.



*General classification of Cryptology*

## Cryptography Process:

The network is the most significant attack source and is vulnerable due to several security flaws.  Even then, internet is so popular and convenient that most confidential messages are exchanged on the network with the help of cryptography mechanisms.

Cryptography is a secure communication method. By using this method only the sender and receiver will be able to know about information. It would be achieved by coding or hiding the information during the transmission process. This method is related to the encryption process. The message along with the cipher text encryption will be done in the sender side. Then, receiver need to use same cipher text for the decryption process (Dayalan, 2019). There has been different type of technique and algorithms are available for providing high security. The encryption and decryption process would be done using 128 bits and 256 bits keys. The modern methods available are advanced encryption standards [AES] and this method would be unbreakable.

The cryptography method is important for the protecting the users data for ensuring the confidentiality of the information. Through this method cyber criminal’s entrance will be prevented and sensitive information can be protected. The examples of this method would include privacy and confidentiality of the information, authentication, integrity, non-repudiation, and key exchange are available (Sharma & Gupta, 2017). There has been different type of the cryptographic algorithms are available they are secret key cryptography, stream ciphers, block ciphers, RSA, etc.

Cryptography principles are approached by researchers or security teams to achieve information confidentiality (Mangore Anirudh K, 2019). Cryptography is used to ensure individual privacy and ensure the transmission of information in a secure way and the authorized user access the information. Only the intended user can access the confidential information as per data security and it prevents any modification or alteration of data (Abdalbasit Mohammed, 2019). A cryptographic system’s fundamental idea is to cipher data or information to achieve secrecy of the information in a way that prevents an unauthorised person from deducing its meaning. In cryptography, the information that is hidden is typically referred to as “plaintext,” and the act of hiding it is referred to as “encryption.” The plaintext that has been encrypted is referred to as “ciphertext.” The “encryption algorithms” are a set of rules that enable this procedure (Anjali Krishna A, 2020). The “encryption key,” which is typically provided to the encryption algorithm along with the information, is what makes the encryption process work. The receiving side can extract the original data using the “decryption key” using a “Decryption algorithm.”

Cryptographic functions helps in exchange of the message that can be of same hash and can deal with the following properties:

* It is quick in computing of the hash functions for any given message.
* It is easy generation of the message that can yield a give hash value
* It is infeasible to find two different messages that has the same hash value.

The major principles of cryptography includes

**Confidentiality**

The degree of confidentiality helps in finding the secrecy of the data. the principle specifies that only the sender and receiver can be able to access the information that is shared among them. Confidentiality helps in compromising the situation if any unauthorized person is able to access a message.

**Authentication**

It is the mechanism where in for finding the user or system or entity.  It will ensure the identity of the person who is trying to access the data. The secured process is through username and password. The person who is authorized and whose identity is preregistered can help in providing his or her identity and therefore can easily access the sensitive data.

**Integrity**

It helps in giving the assurance whether the data is received is same and accurate. If in case the content of the message is altered after the sender sends the data but before reaching the intended receiver then it is called as the integrity of the message lost.

**Non - Repudation**

It is considered as the mechanism that helps in prevention of the denial of the message content that is sent via network. In some scenarioes the sender will send the message and later he will denies it. But here the non repudation will not allow the sender to reject the reciever.

Access Control: This principle depends on the availability of the resources that are available for authorizing the party at all times. The information is not useful if it dont have the access. Systems should have sufficient amount of availability of data in order to satisfy the user request.

There is always a cryptographic algorithms that are being used when there is more security is needed to pull out the data. The usage of the confidentiality helps in enhancing the encryption of messages that comes across the available data and therefore can be more leniant when there is less scope for the cryptoanalysis. There is always a strong belief that the terms and conditions that are adhered with the main logic behind the encryption of data can be carried over with the cryptographic principles. To begin the hash functions concept in the symmetric encryption makes the messages to be altered with the message Sk (E,m). The hashed functions can be cipher or CBC mode that can control each message encyrption more frequently and thus can be varied depending on the type of the control measured with the encryption standards. there is always a sense of sending the messages that can be obtained with varying process values and thus cipher text to plain text conversion.

**Symmetric Cryptography**

Here all the key will be known and keys can be sent at any time

ASymmetric Cryptography: There will be both public and secret keys. The secret keys are known by the owner . They will use different keys for the exchange and uses the simpler protocol and have primitives in difficulty in design.

Importance of the Cryptographic principles:

The importance of cryptographic principles lies in the range of encryption and decryption process. Confidentialty makes the message more secured that there will be no easy access in order to access the data . The more the confidentialism in the data exchange then there will be more security for the message. There might be a difference when there is less available data is considered with more data access points that can be regarded as the major outcome in the process.

the availability of the data is more when there is less encryption standards used with all necessary changes in the process. In order to have the major contribution through out the encyrption process makes it more easy to understand and begin the data with all normal closures. If the available data is more convenient to use than the average available data then there is less chance for the integration of the source type that can be mostly fitting with all necessary encryption schemes that are available. The integrity of the data is also important as it can help in building the prototype of the encryption standards that could be of more use when there is less scope for the mix of the encryption schemes that are available in the data. In order to best fit the data standards with all necessary cryptographic principles makes it more easy to understand with the major cryptographic hash functions.

There is always a measure in the encryption standards that can be easily configured with all necessary changes done in the process of encryption schemes that can be taken as the major principle for the cryptographic algorithm. In order to have the principles of cryptographic in the execution it is important to know what is the role of the plain text, cipher text, and other known formats that can be mismateched when there is necessity for the cryptographic algorithms to be fairly concised. To be on the encryption schema it is important to note that there is always a control over the encyrption schemas that are available in the data standards. It is imporant to know what is the major contribution in dealing with the necessary encryption schemes and standards who can full fill the data themes more easily. There is encryption schema that is more frequently being avoided when the CIA is measured with all necessary changes done.

## Encryption:

When person A wants to send a secure message to person B over the network, encryption is a methodology to solve the problem.  Applying a specific algorithm in the encryption process can produce secrecy in the message(Christof Paar & Jan\_Pelzl, 2009).  However, the output of the encrypted message may seem unintelligent to unintended recipients interested in the message.   Without the corresponding decryption key, the recipient cannot unlock the data and access the actual message.  It leads us to understand encryption and decryption processes in simple terms.  “The process involved in converting data from ‘plain text’ to ‘cipher text’ with the intent to conceal robustly is ‘encryption.’  Similarly, the conversion process from ‘cipher text’ to ‘plain text’ is decryption.” The sender employs a robust concealing application of the mathematical algorithm to convert the original data into concealed data.  In this encryption process, the decryption key is also a key component in the same cryptosystem.  The concept of a cryptosystem in the context of cryptography includes specific cryptographic algorithms needed to implement a concealed outcome in a particular format.  The cryptosystem is comprised of three methodical applications using mathematical algorithms.

1.     Key Generation

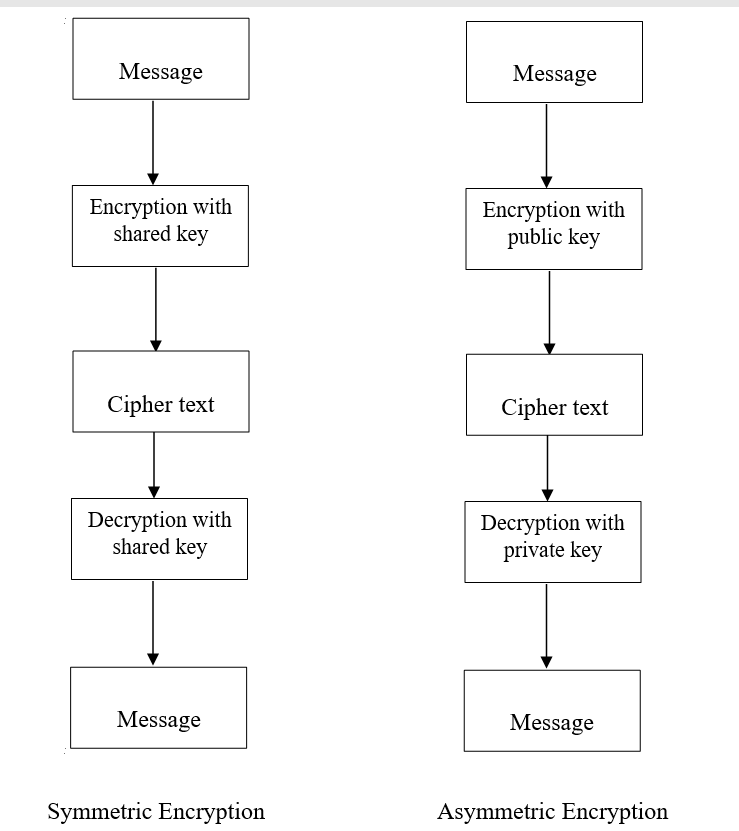
2.     Encryption process

3.     Decryption process

Algorithms/Ciphers used by Encryption process fall into two categories as shown in Figure.3

1.     Symmetric ciphers/algorithms

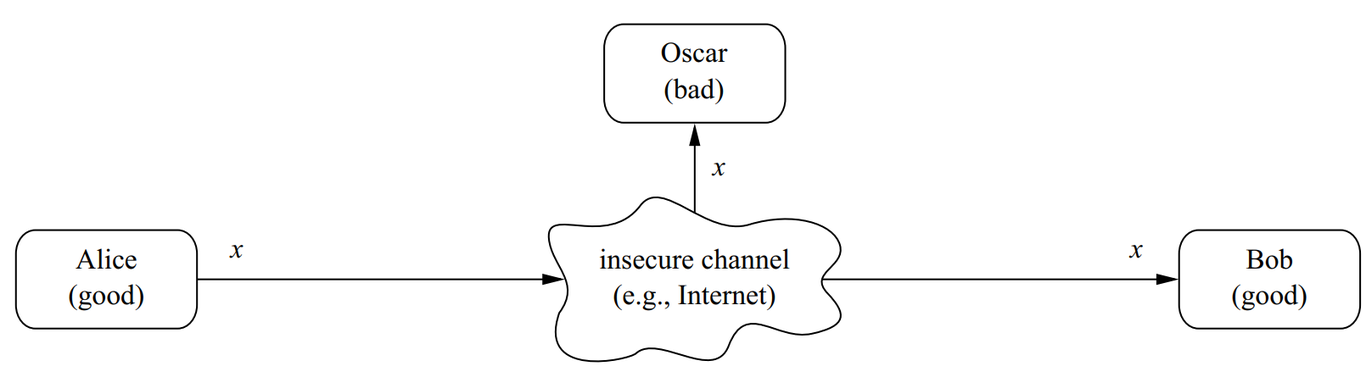
2.     Asymmetric ciphers/algorithms.



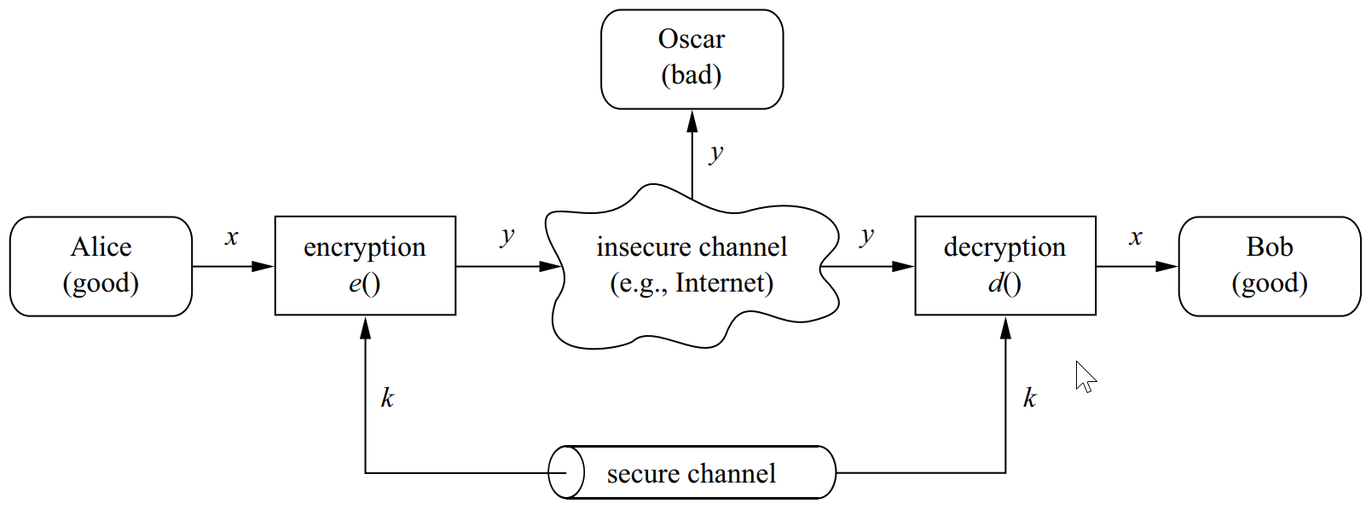
Simplistic depiction of Symmetric and Asymmetric Encryption in Cryptosystem

Before understanding the types of algorithms and ciphers, it is essential to know about the problems related to secure communication (encryption) in the context of cryptography.

Symmetric encryption maintains separate instances of the same key to encrypt and decrypt the data, as shown in Fig.3. These algorithms are comparatively more efficient than asymmetric algorithms. However, they need more efficient key distribution and key management methods with the increase in the number of keys/users. These algorithms and their mathematical application only address/maintain the information’s secrecy and do not assure message integrity. In such a scenario, if the threat actor can modify the cipher text either partially or entirely, then Person B would not realize what happened when he/she received the message. When using symmetric algorithms, the sender and receiver must transmit the key confidentially. Otherwise, the cryptosystem is compromised, and the message integrity is lost. Additionally, keys increase with the number of users, creating a new problem of efficiently storing and managing keys securely. Below is an example of Alice and Bob communicating with each other using symmetric encryption as described in Christopaar’s book(Christof Paar & Jan\_Pelzl, 2009).



*Communication over insecure channel without Symmetric Cryptography*



Communication over insecure channel with Symmetric Cryptosystem

The variables x, y, k has special prominence. xà plain text, yàcipher text, kà key. Variable y looks like random bits to Oscar providing confidentiality to Bob and Alice. Confidentiality is broken if Oscar gets hold of k and cracking the algorithm.

In Asymmetric encryption, the sender and the recipient use different keys (public & private) to encrypt and decrypt messages. Message encryption is achieved with the public key, and message decryption is done with the private key. Public keys are public information, while private key is reserved for the recipient. It is important to note that the two keys are part of the same cryptosystem and are comparable mathematically. These techniques take advantage of secure network protocols to enable both parties to exchange data using public and private keys that accept the protocol standard. Asymmetric encryption is slower compared to symmetric cryptography. This is because asymmetric cryptography follows security protocol rules of authenticity and non-repudiation. Because the sender’s key is public, it authenticates the source identity as well as the integrity of the data. The recipient has a private key used to “unlock” the data and serves to authenticate his identity simultaneously.

**What is a key:**A key is a value with an extensive sequence of random bits. It is difficult to crack the algorithm if the key is larger. The algorithm and key are the fundamental components of a cryptosystem.

# Ciphers

A cipher is a method of performing encryption. Ciphers play a vital role in Communication technologies to maintain both privacy and security.

## Substitution Cipher

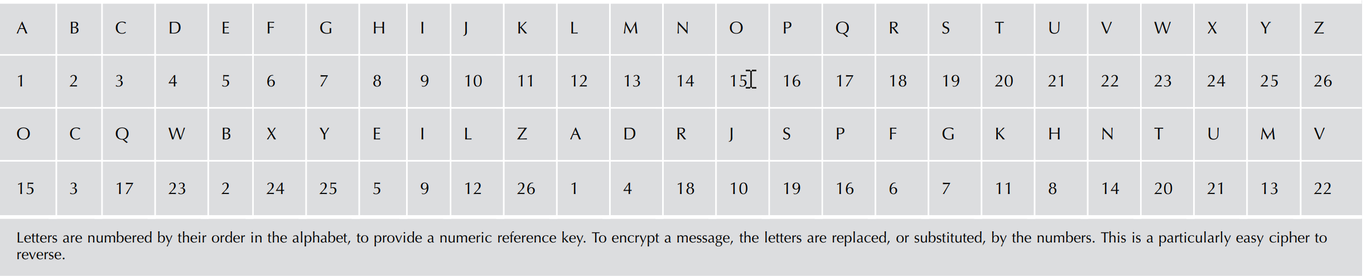
Substitution Cipher falls into the symmetric ciphers category.  The three main components for the cipher are

1.     Plain text

2.     Key

3.     Cipher text (Short encrypted text is referred to a ‘cryptogram’)

In the encryption process, all letters in the original text are substituted with the corresponding letters from the cipher key. The advantage is using the algorithm is one of the fastest ways. However, the downside is that anyone can easily crack the cipher text with enough analysis and insights into the manuscript. This is a good reason to incorporate a strong cipher algorithm instead of simple substitution. After detailed analysis to identify unique letter groupings, it can lead to reconstructing on of the cipher through experimentation(Christof Paar & Jan\_Pelzl, 2009).



*Simple substitution cipher*

## 

## The Shift Cipher (known as Caesar Cipher)

Encryption is achieved by shifting the alphabet by a few positions, by doing so, the encrypted text becomes unreadable by the unintended recipient

*Shift value is 3. Top row is original. Bottom row is the cipherkey.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |

With the assumption that all letters in the original message are uppercase, it replaces with the corresponding shift letter in the cipher key to produce the encrypted text. The shift value is originally agreed by the legitimate sender and the receiver. The snooper may not know the shift value, however Mr.Snooper (threat actor) can be a master in frequency analysis and can derive insights to guess the shift value. Some letters in the alphabet key are used frequently than others. Example: Vowels are everywhere. Z,X, Q are not so frequently used. By analyzing the frequencies of letters in the ciphertext you can derive the cipher key that produced the ciphertext. If you can predict the key, you can easily crack the code to decrypt the message. The likelihood of predicting the shift value correctly is based on the letter-frequency. There are several algorithms that that can easily crack the code.

Substitution Cipher and Shift Cipher belong to the monoalphabetic category where each letter in the plain text corresponds to one letter in the cipher key. These methodologies are vulnerable and weak due to the nature of one-to-one substitution, word pattern prediction in combination with letter-frequency analysis. Large text serves as favorable input to crack the cipher key because it has a larger sample text. Also, it is important to remember that the cipher key is only as large as the number of alphabets. So, the key is relatively smaller compared to polyalphabetic cipher. The smaller the key, the easier it is to crack the code.

## The Polyalphabetic Cipher (Vigenere’s Cipher)

Each letter in the original text can be encrypted by any letter in the cipher key. In other words, each letter in the cipher key represents different letters from the plain text each time it occurs. Generally, if a same letter occurs more than one time at different positions in the plaintext, it does not get mapped to the same character in the ciphertext, since the key-character written above plays a role in the encryption. Letter frequencies in the plaintext is not a problem in this methodology. To decrypt a character in the ciphertext, identify the column given by the key character above the ciphertext character. Find the ciphertext character in that column. The row at which it appears is labeled with decrypt value, i.e. with the corresponding plaintext character. Due to its larger key, it addresses the problems that substitution ciphers had. It follows the methodology that is a combination of different monoalphabetic ciphers. Cryptanalysis becomes harder to predict the original text because it reduced the frequency distribution methodology. Varying substitution contributes to the strength of this approach.

## The KasiskieKerckhoff Cipher

Named after Friedrich Kasiski, a Prussian major who proposed a method to crack the Vigenère cipher. Briefly, his method required the cryptographer to deduce the length of the keyword used and then dissect the cryptogram into a corresponding number of ciphers. This is accomplished simply by examining the distance between repeated strings in the ciphertext. Each cipher would then be solved independently. The method required a suitable number of **bigrams**/**trigrams** to be located((n.d.). YouTube).

A bigram is a portion of the ciphertext two characters long, which repeats in a discernible pattern. Similarly, a trigram is three characters long. Once the common bigrams/trigrams are identified, we’ll find the distance between the repetitions. The harmonic is created by the overlaying keyword with the underlying text; when the bigrams “line up” and repeat themselves.

Christof Paar & Jan\_Pelzl. (2009, October 27). *Understanding Cryptography*. <https://asset-pdf.scinapse.io/prod/1279320161/1279320161.pdf>.

Dan Boneh and Victor Shoup. (2020). *A Graduate Course in Applied Cryptography*.

Vacca, J. R & Morgan KaufmannS. (2009). *Computer and information security handbook*.

## 

## Hash function

    Hash functions are mathematical operations that “map” or convert a set of data into a bit string        with a certain length, commonly referred to as the “hash value.”

    Cryptocurrency, communication security and password security all use hash functions.

### Specifications of a Hash Function :

* Hash Function is irreversable

     Hashing is a one way function.That means Based on the hash value , you cannot determine the            original data.

* Hash Values Are Unique

    It is preferable if different input data never provide a same hash value.If they do coincide ,it             results in a collision, which makes the algorithm vulnerable and unsafe to utilize.

### Hash function Working

The hash value of first block is sent to second block as an input.In the same way the hashed     output is sent to third block and the combined value is hashed again.This cycle continuous till the     final output which is sum of the all blocks.

### Use cases for hash functions :

* Digital Signatures
* Passwords
* Biometrics
* Password storage
* Code &Email signing certificates
* SSL/TLS certificates

### Weaknesses of hash functions

* Popular algorithms like MD5 and SHA-1 have occasionally produced the same hash value for different material in the past. As a result, the collision-resistance quality was diminished.
* Hackers attempt to decipher unsalted hash values using a mechanism known as “rainbow tables.” Salting before hashing is essential for secure password storage because of this.
* Attackers, security researchers, or even governmental organizations can employ software services and hardware devices (referred to as “hash cracking rigs”) to decipher hashed passwords.
* The hashed data can be cracked using specific brute force tactics.

References :

Frankenfield, Jake. “Cryptographic Hash Functions: Definition and Examples.” *Investopedia*, Investopedia, 7 Nov. 2022, https://www.investopedia.com/news/cryptographic-hash-functions/.

Mehta, Medha. “Hash Function in Cryptography: How Does It Work?” *InfoSec Insights*, 4 Dec. 2020, https://sectigostore.com/blog/hash-function-in-cryptography-how-does-it-work/.

Freda, Anthony. *What Is the MD5 Hashing Algorithm and How Does It Work?*, Avast, 6 Oct. 2022, https://www.avast.com/c-md5-hashing-algorithm.

### Properties of hash functions

**Pre-image resistance**

* The reversing of the hash function is a hard process.
* The hash function will produce the hash value z. In this case it would be difficult for determining the input value which would produce hashes to the z.
* The attackers who are hashing the hash value to make attacks will be difficult and proper protection will be offered.

**Second pre-image resistance**

* The input and hash will be provided and it will be difficult for determining the same hash for the different inputs (Singh, 2020).
* For the input of the x and the hash function will be h and hash value obtained will be h[x]. For the input value of the y determining of same hash value is difficult h[y] = h[x].
* Even if the attackers has the input and the hash value and trying to change original value is not possible through this method.

**Collision resistance**

* The two different type of input which has different length will have same hash. The property is said to be collision free hash function.
* The hash function h and the two different inputs are x and y are difficult to determined and it was obtained as h[x] = h[y].
* By using the fixed hash function compressing function will be determined. Avoiding of collision occurrence is impossible in this case. This property confirms that determination of the collision is harder (Sobti & G.Geetha, 2012 ).
* The attackers will face difficulty for determining the same hash for the two different type of inputs.
* If hash function is collision resistant, it is said to be second pre-image resistance.

**Design**

The mathematical operation will be carried out for the development of the hash. The hash code will be created by using the two fixed size data blocks. The hashing algorithm will be developed by using the hash function. Based upon the algorithm the data block size will differ. The size would range between 128 to 512 bits. Rounds will be carried out in the hashing algorithm as like block cipher. Fixed input size would be considered for each rounds. The combination would be done for the recent message block and the output of the last round (Hullatti & S, 2014). The process would be repeated continuously for obtaining the hash message. The output from each block is provided to the next operation and this effect is said to be avalanche effect. Due to this effect different hash value will be obtained.

 In the security course, hashing techniques and encryption are major parts to ensure security. The process of mapping plaintext data of any length into a distinct ciphertext with a set length, known as a hash, is called hashing (Rajeev Sobti, 2012). It is a mathematical algorithm that takes input data of arbitrary length. H: Dà R is a mathematical function. The main fields of hash functions are the protection of message authentication, stored passwords, digital signatures, and relevant certificates. Unkeyed hash functions and keyed hash functions are two broad classifications of hash functions. SHA (Secure Hash Algorithm), MD (Message Digest), RIPEMD (RACE Integrity Primitives Evaluation Message Digest), BLAKE, Whirlpool, and Curl-P are some examples of cryptographic algorithms. Properties of the hash function should follow to ensure data security and effectiveness which are,

·       One-way function (pre-image resistance)

·       Target collision resistance (2nd pre-image resistance)

·       Collision resistance

·       Deterministic

·       Avalanche effect

·       Hash speed

**Security services of cryptographic functions**

·       Achieving integrity and authentication

·       Implementing efficient digital signatures

·       Authenticate users of computer systems

·       Digital time stamping

·       Hash functions as PRNG

·       Session key derivations

·       Constructions of block ciphers

These are the major security services provided by the cryptographic function. However, hash functions faced with attacks are classified into two Cryptanalytical analysis, and Brute Force attacks. These attacks should be considered while handling data or information to ensure the security of confidential data.

# Types of Hashing

     Below are the popular hashing functions used for file integrity checks

## 1. MD5

The hash is the mathematical function which is useful for conversion of the input value which is in numerical format into the compressed numerical value. The input provided for the hash function will be in the arbitrary length format and output will be in the fixed length (Singh, 2020). The values that are obtained is called as message digest or hash value.

## 2. MD5 Working :

The mathematical hashing algorithm used by MD5 to create a signature that can be compared to the original file. In this manner, the authenticity of a received file in comparison to the original file transmitted may be verified, guaranteeing that the correct files are delivered to their intended locations.

Data is transformed into a 32-character string by the MD5 hashing method. For instance, the hash 938c2cc0dcc0dcc05f2b68c4287040cfcf71 is always produced when the word “frog” is used. Similar to this, a 1.2 GB file likewise produces a hash with the same amount of characters. Your recipient’s computer verifies the hash of the file you provided them to make sure it matches yours.

A message of any length can be entered into the cryptographic hash function algorithm MD5, which converts it into a message with a fixed length of 16 bytes. The message-digest method is also known as the MD5 algorithm. As an advancement over MD4, MD5 was created with more sophisticated security objectives. The digest size (MD5) output is always 128 bits. Ronald Rivest created MD5 in 1991.

## Use Of MD5 Algorithm:

For file authentication, it is employed.

It is utilised for security in online applications. For instance, secure user passwords, etc.

We can save our password in 128-bit format using this approach.

**References:**

What is the MD5 algorithm? (2022) GeeksforGeeks. Available at: <https://www.geeksforgeeks.org/what-is-the-md5-algorithm/> (Accessed: December 8, 2022).

The message digest algorithm is the hashing algorithm. It was a one way cryptographic algorithm which would accept the input messages which are of the any length and the output will be returned in the fixed length digest value. It will be useful for authentication of the original message. This method is designed for the secure cryptographic algorithm. Digital signature authentication can be done by using this algorithm.

The MD5 algorithm is used for the message authentication code for usage in the internet. Now a days it is not considered as reliable for using in the cryptographic checksum. It was because the security experts has explained about the collision occurrence. The collision occurrence is said to be two files are having the same hash (Gupta & Kumar, 2014). The MD5 hashing method will be used for the integrity protection process. The MD5 checksum is acceptable for the usage so that it is used for the inline protection against the errors.

## Characteristics

§      The message digest are the one way functions. It would accepts any size of the input and the output will be provided in the fixed length.

§      It was a third message digest algorithm that has been created.

§      The MD2, MD4 and MD5 are having the same structure and for the MD2 optimization is done for the 8 bit machines.

§      It was an extension of the MD4 from the analysis it was found that it was fastest but some of them are insecure (Mishra, et al., 2013).

§      This algorithm is still not fast as MD4 but it has been offering high security for data.

## Working

In this the encryption process is carried out in the five steps and in each step certain predefined process would be carried out.

Step 1 - Appending of padding bits

To the original message the extra bits would be added. The total bots after padding should be less than 64 and it would be multiples of the 512. The padding process will be done even if the original message is of the congruent to 448 modulo 512. The first bit of the padding will be 1 and other will be 0.

Step 2 - Append length

The 64 bits will be added after padding process and it would be used for recording the original input length.

Step 3 – MD buffer initialization

The entire strings will be converted to the multiple of the 512 bits blocks. In this four different buffers are present and each of them are 32 bits (Mishra, et al., 2013).

Step 4 – Processing of blocks

The auxiliary function will be done and input provided will be 32 bit numbers and 32 bit output will be produced. The logical operators carried out are OR, XOR, NOR.

   A type of encryption known as “Message Digest” uses hash values to alert the owner of the copyright to any modifications made to their work (Sagar, 2016). Specific files that contain the protected works are identified by message digest hash numbers. On 32-bit processors, the MD5 algorithm is intended to be quite quick. The MD5 technique can also be programmed relatively compactly because it doesn’t require any massive substitution tables. The MD4 algorithm is extended to obtain the MD5 algorithm. The MD5 is conservative in design even though it is slower than the MD4 (Shweta Mishra, 2013). In order to use MD5, a message’s entire body must be computed by both the sender and the receiver. In the software industry, MD5 digests are frequently used to ensure the security of files during transmission.

Data is encoded into 128 bit fingerprint using MD5 hash method.

A message of any length can be entered into the cryptographic hash function algorithm MD5, which converts it into a message with a fixed length of 16 bytes. The message-digest method is also known as the MD5 algorithm. As an advancement over MD4, MD5 was created with more sophisticated security objectives. The digest size (MD5) output is always 128 bits. Ronald Rivest created MD5 in 1991.

Use Of MD5 Algorithm:

For file authentication, it is employed.

It is utilised for security in online applications. For instance, secure user passwords, etc.

We can save our password in 128-bit format using this approach.

References:

What is the MD5 algorithm? (2022) GeeksforGeeks. Available at: <https://www.geeksforgeeks.org/what-is-the-md5-algorithm/> (Accessed: december 8 2022)

## SHA1

SHA (Secure Hash Algorithm 1) was developed by US NSA (National Security Agency) and it was published by NIST (National Institute of Standards and Technology). SHA 1 is nothing but a cryptographic hash function that produces 160 bits (20 byte) hash value by taking an input data. SHA 1 is introduced as a replacement of SHA 0 due to its security flaws. This 160 bit output is called as message digest which helps in improving the security. This message digest will be converted into 40 digit hexadecimal value.  SHA 1 is mainly used in the cryptographic applications and in the place where the data integrity is most needed. The checksum errors are easily identified by the SHA-1 algorithm. The security protocols and application also uses the SHA-1 algorithm which includes TLS, SSL, IPsec, S/MiME, and PGP. They are widely used in the large organization such as Microsoft, Google, Mozilla, and so on. Due the identification of security vulnerabilities they have completely stopped using SHA-1 algorithm and moved to SHA-3 algorithm. However, cryptographic community consider SHA-1 is basic for the modern digital signatures.

**Cryptographic application of SHA-1**

SHA-1 is used in real world application by websites to verify the user in the secure way. One real world example of usage of SHA-1 algorithm is in the login page. When the user enters the password, the website uses the SHA-1 algorithm which converts the password into checksum. Then the converted checksum is verified with the checksum that is stored in the database. When the match is found the access is provided or else the access will be denied.

It helps in providing security to the data during transaction in the electronic devices. The security is provided against the eavesdropping attack, and replay attack. SHA-1 is considered to be the complex algorithm which involves complex logical functions, and great deal of repetition. In SHA-1 algorithm functions b multiple 32 bit 5 way adds. It also performs data shifting which all together makes the algorithm a complex one. The SHA-1is implemented with the large die area silicon making it expensive token. Later, new method has been identified to perform the algorithm making it reasonable price. This token is globally unique and unaltered. For example, when the token is in transaction and the third party tries to alter the data then the token is considered to be invalid.

Thus SHA-1 is widely used in the cryptographic application for secure access to the information.

## Data integrity

SHA-1 algorithm is not only used in the cryptographic applications but it is also used for making sure the data integrity is maintained. It is used to make sure that the data is not corrupted during retrieval. SHA-1 helps in performing the consistency check. For example, when the file verification is done using SHA-1 algorithm when the file is downloaded from the webpage. The checksum verification is done when it is downloaded from the non-developer website to the developer website to make sure same version is of file is downloaded (Fisher, 2022).

SHA is based on MD4 and it shares the same building blocks. The SHA algorithm’s design added a new procedure that, among other things, increases the 16-word message block input to the compression function to an 80-word block. SHA is founded with a technical flaw that makes the algorithms less secure (H. B. Pethe, 2016). It produces a 160-bit message digest and it is a part of the Digital Signature Algorithm. It is not used in cryptographic functions because of its weaknesses (Surbhi Gupta, 2014). The message of arbitrary length is an input for SHA 1 and the output is a 160-bit hash code.

A 160-bit (20-byte) hash value is produced by the cryptographic hash function known as SHA-1, or Secure Hash Algorithm 1. The phrase “message digest” refers to this hash value. The result of this message digest is typically a 40-digit hexadecimal number. It was created by the US National Security Agency and is a U.S. Federal Information Processing Standard. Since 2005, SHA-1 has been regarded as being insecure. By 2017, major computer heavyweights including Microsoft, Google, Apple, and Mozilla no longer supported SHA-1 SSL certificates. Java’s Message Digest Class, which is part of the java. Security package, is used to determine cryptographic hashing values. To determine a text’s hash value, the Message Digest Class offers the following cryptographic hash algorithm.

**Reference:**

SHA-1 Hash (2022) GeeksforGeeks. Available at: <https://www.geeksforgeeks.org/sha-1-hash-in-java/> (Accessed: December 8 2022)

## SHA2

SHA-2 is a cryptographic hash function which belongs to the SHA family which was developed US NSA. In the modern world SHA-2 is considered to play important role in the network security. SHA-2 is a successor of SHA-1 algorithm. When analyzing the working of both the algorithms they have same role. SHA-2 also performs cryptographic hash function of the input data. The only difference between SHA-1 and SHA-2 is SHA-1 has the fixed hash value of 160 bits but SHA-2 provide output of different size. Still SHA-2 is considered as a secure way of online security and it is mainly preferred over MD5 in many places. Different sizes of hash output provided by SHA-2 algorithm includes

·         SHA-224

·         SHA-256

·         SHA-384

·         SHA-512

·         SHA-512/224

·         SHA-512/256

Among these different SHA-2 algorithms SHA-256 is the most commonly used. Depending on the size the hashing length gets varied. If the length of the hash is smaller than it is easy to find collision between the numbers but when the hash is longer than it needs long time to calculate and it consumes high computation resources thus offering the collision resistance (Florian Mendel, 2011). It helps in preventing the attackers from gaining access to the information that is being shared. In the modern days the computational power also increased thus allowing to use longer and resource-intensive hashes. SHA-2 algorithm is built from one-way compression functions.

## Applications

SHA-2 is also widely used for security protocols like SHA-1 which includes TLS(Transport Layer Security), IPSec(Internet Protocol Security), PGP (Pretty Good Privacy), S/MIME (Secure/Multipurpose Internet Mail Extensions), and SSH (Secure Shell).

TLS is the most commonly used security protocols. In the website, it is often notice that Https in which s stands for secure for establishing secure connection between the device and the service which uses SHA-2. In the SSH the file forwarding and transfer are done in the secure manner using the SHA-2 algorithm.  Other the security protocols SHA-2 algorithm are used for other purposes which includes

## Data authentication:

SHA-2 is used for making sure that the data is not altered. This authentication helps in making sure that the software packages downloaded from the online sources are legitimate and not altered.

## Hashing password:

In some cases SHA-2 algorithm is used for hashing password. But it is not considered to be a good practice. There are other secure solutions for handling password hashing such as crypt (LAKE, 2022).

## Blockchain technologies:

In Bitcoin and other crypto currencies SHA-algorithm is used for proof-of-work. In the blockchain projects SHA-256 is used for proof-of-stake purpose.

## Government data:

SHA-2 algorithm is widely used in the US federal agencies. It is important to note that National Institute of Standard and Technologies (NIST) has recommended the use of SHA-2 and SHA-3 algorithm for most of the federal applications.

The main drawback with the SHA-2 algorithm is that some of older applications and operating system does not support it leading to the compatibility issues. Due to this issue in majority of the cases SHA-2 is not adopted.

SHA 2 is used in cryptography which helps to generate new messages corresponding to the original messages by performing operations. Data integrity can be verified by applying SHA 2 and also it is applicable in digital signature applications (S.K. Shaw¸ M. Jain, 2016). Different SHA-2 family hash functions produce hashes with different lengths. For example, SHA-512 generates a hash of 512 bits and the length of 256 bits of the hash will be generated by SHA-256. It is a one-way encryption algorithm and uses 640 bits in the hash by SHA 2.

## References

## 

1.Frankenfield, Jake. “Cryptographic Hash Functions: Definition and Examples.” *Investopedia*, Investopedia, 7 Nov. 2022, <https://www.investopedia.com/news/cryptographic-hash-functions/>.

2.Mehta, Medha. “Hash Function in Cryptography: How Does It Work?” *InfoSec Insights*, 4 Dec. 2020, <https://sectigostore.com/blog/hash-function-in-cryptography-how-does-it-work/>.

3.Freda, Anthony. *What Is the MD5 Hashing Algorithm and How Does It Work?*, Avast, 6 Oct. 2022, https://www.avast.com/c-md5-hashing-algorithm.

# System and Network Security

Network security is essential for safeguarding client data and information, maintaining the security of shared data, guaranteeing dependable network performance, and defending against online attacks. An effective network security solution lowers overhead costs and protects businesses from significant losses brought on by a data breach or other security event. Ensuring appropriate access to systems, applications, and data facilitates company operations and customer service.

## Types of Network Security Protections :

### Firewall:

Using pre-established security rules, firewalls manage the incoming and outgoing traffic on networks. Firewalls are an essential component of daily computing since they block malicious traffic. Firewalls, particularly Next Generation Firewalls, which concentrate on thwarting malware and application-layer assaults, are crucial to network security.

### Network Segmentation :

When assets within a group have a common function, risk, or role within an organization, network segmentation establishes boundaries between such groups of assets. The perimeter gateway, for instance, isolates a corporate network from the Internet. Sensitive data of an organization is kept inside the network by preventing potential outside threats. Organizations may take things a step further by creating more internal network borders, which can enhance security and access management.

### Access control :

Access control limits unauthorized access and potential dangers by defining the individuals, organizations, and devices that have access to network applications and systems. Role-based Access Control (RBAC) regulations make that the person and device have permitted access to the asset, while integrations with Identity and Access Management (IAM) solutions may accurately identify the user.

### Remote Access VPN :

Telecommuters, mobile users, and extranet users may all access a workplace network remotely and securely with the use of a remote access VPN. Each host normally utilizes a web-based client or has VPN client software installed. Multi-factor authentication, endpoint compliance screening, and encryption of all transferred data all contribute to securing the privacy and integrity of sensitive data.

### Zero Trust Network Access (ZTNA) :

According to the zero trust security paradigm, a user should only have the access and privileges necessary to carry out their assigned responsibilities. This strategy differs significantly from that offered by conventional security solutions, such VPNs, which provide a user complete access to the target network. Zero trust network access (ZTNA), often referred to as software-defined perimeter (SDP) solutions, allows users who need granular access to an organization’s applications to do their jobs.

### Email Security:

Any procedures, items, and services aimed at keeping your email accounts and email content safe from outside dangers are referred to as email security. Although the majority of email service providers have built-in security measures to protect you, they might not be sufficient to prevent hackers from accessing your data.

### Data Loss Prevention (DLP):

Data loss prevention (DLP) is a cybersecurity methodology that combines technology and best practices to stop the exposure of sensitive data outside of an organization. This includes regulated data, such as personally identifiable information (PII), and compliance-related data, such as HIPAA, SOX, PCI DSS, etc., as well as data that is subject to regulation.

### Intrusion Prevention Systems (IPS):

These solutions are able to recognize and stop network security assaults including brute force, DoS, and exploitation of known flaws. An exploit is an assault that takes advantage of a vulnerability, such as one in a software system, to take over that system. A vulnerability is a flaw, for example. When an exploit is disclosed, there is frequently a window of time for attackers to take advantage of that weakness before the security fix is implemented. In these situations, an intrusion prevention system can be employed to effectively stop these attacks.

### Sandboxing:

Sandboxing is a cybersecurity technique that allows you to run programs or access data on a host computer in a secure, isolated environment that closely resembles end-user operating environments. To stop threats from entering the network, sandboxing watches the opened files or code while it searches for dangerous activity. Before the files reach an unwary end user, malware, for instance, may be safely discovered and prevented in formats like PDF, Microsoft Word, Excel, and PowerPoint.

### Hyper scale Network Security:

Hyper scale refers to an architecture’s capacity to scale effectively as the system is subjected to rising demand. Rapid deployment and scaling up or down are features of this system that can adapt to shifting network security requirements. It is feasible to completely utilize the hardware resources offered in a clustering solution by tightly integrating networking and computation resources in a software-defined system.

### Cloud Network Security:

Applications and workloads are no longer just housed locally in a data center on-site. Greater adaptability and creativity are needed to protect the contemporary data center as application workloads move to the cloud. Network security solutions are made possible by software-defined networking (SDN) and software-defined wide area networks (SD-WAN) in private, public, hybrid, and cloud-hosted Firewall-as-a-Service (FWaaS) deployments.

References: <https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/>

# 

# Abstract

Network security has increased in importance for businesses, the military, and individuals using personal computers. People are becoming more aware of the significance of network security as computer network technologies and internet technology evolve more quickly. Security became a top concern with the development of the internet. The primary problem in computing is network security because the number of different types of attacks is always growing. There are various security dangers today because of the structure of the internet. The likelihood of assaults being propagated across the network is reduced when the design of the internet is altered. Knowing the attack strategies enables the development of the right security. Many organizations use firewalls and encryption techniques to protect themselves from the internet. Information transmission-related security violations can be, prevented, discovered, and fixed using techniques in the field of network and Internet security.

# 

# Introduction

The world is getting more interconnected as a result of the growth of the Internet and new networking technology. There is a ton of information that is private, commercial, military, and governmental on networking infrastructures around the world. Because it is so simple to obtain intellectual property through the internet, network security is becoming more important. A network security is the defense provided to an automated information system to achieve the relevant goals of maintaining the integrity, availability, and confidentiality of information system resources. The “CIA Triade” is made up of these three ideas. The three ideas represent the essential security goals for information and computer services, data, and both.

Confidentiality: Maintaining lawful limitations on the access and disclosure of information, including measures for safeguarding individual privacy and private information. Unauthorized information sharing is a breach of confidentiality.

Integrity: Integrity is the prevention of erroneous information alteration or deletion, as well as the assurance of information authenticity and nonrepudiation. Unauthorized alteration or destruction of data constitutes a loss of integrity.

Availability: Ensuring prompt, dependable access to and use of information is known as availability. The interruption of usage or access to information or an information system is referred to as a loss of availability.

# Complications with computer security

Security is more complicated than the naive may initially believe. The criteria appear to be simple; in fact, the majority of the key specifications for security services may be summed up in one word with the following definitions: secrecy, authentication, nonrepudiation, or integrity. However, the methods employed to fulfill those requirements might be rather complicated and comprehending them may call for more delicate reasoning. One must always consider potential attacks on the security features while creating a specific security mechanism or algorithm. In many instances, effective assaults are created by approaching the issue from a completely different perspective, thus taking advantage of an unanticipated flaw in the system.

The processes employed to supply specific services are frequently illogical. A security mechanism is typically complicated, and it may not be clear from the description of a given requirement that such complex safeguards are necessary. Only when the threat’s many facets are taken into account do complex security measures make sense. It is vital to choose where to use the various security methods that have been created. This is true in both a physical and logical sense, such as what layer or layers of an architecture such as TCP/IP should mechanisms be put. Security measures frequently go beyond a specific algorithm or protocol. Additionally, they raise concerns about the production, transmission, and security of any secret information that is required for participation (such as an encryption key). There also may be a reliance on communications protocols whose behavior may complicate the work of building the security mechanism. For instance, any protocol or network that causes variable, unpredictable delays may make any time limitations that must be imposed for a message’s transit time from sender to receiver in order for the security mechanism to function properly meaningless.

# Attacks

Common internet attack techniques are categorized. Eavesdropping and phishing are two examples of attacks that obtain system knowledge or personal data. Attacks from viruses, worms, and trojan horses can also stop the system from working properly. The other kind of attack, known as a denial of service (DoS) attack, may wastefully drain the system’s resources. Intrusions into networks can also take the form of land assaults, smurf attacks, or teardrop attacks. Although these attacks aren’t as well-known as DoS attacks, they are nonetheless employed in some capacity even when they aren’t named specifically.

# Attacks Using IP Spoofing

To get access to other computers, spoofing refers to changing the computer’s address to look like the address of another reliable machine. Different techniques are used to conceal the intruder’s identity, making identification and prevention challenging. Spoofed packets using the IP protocol cannot be completely eradicated with present technology.

# Denial of Service

When a system receives an excessive number of requests and is unable to respond to the requestors, this is known as a denial of service assault. As a result, while it waits for the handshake to be completed, the system needs resources. When that happens, the system is rendered unusable and unable to serve any further requests.

# Phishing

Phishing is an attempt to get access to a person, group, or organization’s private information. Phishers deceive consumers into providing sensitive information including credit card numbers, login passwords for online banking, and other personal information.

# Network Security

Biometric identification is being employed together with the same approaches. Compared to passwords, biometrics offers a more reliable authentication mechanism. As a result, there may be far less unauthorized access to secure systems. Researchers studying network security are discovering new technology, such the smart card. Software is a dynamic element of network security. There are always new firewalls and encryption methods being deployed.

The scope of network security’s software component is enormous. It covers intrusion detection, VPNs, firewalls, antivirus, and many other things. It would not be practicable at this moment to evaluate the research and development of every security program. The goal is to determine the future direction of security software based on existing priorities. The usual security software has not changed despite its improvement. To be able to defend against brand-new viruses as they emerge, the antivirus program is regularly updated. Both firewalls and intrusion detection systems go through the same procedure

References

1. Heberlein, L T, Dias, G V, Levitt, K N, Mukherjee, B, Wood, J, & Wolber, D. A network security monitor. United States.

2. Dowd, P.W.; McHenry, J.T., “Network security: it’s time to take it seriously,” Computer, vol.31, no.9, pp.24‐ 28, Sep 1998 .

3. https://crypto.stanford.edu/cs155old/cs155-spring11/lectures/01-intro-thompson.pdf

Network security is designed to respond to potential threats in a computer network, and includes the following levels:

·       Email and server protection

·       Server protection

·       Network protection

·       Data protection

·       Cloud service application

Network threats, illegal or malicious activities, aim to exploit vulnerabilities in networks, servers, and access. The goal of attackers is to hack, harm or sabotage valuable data. Cloud Networks engineers design, install, and manage business security solutions tailored to the specifics of the industry. Install software, networks, and other necessary equipment for the safe operation of the company.

Setting up strong network security is possible only after a thorough risk assessment. The cybersecurity officer determines the nature and extent of existing and potential threats. The following are some tools for fixing vulnerabilities and countering problems that could harm the system in the future.

* Using strong authentication methods.
* Updating the software to the latest version.
* Set up cybersecurity rules for employees and talk about phishing, social engineering, and malware.
* Secure access to the external network.
* Conduct regular internal security audits and plan for improvements.

To reduce the risk of an attack or data breach, organizations are encouraged to implement controls to keep their IT systems running securely. Network security consists of hardware and software technologies and layers that include applications, antivirus, access control, servers, firewalls, physical access, and policies.

An effective network security policy reduces the chances of data theft and sabotage. Setting up and enforcing network security policies is the key to protecting data from spyware and threats. The policy will also increase the digital literacy of employees.

## 

## 

# Solutions for Network Security

It is difficult to detect anomalies in the network. Mechanisms for detecting network anomalies will allow businesses to analyze the network and find violations. Access control will improve network security by limiting user access to only those resources that are directly related to their duties.

## Anti DDoS

Organizations are always at risk of DDoS attacks. Their goal is to make an application or network inaccessible, but the targets of the attack can be different: available bandwidth, application resources such as CPU and memory, or important infrastructure protocols such as DNS and TLS. DDoS attacks threaten application availability and can lead to loss of revenue and brand damage. Multi-layered protection against DDoS attacks will help keeping a business secure.

## Firewall Management

Firewall management is the process of configuring and monitoring the firewall to maintain network security. There are many firewalls in an organization that protect devices and networks as a standard. Managing them requires setting rules and policies, tracking changes, and monitoring compliance logs. FWM solutions will help organizations instantly respond to vulnerabilities and keep organizations running optimally. ( *Firewall management: The expert guide*. Titania)

## IDS/IPS

Intrusion detection is the process of monitoring events on network and analyzing them for potential incidents, breaches, or imminent threats to security policies. Intrusion prevention is the process of detecting intrusions and then stopping the detected incidents. The Intrusion Detection and Prevention System (IDPS) monitors network traffic for signs of attack (K. 2007), alerting administrators to possible attacks and preventing potential incidents.

## Deceptions

Deceptions are fake servers or systems that are deployed next to the real network. Lures look like potential targets for intruders. This is usually a server or other valuable asset. They collect information and notify IT professionals of any attempt to access the honeypot by unauthorized users. Hence, the organizations will be able to monitor security reactions and study attempts to compromise the infrastructure.

## Network Anomaly Detection(NAD)

Network Anomaly Detection (NAD) systems continuously analyze traffic to look for dangerous activity. Deviations from the norm in the behavior of network devices, incorrect use of the network by users or devices are checked. NAD allows organizations to find existing network performance issues, prioritize their resolution, and automatically respond to new vulnerabilities.

## 

## Next Generation Firewalls(NGFW)

Next Generation Firewalls (NGFW) are network security appliances that go beyond traditional firewalls. These include intrusion prevention, threat intelligence, and application awareness. NGFWs still track incoming and outgoing traffic on the network down to individual applications. NGFW is designed specifically for application analysis, but they also block malware from entering the network.

## 

## Virtual Private Network(VPN)

Virtual Private Network (VPN) is one of the important tools to keep organizations protected from data leakage. A corporate VPN gives you secure remote access and control over who gets access to what. Regardless of the size of a business or where employees work, organizations need a VPN to keep their business data from falling into the wrong hands.

Reference:

Ahmed, M., Naser Mahmood, A., & Hu, J. (2016). A survey of Network Anomaly Detection Techniques. *Journal of Network and Computer Applications*, *60*, 19–31. <https://doi.org/10.1016/j.jnca.2015.11.016>

*Firewall management: The expert guide*. Titania. (n.d.). Retrieved December 3, 2022, from https://www.titania.com/resources/guides/firewall-management/#:~:text=Firewall%20management%20is%20the%20process,devices%20and%20network%20as%20standard.

K. Scarfone, P. Mell, Special Publication 800-94: Guide to Intrusion Detection and

Prevention Systems (IDPS), National Institute of Standards and Technology (NIST) (2007)

Kaspersky. (2022, October 21). *What is VPN? how it works, types of VPN*. www.kaspersky.com. Retrieved December 1, 2022, from https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

Gupta, B. B., Dahiya, A. (2021). Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures. United States: CRC Press.

1. Password system

- Traditional OS’s password system

- Modern OS’s password system

**2. Cracking password system**

Theoretically any kind of password can be “decodable”. Possibility of Figure-out password could be performed with the help of rainbow tables. Rainbow tables are tables which contain pre-computed password hashes. Let us discuss here in elaborate way about rainbow table. The Rainbow table which shall be designed with all possible password for said character establish to a certain character length. When we try to break password hashes all kind of accessories may then search. For creating rainbow tables, it is required huge quantity of storage space and generating time is also very much needed. Passwords which use salting, primary time may be ineffective against hashing of password.

The process of encompassing random pieces of information in password hashing that diminishes the likelihood of identical passwords returning to the same hash is called salting. In case of not considering the salting, rainbow tables shall not generate accurate results, but this remarkably accumulate the amount of storage space that tables required.

Despite developments in authenticating the user, passwords are still a common method of governing if a person or process is supposed to have an access. When some one may try and crack your password manually by guessing social engineering ways, there are also tools that shall self-activating try some combination of letters, numbers, special character, dictionary words check for patterns and other methods to find out the password. We cannot ensure that password cannot be cracked, even though password is encrypted. Till password hackers get success in discovering passwords, they try to use barbarian force cracking tool by thousands of combinations per millisecond.

Password attack shall be considered as offline attack since hacker has gained access to the password has for a specific account or the complete password database. Most databases store the password as hashes other than clear test. That is the reason cryptography hashes are designed by running the plain text password through a hashing algorithm, for example MDS, LM, NT Hash(MD4) etc.

The tools for cracking passwords are very commonly coalition with hacking as account on site, app, or computer, but there are also once crafted to crack the encryption keys used on Wi-Fi networks. Some of the password cracking tool that may be used include

·         Dictionary attacks

·         Rainbow table attacks

·         Guessing password

·         John the Ripper

 Regardless of some fail to differentiate between password guessing and password cracking, it is sensible to distinguish between the password guessing and password cracking as the methodologies differ. Password guessing is the easiest of the two techniques from both attackers and defender’s vintage point. The online technique which involves attempting to authenticate a specific user to the system is called password guessing.

An offline technique, in which cyber attacker avail access to the password hashes or database called Password cracking. Most web-based hacking on passwords is of the password guessing diversification. That way web applications must be designed with in mind from a detective and preventive standpoint.

**Dictionary attacks**

With dictionary attack we can load files of dictionary words into the password cracking tool, and if the dictionary contains one of the passwords, then password shall be cracked. As we need to remember that dictionary files are available for many languages, so finding the right password is easy in we do find out country wise. Using these methods most consultants will find out the password for foreign languages.

**Rainbow table attacks**

A Rain bow table is a precomputed compendium of plaintext and matching ciphertexts (Typically passwords and matching hashes). Rainbow tables speed up many kinds of password cracking attacks, often taking minutes to crack where other approaches (like dictionary, hybrid, and brute-force password cracking attempts) may take much longer. These tables act as a database, they are more composite under the hood, relying on a time/memory trad-off to represent and recover passwords and hashes.

**Guessing password**

Password guessing might be achieved by observing the failed login system logs. Clipping levels are very useful to differentiate among normal users accidentally mistyping their passwords and the attackers. Clipping levels elucidate the minimum reporting threshold level. Clipping level would be established by using password guessing examples such that audit system only notify in case of failed authentication eventuate more frequently than five times in an hour for a specific user.  Also clipping levels help us to differentiate the attacks from noise, however they also can cause false negatives if the hackers can garner threshold underneath which they most operate.

All the passwords must have the stronger authentication way in order to exhibit with the type of the password chosen. Always choose the passwords with the strong authentication methodology.

**John the ripper**

It is a quick password cracking tool that will crack all kinds of windows-based passwords, UNIX and Linux systems. It is also an open-source password security auditing and password recovery tool available for many operating systems. It is very easy to install and use while developing the optimal performance.

The network security is important for all the system and policy would be available for ensuring the security for the software, hardware and assets in the organization. It is also helpful for monitoring and controlling the unauthorized access and modifications in the network systems (Marin, 2005). For this process commonly the authorization method is used in many places which will helps to ensure safety.

**Need**

§      It would provide protection against the unwanted access in the organization database.

§      Occurrence of delay in the network can be avoided.

§      The entry of the particular users can be prohibited and I may include emails, messages, etc.

§      The hardware in the network can be protected and it would include laptops, PC, virus, malware, etc.

§      The protection for the software will be provide so that undesired attacks can be avoided.

**Types of security**

§      Anti-virus and anti-malware will act as a shield for the systems from worms, Trojan attacks, virus, etc.

§      Data loss prevention need to be provided so that confidentiality to the data will be provided.

§      The attackers will send virus through emails so that email security also provided.

§      Proper firewalls need to be used for the networking systems. So that unauthorized access to the network can be prevented (Chen & Hui, 2020).

§      Access control measure need to incorporated so that based upon the role access to information will be provided.

§      VPN will provide high security and in this authentication and encryption methods would be used together.

In any organization, it is necessary to ensure security, because security threats are get increased when technologies are raised. Network and internet services might be insecure and unreliable due to their size and evolution. For establishing a network it is necessary to focus on security requirements that ensure security for the network. Protection of networks and their services from hackers or attackers or unauthorized users. They are ready to alter the data, destruct the data, or disclose the data so it is necessary to protect the network. Some of the common network security measures proposed to ensure network security that is,

·       Keep unwanted people out of the network by implementing a firewall and proxy to the network.

·       Install the Internet Security Software package and Antivirus software package.

·       Assist the administrators and other employees in the organization to use strong passwords for achieving authentication and train them to change the passwords on a weekly or bi-weekly basis.

·       Use a robust password when using a wireless connection.

·       It is necessary to be aware of physical security.

·       It is essential to focus on a network monitor or network analyser and use if it necessary.

·       Physical security measures should be implemented in the network which is like closed circuit television for restricted zones (Pandey, 2011).

·       The organization’s perimeter should be restricted by using security barriers.

Some of the network security tools are used in the organization to avoid network security issues that is,

·       For network exploration or security auditing, organizations can use N-map Security Scanner which is a free and open source.

·       A network vulnerability scanner called Nessus is the best free security tool.

·       A network protocol analyser like wire shark or Ethereal is suggested for UNIX and windows.

·       Analysing traffic in the network and managing logging on IP networks can be handled by Snort which is lightweight network intrusion detection and prevention system.

·       Reading and Writing data across TCP or UDP can be managed by a simple utility tool like Net Cat.

·       Kismet is suggested which is a powerful wireless sniffer.

Types of network security are detailed through image representation which is as follows,

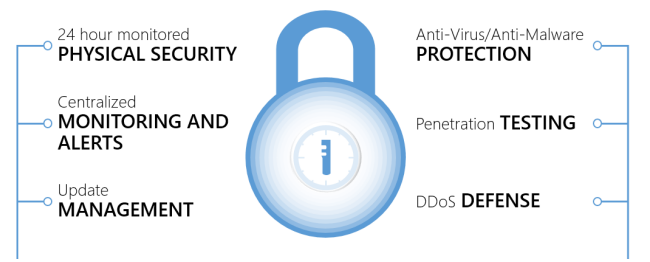


                                                        Figure 2 - Network security types

                                                             Source - (Prabhakar, 2017)

**Defence against network attacks**

Poor design, poor configuration, poor implementation, poor management, deficient physical vulnerabilities with hardware and software, information interception, and human vulnerabilities are the main causes of vulnerabilities. So it is essential to focus on security requirements while implementing the network,

**Configuration Management -** If all of this information is accessible to anyone online, all of the network setup’s remittance logins, IDs, and addresses must be changed as soon as possible. The configuration files must not have any known security holes, all the data is backed up in a secure manner, and the machines inside the core of the network must be running the run-up to update the copies of O.

**Firewalls –** It separates the local network from the internet, filter traffic, and prevent the majority of network threats. Any sort of internal traffic will not be controlled by using firewall. However it can measure the speed and network performance by investigating the incoming and outgoing traffic.

**Encryption –** Through this technique, attackers will not enter the data or system without the legitimate key. Due to the fact that all encrypted emails and websites are permitted through firewalls, they may also contain malware. Stronger encryption is essential to avoid security issues.

**Defence against DOS attacks -** Numerous technologies, including intrusion detection systems (IDSs), improved routers, firewalls, etc., have been developed to prevent DDoS attacks.

# Malware

## Introduction

Any invasive program created by cyber criminals (often referred to as “hackers”) to steal data and harm or destroy computers and computer systems is referred to as malware, which is short for “malicious software.” Malware types that are often encountered include worms, Trojan horses, spyware, adware, and ransomware. Massive quantities of data have been exfiltrated by recent malware assaults.

Businesses often concentrate on preventative measures to halt breaches. Businesses presume they are secure by guarding the perimeter. However, some sophisticated viruses will ultimately enter your network. Deploying technologies that continuously monitor and identify malware that has gotten past perimeter security is therefore essential. Modern network visibility and intelligence, together with many layers of security, are necessary for adequate defense against advanced malware.

Your network will certainly become infected with malware. Defenses that offer extensive visibility and breach detection are a must. You need to be able to recognize harmful actors instantly in order to eliminate malware. It calls for ongoing network inspection. You need to delete the virus from your network as soon as the danger has been recognized. Modern antivirus software is insufficient to defend against sophisticated online attacks. Find out how to upgrade your antivirus program.

## Impact of malware on computer system

The malware attacks can create negative impact in the security and privacy of the resource data present in the organization database. It is capable to crack the weak passwords, drill down into the system and can spread through the interconnected networks. The confidential and private information will be accessed and the same can be brought to public. Sometimes the attackers, demands huge ransom for not to leak the private information. The malwares can interrupt the business continuity and is capable of looking important files thus affecting the organization performance .

It is also capable to flood the webpage with lots of unwanted ads and contents thus slowing down the operations and making the user interaction low on the webpage. Thus in many case, it is noted that the web browser gets redirected to the malicious websites thus increasing the impact of attacks .

## Mode of malware infections

Phishing emails: A link will be sent to the user persuading him to click the link to get some attractive offers or benefits. The links looks legitimate to the user and so he without any suspicion will be clicking the link and on doing so, the page will be redirected and the malicious codes get automatically installed on the system. In other cases, while downloading any attachments, or else while opening up any attachments the malicious code gets installed.

Social network spam: This is the new aspect of malware attacks being practiced by the attackers. They aim at users who will be browsing the social sites and when they click upon any images or videos, it will be redirected to a website. The website looks legitimate and will persuade the user to download and install any video plugin to play any videos. On doing so, the malicious code gets installed into the PC and the attackers will be able to monitor and control the system functionalities .

## Remote Desktop Protocol:

In the recent times, remote management is gaining popularity as it enables virtual users to connect globally. This is mainly achieved by making use of the Remote desktop Protocol (RDP) and now the cyber criminals will be looking for computers that are open to RDP. They gain access to the remote connections by hacking the users credentials and will be able to proceed with illegal activities.

## Indications of malware infection

### Few notable symptoms include:

**Poor system performance**

The web pages will take too long to load and the normal system operations will be slow. The malwares are capable to freeze the system and hence it is noted in many cases that the system reboots all by itself. This will be frustrating for the users and it consumes long time of users.

**Corrupted/Missing files**

When the system is infected with malware, it is noticed that most of the files will be corrupted or some becomes inaccessible. Sometimes few files will be missing and it will be difficult for the admin to retain the same .

**Pop ups and Ad’s**

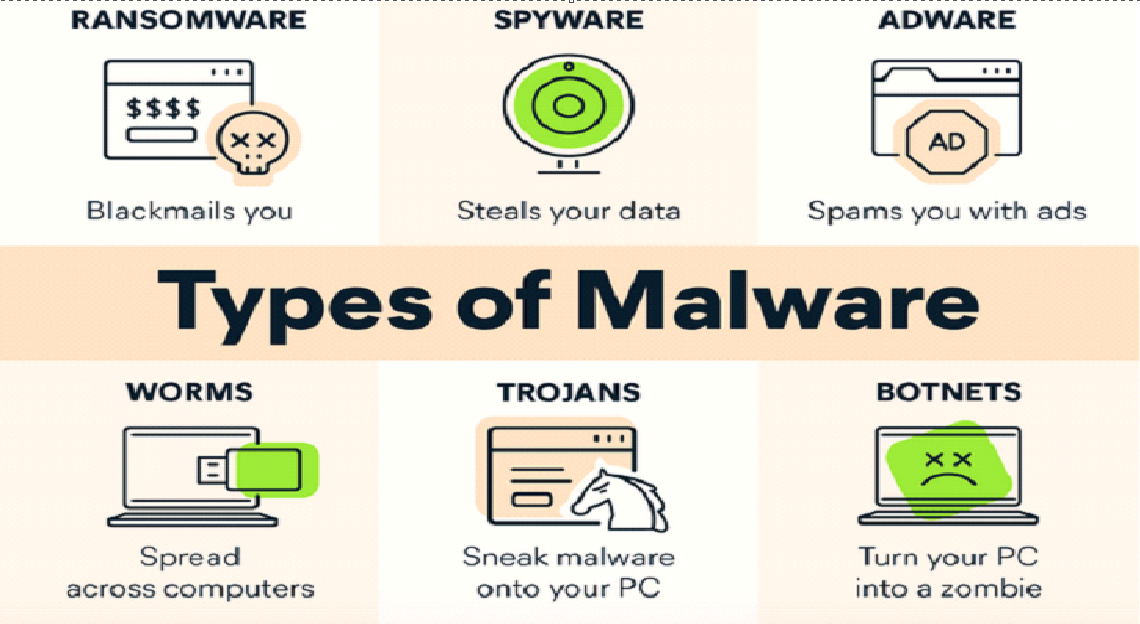
Amidst of the browsing activities, the user may note that several pop up appears and unwanted advertisement gets appears in the webpage. Lot of fake alerts and warning messages will be appearing in the screens which are the indication of the presence of malware in the computer. Also it is noted that the browser gest redirected to other pages of its own.

**Inappropriate system behaviour**

The malware is capable to gain access to the user’s contact list and send them messages in the user name. Sometimes, a ransom note will be displayed in the PC to get the files back and on scanning the computer one can view additional applications which the user has not installed. These are the clear indication that the system is affected with malware .

Types of malware attacks

**Ransomware** **attack** – This kind of malware attack deny the user form accessing his files and demands ransom to unlock the same.



This is a caption

**Spyware** – These kinds of malware attacks collects the complete information about the network and relay this data back to the attacker. Here the hacker will be getting the complete information about the victim’s computer and network details including the person’s internet activity, login credentials and financial information. Such information may be used by hackers for the purpose of identity theft or for financial fraudulent .

**Worms**- Worms are the kind of computer programs that replicates itself in faster rate and spread across the network in a higher speed. Some of the worms are capable to install additional malwares and harm the network performance. They will be occupying high memory space and system power thus leading to poor system performance.

**Adware** – They are the malwares that is responsible to send advertisements to the viewers and by making the viewers to view the ads, the hackers will be gaining revenue. The adware’s are capable of collecting the personal details of the users and customize the ads and sent it to them while the user is online.

**Trojans** – This is the kind of malware that impersonates as the legitimate software and gain access to the user system. Once the Trojan gets installed, it downloads malicious software into the system and does the harmful activities .

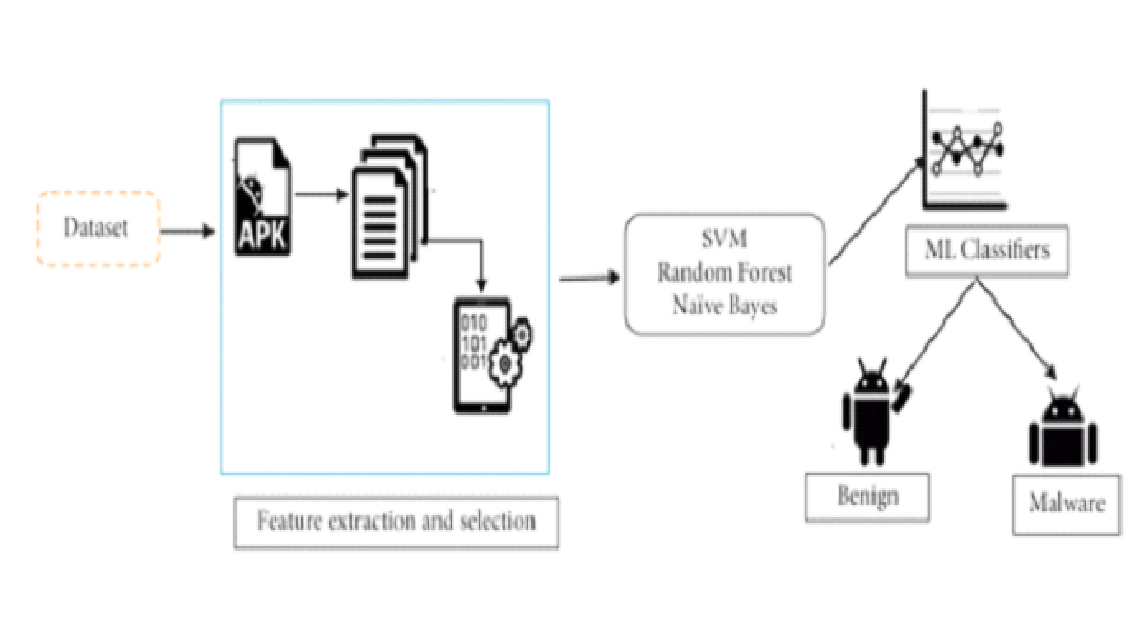
**Botnets** – Group of computers that are interconnected will carry out the malware activities, the hackers will be infecting the group of computers and the system will be under the hacker’s control. The system will be behaving based on the command given by the hacker.

**Research approach to detect malware in the network**

Modern technologies are much helpful to detect the presence of malware in the network and intimate the system admin about the same. The timey action will be much helpful to limit the spread of any infection and thus protect the resources.

Machine learning algorithms are much helpful to carry out detection process and when the algorithms are properly trained, they will be able to make up excellent detection to identify the threat either as malware benign.

The stage of operation of the research approach is dataset preparation, feature extraction and selection, Machine learning algorithm training that classifies the given sample as benign or malware .



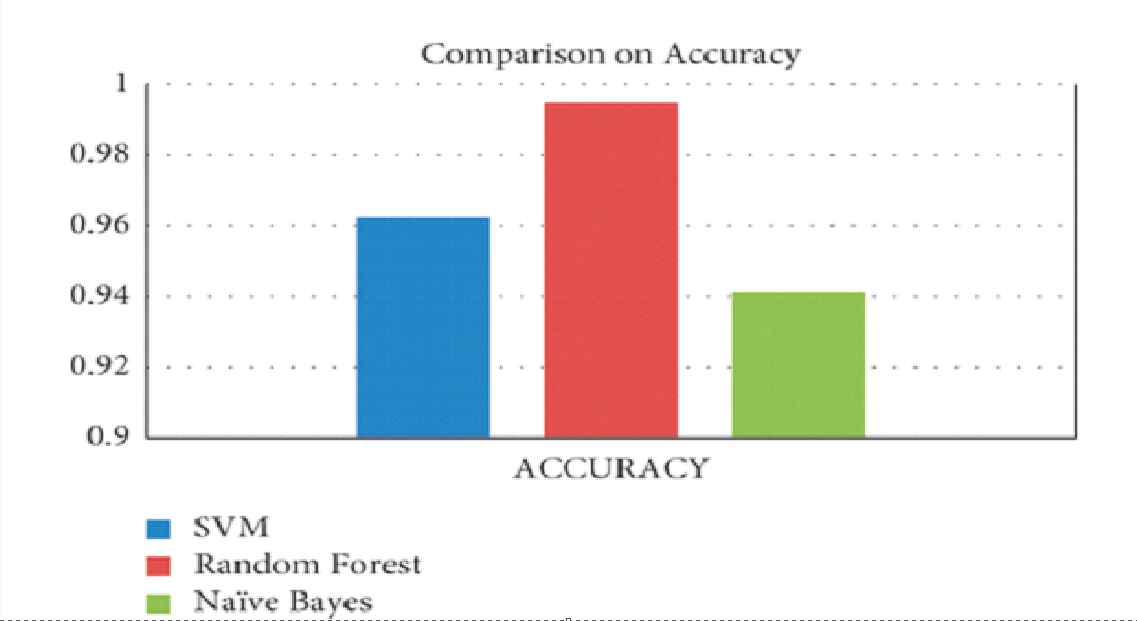
This is a caption

**Data Collection and Preprocessing**: The dataset has to be collected from the valid source like Kaggle and it should be the combination of threats as well as non-threats. For computation, the dataset is transformed to.csv format and the dataset allocation is done as 80% for training and the balance for testing.

**Feature extraction**: For the ML models to be trained effectively, it is necessary to identify the relevant features and to extract the same. This approach will enhance the quality of the dataset detection. The important features that are extracted in general are the user permissions, user specific intent filters, process name, file details etc. The extraction of the features is carried out using the reverse engineering concepts .

**Algorithm application**: For research purpose, three main ML algorithms like Random Forest, Naive Bayes, and Support Vector Machine is chosen for malware detection. The sample input is fed into each model to examine its detection and the accuracy is chosen as the performance metrics. On evaluating the accuracy score, one will be able to know the performance of the ML models.

**Result Analysis**: on looking into the accuracy score, it is noted that the Random Forest algorithm performs well as the accuracy of the same is around 98%, this proves the algorithm is well able to detect the malware present in the network .



This is a caption

**Security measures to prevent malware attacks**

**Anti-virus software’s**:  It is essential to install the anti-virus and anti-spyware software in all the computers. These tools will be much helpful to identify and remove the malware. Also it is noted that these tools are useful to audit the missing files and unauthorized additions.

**Strong authentication and authorization procedures**: Good password policies have to be designed to prevent the password attacks and it is recommended to go for multi authentication process for enhanced security. It is suggested not to save the computer passwords in the system. Access has to be granted only to the authenticated personals .

**Limited administrative controls** – There should be a control set in using the administrative privileges for browsing the web or to check the email. If any software to be installed, then the same can be done through logging using administrator credentials.

**Software update**: The software manufacturers will be updating their product and they will be releasing the patch files as and when required. These patch files contain the necessary supportive files to limit the infection and to avoid the cyber threats. Hence it is necessary to validate and install the new software patches.

**Access control to system:** For to strengthen the network security, it is suggested to implement firewall, Intrusion detection and prevention system, which will be acting as the wall to prevent the malware attacks. If any ports are opened, they have to be closed and unused protocols have to be disabled. It is necessary to remove the inactive user accounts and before installation of any software, the legitimacy of the same has to be double checked .

**Implementation of email security** – The email is the easiest entrance for the hackers to get into the network and hence it is necessary to scan all the necessary email messages including the attachments. Proper spam filters has to be set to reduce the unwanted emails.

**Suspicious activity monitoring**: The system should be continuously monitored for any abnormality. The incoming and outgoing traffic has to be monitored and it should be looked for aberrations.

**User Awareness** – The users should be given proper awareness on how to identify the malware threats and what possible actions they have to take when the attack is noticed.

**Conclusion**

Along with the advancement in technology, the cyber threats are also increasing and one of the prominent threats that are noted in this era is the malware attacks. It is the kind of malicious code that gets installed in the system and indulges in malicious activities. When the computer is infected, it shows numerous indications to denote the attack. Earlier the identification of attacks, the spreading of infection can be highly controlled and the resources can be saved. There are numerous malware types like worms, virus, trojan, ransom attacks etc. and there are several methods to detect the same. Though modern technology helps in detecting the malware attacks, it is necessary that the system admin and users should take necessary steps to ensure that the network is secured and strong to prevent the attacks. Some of the best practice includes installation of antivirus software, enabling access control, implementing firewalls, creating user awareness etc. By educating the users, they will be able to take timely actions to avoid becoming the victim of malware attacks.

**References**

Alkahtani, H., & Aldhyani, T. H. (2022). Artificial Intelligence Algorithms for Malware Detection in Android-Operated Mobile Devices. IEEE Access, 1-6.

Arunlal. (2019). Impact of Malware in Modern Society. Journal of Scientific Research and Development 2(3):, 593-600.

Avast. (2022). What is Malware? . Retrieved from avast: <https://www.avast.com/c-malware>

Baker, K. (2022, August 11). The 12 Most Common Types of Malware. Retrieved from crowdstrike: <https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/>

Brown, S. (2022). The Top 4 Ways Malware Is Spread. Retrieved from snaptechit: <https://www.snaptechit.com/article/the-top-4-ways-malware-is-spread-2/>

Burnap, P., & Wedgbury, A. (2021). Real-Time Malware Process Detection and Automated Process Killing. Open Access, 1-9.

Choudhary, S., & Sharma, A. (2020). Malware Detection & Classification using Machine Learning. 2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3), 1-9.

Cisco. (2022). Malware Protection Best Practices. Retrieved from cisco: <https://www.cisco.com/c/en/us/products/security/malware-protection-best-practices-detection-prevention.html>

Ding, Y., Yuan, X., & Tang, K. (2013). A fast malware detection algorithm based on objective-oriented association mining. IEEE Access, 315-324.

Harford, I. (2022). 10 common types of malware attacks and how to prevent them. Retrieved from techtarget: <https://www.techtarget.com/searchsecurity/tip/10-common-types-of-malware-attacks-and-how-to-prevent-them>

Hussain, A., Asif, M., & Ahmad, M. B. (2022). Malware Detection Using Machine Learning Algorithms for Windows Platform. Proceedings of International Conference on Information Technology and Applications, 619-632.

Kulshrestha, R. (2019). Malware Detection Using Deep Learning. Retrieved from towardsdatascience: <https://towardsdatascience.com/malware-detection-using-deep-learning-6c95dd235432>

Mcafee. (2022). What is malware? Retrieved from mcafee: <https://www.mcafee.com/en-in/antivirus/malware.html>

Megira, S., Pangesti, A. R., & Wibowo, F. W. (2018). Malware Analysis and Detection Using Reverse Engineering Technique. Journal of Physics: Conference Series, 1-12.

Pavithra, J., & Samy, S. S. (2022). A Comparative Study on Detection of Malware and Benign on the Internet Using Machine Learning Classifiers. Open Access, 1-8.

Here are 7 types of Malware :

**Virus:** Malware includes viruses as a subcategory. A virus is a piece of malicious software that is attached to a file or document and uses macros to run its code and propagate from one host to another. The virus will remain dormant once it has been downloaded until the file is used and opened. Viruses are made to interfere with a system’s functionality. Consequently, infections might result in serious operational problems and data loss.

**Worms:** Worms are a type of malicious software that spreads quickly to all devices connected to a network. Worms may spread without a host application, unlike viruses. A worm enters a system by a network connection or a downloaded file, where it then multiplies and spreads at an exponential pace. Worms, like viruses, can seriously impair a device’s functionality and destroy data.

**Trojan Virus:** Trojan viruses are camouflaged as functional software. But when the user downloads it, the Trojan virus has access to private information and can change, suppress, or remove the data. The performance of the gadget may be seriously harmed by this. Trojan viruses are not intended to multiply themselves, in contrast to common viruses and worms.

**Spyware:** Malicious software called spyware operates covertly on a computer and sends information to a remote user. Spyware targets sensitive information and can provide predators remote access rather than just interfering with a device’s functionality. Spyware is frequently used to steal personal or financial data. Keyloggers are a particular kind of malware that track your keystrokes and leak passwords and other private data.

**Adware:** Adware is harmful software that tracks how you use your computer so it can show you relevant advertising. While adware is not always harmful, it may sometimes interfere with your system. Adware may reroute your browser to risky websites and even include spyware and Trojan horses. A substantial amount of adware can also dramatically slow down your PC. It is crucial to have security that continuously and intelligently monitors these apps since not all adware is dangerous.

**Ransomware:** Ransomware is malicious software that accesses private data on a computer, encrypts it so the user cannot access it, and then demands payment in exchange for the data’s release. A ransomware attack sometimes includes a phishing fraud. The consumer downloads the malware by accessing a fake link. The attacker then goes about encrypting particular data that can only be decrypted using a mathematical key they are aware of. The data is opened after the attacker has been paid.

**Fileless Malware:** A kind of memory-resident malware is fileless malware. As the name implies, this virus runs from the computer’s memory rather than from data on the hard drive. It is more difficult to find than conventional malware because there aren’t any files to search. Due to the malware’s tendency to vanish after a reboot of the target machine, forensics is also made more challenging. The Cisco Talos threat intelligence team published DNSMessenger as an example of fileless malware in the latter part of 2017.

**Protect Against Malware :**

When it comes to safety, there are essentially two factors to take into account: user attentiveness and defensive tools. The first is sometimes the simplest to put into practice since best-in-class defensive software that controls and upgrades itself is frequently something you can set and forget. On the other side, users might be readily swayed by other emotions like fear or desire “Check out this wonderful website!” or  “install this antivirus software immediately”. The anti-malware programs have less of a chance of delivering their payload when the network, email, online requests, and other actions that can endanger your firm are continually monitored.

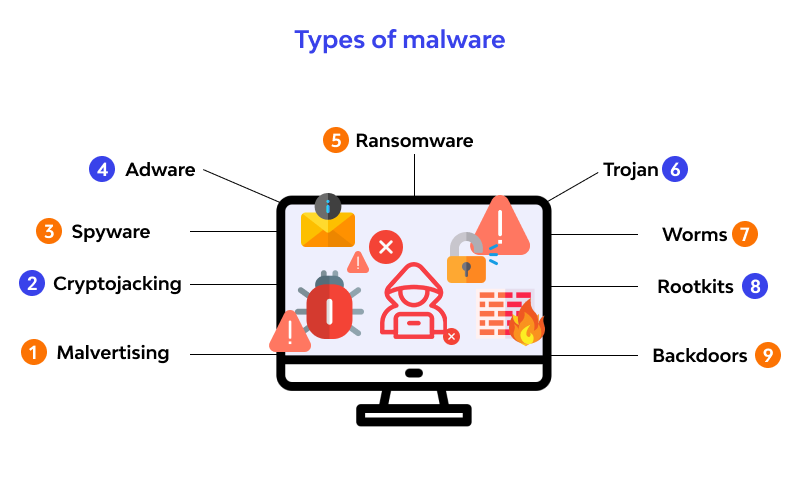


Fig is from google -only for reference

**Introduction**

The malware is the combination of the both the software and the malicious. The cyber criminals would develop the script or software which would destroy or damage the computer systems, networks, smartphones, etc. The damage occurrence will be of any type like browser hijacking, important files locking, performance degradation of the devices, etc. It has been existing in the form of virus (Namanya & Cullen, 2018). All the virus are said to be malware but all the malware are not virus. There has been different type of malware are available.

**Malware entry to devices**

Bundled software – while downloading the free software along with it malware application or anything will combine with it. It would be not be noticed by the users.

Peer to peer file sharing – the files will be shared through the torrent and it would act as a malware gateway for all the systems. The cyber criminals will usually change the original file with malware.

Intriguing pop-ups – several pop ups will raise while browsing through the websites like ads, banner, etc. by providing in the attractive manner. Once, it was clicked malware will enter into the systems.

Downloading from unknown source – from the unknown sources the paid version software will be downloaded for free. Such sources will mostly contains malware in it (Saeed, 2020).

Spam mails - the mails along with the malware will be shared to many users as a spam. When it was clicked automatically spam will be introduced into their system.

**Malware types**

§      Computer virus would affect the files and it would spread to all files in the system in the uncontrollable manner and damage or corrupt the files present in it.

§      The macro virus will affect the Microsoft office applications like excel, word, etc.

§      Router virus is present in the Wi-Fi and it would redirect the user to malware sites and obtained the personal information of the users in the tricky manner.

§      Trojans will act as legitimate software or hide with the software and enter into the devices.

§      Spyware is used to spy and collect the information about the users like passwords, financial data, etc.

§      Worms does not require any host file and spread in the systems and infect the entire device or network.

§      Ransomware is used for threatening the users by asking for the ransom by encrypting all the file that are present in the system (REHMAN, et al., 2011).

§      Logic bombs are used for execution after meeting the specific condition until that it would act as dominant.

**Identification of device infected with malware**

§      The device will be slow down completely without any reasons. It was because the malware will consume more power than other type of process.

§      In the devices the file will be downloaded and installed automatically so that there would be shortage of the storage space in the device.

§      Unwanted pop-ups will occur in the device in the unlikely manner and it would indicate malware is infected in the device.

**Prevention of malware attacks**

§      It is necessary that stranger’s device should not be trusted like strange emails, fake profiles, abrupt alerts, etc.

§      Before downloading the software or file it is necessary to double check download source.

§      The ad occurrence need to be blocked in the proper manner.

§      While browsing in the website need to be careful about the malware (.K.S., 2019).

§      It is necessary to update the software continuously to avoid security vulnerability occurrence.

§      Antivirus application need to be used in the device for providing a proper protection.

Malware is developed by cyber-criminals for stealing private data, gaining access to a personal computer, bypassing access controls, or harming the targeted data, its systems, or its applications. Due to the malware industry’s current high profitability, cybercriminals have increased their efforts, leading to an exponential increase in the quantity, variety, and complexity of malware produced. It is too difficult to detect malware mutations and their mutations by generic anti-virus software and it focuses on making the user and system vulnerable at the specified time. First-generation malware and second-generation malware are the major two categories of malware.

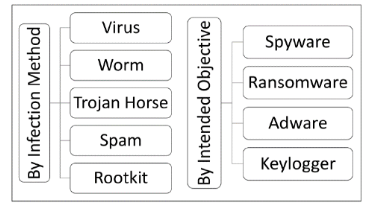


                                                                       Figure 3- Malware classifications

                                                                   Source - (Mohammed N. Alenezi, 2020)

The sophistication and severe malice of malware have increased, and it now generates billions of dollars in revenue. Malware’s initial design tended not to focus to generate profits or cause damage to data or other’s systems. At an earlier stage, all of the malware have the same characteristics. In the early phases, malware damage will be restricted to infected machines. Infected floppy discs were frequently used in the early stages of malware propagation. Windows operating system is focused on the second stage of malware evolution. In the evolution period, the windows operating system is a personal computer. Malware creators are focused on their attacks on operating systems. The spread of malware is high because of the usage of the Internet. Ease of connectivity and information exchange is a greater advantage of the internet. Microsoft’s macro language is taken by the malware authors for craft malware and infection methods will be varied in the second phase. The spread in the second phase will take place were sharing infected Microsoft files and also attackers send email attachments. Increased creation of network worms is witnessed in the third phase of malware. Email attachments and visits to compromised websites are the most common form of propagation for malware. The malware in this stage is distinguished by its exploitation of operating system flaws that are already present. Memory resistants like code red and network worms are executed when the OS loads. A file is required and it should be executed to infect the system in previous stages of the malware. Billion dollars of damage has happen in the third phase of the malware and it caught the media’s attention. SoBig.F and Conficker were making headlines. The fourth phase of malware is introduced with a rootkit that focused on stealth. The birth of ransomware is registered at this stage. Researchers focused on encryption techniques for ensuring data security. Attackers can pay and use the ransomware services using the payment services. The purpose of virtual espionage, the fifth stage of malware is introduced.

**Types of Malware**

**Virus** – All types of malicious code in the IT industry is the virus. It is attached to the program or file. It infects computer devices without users’ knowledge. It is spread to other devices with help of human action. Malicious code will be detected by using signatures and sandboxing, heuristics, behaviour monitoring, Artificial Intelligence, and emulations used by the AV companies.

**Worms** – Without human actions, worms can replicate itself from one system to other system. The network can be scanned by the worms and gather IP addresses of the network and replicate to other systems using these details.

**Trojan horse** – It claims to access legitimate user details and gain access to their systems to access private data. It misleads the software’s real intent so users can diversify their proper access. It is not having the ability to replicate itself. The attacker can access the system remotely when the legitimate user can activate the computer.

**Rootkits** – It has the ability to hide the files and processes from other applications, processes, AV engines so it is technically not malicious. A rootkit can be used by commercial companies for user behaviour restriction. For administration purposes, a rootkit is installed in the system. Attackers can gain remote access without any legitimate user information and it effectively avoids detection. It will be hidden in the system and steal the data from the infected system for years. User-mode rootkits and Kernel-mode rootkits are two categories of rootkits.

**Backdoors** – It is related to rootkits. The Backdoor opens for the attackers to gain access and they can steal data from the legitimate user system. Unauthorized access will happen once the rootkit is installed in the system (.K.S., 2019). Like rootkits, backdoors allow hackers to enter the system and gain access remotely.

 The  malware detection can be more structured when there is less scope for the virus that is being attacked or exploited with all necessary changes done on the system exploitation properties.

 Different types of Malwares:

**1.Ransomware:**

Software known as ransomware employs encryption to prevent a target from accessing its data unless a ransom is paid. There is no certainty that the victim group will be completely or partially unable to operate until it pays. Payment will yield the required decryption key, or the given decryption key will work as intended.

**2.Fileless Malware:**

Malware that is “fileless” doesn’t initially install anything; instead, it modifies files that are inherent to the operating system, such PowerShell or WMI. A fileless assault is not detected by antivirus software because the operating system perceives the modified files as genuine. These attacks are stealthy and up to 10 times more effective than conventional malware attacks.

**3. Keyloggers:**

A sort of spyware that keeps track on user activities is a keylogger. Keyloggers may be used in acceptable ways by businesses to keep an eye on employee conduct and by families to monitor their children’s internet activities. However, keyloggers may be used to steal financial information, sensitive information, and password data when installed for nefarious purposes. Through phishing, social engineering, or malicious downloads, keyloggers can be installed on a machine.

**4. Rootkits:**

A root kit is software that allows malevolent users to take complete administrative control of a victim’s computer from a distance. Applications, kernels, hypervisors, and firmware may all be compromised to introduce rootkits. Phishing, malicious attachments, malicious downloads, and infected shared folders are some of the ways they propagate. Keyloggers and other types of malwares can be hidden using rootkits.

**5.Worms:**

Worms use operating system flaws as their entry points into networks. They could get in via flash drives, inadvertent programme flaws, or backdoors integrated into the software, among other methods. Worms can be used by hostile actors to execute DDoS assaults, steal confidential information, or carry out ransomware operations once they have been installed.

**6. Trojan:**

A Trojan cloak itself as desired software or code. The Trojan can take control of victims’ systems for harmful reasons after being downloaded by unwary users. Trojans can conceal themselves in software patches, games, apps, and even applications themselves, or they can be found in the attachments of phishing emails.

**7.Adware:**

Adware monitors a user’s browsing habits to decide which advertisements to show them. Adware is similar to spyware, except it doesn’t install any programmes or record keystrokes on a user’s computer. Adware poses a threat to user privacy because it gathers information about a user’s online activities, whether overtly or covertly, and uses that information to build a profile of that person that includes information about their friends, purchases they’ve made, travels they’ve taken, and other things. Without the user’s permission, this information may be sold or shared with advertising.

**Reference:**

Tathagat (2021) Essential Cyber Security Concepts, CYBERVIE. Available at: <https://www.cybervie.com/blog/essential-cyber-security-concepts/> (Accessed: December 8 2022).

# Cyber Security and Cloud Computing

The term “cybersecurity” encompasses all relevant aspects of security. The management depends on a combination of technology and advice to secure the cloud. It involves managing the framework, information applications, safe-secure guidelines, consistency leaders, and secure infrastructure data applications that pertain to cloud computing. The same principles that underpin security for modern cloud computing platforms and historic knowledge centers are secrecy, integrity, and usability. Every physical and logical security risk in relation to the various service models of code, platform, and infrastructure is addressed by cloud computing security. Additionally, it discusses how these services are provided (public, private, or hybrid delivery model).

There is no question that “cloud technology” is more secure than “conventional or native servers” when compared. The opinions could diverge, though, if we examine the levels of security between public, private, and hybrid cloud delivery methods. Clients would want the highest level of security assurance before they shared their sensitive information with a third-party cloud provider, which makes the cloud’s core functionality more pertinent in the context of safety.

Here are five things you need to see to basically get started:

**Network Segmentation:** Examine strong zone access to isolate information, objects, devices, and whole systems from one another where practical. It is intended to prevent any threat actor from moving their targets during an attack or incorrectly associating different systems.

**Cloud-based Access Controls:** Access to management lists should be available for all areas of cloud computing. It is more practicable than it is for one foundation to describe and apply the appropriate approach to management since services sort of information will start out multiple times. It incorporates any virtual basis, effective systems, programs, and even instruments used to monitor the situation.

**Multi-tenancy in Cloud Computing:** While multi-holding offers purposeful ascent and analysis assistance, there is also a danger of information loss and inaccurate navigation, which may not be controllable in the cloud. Consider policy compass and association management in a highly multi-holding situation for any account that will have an association across holders.

**Cloud Access Management:** Need to manage the influential association to any or all cloud impacts as well as look at disaster improvement and any deficiencies in your excellent association chance. These days, when we countersign administration clarification and administrator accounts, we tend to feel appreciated. Although we “want” the unique method in the cloud, we don’t want cloud administrator rights to be available everywhere.

**Cloud Computing Threats and Liability:** The assertion of responsibility is completed using the operator and other combination technologies, however, this impression simplifies one for one from one assertion operation. After analysis, they must be quickly computed for victimization threat brilliance and submitted.

Security measures used to protect the cloud are referred to as cloud computing security. Cloud computing is an attitude to computing rather than a technology; it incorporates all available computing methods. Therefore, handling the complex and vast side of cloud computing security may be necessary. The complexity and complexity of security issues in cloud computing are perhaps even more sophisticated and perplexing than cloud computing itself. Strangely, many security issues with cloud computing don’t seem to be tech-related; instead, strategic higher cognitive process and human aspects are typically involved.

References : <https://gca.isa.org/blog/cloud-computing-and-cybersecurity-everything-you-need-to-know#:~:text=Cloud%20cybersecurity%20requires%20tools%2C%20data,and%20infrastructure%20within%20your%20company>

Understanding the risks of cyberspace and the significance of public education can help prevent attacks before they occur. In the world of cyber security, identifying possible security hazards is a challenging task. The predominance of extensive multidisciplinary links and sophisticated entity-to-entity relationships are the primary sources of this issue .In today’s financial institutions, operational, tactical, and strategic levels of cyber threats can be distinguished, according to our findings. The three pillars of information security are privacy, reliability, and accessibility(Mehrban et al., 2020).

Financial technology companies are readily identifiable by their unique technological applications. In 2015, global spending on financial technology increased by 75 percent to $22.3 billion (Accenture, 2016). Financial technology (FinTech) firms assure the security of a variety of financial products and services, including credit, currency exchange, international money transfers, two-factor authentication, and payment protection solutions for mobile apps, e-commerce, and financial advising. The introduction of financial technology (FinTech) has had an impact on businesses outside of finance, such as accounting software and practises (ACCA, 2016a). For instance, several of the more recent FinTech companies provide aid with retail banking, fraud detection, and wealth management. Businesses are “reformulating the design and delivery of services” due to technological improvements and advancements in apps, user experience, and data mining. Accounting and lending technologies are used to simplify the loan application procedure (KPMG, 2015). Therefore, there is an opportunity for auditors to refocus their clients’ attention to other lucrative services. Cloud computing poses risks to data and privacy, but the legal, tax, and financial ramifications of the FinTech industry present opportunities for the accounting profession (ACCA, 2016a). The objective of a distributed denial of service (DDoS) attack is to make an online resource inaccessible by bombarding it with requests from multiple users simultaneously. Because banks, news outlets, and government databases are major targets, it is impossible for citizens to freely debate sensitive matters or undermine authority.

Those behind these assaults may have a number of purposes and motivations, including intellectual challenges, cyberwarfare, network slowdowns, and the theft of personal information or money. There are a variety of detecting technologies available to prevent these security breaches. Among these are signature-based, hybrid, and anomaly-based techniques.

**MEHODOLOGY**

Due to the rising cloud computing cyber security business, financial institutions in developed economies can protect themselves from cybercrime. Cyber security relies significantly on threat classification, but as the breadth of the service model increases, it becomes more difficult to accurately characterize risks. Miscommunication regarding potential threats might incur time and financial costs. Cyber security is a fantastic alternative for FSIs since it reduces the likelihood of cyber-occurrences and increases the rate of success for those defending against cyber-attacks. Consequently, many nations consider cyber security as a formidable obstacle to cloud computing.

## BASIC ASPECTS OF CYBER SECURITY IN CLOUD

As a starting point for our discussion of cyber security, we may argue that cloud administration security must be at least as strong as what system administration already offers clients through their integrated system frameworks. It’s a tried-and-true (and obvious) argument, but it’s so essential that it bears repeating. Therefore, it is essential for a cloud service provider to comprehend the following perspectives:

·         Regular upgrades to firmware, OS frameworks, and app stores compel cloud service providers to always seek compatibility enhancements. Incompatible updates may contribute to cloud problems. Therefore, a function to “roll back” the system to a previous, safe state should be available.

·         It is necessary to differentiate data amongst virtual machines running on the same physical host. In addition, new protective shells for hypervisors are required.

·         In a cloud-centric paradigm, the immense potential for unified administration is articulated differently. Operations such as heap-editing and security-hardening are being offloaded from the administrator’s central processing unit (CPU) to the cloud, where they can be carried out by very accurate computers located in widely distributed data centers (Sherryl, et al . 2013). As the cloud foundation may be a network of mists, it is crucial that prior core boxes are distributed and assisted throughout verifiable device locations. Consequently, the middle boxes can be utilized alongside the new safe spaces.

·         For both customers and suppliers, authentication and trust technologies are important. Then, it could serve as a catalyst for action. Email spam regulation is another advantage of cloud computing (for example, spam could be reviewed & sifted in hypervisor-related VS). Use of tools such as Sender Policy Framework (SPF) to validate the legitimacy of each email’s sender and the Apache Spam Assassin Project to categories, rank, and route undesirable communications are potential solutions for reducing cloud-based spam(Wong, 2006).

·         To allow communications between various cloud assets/has (often from incontestable providers), the cloud provider’s assets/has should be nearest in a consistent virtual private network (VPN) burrow path, such as that of a closed neighborhood arrangement. The Virtual Private Cloud (VPC) solution from Cloud Net combines CC and VPN technologies to provide users with access to a shared pool of cloud computing resources. (Wood, 2011).

·         Cloud-based administration is available whenever it is required. As soon as this is finished, we must take additional measures to prevent unauthorized individuals from entering. Infected consumer devices participate in distributed denial of service (ddos) assaults, resulting in a substantial amount of erroneous traffic. In an effort to prevent it from having a negative impact on the implementation of the circulation process, which has a “dark beginning,” the cloud infrastructure will attempt to detect the circulation and then dispose of it with the machine.

## 

## Cloud Computing Help to Improve Cyber Security

As more businesses migrate their activities online, the necessity to safeguard cloud-based infrastructure and data increases. In order to secure the dependability and durability of a network’s backbone, cloud security frequently employs many layers of protection. It is a major aspect that makes the world conducive to commercial enterprise. If your business contracts with a modern private cloud storage provider, it may enjoy the cost-savings of cloud computing without losing data security.

Using cloud security has numerous benefits, including:

***Data security***

It is necessary to take additional safeguards when transmitting and storing sensitive data in the cloud, given the prevalence of data breaches in the current world.

***Protection against DDoS***

The most effective security solution is preventing DDoS attacks on a company’s cloud server. By modelling, storing, and releasing simulated distributed denial of service (DDoS) attacks, one can practice defenses against DDoS attacks.

***Regulatory compliance***

The most cost-effective cloud computing security solutions safeguard the privacy and security of sensitive client data for businesses in highly regulated industries.

***Flexibility***

Whether your organization is expanding or declining, a cloud storage solution can provide the necessary security. Increasing the capacity of your cloud service before peak demand may prevent server outages. By downsizing, you can free up some funds.

***Centralized security***

Similarly to how cloud-based apps and data are centrally kept, so is cloud-based security. It is difficult to monitor cloud-based corporate systems in this era of omnipresent mobile devices and Wi-Fi hotspots because employees embrace shadow IT and bring-your-own-device policies. By centralizing the management of these communities, better traffic and page filtering, simpler network event monitoring, and less frequent policy and program changes are made possible. Regarding planning and implementing a business continuity strategy, there is no need to reinvent the wheel.

**Reduced Administration**

With the assistance of a cloud service provider or cloud security platform, you may regulate the frequency of automated updates and the safety of your data. It is feasible to save a significant amount of money and increase security by storing and managing your own data on the cloud.

**Reliability**

When required, cloud services may be counted upon to always be accessible. Cloud computing enables users to access their files and applications from any device, anytime, so long as they take the necessary safeguards to prevent data loss.

**Proposed Method for DDOS Attack Detection**

The complexity of detecting DDOS attacks can be reduced to two classes. In the sections that follow, we will investigate what distinguishes malicious network activity from benign network traffic. The suggested method for detecting DDOS attacks is represented in the figure below. The development of a novel approach involves two stages: training and testing. During the training phase, system models are utilized, and during the testing phase, a smart controller collects real-world traffic data. Every system has four primary components: data collection (traffic), feature normalization (features), feature classification (features), and testing (features). Next, I will delve deeper into each topic.

**Fetch traffic data**

The controllers of a network are responsible for coordinating the operations of the switches that connect specific hosts to the system. In a software-defined networking environment, it is now possible to build virtual networks (Sezer et al., 2013). Using the entropy metric to extract data from network traffic will reveal suspicious traffic, which can then be normalized for classification and use by other system components. The entropy of a property can be used to define its boundaries or assess its relevance. If network traffic exceeds a specified threshold during a given time frame, the system will gather data from all hosts connected to the same switch (Nife et al., 2018). Mininet, whose network architecture is depicted in Figure 2, has been utilized throughout. Mininet enables us to develop our own network architecture and assess its performance in a variety of realistic scenarios. In this design, a single smart Pox controller controls nine different switches. The POX controller can run eight separate switches using a single switch (Prete et al., 2014).

**Feature normalization**

If the average entropy measurement provides meaningless findings, it is possible that the data are not relevant. First, we will remove any empty or 0-filled rows. Keep safe and unsafe traffic separate. Then, we filter features based on their entropy levels to identify those that fall inside a predetermined threshold. Normal traffic is presumed if an instance falls within the permitted range; otherwise, it is labelled as abnormal. Four major feature categories are Time-based network traffic entropy analysis (TBNETA), Transmission Control Protocol (TCP) basic features (TBPF), TCP content features (TBCF), and host-based network traffic analysis (HNTA). The data will then be sent to a classifier, which will classify incoming traffic. Transform the standard data into an entirely arbitrary arrangement.

**Classification**

SVM is frequently applied to the classification problem, particularly for binary classes, due to its excellent prediction ability in a variety of scenarios .Using SVM with an RBF kernel made it possible to apply the classification issue to a large variety of data. At the conclusion of the proposed procedure, an SVM model with an RBF kernel was developed and assessed.

**DISCUSSION**

Companies making the switch to the cloud must implement cloud-based security. Changes in the nature of security threats render all networks susceptible to intrusion. There is mention of “the cloud” here. If you’re concerned about the security of your cloud-stored data, it’s essential to pick a provider with advanced protections that can be tailored to your system.

As technology improves, the rising frequency of cloud-based services and applications will make network management more difficult. The fundamental objective of this study is to get an understanding of a well-known type of cloud-based DDoS attack. Numerous research teams must exert considerable effort to develop cutting-edge DDoS detection, categorization, and defense techniques. The proposed approach for defending against DDoS attacks was also examined. On the basis of our findings, we feel that machine learning-based solutions offer the maximum degree of precision. As a result of the IoT’s persistent efforts to transform cloud computing, cloud security is now at risk. To create effective approaches for spotting cloud-based distributed denial of service (DDoS) attacks, additional study is required.

**CONCLUSION**

In the cloud computing model, since fewer people are directly accountable for the supply of certain services, more people have access to those resources. The user is capable of storing and analyzing the information acquired online. Cybersecurity must be a major consideration for organizations developing financial technologies. Authorities are concerned about the possibility of hacking, and this has increased the significance of protecting customers’ and businesses’ financial information. The internet financial sector is increasingly susceptible to DDoS attacks, which often target publicly accessible websites. As cloud computing evolves, the rising prominence of cloud-based services and apps will make network management more difficult. Companies considering a migration to the cloud must implement cloud-based security. Cloud computing is just as susceptible as any other environment to the ever-evolving and more sophisticated security threats that exist today. This emphasizes the need of collaborating with a cloud service that offers superior, granular security choices. The major objective of this study is to get an understanding of the ubiquitous threat that distributed denial of service (DDoS) attacks provide to the cloud computing industry. Numerous research teams must exert considerable effort to develop cutting-edge DDoS detection, categorization, and defense techniques.

REFERENCES

 [1] H. Yin and K. Gai, “An empirical study on preprocessing highdimensional class-imbalanced data for classification,” in Proc. IEEE 17th Int. Conf. High Perform. Comput. Commun., IEEE 7th Int. Symp. Cyberspace Saf. Secur., IEEE 12th Int. Conf. Embedded Softw. Syst., Aug. 2015, pp. 1314–1319

[2] S. Mehrban et al., “Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges,” in IEEE Access, vol. 8, pp. 23391-23406, 2020, doi: 10.1109/ACCESS.2020.2970430.

[3] Vaquero, L.M., Rodero-Merino, L., Moran, D.. 2011. Locking the sky: a survey on IaaS cloud security. Computing 91(1), 93-118.

[4] ACCA, (2016a), “FinTech – transforming finance”, September, <http://www.accaglobal.com/content/dam/ACCA_Global/Technical/Future/FinTech-transformingfinance.pdf>

[5] ACCA, (2016b), “Professional accountants – the future: Drivers of change and future skills”, <http://www.accaglobal.com/content/dam/members-beta/docs/ea-patf-drivers-of-change-and-futureskills.pdf>

[6] Accenture, (2016), “The future of Fintech and banking: digitally disrupted or reimagined”, <https://www.accenture.com/au-en/insight-future-fintech-banking>.

[7] Pan, G., Seow, P.S., (2016), “Preparing accounting graduates for digital revolution: A critical review of IT competencies and skills development”, February, Journal of Education for Business, 91(3), 166-175.

[8] Gibbs, S., (2014), “Cybersecurity break-ins a ‘daily hazard while firms skimp on protection’, <https://www.theguardian.com/technology/2014/jun/03/cyber-security-break-in-firms-protectioncryptolocker>.

[9] Bullock, L., (2017), “Australian accountants top global tech chart”, Accountants Daily, <https://www.accountantsdaily.com.au/technology/10113-australian-accountants-top-global-tech-chart>

[10] Navaretti, G. B., Calzolari, G., Mansilla-Fernandez, J. M., & Pozzolo, A. F. (2018). Fintech and Banking. Friends or Foes?. Friends or Foes.

[11] Puschmann, T. (2017). Fintech, Business & Information Systems Engineering, Vol 59, No 1

[12] Callen-Naviglia, J. & James, J. (2018). Fintech, RegTech and the Importance of Cybersecurity. Issues in Information Systems, Volume 19, Issue 3.

[13] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012

[14] Bina Kotiyal, R H Goudar, and Senior Member, A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena, IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2016

[15] Erdogmus, H. 2019. “Cloud Computing: Does Nirvana Hide Behind the Nebula?,” IEEE Software (26:2), pp 4-6.

[16] Abusitta, A., M. Bellaiche, and M.J.J.o.C.C. Dagenais, An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment. 2018. 7(1): p. 9.

[17] Prete, L.R., et al. Simulation in an SDN network scenario using the POX Controller. in 2014 IEEE Colombian Conference on Communications and Computing (COLCOM). 2014. IEEE.

[18] Sezer, S., et al., Are we ready for SDN? Implementation challenges for software-defined networks. 2013. 51(7): p. 36-43.

[19] Nife, F., Z. Kotulski, and O.J.A.M.I.S. Reyad, New SDN-oriented distributed network security system. 2018. 12(4): p. 673-683.

[20] Abeshu, A. and N.J.I.C.M. Chilamkurti, Deep learning: the frontier for distributed attack detection in fog-to-things computing. 2018. 56(2): p. 169-175.

[21] Wood, Timothy, K. K. Ramakrishnan, Prashant Shenoy, and Jacobus van der Merwe. 2011. CloudNet: Dynamic Pooling of Cloud Resources by Live WAN Migration of Virtual Machines. Proceedings of the 7th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments. New York, NY, USA: ACM, 2011, 121-132

[22] Sherry, Justine, Shaddi Hasan, Colin Scott, Arvind Krishnamurthy, Sylvia Ratnasamy, and Vyas Sekar. 2012. Making Middleboxes Someone else’s Problem: Network Processing As a Cloud Service. Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. New York, NY, USA: ACM, 2012, 1324.

[23] Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, and Muttukrishnan Rajarajan. 2013. A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications 36, n.º 1 (#jun# 2013), 42-57.

[24] Fernandes, D., et al.. 2014. Security issues in cloud environments: a survey. Int. J. Inform. Sec. 13 (2), 113–170.

[25] Subashini, S., and V. Kavitha. 2011. Review: A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Network and Computer Applications (Academic Press Ltd.) 34, n.º 1 (#jan# 2011), 1-11.

[26] Abusitta, A., M. Bellaiche, and M.J.J.o.C.C. Dagenais, An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment. 2018. 7(1): p. 9.

[27] Alzahrani, S. and L. Hong. Detection of distributed denial of service (DDoS) attacks using artificial intelligence on cloud. in 2018 IEEE World Congress on Services (SERVICES). 2018. IEEE.

[28] Idhammad, M., et al., Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest. 2018. 2018.

[29 ]   K.S., A. (2019). Impact of Malware in Modern Society. *Journal of Scientific Research and Development , 2*(3), 593 - 600.

[30] Certmike. (2022). *Confidentiality, Integrity and Availability – The CIA Triad*. Retrieved from certmike: https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/

[31] Chen, C., & Hui, Z. (2020). Computer Network System Security Management and Maintenance Strategy.  *Journal of Physics Conference Series, 1533*(2), 1 - 7.

[32] Dayalan, M. (2019). Cryptography in Computer Security . *Journal of Emerging technologies and innovative research [JETIR], 6*(5), 185 - 189.

[33] El-Taj, H. R. (2015). Intrusion Detection and Prevention Systems (IDPS) State of Art. *International Journal of Computer Science and Information Security (IJCSIS),, 13*(9), 28 - 35.

[34] Fisher, T. (2022, Sep 15). *SHA-1: What It Is & How It’s Used for Data Verification*. Retrieved from Lifewire: https://www.lifewire.com/what-is-sha-1-2626011

[35] Florian Mendel, T. N. (2011). Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions. *International conference on the Theory and Application of Cryptology and Information Security* (pp. 288-307). SpringerLink .

[36] Github. (2022). *The 3 Pillars of Cyber Security*. Retrieved from github: https://github.coventry.ac.uk/pages/CUEH/245CT/1\_Introduction/SecurityConcepts\_Pillars/

[37] Gupta, P., & Kumar, S. (2014). A Comparative Analysis of SHA and MD5 Algorithm . *International Journal of Computer Science and Information Technologies, 5*(3), 4492 - 4495.

[38] Hullatti, P. M., & S, S. (2014). Design and Implementation of Cryptography Hash Function. *International Journal of Engineering Research & Technology (IJERT), 3*(5), 1593 - 1596.

[39] LAKE, J. (2022, Feb 17). *What is SHA-2 and how does it work?* Retrieved from Comparitech: https://www.comparitech.com/blog/information-security/what-is-sha-2-how-does-it-work/

[40] Marin, G. (2005). Network Security Basics. *IEEE Security and Privacy Magazine , 3*(6), 68 - 72.

[41] Mishra, S., Mishra, S., & Kumar, N. (2013). Hashing Algorithm: MD5. *International Journal for Scientific Research & Development, 1*(9), 1931 - 1933.

[42] Namanya, A. P., & Cullen, A. J. (2018). The World of Malware: An Overview. *2018 IEEE 6th International Conference on Future Internet of Things and Cloud* , 420 - 427.

[43] Paul. (2022). *What is Cyber Security? – A Beginner’s Guide to Cyber Security.* Retrieved from https://www.edureka.co/blog/what-is-cybersecurity/

[44] REHMAN, R., HAZARIKA, G., & CHETIA, G. (2011). MALWARE THREATS AND MITIGATION STRATEGIES: A SURVEY . *Journal of Theoretical and Applied Information Technology , 29*(2), 69 - 73 .

[45] Saeed, M. H. (2020). Malware in Computer Systems: Problems and Solutions. *International Journal on Informatics for Development, 9*(1), 1 - 8.

[46] Seemma P.S, N. S. (2018). Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 5.

[47] Sharma, S., & Gupta, Y. (2017). Study on Cryptography and Techniques. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2*(1), 249-252.

[48] Singh, A. (2020). hash functions. *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems, 2*, 1 - 8.

[49] Sobti, R., & G.Geetha. (2012 ). Cryptographic Hash Functions: A Review . *IJCSI International Journal of Computer Science Issues, 9*(2), 461 - 479 .

[50] Tasneem, A., & Kumar, A. (2018 ). Intrusion Detection Prevention System using SNORT. *International Journal of Computer Applications , 181*(32), 21-24.

[51] Tiwari, M., Kumar, R., & Bharti, A. (2017). INTRUSION DETECTION SYSTEM. *International Journal of Technical Research and Applications, 5*(2), 38 - 44 .

[52] Brooks, Ryan, and Ryan Brooks                                                                                        Product Evangelist at Netwrix Corporation. “The CIA Triangle and Its Real-World Application.” The CIA Triad and Real-World Examples, Netwrix Blog Insights for Cybersecurity and IT Pros, <https://blog.netwrix.com/2019/03/26/the-cia-triad-and-its-real-world-application/>.

[53] “What Is the CIA Triad? Definition, Importance and Examples.” Intellipaat Blog, 25 Nov. 2022, <https://intellipaat.com/blog/the-cia-triad/#4>.

[54] Prakash, M. (2022, December 3). *CIA Triad in cyber security: Definition, examples, importance*. KnowledgeHut. Retrieved December 11, 2022, from https://www.knowledgehut.com/blog/security/cia-in-cyber-security

.K.S., A., 2019. Impact of Malware in Modern Society. *Journal of Scientific Research and Development ,* 2(3), pp. 593-600.

Abdalbasit Mohammed, N. V., 2019. A Review Paper on Cryptography. *International Symposium on Digital Forensics and Security (ISDFS).*

Anjali Krishna A, M. L. C., 2020. A Study on Cryptographic Techniques. *International Journal of Scientific Research in Computer Science Engineering and Information Technology,* 6(4), pp. 321-327.

Azhagiri Mahendiran, R. A. K. S., 2015. Intrusion Detection and Prevention System: Tchnologies and Challenges. *International Journal of Applied Engineering Research ,* 10(87), pp. 1-12.

Coulibaly, K., 2020. An overview of Intrusion Detection and Prevention Systems. *Computer Security and Reliability .*

H. B. Pethe, S. R. P., 2016. An overview of Cryptographic Hash Functions MD-5 and SHA. *IOSR Journal of Computer Engineering (IOSR-JCE),* pp. 37-42.

Macharia, W., 2021. Cryptographic Hash Functions. *Computer Security and Reliability .*

Mangore Anirudh K, M. R. M., 2019. Efficient Cryptographic Encryption Techniques for Data Privacy Preservation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* 8(7S).

Mohammed N. Alenezi, H. A. A. A. A. a. M. M. A., 2020. Evolution of Malware Threats and Techniques: A Review. *International Journal of Communication Networks and Information Security (IJCNIS) ,* 12(3).

Pandey, S., 2011. MODERN NETWORK SECURITY: ISSUES AND CHALLENGES. *International Journal of Engineering Science and Technology,* 3(5).

Prabhakar, S., 2017. NETWORK SECURITY IN DIGITALIZATION: ATTACKS AND DEFENCE. *INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS,* 5(5), pp. 46-52.

Rajeev Sobti, G., 2012. Cryptographic Hash Functions: A Review. *IJCSI International Journal of Computer Science Issues,* 9(2).

S.K. Shaw¸ M. Jain, J. S. D. R. V. P. M., 2016. A proposed design for secure hash algorithm-2 (SHA-2) using 640 bits. *International Journal of Pharmacy and Technology,* 8(4), pp. 26515-26523.

Sagar, F. A., 2016. Cryptographic Hashing Functions - MD5. pp. 1-9.

Shweta Mishra, S. M., 2013. Hashing Algorithm: MD5. *IJSRD - International Journal for Scientific Research & Development,* 1(9).

Surbhi Gupta, N. G. K. A., 2014. A Review of Comparative Study of MD5 and SSH Security Algorithm. *International Journal of Computer Applications ,* 104(14), pp. 1-4.

# Intrusion Detection & Prevention

 An intrusion detection and prevention system are a network protection mechanism that continually analyzes network activity for unusual activity and takes preventative measures. In addition, Intrusion Prevention System technologies are highly successful in detecting and preventing vulnerability exploitation. When a vulnerability is found, threat actors often have a window of opportunity to exploit it before a security fix can be implemented.

The intrusion detection and prevention are the two different methods used for the security purposes and mitigating the threats. The intrusion detection systems is used for identifying and mitigating the attacks. It would include of malware, social engineering attacks. Another method is intrusion prevention the security measure would be taken to block the attack occurrence (El-Taj, 2015). This would include SQL injections, malware injections, etc.

the intrusion detection system can perform better when there is less scope for the identification of each mitigation that can be easily be structured based on the type of the malware injections done.

Generally, firewalls mitigate risk, allow/deny traffic, ensure access control based on rules, and provide a defense strategy over the network for your host system. HIDS(Host Intrusion Defense System) defends the OS. Firewalls prevent suspicious traffic and keep your network/system safer from unwanted events. However, they are not foolproof from the evolving cybercriminal techniques. Intrusion Detection and Prevention will bolster your system. Detection techniques like monitoring threshold triggers red flags when a certain suspicious pattern is detected.

In short, IDP helps detect suspicious activity and provides security measures to avoid/prevent the attack. Primarily, there are four types of intrusion prevention systems

Network-based Intrusion Prevention

Wireless Intrusion Prevention

Network Behavior Analyst

Host-based intrusion prevention system

Network-based Intrusion Prevention: In this method, IDPS monitors inbound and outbound traffic, it detects suspicious activity by analyzing network protocol activities.

Wireless Intrusion Prevention: In this method, IDPS monitors wireless inbound and outbound traffic, it detects suspicious activity by analyzing the wireless network

Network Behavior Analyst: It looks for unusual traffic and detects DDoS attacks

Host-based Intrusion Prevention System: Monitors activities of a single host and detects malicious activity.

References: What is IDPS or Intrusion Detection and Prevention System? - The Security Buddy

**Intrusion detection systems [IDS]**

The IDS is the software application or the hardware device it make use of the intrusion signatures for both the detection and analyzing the network in the inbound and outbound traffic for all the abnormal activities.

It would be carried out in the different forms are

§      The comparison of the file systems against the malware signatures.

§      The harmful patterns would be detected through the scanning processes.

§      The behaviour of the users will be monitored for detecting the malicious intent.

§      The setting and configurations of the systems need to be monitored.

Once the security policy violation, configuration error the IDS will be start to kick off the user from the network and alert will be sent to the corresponding user. In this there has been three types present.

Network intrusion detection system [NIDS] – it was an independent platform which would examine the traffic occurrence in the network and monitor the hosts. The access will be obtained by connecting with network hub, configured with the network switch for monitoring the port, etc. the example of this method is snort.

Host based intrusion detection system [HIDS] – in the host there will be agent which will determine the intrusion with the help of the system calls, file system modifications, application logs, etc. the example of this method would include OSSEC and tripwire (Tiwari, et al., 2017).

Stack based intrusion detection system [SIDS] – the evolution of the HIDS systems. All the packets will be examined using the TCP/IP stack and it would be useful for network interface.

**Intrusion prevention systems [IPS]**

The IPS network make use of the application firewalls, traffic filtering for the appropriate solution for providing security. It would prevent the attack occurrence by blocking the IPs dropping of the malicious packets, and providing proper alert to the corresponding officials. There has been different methods exist in this.

Network intrusion prevention system [NIPS] – the overall network will be monitored for the occurrence of the suspicious traffic with the help of protocol.

Wireless intrusion prevention system [WIPS] – the wireless network will be monitored for occurrence of the suspicious traffic with the help of suitable protocol (Tasneem & Kumar, 2018 ).

Network behavior analysis [NBA] – the traffic in the network will be determined by analyzing the traffic flows which would leads to DDoS attacks, etc.

Host based intrusion prevention system [HIPS] – the software will be installed which would be useful for monitoring the host for determining the suspicious activity.

# Summary

The cyber security is the important factor which would be useful for providing security for all the organization and information present in it. In this three has been different factors are available which would be useful for providing high security, so that in this different terms are discussed which are helpful for providing security in the different manner. Initially security concepts, requirements and strategy that are available are discussed. Cryptography is the method in which the messages transmitted will be encrypted and in the receiver side it would be decrypted. In this there was different methods are available they are hash function, MD5, SHA1 and SHA 2. In this working of these methods are discussed. The system and network security provides security for the information that are present in the organization and networks. Then, different methods available are discussed. The malware will affect the files that are present in the system. So that impact occurrence and determination and types of malware that are available and mitigation measures are discussed. Finally, the intrusion detection and prevention IDS and IPS are useful for providing the security to all the devices present.

Overall this malware detection using the different standards taken from the IDS and IPS can help in giving the assurance towards the major hash functions that can be determined with all necessary functionalities specified. In order to have the clear impact of the MD5, SHA1, SHA2 and working standards it is necessary to understand the each type of the measure that can be easy enough to measure the resources types to be more substantiate towards the outcomes.

**Summary of cryptographic algorithms**

A system’s cryptographic safety towards assaults and malicious penetration is decided through different factors. If cryptographic offerings are required, cryptographic strategies which can be both FIPS-permitted or NIST-encouraged need to be employed, consistent with NIST. These algorithms have passed through complete safety studies and are continuously examined to make sure appropriate safety. Cryptographic keys are normally utilized in cryptographic algorithms, and while those algorithms want to be improved, large keys are often used.

**Classes of Cryptographic Algorithms**

**Hash functions:**

The fundamental operation of a cryptographic hash feature does now no longer encompass using keys. Through a one-manner procedure, this feature generates a tiny digest or “hash value” from large quantities of data. Hash features are generally used to generate the constructing blocks for key control and to offer safety offerings such as: Providing supply and integrity authentication offerings via way of means of producing message authentication codes (MACs). Compressing messages for the technology and verification of virtual signatures. Deriving keys in key-established order methods

**Symmetric-key algorithms:**

A symmetric-key technique additionally called a mystery-key algorithm, alters information to make it extraordinarily tough to look at without a mystery key. Because its miles are used for each encrypting and decrypting, the key’s termed symmetric. One or greater legal entities typically have got right of entry to those keys.

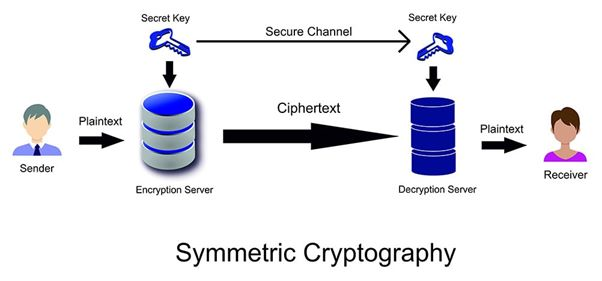
**Symmetric key algorithms are used for:**

·       Encrypting and decrypting facts with the equal key guarantees facts confidentiality.

·       Message Authentication Codes (MACs) are supplied for supply and integrity authentication services. The key’s used to generate and validate the MAC.

·       Creating keys at some stage in key-introduction operations.

·       Creating deterministic random numbers



**Asymmetric-key algorithms**

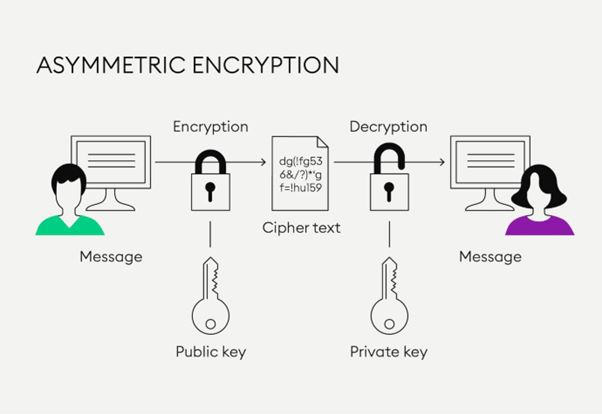
Asymmetric-key algorithms, frequently referred to as public-key algorithms, use paired keys to execute its job. The public secret is acknowledged to everyone; however, the non-public secret is simplest acknowledged to the proprietor of that key pair. Even though they’re cryptographically related, the non-public key cannot be computed mathematically the usage of the general public key.

**Asymmetric algorithms are used for:**

·       Computing virtual signatures

·       Developing cryptographic keying material.

·       Dealing with identities



This is a caption

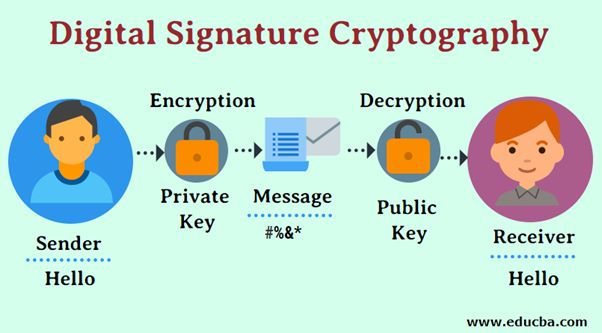
**Security Services Provided by Cryptographic Algorithms**

**Hash Values:**

Hash algorithms convert binary values of any period into smaller binary values of a described period, which might be called hash values. A hash cost is a numerical illustration of information. If you hash a plaintext paragraph then adjust even one letter, the subsequent hash will produce a distinctive cost. The cost of the hash will modify dramatically if it’s miles cryptographically strong. An effective hash function, for example, might also additionally yield an output that differs via way of means of 50% if a unmarried little bit of a message is modified. A massive range of enter values might also additionally hash to the identical output cost. However, locating separate inputs that hash to the identical cost is computationally impossible.

**Digital Signatures:**

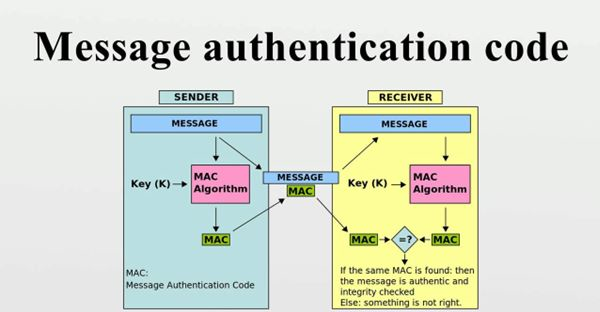
Digital signatures also can be created the usage of public-key algorithms. Digital signatures validate a sender’s identity (assuming you accept as true with the sender’s public key) and help make certain facts integrity. The recipient of Alice’s facts can affirm that it changed into transmitted through Alice through evaluating the virtual signature to Alice’s facts and Alice’s public key.



This is a caption

**Message Authentication Codes (MACs):**

Message Authentication Codes may be used to offer authentication for message starting place and integrity. By producing a MAC key this is shared through each the message originator and the recipient, this cryptographic method solves the hassle of attackers enhancing messages.



This is a caption

**References:**

D. Stinson, Cryptography: Theory and Practice, CRC Press, 3rd Ed., 2005. Solid introduction, but only for the mathematically inclined.

Kaminsky, A., Kurdziel, M., & Radziszowski, S. (2010, November). An overview of cryptanalysis research for the advanced encryption standard. In 2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE (pp. 1310-1316). IEEE.

Sasi, S. B., Dixon, D., Wilson, J., & No, P. (2014). A general comparison of symmetric and asymmetric cryptosystems for WSNs and an overview of location based encryption technique for improving security. IOSR Journal of Engineering, 4(3), 1.

Jirwan, N., Singh, A., & Vijay, S. (2013). Review and analysis of cryptography techniques. International Journal of Scientific & Engineering Research, 4(3), 1-6.

# Intrusion Detection & Prevention

Organizations implement Intrusion Detection Systems for preventing confidential data and networks from cyber-attacks and breaches. ID and IP help to block offending IPs and drop malicious packets to the network. It alerts the network administrator about potential threats and their entrance. Organizations focus on installing security systems such as antivirus software, IDSs, firewalls, etc for ensuring their network security. However, these security systems have some issues and drawbacks. For example, firewalls do not protect against malware or viruses rather it restricts unauthorized access, and accessing private networks. Likewise, IDSs have the drawback which has not had the ability to process encrypted packets (Coulibaly, 2020). It is a secondary defence mechanism so it is added with other systems like firewalls to ensure security for the network. However, IDPs are installed in organizations for monitoring and analysing security issues and undesirable activities. The following functions are managed by IDPS technologies,

·       Observed event information are recorded. Centralized logging servers, security information and event management programmes, and enterprise management systems are received from IDS which is records information locally.

·       It alerts the security administrators through several methods such as pages, emails, Simple Network Management Protocol (SNMP) traps, messages on the IDPs user interface, user-defined programs and scripts, and Syslog messages. The administrators can receive basic information about the events through this alert. For getting additional information about the event then the administrators need to access IDPs.

·       Summarized reports can be achieved from IDPs that detail the monitored events or detail the particular event if the administrator approach it. Security profiles can be changed by some IDPs if a new threat is identified.

**IDPs Detection methodologies** – It utilizes many methods for detecting attacks in the network. Anomaly-based, signature-based, and stateful analysis are the primary methodologies in IDPs.

**IDPs Security Capabilities** – It offers broad detection and extensive capabilities. Accurate detection and more flexibility are achieved by the combination of detection techniques. Depending on the IDPS technology, there are significant differences in the events that can be recognised and the average accuracy of detection (Azhagiri Mahendiran, 2015). To increase the effectiveness, usability, and accuracy of their detection, the majority of IDPs need at least some tuning and customization. Some of the tuning and customization capabilities of IDPs are information-gathering capabilities, logging capabilities, detection capabilities, and prevention capabilities.

Types of IDPs Technologies are network-based IDPs, Wireless IDPs, Network behaviour analysis (NBA) systems, and Host-based IDPs.

**IDPs Components**

Sensor or Agent – It helps to monitor and analyse events or activities. The sensor supports monitoring networks and Agent is named because it monitors a single host.

Management server – Receives information from sensors or agents and it can be managed effectively. Some management servers analyse the information they receive to find incidents that are not identified by sensors or agents. Correlation is the process of comparing event data from several sensors or agents, such as identifying occurrences caused by the same IP address. Administration servers are employed in large IDPs rather than small IDPs to avoid it.

**Database server-** Event information that is recorded by sensors, agents, and management servers is handled by the database server as a repository.

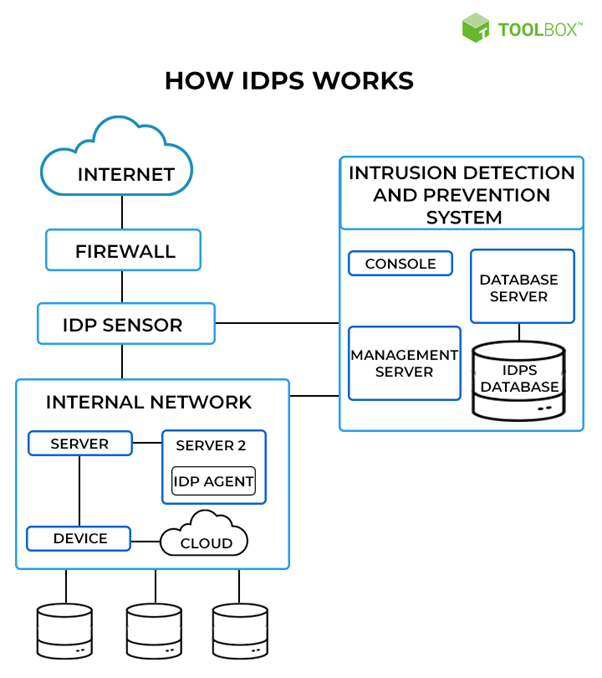
**Console -** A console is a piece of software that gives users and administrators of the IDPS an interface. Typically, console software is installed on regular desktops or laptop computers.

# Summary

Understanding and being aware of cyber security techniques and their attacks is essential for safeguarding the cyber environment of the organization. Cyber-security manages the set of techniques for securing the data and network from unauthorized access. The current paperwork details the security techniques and methods for securing the network in the organizations. It helps to save the network integrity, data, and programs from unauthorized access. The cyber security methodologies, techniques, and possible malware attacks are detailed in this current work. Organizations and network administrators or analysers should be aware of security issues and security standards to protect confidential data and other secured network assets.

A system that monitors a network and scans it for potential threats to notify the administrator and stop any assaults is known as an intrusion detection and prevention system (IDPS).

An intrusion detection and prevention system (IDPS) keep an eye on a network for any potential dangers and notifies the administrator to stop any assaults.



This is a caption

**How IDPS works**

**Functions of an IDPS**:

Protects critical data and technical infrastructure: No system can operate in a vacuum, especially in the modern world of data-driven organisations. Since data is continually moving around the network, hiding inside the data itself is the simplest approach to attack or obtain access to a system. IDS is a reactive component of the system that warns security professionals of potential occurrences like these. The proactive nature of the IPS component of the system enables security professionals to counteract threats that might harm the organization’s finances and reputation.

Review the current user and security rules: Every business that prioritises security has its own set of user policies as well as access-related policies for its systems and applications. By restricting access to vital resources to a small number of trusted user groups and systems, these policies significantly decrease the attack surface. Administrators are certain to discover any gaps in these policy frameworks as soon as they arise thanks to ongoing monitoring by intrusion detection and prevention systems. Additionally, it enables administrators to test rules for optimal security and effectiveness.

assembles data about the network’s resources: The security team’s IDS-IPS also provides a bird’s-eye view of the traffic traversing its networks. By monitoring network resources, they can adjust a system in the event of a traffic overload or underutilization of servers.

assists in complying with regulations: To safeguard the security and privacy of customer data, all businesses—regardless of industry vertical—are subject to a growing amount of regulation. Deploying an intrusion detection and prevention system is typically the first step in achieving these standards.

**IDPS Types:**

Network-based intrusion prevention system (NIPS): These systems keep an eye out for harmful activity on whole networks or specific network segments. Usually, protocol activity analysis is used to do this. A database of known attacks is checked to see whether the protocol activity matches, and if it does, the related information is blocked. NIPS are often set up behind firewalls, routers, and remote access servers at network borders.

Wireless intrusion prevention system (WIPS): By examining protocols related to wireless networking, wireless intrusion prevention systems keep an eye on wireless networks. WIPS are useful within the wireless network area of an organisation, but these systems do not evaluate more advanced network protocols like Transmission Control Protocol (TCP). Within the wireless network and in locations vulnerable to unlawful wireless networking, wireless intrusion prevention systems are installed.

Network behaviour analysis (NBA) system: Unlike NIPS, which examines variations in protocol activity, NBA systems look for atypical traffic patterns to spot threats. Policies being broken, malware-generated assaults, or distributed denial of service (DDoS) attacks are the usual causes of such patterns. NBA systems are set up in an organization’s internal networks and at transition points between those networks and the outside world.

HIPS, or host-based intrusion prevention system Host-based intrusion prevention systems are unique from the others in that just one host is where they are implemented. These hosts might be gateways to internal systems or crucial servers holding crucial data that are available to the public. By keeping an eye on active processes, network activity, system logs, application activity, and configuration changes, the HIPS keeps track of all the traffic entering and leaving that specific host.

**Detection–level functionalities of IDPS**

1. Threshold monitoring

2. 2. Profiling

**Prevention–level functionalities of IDPS**

1. Stopping the attack

2. Security environment changes

3. Attack content modification

Reference:

Mohanakrishnan, R. (2022) What is intrusion detection and prevention system? definition, examples, techniques, and best practices, Spiceworks It Security. Available at: <https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-idps/> (Accessed: December 8 2022).

# References

(2016). *4*.

*Developing a Security Strategy*. *3, 5, 7*.

(1996).

*Cybersecurity Concepts*.