International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

CIA Triad-based Framework for Situation Awareness in Network Security: A Review

Manaswinee Madhumita Panda[1], Jagyanseni Panda[2]

[1]Associate Professor, Computer Science and Engineering, GITA Autonomous College, Bhubaneswar
[2]Assistant Professor, Electronics and Communication, ITER, SOA University, Bhubaneswar

Abstract:
Network security has become more crucial in recent years since it shields data from threats and cyber-attacks. The tools, regulations, personnel, and practices that protect any communication infrastructure against online attacks, unauthorized access, and data loss are together referred to as network security. They protect not only the network itself, but also the traffic and resources that are available through it at the network edge and surrounding area. The CIA (confidentiality, integrity, and availability) principles are among the security objectives. The purpose of this paper is to provide an overview of security goal attacks, to provide a detailed description of several network security attack types, and to talk about some of the attackers' defense mechanisms using various network situations. Additionally, the article offers a clearer knowledge of security objectives that may be used to actually securing networks**.**

Keywords CIA, Confidentiality, Integrity, Availability

1. Introduction

Every part of our life is impacted by technology, which offers us numerous benefits but also presents a number of issues. As technology advances daily, one of these issues is the rise in cyber security risks. To protect networks, computers, programs and data from damage, unauthorized access in a organization cyber security is a crucial part. An essential component of cyber security is safeguarding computer networks, systems, and data against loss, damage, or unauthorized access [1]. In today's digital age, effective cyber security measures are necessary to protect sensitive data and keep technology running smoothly. Cyber security encompasses a wide range of practices that are meant to protect digital assets from different types of risks. The risks can take many forms, such as malware, phishing attacks or ransom ware. Effective cyber security involves not only technical measures like firewalls and encryption but also policies, procedures and user education aimed at mitigating risks and responding to incidents [2]. A single act that is meant to target a computer or any other part of a computerized information system so as to change, destroy or steal information and/or exploit or harm the network is what is called cyber-attack [3]. Cyber-attacks have increased with the upsurge in digitalization of business which has become more and more popular over the last few years. Digital systems are safeguarded from harmful and unintentional attacks using several forms of cyber security. With a multitude of specializations and security measure kinds, each concentrating on a distinct facet of securing digital assets, cyber security is a wide field. Some important categories of cyber security are: Network security play a vital role while cyber security part is considered. Using hardware, software, and protocols, vast volumes of data are continuously sent over networks in modern systems, going from one network access point to one or

more access points. Nevertheless, irregularities could occur throughout this procedure, potentially seriously affecting both the environment and the system [4]. Effective network security controls access to the network and targets a variety of threats, preventing them from entering or spreading on it. Network security is any activity intended to maintain the usability and integrity of details network and data. It encompasses both hardware and software technologies. Network security is a significant responsibility for organizations and users in the digital era. Strong security measures are essential to safeguard critical data and digital platforms from sophisticated cyber threats and the expanding complexity of networked systems [5]. firewall types for network security, Email protection, anti-malware and antivirus software, Access control, application security, network segmentation, behavioural analysis, data loss prevention, and intrusion prevention systems Mobile device security, Web security, VPN, wireless security, and security information and event management. The objective of this paper is to describe types of network security b) Methods applied to secure the network c) Awareness of various network security attacks d) Restricting access to information to authorized users only.

A. Types Of Networks Security:-Network security employs a range of strategies and tools to protect the confidentiality, integrity, and accessibility of data over a network. The following are the primary types of network security:

- Firewalls are three types -Hardware Firewalls: Physical devices that filter traffic between networks, Software Firewalls: Programs installed on individual computers or servers to control inbound and outbound traffic, Next-Generation Firewalls (NGFW): Combine advanced security capabilities like intrusion prevention, application awareness, and deep packet inspection with conventional firewall capability.
- Systems for detecting intrusions (IDS) and preventing them (IPS): IDS: Keeps an eye on network traffic to spot unusual activity and notifies administrators of any dangers [6].IPS: Real-time detection and action to stop or lessen hostile activity. Virtual Private Networks (VPNs): To ensure data integrity and privacy when transmitting data over public or untrusted networks, use secure encrypted tunnels [7].
- Network Access Control (NAC): Controls access to network resources by enforcing security policies. Authentication: Ensures users and devices are properly identified and authenticated before gaining access [8]. Authorization: Restricts access to certain areas based on user roles or device types. Antivirus and Antimalware Software:-Malicious software, such as viruses, worms, and ransom ware, that can infect network systems is found, stopped, and eliminated by antivirus and antimalware software.
- Web application firewalls (WAF): Guard against malicious content by screening and keeping an eye on HTTP traffic [9]. All of these network security features work together to provide a strong barrier against unwanted access, guarantee data privacy, and keep network services available.

2. Various Methods used for Network Security

An effort to breach system confidentiality, availability, or integrity, or to obtain unauthorized access to system resources, services, or data. The foundation of a strong and long-lasting network security system is the "CIA"-Confidentiality, Integrity and Availability) [10]. Figure 1 shows the CIA triad. Information stored on a computer may be viewed and used by unauthorized individuals, which is known as unauthorized disclosure of information (confidentiality).This domain of interest may also include "traffic analysis," in which the hacker merely examines the information's usage trends. By analyzing those

patterns, the hacker can infer certain facts. Additionally included in this category is using a proprietary program without permission [11].



Fig. 1.CIA triad

In terms of network security, confidentiality is the act of preventing unauthorized access or exposure of data transmitted over networks. One of the three guiding principles of the CIA trinity 'Confidentiality', 'Integrity' and 'Availability'. It is essential for information system protection.

3. Essential Ideas in Confidentiality:

Protecting sensitive data from unwanted access or exposure is referred to as maintaining confidentiality in network security. It guarantees that data cannot be viewed or accessed by anyone other than authorized users or systems. Keeping sensitive data private, including financial records, personal information, intellectual property, and classified material, is a major goal of security measures for networks [12]. Protect private information against unwanted access while it's being transferred or stored on the network.

Data Encryption: One of the most prevalent approaches to ensure confidentiality is encryption. It involves utilizing algorithms and keys to transform plain text data into unintelligible ciphertext, rendering it unreadable and unavailable to unauthorized users. In network security, confidentiality refers to shielding private data from illegal access or disclosure. It guarantees that the data can only be viewed or accessed by authorized individuals or systems. Maintaining confidentiality is one of the primary objectives of network security techniques, particularly when working with sensitive data such as financial records, personal information, intellectual property, or classified material [13]. To guarantee that information is unreadable by unauthorized parties even if intercepted, data in transit can be encrypted using protocols like IPsec, VPNs, or SSL/TLS (for HTTPS).

Data is changed by the mathematical process of encryption, which uses a key and an encryption algorithm. Consider the scenario when Ram writes "Good morning" to shyam, but instead of using the letter that appears three positions later in the alphabet for each letter, she substitutes it. Rather than saying "Good Morning," her message now says "jrrgpruqlqj" Fortunately, shyam is able to decrypt her message back to "Good Morning" because she knows the key is "3". Figure 2 shows how plaintext converted to cipher text. Ram sent Shyam a message that was encrypted using a very basic encryption method. Further encoding scheme complexity can further jumble the message:

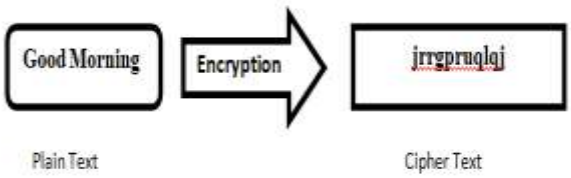


Fig. 2.Convert Plaintext to Ciphertext

Encryption functions logically and predictably, even though encrypted data appears random. This implies that material that has been encrypted can be decrypted and converted back to plaintext by anyone with the right key. An encryption that is truly secure will use keys that are hard enough to guess, making it very unlikely for someone else to use brute force to decrypt or break the cipher text. This implies that material that has been encrypted can be decrypted and converted back to plaintext by anyone with the right key. An encryption that is truly secure will use keys that are hard enough to guess, making it very unlikely for someone else to use brute force to decrypt or break the cipher text. Ram's first encryption technique would be cracked in a hurry. So two keys Private key and Public key used to get the original data which send by the sender. Figure 3 shows to get original data by using encryption and decryption algorithms.

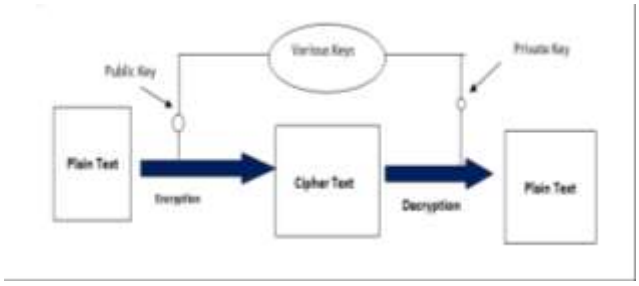


Fig. 3.Encryption and Decryption algorithm

The main technique used in network security to guarantee confidentiality. Data is converted into unintelligible cipher text using encryption, guaranteeing that only those with the proper decryption key and authorization may decipher the content. Depending on the requirements of the network, both symmetric and asymmetric encryption techniques are employed (e.g., rapid communication vs. safe key distribution).Segmentation of network is also another method for providing network security.

Segmentation of Network: A computer network can be divided into more manageable, independent sections, or subnetworks, using a network security approach called network segmentation. Segmentation is mostly used to separate critical areas and control traffic flow across them, which enhances a network's security, performance, and manageability [14]. The following are the primary benefits of network segmentation and its methods of implementation: A method that substitutes symbols or other values for certain data points to conceal sensitive information. As an illustration, conceal credit card numbers. In non-production environments, data masking is frequently used to keep testers and developers away from sensitive data. Network Segmentation technique keeps sensitive data isolated from less important areas of the network in order to protect it. Sensitive areas (such financial systems, HR databases, or intellectual property) might be isolated to make it harder for bad actors or unauthorized individuals to obtain private data.

Steganography: A little-known method of evading detection that entails enclosing sensitive information in non-sensitive material, such audio files or image files. It can be used for secret communication even if it's less popular than encryption. Network Protocol Steganography: Data is hidden in network communi-

cation protocols such as TCP/IP, HTTP, or DNS. This can involve embedding information in the headers, timing of packet transmissions, or unused fields of protocol structures. Example: Information could be concealed in the metadata of packet headers or even in the timing patterns of packet transmissions in network traffic, allowing covert communication between systems.

Employing Secure Protocols: Security measures such as encryption and other protocols are frequently used to safeguard network communication. Examples include HTTPS-secured web communications using SSL/TLS [15].IP networks can use IPsec (Internet Protocol Security) to communicate securely Virtual Private Networks, or VPNs, are used to encrypt user connections to distant servers.

To protect secrecy, organizations set up stringent security rules and processes. Data management (who can access data, how it's shared, and how it's stored) and data classification (designating data as confidential, restricted, etc.) regulations can fall under this category[16].Employees must receive regular training if they are to detect phishing efforts, safeguard their devices, and handle sensitive data according to best standards [17].

3.2 Integrity in network security

In terms of network security, integrity is the guarantee that correct, consistent, and unmodified information is being sent, stored, or processed. It guarantees that the data read or received is precisely as it was sent or stored by guarding against inadvertent or unauthorized changes. Integrity is essential for preserving communication confidence, particularly in systems like financial transactions, medical records, and vital infrastructure where precision is necessary. Data integrity guarantees complete assurance that the information you are getting from the sender is real, legitimate, and unaltered. Figure 4 display to protect message from integrity using MAC method.



Fig. 4.Integrity of message using MACS

3.3 Techniques for Verifying Authenticity:

Authentication is the process of confirming a user, device, or system's identity. It is among the most often used techniques in network security to guarantee authenticity.

Authentication Types: Password-based Authentication: To authenticate, the user enters a password or PIN. Despite being widely used, it is susceptible to phishing, password cracking, and brute-force attacks. Multi factor Authentication: Using two or more ways of verification, such as PIN or password), is known as multi-factor authentication (MFA). Something you own, like a smart card or token [18]. Authentication on Biometric -It verifies identity through the use of distinct physical traits such as fingerprints, facial recognition, or retinal scans. Authentication based on Token: This method uses a virtual token, such as an OTP (one-time password), or a physical token, such as USB token or a smart card, to create authentication codes.

Digital Signatures: Cryptographic techniques that offer integrity and validity are called digital signatures. They function by signing a message or document with a private key and validating it with a matching public key. The integrity of the message is ensured by the digital signature.The sender of the

communication has been confirmed (authenticity). Use cases: Software packages, communications, and digitally signed documents (such as contracts and legal papers) to verify their provenance.

Infrastructure of Public Key : PKI is a system that facilitates digital certificate distribution and maintenance. It offers a framework for employing public and private keys to authenticate people, things, or services. PKI provides authenticity in a number of methods: confirming that public keys are legitimate. Overseeing the certification process from issuance to renewal and revocation. Frequently utilized in encrypted file systems, email security (S/MIME), and SSL/TLS.

Kerberos is a network authentication protocol that authenticates users and computers on a network by using secret-key cryptography to confirm their identities. It issues tickets for network resource access and performs user and service authentication through a reliable third-party, the Key Distribution Center, or KDC [19]. Authenticity is guaranteed by Kerberos since tickets are used to confirm the identities of the client and the server during a communication session.

In order to authenticate users to servers and servers to users, Kerberos offers a centralized server for authentication. The server and database manage client authentication in Kerberos authentication. Kerberos is managed by a trustworthy third-party server called the Key Distribution Center (KDC). Every principal on the network is a user or service. Figure 5 shows how Kerberos providing authenticity. Ticket Granting Service's initial authentication and ticketing are handled by the Authentication Server (AS). Database: The Authentication Server confirms each user's permissions to access the data. Ticket Granting Server (TGS): The ticket is issued for the server by the TGS [20].

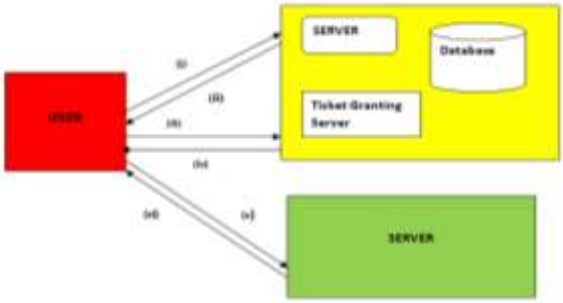


Fig. 5.Authenticity using kerberos

Doing this experiment first step: Log in and make a service request on the host. Users consequently request the ticket-issuing service. Next step is the authentication server issues a ticket-granting ticket and a session key after using a database to confirm the user's access privileges. The user password is used to encrypt the results. Third step is send the ticket to the Ticket Granting Server after decrypting the message with the password. Authenticators such as network addresses and user names are contained in the ticket. Fourth step is to request the server's services, the Ticket Granting Server generates a ticket especially for that purpose. Fifth step is the authenticator and ticket are sent to the server by the user. Sixth Step is after authenticators have verified the ticket, the server generates access to the service. The user is then able to use the services.

OAuth and Connected OpenID: Access delegation via OAuth, an open standard, is frequently used to allow third-party services restricted access to user resources without disclosing user credentials. OpenID Connect is an authentication system that expands upon OAuth 2.0. It enables users to authenticate with the help of a third-party service (like Google or Facebook), which issues authentication tokens and confirms the user's identity. Extensively employed in web applications for user authentication. Security Extensions of Domain Name System: The legitimacy of DNS (Domain Name System) answers is guaran-

teed by DNSSEC. In order to confirm that DNS records are authentic and unaltered, it appends cryptographic signatures. By stopping hackers from faking DNS answers, Domain name system security extension guarantees that users get at the proper and authentic website or service.

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

In MITM attacks, an attacker intercepts communication between two parties, pretending to be one or both parties, to gain unauthorized access or alter communications. Countermeasures are the another method in which SSL/TLS encryption, certificate pinning, and PKI for authenticating communication endpoints. In network security, authenticity refers to confirming the legal status of users, devices, and systems. It is essential for stopping fraud, spoofing, and impersonation. Organizations may preserve trust in their network security infrastructure and guarantee the validity of communications by utilizing strategies like multi-factor authentication, certificates, and digital signatures. In network security, authenticity refers to confirming the legal status of users, devices, and systems. It is essential for stopping fraud, spoofing, and impersonation. Organizations may preserve trust in their network security infrastructure and guarantee the validity of communications by utilizing strategies like multi-factor authentication, certificates, and digital signatures. Details Availability refers to the idea that the data that authorized users need or request should always be accessible. This implies that the information must be properly processed and stored by the computer systems, protected by security measures, and transported over communication channels. Availability is frequently the most crucial attribute in service-oriented enterprises that depend on information. Figure 6 shows the different components of availability. There are three parts to availability:



Fig. 6.Components of Availability

- **Reliability**: -The likelihood that a system will function as intended for the duration planned under the encountered operating conditions is known as reliability. There is no point in having the system if it is unreliable. Consumers do not want to rely on a system that they cannot rely on to reliably carry out their demands.
- **Accessibility:** -"The degree to which a system is usable by as many people as possible without modification" is what accessibility refers to. Access control services like Role Based Access Control (RBAC) enable a number of access control rules, including Mandatory Access Control (MAC) and Discretionary Access Control (DAC).
- **Timeliness:** The capacity to obtain information and services promptly is known as timeliness. It refers to how quickly a system or resource responds to a request from a user. The primary indicator of information availability is the duration of time (uptime and downtime) that an information resource is either processing or not. Instantaneous responses to requests are desired by both users and organizations; yet, in the absence of adequate information availability, this need might not be fully satisfied.

3.5 Results and Discussion

One significant concern with the infrastructure of each and every business and institution. To put it succinctly, an enterprise or group founded on cyber security can attain elevated standing and numerous accomplishments, as these outcomes stem from the capacity of the business to safeguard consumer and private data against an opponent. Businesses that compete with clients and People abuse each other. An enterprise or group needs to begin with and first, give this security in the most effective manner to create and grow on its own Cyber security includes safeguarding information, networks, and data from both internal and external threats. Professionals in cyber security safeguard computer systems, networks, servers, and intranets. Cyber security makes sure that information may only be accessed by authorized individuals. Network security protects computer networks against intrusions like viruses and hackers. A group of techniques known as network security enables companies to defend their computer networks from organized crime, malware, and hackers. The three pillars of availability, integrity, and secrecy form the foundation of any organization's security. These three concepts have been referred to as the security triangle, or CIA, since the development of computer systems, and have governed system security. According to the secrecy concept, only people with permission can access sensitive data and features. Example: Confidentiality (defense secrets) .According to the integrity principles, only resources and people with permission are able to add, edit, or remove sensitive data and features. A voting system (integrity) is one example. Systems, functions, and data must be accessible on demand within predetermined boundaries based on SLA service level (Availability), according to availability principles .

Effective cyber security techniques extend the previously described principles. This is a simple defense that any skilled hacker can get around. Cyber security is more challenging as a business expands. Cyber security's handling of the increasing amounts of data exchanged between the real and virtual worlds is another drawback. In terms of general skills, many people fall at the lower end of the cyber-security spectrum . Many people are at the lower end of the cyber-security spectrum in terms of general skills. The topic of cyberspace coverage is wide. We shall examine the primary categories of cyber security in the upcoming post. Not one of these elements is missed in a thorough plan that addresses them all. The field of cyber-security is become more intricate. Thus, being aware of security issues is crucial . The major categories of cyber security will be reviewed in this essay. A thorough plan addresses each of these factors and doesn't leave any out. Organizations must view cyber-security from a "security perspective." Because of this, it's essential to constantly have good security to stay one step ahead of hackers. Investment in cyber-security services and systems is growing as a result of increased security initiatives.

3.6 Conclusion

In cyber security environment, network security is the major concerns of all types of security. Network security is the term used to describe the set of rules, practices, and technological instruments designed to protect the availability, confidentiality, and integrity of a computer network and the information on it. This paper presents a detail discussion about the CIA triad in network security and some protection mechanism with examples. A greater understanding of security threats that may be applied to really secure networks is also provided by the article.

Reference

1. of data availability. The Geneva papers on risk and insurance. Issues and practice, 47(3), p.698.
2. Toussaint, M., Krima, S. and Panetto, H., 2024. Industry 4.0 data security: A cyber security frameworks review. Journal of Industrial Information Integration, p.100604.
3. Ajala, O.A., Okoye, C.C., Ofodile, O.C., Arinze, C.A. and Daraojimba, O.D., 2024. Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time. Magna Scientia Advanced Research and Reviews, 10(1), pp.312-320.
4. Lim, W., Chek, K.Y.S., Theng, L.B. and Lin, C.T.C., 2024. Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. Computers & Security, p.103733.
5. Maddula, S.S., 2024. Enhancing Network Security: Kali Linux Tools and Their Applications in Cyber Defense.
6. Khan, M. and Ghafoor, L., 2024. Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions. Journal of Computational Intelligence and Robotics, 4(1), pp.51-63.
7. Olabanji, S.O., Olaniyi, O.O., Adigwe, C.S., Okunleye, O.J. and Oladoyinbo, T.O., 2024. AI for identity and access management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. Authorization, and Access Control within Cloud-Based Systems (January 25, 2024).
8. Admass, W.S., Munaye, Y.Y. and Diro, A.A., 2024. Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, p.100031.: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/
9. Aboukadri, S., Ouaddah, A. and Mezrioui, A., 2024. Machine learning in identity and access management systems: Survey and deep dive. Computers & Security, p.103729.
10. Osazuwa, O.M.C., Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature.
11. Samonas, S. and Coss, D., 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3). https://doi.org/10.1016/j.csa.2023.100031
12. Kale, R.S., Hase, J., Deshmukh, S., Ajani, S.N., Agrawal, P.K. and Khandelwal, C.S., 2024. Ensuring data confidentiality and integrity in edge computing environments: A security and privacy perspective. Journal of Discrete Mathematical Sciences and Cryptography, 27, pp.421-430.
13. Chen, Z., 2024. Campus Network Security Intrusion Detection Based on Feature Segmentation and Deep Learning. Journal of Cyber Security and Mobility, pp.775-802.
14. Kizza, J.M., 2024. Computer network security protocols. In Guide to Computer Network Security (pp. 409-441). Cham: Springer International Publishing
15. Abubakar, A., Najmuddin, N.M., Alwi, R.A.M. and Faizal, N.A.I.M., 2024. Examining Potential Threats of Eavesdropping in TCP Stream of Personal Interactive Transmission Session. International Journal on Perceptive and Cognitive Computing, 10(1), pp.98-104
16. Bikku, T., Biyyapu, N.S., Sekhar, J.C., Kumar, M.K., Nokerov, S.M. and Pratap, V.K., 2024. The Social Network Dilemma: Safeguarding Privacy and Security in an Online Community. International Journal of Safety & Security Engineering, 14(1).
17. Pillai, S.E.V.S. and Polimetla, K., 2024, February. Mitigating DDoS Attacks using SDN-based Network Security Measures. In 2024 International Conference on Integrated Circuits and Communi-

cation Systems (ICICACS) (pp. 1-7). IEEE.
18. Sirigade, R., 2024. SIMPLIFYING BIG DATA SECURITY: KERBEROS, SENTRY, AND RANGER. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET), 15(5), pp.317-328.
19. Lafourcade, P., Mahmoud, D., Marcadet, G. and Olivier-Anclin, C., 2024, July. Transferable, Auditable and Anonymous Ticketing Protocol. In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (pp. 1911-1927).
20. Lyu, M., Gharakheili, H.H. and Sivaraman, V., 2024. A survey on enterprise network security: Asset behavioral monitoring and distributed attack detection. IEEE Access.