Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature

Osaro Mitchell Christopher Osazuwa
G22/MSC/CPSS/CSS/FTY/001
University of Port-Harcourt
Centre for Peace and Security Studies
Postgraduate School

Abstract:- This paper delves into the intricate tapestry of information security in network systems, scrutinizing the quintessential "CIA triad" – confidentiality, integrity, and availability – through the lens of contemporary challenges and solutions. We embark on a comprehensive journey across diverse technical landscapes, traversing the burgeoning Internet of Things (IoT), the enigmatic realm of blockchain technology, and the dynamic frontiers of Software-Defined Networks (SDNs). As we navigate these disparate terrains, the paramount importance of the CIA triad as a cornerstone of information security becomes increasingly apparent. Yet, we acknowledge the inherent fluidity of the security landscape, necessitating a critical reappraisal and potential expansion of the traditional CIA framework. This review underscores the interdisciplinary nature of security concerns, dismantling the artificial silos between technical prowess, policy formulation, and ethical considerations. We advocate for a collaborative and multifaceted approach where engineers, policymakers, and ethicists join to weave a robust security tapestry. By embracing this holistic perspective, we can effectively confront the multifaceted challenges posed by malicious actors and evolving threats within the digital domain. The paper culminates in a set of forward-looking recommendations for future research endeavours. We call for seamlessly integrating emerging technologies, such as artificial intelligence and quantum computing, into the security paradigm. We champion a holistic approach to security that transcends technical solutions and encompasses broader societal and ethical dimensions. We advocate for cross-disciplinary collaborations that bridge the gap between academia and industry, translating theoretical advancements into practical solutions. Finally, we emphasize the need for continuous adaptation and real-time threat intelligence, ensuring our defenses remain agile despite ever-evolving adversaries. In conclusion, this paper serves as a springboard for further exploration of the CIA triad in the context of contemporary network systems. By acknowledging its limitations, embracing interdisciplinarity, and constantly adapting to the evolving threat landscape, we can build a more secure and resilient digital future for all.

Keywords:- *Confidentiality, Integrity, Availability, Network Systems and Information Security.*

I. INTRODUCTION

In the contemporary globalised society, network systems assume a crucial function in enabling the exchange of information, collaborative data sharing, and efficient allocation of resources across diverse sectors. Network system security and functionality are becoming increasingly crucial for organisations as they depend on digital infrastructure. Confidentiality, integrity, and availability (CIA) form the core of a strong and resilient network security system (Whitman & Mattord, 2017). Network systems facilitate communication, data sharing, and resource utilisation across multiple domains in today's interconnected world (Alenezi & Almuairfi, 2020). As organisations become more dependent on digital infrastructure, ensuring the security and functionality of network systems becomes crucial. (Alenezi & Almuairfi, 2020) Confidentiality, integrity, and availability (CIA) are fundamental principles forming a robust and resilient network security framework. Cybercriminals have made a career out of breaching software security for their benefit, necessitating the development and implementation of secure software. Through literature review, this work introduces concepts and terms used in secure software development, presents best practices, and examines the models that could be employed. Confidentiality, integrity, availability, and non-repudiation are terms associated with secure software, which implies that it must be kept private, safe, accessible, and able to record all activities performed.

Network systems consist of a diverse range of networked devices, servers, and data channels that facilitate the smooth and uninterrupted transmission of information. The systems play a crucial role in contemporary communication, providing essential assistance for vital functions across various sectors such as banking, healthcare, government, and education (Whitman et al., H. J. (2017). The rise in cloud computing, Internet of Things (IoT) devices, and mobile apps has led to heightened intricacy in network systems. Consequently, this has introduced novel difficulties in security and stability maintenance (Khan et al., A., 2019).

The CIA triad is a conceptual framework encompassing the fundamental principles of network security (Whitman & Mattord, 2017). Confidentiality is crucial to information security since it guarantees that sensitive material is only available to individuals or institutions who have been granted authorisation. This measure effectively protects against any unauthorised disclosure of data (Whitman & Mattord, 2017). Whitman and Mattord (2017) agree that integrity serves as a safeguard to ensure the precision and uniformity of data, hence reducing the potential threats associated with unauthorised manipulation or modification. The concept of availability pertains to the assurance of network resources and services being readily accessible as required, hence minimising periods of inactivity and guaranteeing the uninterrupted flow of activities (Whitman & Mattord, 2017).

The objective and scope of the literature review are crucial elements in scholarly research. This literature review aims to thoroughly examine and integrate established academic literature on a specific research subject. The primary objective of this study is to discern any deficiencies, incongruities, and contentious aspects within the current body of literature, thereby highlighting the necessity for more research. Moreover, the literature review serves the purpose of contextualising the research within its scholarly framework.

This literature review examines the current corpus of research and scholarly work on confidentiality, integrity, and availability in network systems. Through a comprehensive examination of pertinent scholarly works, this study aims to offer valuable perspectives on the diverse tactics, technologies, and frameworks utilised to sustain the principles of confidentiality, integrity, and availability (CIA) in response to the ever-changing landscape of cyber threats.

➢ *Theoretical Foundations*

Confidentiality, integrity, and availability (CIA) are essential information security components that are the foundation for a robust network system. A comprehensive comprehension of the unique characteristics associated with each principle is vital to developing security measures that are efficient and successful.

➢ *Confidentiality*

Confidentiality refers to the ethical and legal need to protect sensitive information from unauthorised access or disclosure. Confidentiality pertains to using protective measures to prevent unauthorised individuals from gaining access to sensitive information. This suggests that access to sensitive information should be limited exclusively to officially authorised individuals or institutions. Whitman and Mattord (2017) examine that a firm must maintain the confidentiality of its financial information, ensuring that only allowed individuals have access to it. Confidentiality also refers to safeguarding sensitive information from unauthorised access, disclosure, or exposure. The study conducted by Banwani and Kalra (2021) is of significant academic importance. This principle is designed to guarantee that only duly authorised individuals or entities can access specific data, hence ensuring the privacy of sensitive data. Mavhandu-Mudzusi et al. (2007) assert that organisations may experience financial losses, reputational harm, and legal consequences due to data breaches or unauthorised access. Encryption algorithms, such as the widely used Advanced Encryption Standard (AES) and the establishment of access controls, play a crucial role in upholding the principle of confidentiality within network systems (Carta et al., 2020).

➢ *Integrity*

Integrity refers to the protection of information from unauthorised changes or alterations. This necessitates that information should not be altered without proper authorisation and that any changes must be recorded and documented. Whitman and Mattord (2017) assert that preserving the integrity of a company's product designs is crucial, ensuring that any modifications are made only with the appropriate authorisation. Integrity also implies maintaining data's precision, consistency, and reliability throughout its lifecycle (Carta et al., 2020). Ensure data integrity by preventing malicious actors from altering, deleting, or tampering with data. Hash functions and digital signatures are frequently used cryptographic methods for verifying data integrity, as any modification to the original content will result in a detectable change in the hash value (Carta et al., 2020). (Covert et al., 2020) posits that maintaining data integrity is essential to prevent dissemination of deceptive or corrupted information, which could have severe repercussions in vital sectors such as healthcare and finance.

➢ *Availability*

The concept of availability pertains to the assurance that authorised individuals can easily access information when needed. This suggests that it is crucial to protect information systems from interruptions that could hinder users' access to information. Whitman and Mattord (2017) opine that a company's website must have constant accessibility for clients. The concept of availability pertains to the assurance of accessibility and usability of network resources, services, and data, specifically when those with proper authorisation need them (Sayyad et al., 2021). Unforeseen periods of operational inactivity, arising from either technological malfunctions or cyber intrusions, possess the capacity to impede organisational processes, generate financial deficits, and inflict damage on an entity's standing within the public sphere (Sayyad et al., 2021). The maintenance of uninterrupted access to network services is contingent upon high-availability architectures and failover methods, as highlighted by Sayyad et al. (2021). The CIA triad is a widely recognised security framework that delineates the primary objectives of information security, namely confidentiality, integrity, and availability. The interconnectedness of these three objectives renders any violation potentially resulting in significant ramifications. An instance of a data breach, wherein sensitive information is disclosed without authorisation, has the potential to adversely impact a company's reputation and result in financial detriment. A cyberattack that leads to the unauthorised alteration of data can potentially interrupt operational processes and result in financial detriment. A denial-of-service attack, which hinders users' access to information, can potentially interrupt organisational operations and result in financial ramifications. Various security controls can be implemented by organisations in order to safeguard confidentiality, integrity, and availability.

The CIA triangle represents a key and widely recognised idea within the field of information security. Organisations can safeguard their information assets and limit the potential dangers of a security breach by comprehending the three objectives of the CIA triad and applying suitable security policies.

- *The CIA Triad: Exploring the Relationship between the Three Principles*

The concept of availability pertains to the assurance of accessibility and usability of network resources, services, and data, specifically when those with proper authorisation need them (Sayyad et al., 2021). Unplanned downtime, whether attributed to technological malfunctions or cyber intrusions, can potentially interrupt operational processes, incur financial setbacks, and negatively impact an organisation's reputation (Sayyad et al., 2021). The implementation of many strategies can successfully boost availability. These strategies include using mirrored systems to ensure redundancy, implementing load-balancing techniques to distribute traffic efficiently, and developing comprehensive disaster recovery plans (Sayyad et al., 2021). Maintaining uninterrupted access to network services necessitates the inclusion of high-availability architectures and failover mechanisms as crucial components (Sayyad et al., 2021).

Availability refers to the guarantee that authorised individuals may readily access information at the time it is required. This implies that it is imperative to safeguard information systems from any disruptions that may impede users' ability to access information. Whitman and Mattord (2017) assert that a company's website must always be accessible to clients without interruptions. Unforeseen periods of operational interruption, arising from either technical malfunctions or malicious cyber intrusions, possess the capacity to impede organisational functioning, incur financial detriments, and undermine the reputation of an entity. Several strategies may be employed to improve availability. These include implementing redundancy using mirrored systems, employing load-balancing techniques to disperse network traffic effectively, and developing comprehensive disaster recovery plans. Including high-availability architectures and failover mechanisms is of utmost importance in ensuring continuous accessibility to network services.

The CIA triad is commonly illustrated in a triangular form, wherein a vertex on the triangle symbolises each of the three objectives. The three goals exhibit interdependence, so violating one objective can affect the remaining two goals. For instance, in the event of a breach of confidentiality, integrity and availability might also be affected. In the event of a breach of integrity, there is a potential for compromise regarding availability. In the event of a breach in availability, confidentiality and integrity can also be compromised.

Organisations can implement security controls to safeguard confidentiality, integrity, and availability. The controls above encompass technical measures like firewalls, intrusion detection systems, and encryption. In addition, administrative controls may encompass several measures, including but not limited to user training initiatives, security rules, and procedural guidelines. Physical controls, such as access control and perimeter security, can be incorporated.

The CIA trio is a foundational principle in the field of information security. By comprehending the three objectives of the CIA triad and implementing suitable security measures, organisations can safeguard their information assets and alleviate the potential hazards of a security breach.

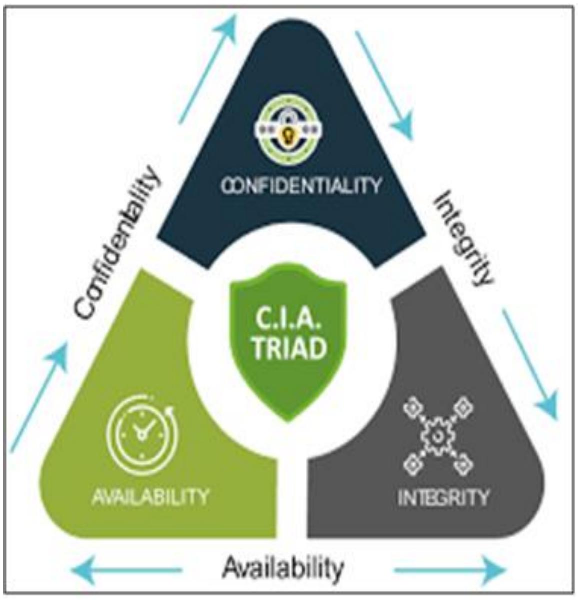

Fig 1 C.I.A Triad
https://encrypted-tbn0.gstatic.com/images - THE CIA TRIAD

➢ *Threats to Confidentiality, Integrity, and Availability in Network Systems*

- *Threats to Confidentiality*

Preserving confidentiality, integrity, and availability in network systems is paramount within information security. Numerous scholarly investigations have examined these perils and their ramifications.

Confidentiality risks encompass deliberate efforts to illicitly acquire sensitive information, including but not limited to financial data, intellectual property, and customer records. These threats can be executed using a range of techniques, which encompass:

- *Phishing*

Phishing refers to a form of social engineering attack wherein perpetrators employ deceptive emails or text messages that mimic the appearance of authentic communications originating from reputable entities, such as financial institutions or credit card companies. Frequently, electronic communications, such as emails or text messages, will encompass a hyperlink which, upon being activated, redirects the recipient to an imitation website that closely resembles the authentic one. Wang et al. (2019) assert that when individuals input their personal information on fraudulent websites, perpetrators can illicitly acquire and appropriate this data.

- *Malware*

Malware refers to a type of software specifically engineered with the intention of causing damage or disruption to a computer system. Installing malware onto a computer system can occur through multiple means, including but not limited to engaging with a malicious hyperlink, accessing an infected attachment, or obtaining a file from an untrusted origin. Pandey and Alsolami (2020) agree that malware within a computer system facilitates the unauthorised extraction of sensitive data, including but not limited to passwords, credit card details, and social security numbers.

- *Data Breaches*

Data breaches occur when confidential information is illicitly obtained from a computer system or network. Data breaches can manifest through multiple avenues, including but not limited to hacking, insider threats, or physical theft (Taheri et al., 2020).

- *Threats to Integrity*

In contrast, integrity preserves data's precision, coherence, and reliability during its lifespan (Satoh et al., 2021). Data integrity is paramount to prevent unauthorised alteration, deletion, or information tampering (Satoh et al., 2021). Integrity attacks are designed to alter or eradicate confidential data. These threats can be executed via many methodologies, encompassing:

- *Viruses*

Viruses are a form of malicious software capable of altering or causing damage to files within a computer system (Taheri et al., 2020).

Trojan horses are a form of malicious software that disguises itself as standard software yet harbours harmful code within its structure. Taheri et al. (2020) opine that the installation of a Trojan horse on a computer system has the potential to alter or delete files within the system.

- *Ransomware*

Ransomware refers to malicious software that uses encryption techniques to render files inaccessible within a computer system. Subsequently, the perpetrators demand a payment, commonly known as a ransom, in exchange for decrypting the files (Wang et al., 2019). Cryptographic techniques, like hash functions and digital signatures, are frequently employed to authenticate data integrity (Satoh et al., 2021). Data integrity is paramount to mitigate the propagation of inaccurate or compromised information, mitigating potentially grave repercussions in vital domains such as healthcare and finance (Satoh et al., 2021).

- *Threats to Availability*

The concept of availability pertains to the assurance of accessibility and use of network resources, services, and data, specifically when individuals with proper authorisation need them. Unforeseen periods of operational inactivity, either from technical malfunctions or malicious cyber intrusions, can impede organisational processes, incur financial detriments, and inflict damage upon an entity's standing.

Availability threats are designed to impede the ability of authorised users to access information or systems. These threats have the potential to be executed via many methodologies, which encompass:

- *Denial-of-Service (DoS)*

Denial-of-service (DoS) attacks refer to malicious activities inundating a computer system or network with excessive traffic, rendering it inaccessible to legitimate users (Kobayashi et al., 2016).

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

Distributed denial-of-service (DDoS) refers to a type of denial-of-service (DoS) attack wherein numerous sources are utilised simultaneously to carry out the attack (Reyns, 2015). Infrastructure attacks are deliberate actions to compromise the fundamental infrastructure that sustains a computer system or network, encompassing critical components like power grids and telecommunications networks.

There exist multiple sources from which threats to confidentiality, integrity, and availability can arise. Hu et al. (2020) posit that insider threats, characterised by authorised personnel misuse of access privileges, present a substantial risk to network systems. Data confidentiality, integrity, and availability can compromise due to attacks targeting the quantum internet and social networks (Satoh et al., 2021; Alguliyev et al., 2018). Covert channels pose a significant risk to preserving confidentiality by utilising communication protocols to surreptitiously disclose sensitive information (Jaskolka et al., 2015).

Moreover, it is essential to note that deficiencies in network security can render systems susceptible to various types of attacks that aim to compromise the system's confidentiality, integrity, and availability (Lent et al., 2014; Concha & Suárez, 2013). Comprehending these potential risks and implementing suitable security protocols are paramount in ensuring network system protection and data confidentiality, integrity, and availability. Organisations can safeguard their information assets and limit the dangers of a security breach by comprehending the potential hazards to confidentiality, integrity, and availability and establishing suitable security measures afterwards.

- *Security Models and Frameworks*

The Bell-LaPadula model, as described by McLean (1990), is a security model that emphasises enforcing confidentiality and access control measures. The text explains the ideas of security levels and access modes designed to prevent the unauthorised transfer of data from higher to lower security levels (McLean, 1990). The model is a preventive measure against the unauthorised disclosure of sensitive information and the foundation for several access control techniques in network systems.

The ISO/IEC 27001 framework is widely acknowledged as a global standard for managing information security systems (ISMS) (Rose et al., 2020). Rose et al. (2020) posit that the strategy outlined in the study offers a comprehensive framework for establishing, implementing, maintaining, and enhancing information security. The framework comprises evaluating potential risks, implementing security measures, and monitoring to guarantee the preservation of information assets' confidentiality, integrity, and availability.

The NIST Cybersecurity Framework, formulated by the National Institute of Standards and Technology (NIST), is a widely embraced set of principles to effectively manage and mitigate cybersecurity threats (Penelova, 2021). Penelova (2021) also examines five fundamental functions, namely Identify, Protect, Detect, Respond, and Recover (IPDRR), that organisations can employ to develop a tailored cybersecurity strategy. The framework places significant emphasis on adopting a proactive approach to security and aligns with the principles of confidentiality, integrity, and availability (CIA).

The Zero Trust Architecture is a modern security framework that presents a paradigm shift from conventional perimeter-based security strategies (Rose et al., 2020). Rose et al. (2020) observe that the assumption is made that risks might manifest in both external and internal contexts within the network. As a result, it becomes imperative to verify all users and devices consistently. The study's authors (Rose et al., 2020) highlight the significance of implementing the principles of least-privilege access, micro-segmentation, and continuous monitoring to bolster security, integrity, and availability. The security mentioned above models and frameworks offers organisations systematic approaches to cultivate and augment their network security strategies.

II. LITERATURE REVIEW

In their paper titled "Review on confidentiality, integrity, and availability in information security," Chai and Zolkipli (2021) argue that protecting information security is paramount, as individuals heavily depend on networks and communication systems. Hence, safeguarding information has emerged as a significant hurdle due to the rapid surge in users in recent times. The objective of their article was to provide a comprehensive analysis of the concepts of Confidentiality, Integrity, and Availability (CIA) within the realm of information security. The primary topic of their essay pertains to the concerns surrounding information security and the corresponding prerequisites for ensuring its effectiveness. The publications, journals, and conference papers that scholars reviewed were published between 2016 and 2021. The examination of security concerns is conducted within contemporary approaches. The interaction between each information security requirement and confidentiality, integrity, and availability (CIA) principles is moderate. There is a prevailing recommendation for implementing a cybersecurity risk awareness programme. Consequently, each user has the potential to derive significant benefits from engaging with networks and digital platforms. The potential benefits of implementing the Information Security Strategy (ISSiO) within an organisation are significant. The approach utilised in organisational settings has certain drawbacks. For instance, it perceives the structure as a static document, lacking dynamic mechanisms that enable it to respond to immediate changes in the external environment effectively. The primary emphasis of the study is on the organisational perspective, and the researchers have not sufficiently elucidated the many dimensions for assessing ISSiO (Home et al., 2017). Lundgren and Möller (2017) agree that if individuals' impact on security is adequately considered, the conditions set forth by the Central Intelligence Agency (CIA) may not suffice for the objectives of both individuals and organisations.

In "A Holistic Study on the Use of Blockchain Technology in CPS and IoT Architectures Maintaining the CIA Triad in Data Communication," Bhattacharjya (2022) examines the use of blockchain technology in Cyber-Physical Systems (CPS) and Internet of Things (IoT) architectures to maintain the Confidentiality, Integrity, and Availability (CIA) triad. The current technological shift prioritises blockchain-based cyber-physical systems (CPSs) and the blockchain Internet of Things. DDoS attacks, ARP spoofing attacks, phishing attempts, configuration hazards, and network congestion are all possible with current CPS and IoT designs. This study shows that the centralised Internet of Things (IoT) system's P2P and M2M communication and Cyber-Physical Systems (CPS) architecture is flawed. These architectural frameworks can use the blockchain's consensus algorithms and cryptographic benefits. This study thoroughly evaluates blockchain technology to show its potential to address the limitations of current Cyber-Physical Systems (CPS) and Internet of Things (IoT) architectures while upholding the CIA trinity of confidentiality, integrity, and availability. The primary goal of this study is to assess Blockchain-enabled Internet of Things research priorities. IoT networks have many connected devices that blockchain technology cannot scale. The processing and storage space needed by this technology is well known. Tangle technology was introduced in 2017 to address these issues. Tangle, a directed acyclic graph, authenticates transactions and secures IoT applications (Tangle, 2018). Tangle network transactions require a Proof of Work (POW) on two previous transactions. It is widely accepted that Tangle technology is more decentralised than blockchain. Blockchain technology could connect several IoT devices and a gateway. Thus, the gateway must be part of the blockchain network. As demonstrated, a new model is needed to overcome the limitations.

In their work titled "Security and Privacy in IoT: A Survey," Poornima M. and Mahabaleshwar S. (2020) discuss the prominent aspects of IoT architectures, applications, and research difficulties. Based on the findings of the literature review, it is evident that there is a dearth of adequate privacy and security algorithms specifically designed for the Internet of Things (IoT). Most privacy and security algorithms for the Internet of Things (IoT) are currently being implemented, operating under various assumptions. Nevertheless, these methods have been widely recognised for their significant computational, energy, and memory requirements. The utilisation of IoT devices in this context has the potential to become increasingly intricate. Hence, implementing such lightweight strategies will necessitate ensuring the minimisation of information. Nevertheless, the viability and optimisation of this particular architecture remain unresolved. In the context of the Internet of Things (IoT), objects and platforms must engage in the sharing of personal or secret information. Achieving a harmonious equilibrium between privacy and security remains a topic of ongoing debate and exploration. Furthermore, it is crucial to identify and detect harmful items during the communication process. The identification of a malevolent entity has the potential to result in a rise in latency. Hence, achieving a harmonious equilibrium between algorithm performance and security remains an ongoing and unresolved difficulty. In the Internet of Things (IoT) realm, it is crucial to incorporate apps that provide privacy and security attributes, thereby adhering to the principle of data minimisation and prioritising data control above data acquisition. Therefore, establishing an Internet of Things (IoT) standard is imperative to effectively address the heightened requirements for security and privacy in practical applications. It is imperative to provide a comprehensive explanation of security mechanisms that enable users to safeguard their private information rather than relying solely on implementing features inside IoT systems to uphold their privacy.

In their academic essay titled "The CIA Strikes Back: Redefining Confidentiality, Integrity, and Availability in Security," Spyridon Samonas and David Coss (2023) examine confidentiality, integrity, and availability in security. The study investigates the application of the CIA trinity of confidentiality, integrity, and availability to information security. The study investigates two unrelated viewpoints. First, how information security practitioners have portrayed the triad as a distinct reference frame was analysed. Our investigation also investigated academic research on the security of information systems. It also suggests several socio-technical additions to the CIA's trinity to surmount the limitations of technological controls alone. Our study sought to explain the apparent indifference of security practitioners to these developments and their focus on the CIA trinity. We have proposed a revised triad definition incorporating socio-technical expansions to reconcile the two perspectives. The primary professional certification curricula and standards of practice in security demonstrate that professionals have not contested the relevance and significance of the academic perspective. Beyond the technical aspects of the initial CIA proposal, the triangle is employed with a broader understanding. Despite the chronological disparity in the convergence of methodology, scholarly studies establish professional benchmarks, while practitioners' norms and insights influence the perspectives of security scholars. Over the past four decades, the CIA's three divisions have progressively transformed and reorganised in response to rapid information technology innovation and security shifts. This evolution has included manipulating data transmission and cyber security in addition to its original focus.

During their research, they discovered that availability and privacy are rarely investigated. The expansion concepts of the CIA prioritise data integrity. Due to the increasing use of mobile technologies and privacy concerns, we propose that the CIA triangle emphasise the convergence of availability and privacy. This topic has tremendous potential for research into information security. The relationship between security and privacy has numerous social implications and unanswered questions that future scholars could investigate. Future studies will investigate how industry-wide security practices implement and expand the concepts of confidentiality, integrity, and availability (CIA). The potential narrowing of the divide between current information security practises, and academic research agendas intrigues us greatly. This study examines how technological and managerial advancements impact the components of the CIA triangle.

In an article entitled "Hierarchically defining Internet of Things security: From CIA to CACA," Yin et al. (2020) assert that the proliferation of Internet of Things (IoT) technology, such as wireless sensor networks, has led to the emergence of security concerns on a global scale. The CIA triangle, encompassing confidentiality, integrity, and availability, is a commonly employed framework for defining and conceptualising information security. Nevertheless, the CIA triangle is inadequate in addressing the ever-evolving security demands. This article categorises information systems into four distinct layers: physical, operational, data, and content, referred to as PODC. A proposed framework for the hierarchical organisation of information security is presented. In addition, the authors establish the fundamental security features associated with each layer and demonstrate that the four properties, namely confidentiality, availability, controllability, and authentication (referred to as CACA), are both essential and autonomous in ensuring comprehensive information security. A novel concept of information security is put forth, drawing upon the principles of PODC (Principles of Distributed Computing) and CACA (Control and Assurance in Cloud and Ambient Systems). This proposed definition serves as a robust underpinning for ensuring the security of information systems. The user suggests that the current definitions of information security may lead to confusion and offer limited direction about security objectives. This article presents a novel conceptualisation of information security, aiming to offer valuable insights for advancing security practices. In order to address the growing and evolving security needs, it is imperative to put out novel definitions in the future.

In their 2021 paper entitled "Improved Handshaking Procedures for Transport Layer Security in Software Defined Networks," Li, X., Ma, M., and Hlaing, C. W. assert that software-defined networking (SDN) has emerged as a novel technology that enhances network flexibility, resilience, and centralised management through automation. In recent times, several reports have surfaced that have discovered potential vulnerabilities that might compromise the authenticity, availability, confidentiality, and integrity of a specific entity or system. This study examines various security concerns in Software-Defined Networks (SDNs), focusing on ensuring communication security between the control plane and the data plane. The Scyther Tool has been employed to verify the efficacy of the state-of-the-art security protocol Transport Layer Security (TLS) in Software-Defined Networks (SDNs). Two security approaches, namely TLSHPS and TLSIHP, have been proposed to enhance the handshaking operations of the Transport Layer Security (TLS) protocol. The utilisation of the Scyther tool for security analysis reveals that both proposed solutions effectively mitigate a range of cyber-attacks.

III. DISCUSSION AND FINDINGS

The literature reviews go into many facets of information security, explicitly emphasising the principles of Confidentiality, Integrity, and Availability (CIA) within diverse technical settings. The assessments encompass a diverse array of subjects, such as Internet of Things (IoT) security, blockchain technology, software-defined networking (SDN), and the evolutionary trajectory of the CIA triad. The following is a synopsis of the results and possible areas of discourse that might be extrapolated from these evaluations:

➢ *The Importance of CIA Triad:*

The CIA triangle, consisting of Confidentiality, Integrity, and Availability, is a fundamental concept within information security. The importance of this structure in assessing and developing safe systems is widely acknowledged, spanning many domains, such as information systems and future technologies like IoT and SDNs.

➢ *Challenges and Solutions in Ensuring Security in the Internet of Things (IoT):*

The Internet of Things (IoT) is an expanding domain characterised by many interconnected devices. However, it presents notable obstacles in terms of security. The studies underscore the importance of prioritising data control over data collecting and minimising the dissemination of information in security measures. Although the significance of privacy and security is acknowledged, attaining a balanced coexistence between these elements continues to pose a formidable obstacle.

➢ *Blockchain for Security and Enhancement:*

The utilisation of blockchain technology holds the potential to mitigate security vulnerabilities present in various systems, including the Internet of Things (IoT). The ability of the system to uphold the CIA trinity is emphasised in many reviews, which underscore the effectiveness of decentralised consensus procedures, cryptographic advantages, and safe transaction authentication. Nevertheless, the issue of scalability becomes apparent as the number of interconnected devices continues to grow.

➢ *Reassessment of the CIA Triad:*

The CIA triad has undergone a re-evaluation by scholars such as Spyridon Samonas and David Coss. The research conducted by the authors indicates that the aspects of availability and privacy are frequently disregarded while considering the triad's framework. The authors proposed a more all-encompassing perspective that considers the dynamic nature of technology and the necessity for a holistic approach to security.

➢ *Hierarchical Framework for Information Security:*

In their article, Yin et al. present a hierarchical framework for information security that builds upon the conventional CIA triad. This framework incorporates four layers, namely Physical, Operational, Data, and Content (PODC), and four properties, namely Confidentiality, Availability, Controllability, and Authentication (CACA). This strategy aims to effectively respond to the changing security requirements and provide a more thorough comprehension of the objectives related to information security.

➢ *Enhancing Transport Layer Security in SDNs:*

The study by Li, Ma, and Hlaing aims to improve security within Software-Defined Networks (SDNs), specifically focusing on strengthening communication security between the control and data planes. The proposed additions to the Transport Layer Security (TLS) protocol, namely TLSHPS and TLSIHP, address and mitigate potential vulnerabilities and attacks. This highlights continuous efforts to modify security procedures to accommodate changing network technology.

- *Discussion:*

The studies underscore the dynamic nature of information security, which is transforming due to technological progress. Academic researchers are investigating novel frameworks and improvements to conventional models to tackle the evolving security concerns arising effectively.

The task of striking a harmonious equilibrium between privacy and security continues to pose an enduring and complex dilemma. The studies indicate that maintaining a delicate equilibrium becomes increasingly imperative as technologies progress and data sharing become more prevalent.

The interdisciplinary character of information security is evident from the research conducted on the Internet of Things (IoT), blockchain, and Software-Defined Networks (SDNs). The achievement of effective security solutions necessitates the integration and cooperation of various dimensions, including technical, managerial, and societal components.

The necessity of modifying traditional security protocols such as Transport Layer Security (TLS) to accommodate emerging technologies like Software-Defined Networks (SDNs) demonstrates the ongoing commitment to maintaining the efficacy of security measures in dynamic contexts.

- *Possible Future Directions:*

The studies indicate potential avenues for future investigation, including further clarification of information security definitions, examining the intersection between availability and confidentiality, and assessing the alignment between industry-wide security practices and academic research.

The increasing interconnectedness of gadgets gives rise to security breaches that have ramifications not only in the realm of technology but also in broader societal and ethical contexts. The dynamic nature of the security landscape gives rise to discussions regarding strategies for mitigating its possible risks.

This literature reviews emphasise the necessity of standardised methodologies and optimal practises across many domains, such as the Internet of Things (IoT), blockchain technology, and Software-Defined Networks (SDNs). This can potentially enhance the execution of security measures consistently and efficiently.

The ongoing evolution of the CIA trio indicates the need to reassess security frameworks in response to evolving technical advancements and societal dynamics. This phenomenon prompts inquiries on the long-term relevance of such systems.

In summary, the results and analyses from these literature reviews underscore the significance of addressing security apprehensions in a constantly evolving technology environment. The optimisation of the CIA trinity, the augmentation of security protocols, and the investigation of multidisciplinary methodologies constitute pivotal factors for prospective research and implementation endeavours in information security.

IV. CONCLUSION

This study, Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature, highlights the continued significance of the CIA triad as a fundamental concept in information security. The literature review highlights the ever-changing nature of the security environment, in which technological advancements create both favourable prospects and vulnerabilities.

With network systems' increasing complexity and interconnectivity, it is necessary to re-evaluate and expand the old CIA triumvirate. This expansion should incorporate emerging features like privacy, controllability, and authentication. The effective resolution of the complex issues surrounding network security requires adopting a collaborative and multidisciplinary strategy involving the active participation of specialists from various disciplines.

Conclusively, this paper emphasises the need for research that investigates both the theoretical and practical applications of security so that organisations can effectively implement policies. Protecting the confidentiality, integrity, and accessibility of information necessitates a continuous commitment to enhancing security protocols in network systems due to the constant evolution of technology and the ever-changing nature of potential threats.

RECOMMENDATIONS

Based on the analysis of this paper titled "Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature," the following recommendations can be made:

- *Incorporate Emerging Technologies:*

As the field of network systems continues to evolve, it is recommended that future research considers the implications of emerging technologies like IoT, blockchain, and software-defined networking. These technologies bring unique security challenges and opportunities, and understanding their impact on the CIA triad can contribute to more comprehensive security solutions.

- *Holistic Approach to Security:*

While the CIA triad has been a cornerstone of information security, researchers should consider expanding this framework to encompass additional dimensions, such as privacy, controllability, and authentication. A more holistic approach to security can provide a better-rounded understanding of the complex security landscape.

- *Cross-Disciplinary Collaboration:*

Given the interdisciplinary nature of security concerns, collaboration between technical experts, policymakers, and ethicists is crucial. Future research should seek to bridge the gap between technical solutions and societal implications, addressing the broader context in which network systems operate.

- *Practical Implementation:*

While theoretical discussions are valuable, practical implementation of security measures is essential. Researchers should focus on translating theoretical insights into actionable recommendations and guidelines for organisations and practitioners to enhance network systems' confidentiality, integrity, and availability.

- *Continuous Adaptation:*

Information security is not static; it evolves with technology and user behaviour. Researchers should emphasise the need for adaptive security frameworks to respond to changing threats and challenges in real-time.

Organisations can implement security controls to protect against confidentiality, integrity, and availability threats. These controls can include technical controls, such as firewalls, intrusion detection systems, and encryption. They can also include administrative controls, such as user training, security policies, and procedures. Moreover, they can also include physical controls, such as access control and perimeter security.

REFERENCES

[1]. Alenezi, M. and Almuairfi, S. (2020). Essential Activities For Secure Software Development. International Journal of Software Engineering & Applications, 2(11), 1-14. https://doi.org/10.5121/ijsea.2020.11201

[2]. Alguliyev, R. M., Aliguliyev, R. M., Yusifov, F. (2018). Role Of Social Networks In E-government: Risks and Security Threats. Online Journal of Communication and Media Technologies, 4(8). https://doi.org/10.12973/ojcmt/3957

[3]. Banwani, D. and Kalra, Y. (2021). Maintaining and Evaluating The Integrity Of Digital Evidence In Chain Of Custody. International Journal of Recent Technology and Engineering (IJRTE), 3(10), 90-96. https://doi.org/10.35940/ijrte.c6449.0910321

[4]. Carta, S., Podda, A. S., Recupero, D. R., Saia, R. (2020). A Local Feature Engineering Strategy To Improve Network Anomaly Detection. Future Internet, 10(12), 177. https://doi.org/10.3390/fi12100177

[5]. Chai & Zolkipli (2021). "Review on Confidentiality, Integrity and Availability in Information Security," Journal of ICT in Education (2021). doi:10.37134/jictie.vol8.2.4.2021

[6]. Chai, K. Y., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. Journal of ICT in Education, 8(2), 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021

[7]. Covert, Q., Steinhagen, D., Francis, M., Streff, K. (2020). Towards a Triad For Data Privacy.. https://doi.org/10.24251/hicss.2020.535

[8]. Grote, H., Danzmann, K., Dooley, K. L., Schnabel, R., Slutsky, J., Vahlbruch, H. (2013). First Long-term Application Of Squeezed States Of Light In a Gravitational-wave Observatory. Physical Review Letters, 18(110). https://doi.org/10.1103/physrevlett.110.181101

[9]. Horne, C. A., Maynard, S. B., & Ahmad, A. (2017). Organisational Information Security Strategy: Review, Discussion and Future Research. Australasian Journal of Information Systems, p. 21. https://doi.org/10.3127/ajis.v21i0.1427

[10]. Hu, T., Xin, B., Liu, X., Chen, T., Ding, K., Zhang, X. (2020). Tracking the Insider Attacker: A Blockchain Traceability System For Insider Threats. Sensors, 18 (20), 5297. https://doi.org/10.3390/s20185297

[11]. International Journal of Distributed Sensor NetworksVolume 16, Issue 1, January 2020, https://doi.org/10.1177/1550147719899374

[12]. Khan, S. U., & Khan, A. (2019). Security challenges in cloud computing: A review. International Journal of Computer Science and Information Technology, 11(1), 1-10.

[13]. Li, X., Ma, M., Hlaing, C. W. (2021). Improved Handshaking Procedures For Transport Layer Security In Software Defined Networks. TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON). https://doi.org/10.1109/tencon54134.2021.9707184

[14]. Lihua Yin, Binxing Fang, Yunchuan Guo, Zhe Sun, and Zhihong Tian (2020)

[15]. Lundgren, B., & Möller, N. (2017). Defining Information Security. Science and Engineering Ethics, 25(2), 419–441.

[16]. Satoh, T., Nagayama, S., Suzuki, S., Matsuo, T., Hajdušek, M., Meter, R. (2021). Attacking the Quantum Internet. Ieee Transactions on Quantum Engineering, (2), 1-17. https://doi.org/10.1109/tqe.2021.3094983

[17]. Satoh, T., Nagayama, S., Suzuki, S., Matsuo, T., Hajdušek, M., Meter, R. V. (2021). Attacking the Quantum Internet. IEEE Transactions on Quantum Engineering, (2), 1-17. https://doi.org/10.1109/tqe.2021.3094983

[18]. Sayyad, S., Kumar, S., Bongale, A., Kamat, P., Patil, S., Kotecha, K. (2021). Data-driven Remaining Useful Life Estimation For Milling Process: Sensors, Algorithms, Datasets, and Future Directions. Ieee Access, (9), 110255-110286. https://doi.org/10.1109/access.2021.3101284

[19]. Spyridon Samonas and David Coss (2023). The CIA Strikes Back: Redefining Confidentiality, Integrity, and Availability in Security. Journal of information security. ISSN: 1551-0123 Volume 10, Issue 3, www.jissec.org

[20]. Tangle (2018). Version 1.4.3, https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.

[21]. Whitman, M. E., & Mattord, H. J. (2017). The CIA triad: Confidentiality, integrity, and availability (4th ed.). Waltham, MA: Elsevier/Morgan Kaufmann.