Evaluating the Role of Confidentiality, Integrity, and Availability in Cyber Defence

Akash Tripathi

LLM
School of Law Justice and Governance
Gautam Buddha University

Abstract:
This paper examines the critical roles of confidentiality, integrity, and availability, collectively known as the CIA triad, in modern cyber defence. The CIA triad has long been a foundational model in information security, and this review evaluates how each component contributes to protecting systems against evolving cyber threats. We discuss the meaning and significance of confidentiality, integrity, and availability in the context of cybersecurity and analize how they guide the design of defence strategies. Each element is explored in depth, highlighting common threats (such as data breaches, tampering attacks, and denial-of-service incidents) and corresponding safeguards and best practices. The interdependence among confidentiality, integrity, and availability is also evaluated, noting that an effective security posture requires a balanced approach that does not excessively favour one aspect at the expense of the others. We further consider the trade-offs organizations face in prioritizing these principles under different scenarios and requirements. Finally, emerging challenges are discussed: from the proliferation of Internet-of-Things (IoT) devices to the advent of quantum computing, new developments are testing the traditional CIA framework. The paper concludes that, despite new complexities and calls to expand security models, the CIA triad remains an essential guiding framework in cyber defense, albeit one that must be continually adapted to address modern threats.

Keywords: Cybersecurity, CIA Triad, Confidentiality, Integrity, Availability, Information Security, Risk Management, Data Protection, Network Security, Ransomware, Denial-of-Service (DoS), Cyber Threats, Information Assurance, Security Architecture, Human Factors in Cyber Defense.

INTRODUCTION

Cyber defense strategies fundamentally revolve around protecting information and systems from unauthorized access, alteration, and disruption. The concepts of confidentiality, integrity, and availability, often referred to as the *CIA triad*, form the cornerstone of information security practice and theory (Chai & Zolkipli, 2021). These three principles are widely recognized as the primary objectives that security controls and policies aim to achieve in order to safeguard data and ensure trust in digital systems (Alhassan & Adjei-Quaye, 2017). The CIA triad provides a simple yet powerful framework: confidentiality focuses on preventing unauthorized disclosure of sensitive information, integrity ensures that information remains accurate and uncorrupted, and availability guarantees that authorized users have reliable access to information and services when needed. Together, these principles cover the fundamental aspects of protecting information assets, and a failure in any one of them can undermine an organization's cyber defense posture.

In practice, nearly every cyber threat or security incident can be understood as an attack on one or more components of the CIA triad. For example, the theft of confidential customer data in a breach represents a breakdown in confidentiality, the unauthorized modification of code or records by a malicious actor is a violation of integrity, and a distributed denial-of-service (DDoS) attack that crashes a server directly impacts availability. By analyzing incidents and defence mechanisms through the lens of confidentiality, integrity, and availability, cybersecurity professionals can ensure that they address the full spectrum of risks (Yee & Zolkipli, 2021). Indeed, many international standards and frameworks, such as the ISO/IEC 27000 series, explicitly define information security in terms of preserving confidentiality, integrity, and availability of information.

This underscores the triad's importance as a unifying model for security objectives across different industries and domains.

However, maintaining all three aspects of the triad simultaneously is a challenging task. In real-world systems, there are often trade-offs and tensions between confidentiality, integrity, and availability. Measures to maximize one aspect can sometimes impose limitations on the others. For instance, extremely strict confidentiality controls might require heavy encryption and multi-factor authentication that could introduce latency or complexity, potentially hindering availability or timely access for authorized users. Conversely, prioritizing availability, such as keeping a system openly accessible and redundant for reliability, might open more avenues for potential breaches, impacting confidentiality or integrity if not carefully managed. Organizations must balance these priorities based on their specific threat environment and operational needs (Aminzade, 2018). A military communications system, for instance, might prioritize confidentiality of classified data above all, whereas a public-facing e-commerce website might value availability (uptime and responsiveness) as the top concern to avoid revenue loss, all while still needing to ensure basic data integrity and privacy. Effective cyber defense requires understanding the **context** in which these principles apply and making informed decisions to achieve an optimal balance (Filiz, 2023).

Another important consideration is that the CIA triad, while fundamental, is not exhaustive. Researchers and practitioners have pointed out that other security objectives, such as authenticity, accountability, or non-repudiation, also play vital roles in certain scenarios. Some have proposed extended models (e.g., adding additional pillars to the triad) to address these facets, Donn Parker's "Parkerian hexad," for example, includes authenticity, possession, and utility in addition to the traditional triad. These perspectives suggest that *confidentiality, integrity, and availability*, though necessary, may not alone suffice to characterize all security needs (Lundgren & Möller, 2017). Nevertheless, the CIA triad remains widely used because it captures the most common and universally applicable security goals in a clear manner. It provides a foundational vocabulary for discussing security trade-offs and for aligning security measures with organizational objectives (Alhassan & Adjei-Quaye, 2017).

This paper provides a comprehensive review of each component of the CIA triad in the context of cyber defence, evaluating how confidentiality, integrity, and availability individually and collectively contribute to mitigating threats. We will examine each element in depth in the following sections (confidentiality, integrity, availability), exploring their roles in safeguarding systems and data. We then discuss how these elements overlap and sometimes conflict, including strategies for balancing them. We also address emerging trends and technologies that are shaping the implementation of the CIA principles. By understanding both the enduring importance of the CIA triad and the new challenges that require its adaptation, we gain insight into building stronger, more resilient cyber defences for the future.

CONFIDENTIALITY IN CYBER DEFENCE

Confidentiality is the aspect of information security that aims to ensure that sensitive information is accessible only to those who are authorized to access it. In other words, confidentiality means preventing unauthorized disclosure of information. This concept is vital in cyber defence because unauthorized access or leakage of data can have severe consequences, ranging from privacy violations and intellectual property loss to undermining of national security. In formal terms, confidentiality has been defined as the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO/IEC, 2018). In practice, maintaining confidentiality involves a combination of technical controls, policies, and user training to make sure that private data remains private (Yee & Zolkipli, 2021).

Common mechanisms to enforce confidentiality include authentication and access control systems (to ensure only approved users or systems can access information), encryption (to protect data in transit and at rest from eavesdroppers), and network security measures like firewalls and secure communication protocols (to prevent interception of data). For example, when you send your credit card information to an online store, protocols such as TLS/SSL are used to encrypt that data, safeguarding its confidentiality from anyone who might be listening on the network. Likewise, stored data such as password databases are often hashed or encrypted so that even if attackers gain entry, they cannot easily extract the actual confidential information. In organizational settings, the principle of least privilege is applied: each user or system component should have the minimum access rights necessary to perform its function, thereby limiting exposure of confidential data (Cirnu et al., 2018). If a database administrator does not need access to certain HR records, for instance, then

technical controls should enforce that those records remain inaccessible to that administrator's account. By tightly regulating who or what can see which pieces of information, organizations aim to reduce the risk of data falling into the wrong hands.

The importance of confidentiality in cyber defence is evident from the prevalence and cost of **data breaches**. Breaches that expose personal identifiable information (PII), financial records, health records, or trade secrets are extremely damaging. Such incidents not only harm the individuals whose data is exposed but also cause immense reputational and financial damage to organizations. As a result, confidentiality is often a primary focus of cybersecurity efforts and compliance regimes. Regulations like the European Union's GDPR or healthcare's HIPAA rules are fundamentally about ensuring confidentiality of certain data categories (with legal penalties if organizations fail to protect that data). These regulations force organizations to implement appropriate controls and to promptly report if confidentiality is broken. Thus, cyber defense strategies usually place heavy emphasis on preventing unauthorized data access, through methods such as continuous monitoring for intrusions, data loss prevention systems, and rigorous identity management (Filiz, 2023).

Despite robust measures, threats to confidentiality are constantly evolving. Attackers employ techniques like social engineering to trick employees into divulging passwords or sensitive documents, bypassing technical controls by exploiting human trust. Phishing emails remain one of the most common initial vectors for breaching confidentiality, as they can deceive users into giving away credentials or executing malicious code. Malware such as spyware is specifically designed to covertly collect confidential information from infected systems and send it back to the attacker. More sophisticated adversaries might use man-in-the-middle attacks to intercept communications or deploy network sniffers to capture unencrypted data traveling over networks. If adversaries gain a foothold inside a network (e.g., via a compromised account or system), they often engage in lateral movement to find and exfiltrate sensitive data, a tactic seen in many advanced persistent threats. High-profile incidents like the data breaches at large corporations or government agencies often involve attackers working patiently to avoid detection, sometimes using legitimate credentials, thereby making the protection of confidentiality extremely challenging even for well-defended organizations (Osazuwa, 2023).

Ensuring confidentiality also relies on addressing insider threats and human error. Not all breaches come from external hackers, insiders with legitimate access can intentionally leak information (for example, a disgruntled employee stealing data), or unintentionally cause exposure through negligence (such as misconfiguring a cloud storage bucket to be public). Human error is a significant factor; something as simple as sending an email with sensitive data to the wrong recipient or losing an unencrypted laptop can compromise confidentiality. Thus, a comprehensive cyber defense includes not only technical safeguards but also **policies** (like clear data classification and handling rules) and training programs to educate staff about their role in protecting sensitive information (Cirnu et al., 2018). Regular audits and monitoring can help detect when confidential data is being accessed or transferred in ways that deviate from the norm (as might occur during an insider attack or malware exfiltration), thereby enabling a quicker response to potential breaches.

In the realm of national security and military cyber defense, confidentiality often takes on even greater priority. Classified information, intelligence data, and defense systems plans are guarded with layered controls (including physical security, air-gapped networks, etc.) to prevent espionage. The stakes are extremely high: if an adversary steals military secrets or critical intellectual property, it could erode strategic advantage and even threaten lives. The classic example is the need to keep encryption keys and diplomatic communications confidential during wartime or international negotiations. Historically, breaches of confidentiality such as the leaks of sensitive government documents have had geopolitical consequences. These examples underline why confidentiality measures in such environments are extraordinarily strict (often sacrificing convenience or availability to some extent). Systems might employ encryption that is virtually unbreakable with current technology, multi-person access approval (two-person rule) for critical data, and constant surveillance for any anomaly that might indicate a leak (Whyte, 2024).

To bolster confidentiality, many organizations are now leveraging emerging technologies. For instance, blockchain technology (best known for cryptocurrencies) is being explored as a means to secure data sharing in environments like IoT networks; by its design, blockchain can provide a decentralized yet secure way to control access and record transactions so that data is not tampered with or improperly accessed (Alam, 2019; Almarri & Aljughaiman, 2024). Additionally, as the threat of quantum computing to current cryptographic algorithms looms on the horizon, research into quantum-resistant encryption and even quantum cryptography (like quantum key distribution) has gained momentum. Quantum cryptography promises new methods to

ensure confidentiality by leveraging the laws of physics, for example, any eavesdropping on a quantum communication can be detected inherently due to the disturbance it causes in the system (Whyte, 2024). These developments highlight that while the core principle of confidentiality remains the same, the tools and techniques to enforce it continue to evolve alongside the threat landscape.

In summary, confidentiality is a fundamental pillar of cyber defense concerned with protecting sensitive information from unauthorized access and disclosure. Achieving confidentiality requires a blend of technical safeguards (encryption, access controls, etc.), organizational policies, and awareness training. The success of these measures is constantly challenged by malicious actors employing both technological exploits and social engineering, as well as by inadvertent mistakes from legitimate users. Strong confidentiality controls are essential not only for compliance with laws and protection of privacy but also for maintaining trust, customers trust companies with their data, citizens trust governments with national security information, and businesses trust partners not to leak trade secrets. As part of the CIA triad, confidentiality works in conjunction with integrity and availability to provide a comprehensive defence strategy, which we will explore further in the following sections.

INTEGRITY IN CYBER DEFENCE

Integrity in the context of information security refers to the trustworthiness, accuracy, and consistency of data and systems. Maintaining integrity means that information has not been improperly altered or tampered with, whether intentionally or accidentally, and that systems function in an unimpaired manner. In essence, integrity ensures that when you access data or a system, you can trust that it is in the correct state as expected, and that it has not been corrupted or manipulated en route. This concept is crucial in cyber defence because even if data remains confidential (hidden from unauthorized eyes) and systems are available, a loss of integrity can still render information useless or dangerous. For example, if an attacker subtly alters transaction records in a bank's database, the confidentiality might remain intact (no outsider sees the data) and the system might be up (availability), but the integrity failure could lead to fraud or financial chaos. Thus, integrity is about safeguarding the accuracy and reliability of information and systems, assuring that what you see or use is authentic and unmodified (Aminzade, 2018).

Threats to integrity come in many forms. A classic example is a website defacement, where an attacker changes the content of a public website, this is a direct integrity attack, undermining the trust in the information displayed. More insidious are attacks where data is altered without immediate obvious signs: for instance, an attacker gaining unauthorized access to a database and changing values (like modifying someone's account balance, or altering logs to cover tracks). Such manipulation might be detected only much later, or not at all if no proper integrity checks exist. Malware can also cause integrity breaches: certain viruses or worms might intentionally corrupt data, and ransomware not only locks data (affecting availability) but sometimes also alters or threatens to release data, impacting its integrity and confidentiality concurrently. Insider threats are particularly relevant to integrity; a disgruntled employee could alter or delete critical files (e.g., change figures in a financial report, or sabotage product designs), causing great harm. Even without malicious intent, integrity can be compromised by human error or software bugs, like a faulty script that introduces errors into a dataset, or a technician accidentally deleting important records. Cyber defense must guard against all these possibilities to maintain the integrity of information (Osazuwa, 2023).

A key strategy to preserve integrity is the use of hashing and checksums. Hash functions can generate a unique fingerprint for data (a hash value) such that any change in the data, even a tiny bit, produces a different hash. By storing and routinely verifying these hashes (for example, for critical files or system images), one can detect if any unauthorized changes have occurred. This is the principle behind file integrity monitoring systems: they compute hashes of vital system files and configurations and alert administrators if any modifications are detected that were not authorized. Similarly, digital signatures combine hashing with cryptography to not only detect changes but also to verify the source of the data, ensuring authenticity along with integrity. For instance, software updates are often signed by the vendor; your system will verify the signature before installing to confirm that the update indeed comes from the legitimate source and hasn't been tampered with in transit. Insecure software update mechanisms that lack these checks have been exploited in the past by attackers to distribute malware (a notable example being certain supply chain attacks where attackers compromised an update server to push out malicious updates). Such incidents highlight why integrity checks are vital.

Another important aspect of integrity in cyber defense is access control and change management. Only authorized individuals or processes should be able to modify critical data or system configurations. By tightly controlling who can make changes (for example, requiring special admin privileges or multi-factor authentication for any changes to critical systems, and logging all changes), organizations reduce the risk of unauthorized modifications. Change management processes also typically involve reviews and approvals, which can catch errors or malicious intents before they propagate. For example, a code review process in software development can spot an introduced bug or backdoor that would affect integrity if deployed. In high-security environments, a **two-person rule** might be used for performing sensitive actions, ensuring no single individual can unilaterally alter important data without a second person validating it. Such measures directly reinforce the integrity of operations (Cirnu et al., 2018).

Integrity is also deeply connected to the concept of non-repudiation and accountability in security. Maintaining integrity of logs and records means that in the event of an incident, one can investigate what happened reliably. If an attacker can alter system logs, they might erase traces of their activities (which is why secure logging mechanisms, possibly external write-once logs, are used to preserve a true record). In legal and forensic contexts, evidence needs to be preserved with proven integrity; digital forensics employ hashing and strict chain-of-custody procedures to ensure that any digital evidence collected (say from a suspect's computer) remains unaltered from collection to courtroom presentation (Banwani & Kalra, 2021). A failure in integrity there could lead to evidence being thrown out or wrong conclusions being drawn, with serious consequences. Thus, ensuring integrity underpins trust not only in operational data but also in investigative and legal processes.

Cyber-physical systems and safety-critical infrastructure provide stark examples of why integrity is paramount. Consider an industrial control system (ICS) managing a power grid or a chemical plant. If an attacker or error changes the sensor readings or control parameters (integrity attack), the operators might be misled about the true state of the system. In 2015, for example, a power grid cyber attack in Ukraine involved, among other things, the attackers manipulating breaker status and even wiping firmware, a mix of availability and integrity attacks that made it extremely difficult for operators to manage the outage. Or consider medical devices: if patient data or device settings are altered, it could directly put lives at risk. Ensuring integrity in such systems often involves redundancy and fail-safes, multiple channels of data that cross-verify each other, alarm thresholds that detect anomalous changes, and the ability to revert to known-good states if a discrepancy is detected. In many cases, integrity overlaps with safety: a breach of integrity might translate to unsafe conditions, so systems are designed to default to secure or offline states if integrity cannot be assured.

There are specific integrity-focused attacks that have gained attention. One is data poisoning, particularly in the context of machine learning and AI. If an adversary can subtly manipulate the training data used for an AI system, they can compromise the integrity of that model's output (for instance, causing it to misclassify certain inputs in a way advantageous to the attacker). This is a growing concern as AI systems become more prevalent in cybersecurity as well as other domains. Another is the spread of misinformation or deepfake content in information systems, which can be viewed as an attack on the integrity of information (though this drifts into a broader notion of integrity beyond just technical systems). While misinformation is typically tackled with different tools (media literacy, content verification), it highlights that integrity of information is also a societal challenge, not purely a technical one.

To address integrity threats, the cybersecurity field has developed numerous controls and best practices. Beyond hashing and access control, as mentioned, organizations use intrusion detection and prevention systems that watch for suspicious actions which could indicate an integrity breach (like unexpected processes attempting to modify protected files). Regular backups are an essential part of integrity strategy: if data is corrupted or altered, having recent backups allows restoration of the correct state (assuming the backup itself is secure and its integrity is verified). In fact, many businesses have been saved from catastrophic ransomware attacks by relying on offline backups to restore data to a pre-encryption state, thus mitigating both the availability and integrity impact of such attacks. Some systems implement read-only or append-only modes for certain critical data. For example, append-only logs ensure that once data is written it cannot be modified, new entries can only be added. This is a common feature in secure logging and in some database configurations for audit trails (Tchernykh et al., 2019).

Blockchain technology provides an interesting case study in integrity. A blockchain (like that underlying cryptocurrencies or various decentralized ledger applications) is essentially an append-only ledger of

transactions secured by cryptographic hashing and distributed consensus. Once a block of transactions is added to the chain and enough subsequent blocks are appended, it becomes computationally infeasible for any single party to alter the earlier data without it being detected by others. This makes blockchain ledgers highly tamper-resistant. Consequently, there's a growing interest in using blockchain or similar distributed ledger approaches to ensure data integrity in applications beyond finance, such as supply chain recordkeeping, where maintaining an immutable record of provenance is important, or in securing IoT data (Guguelot et al., 2023). While blockchain is not a silver bullet and introduces other challenges (like scalability and the need for consensus mechanisms), it demonstrates how cryptographic techniques and decentralization can enforce integrity even in a trustless environment.

In summary, integrity is about trust in the accuracy and completeness of information and the correct operation of systems. In cyber defence, protecting integrity involves measures that detect and prevent unauthorized or unintentional changes to data and systems. It is equally important as confidentiality: a system where data can be silently altered is just as insecure as one where data can be stolen or one that is often down. Each of these situations undermines the reliability and trustworthiness of the system. Organizations must implement integrity controls like hashing, digital signatures, strict access controls for modifications, monitoring for changes, and robust backup and recovery procedures. By maintaining integrity, defenders ensure that when decisions are made based on data (whether by humans or automated processes), those decisions are based on correct information. As we continue, we will look at the third piece of the triad, availability, and later consider how all three work together and sometimes require balancing in the face of limited resources and evolving threats.

AVAILABILITY IN CYBER DEFENCE

Availability is the security principle that ensures that information systems and data are accessible to authorized users whenever needed. In practical terms, maintaining availability means keeping services online, networks running, and data retrievable in a timely manner. A system with poor availability, even if its data is secure from disclosure and alteration, fails its purpose, as legitimate users are unable to use it or get the information they require. In cyber defence, ensuring availability involves protecting systems against a range of disruptions, from malicious attacks like denial-of-service to unexpected outages caused by hardware failures or natural disasters. According to standard definitions (e.g., ISO/IEC 27000), availability is the property of being accessible and usable upon demand by an authorized entity. This implies not just uptime, but also performance meeting expected service levels (an extremely slow system may technically be "up" but not effectively usable, which is also an availability issue). Availability is especially critical in contexts such as healthcare (e.g., hospital systems must be up for patient care), industrial control (power grids, manufacturing can't afford downtime), and financial services (where trading or transaction systems being unavailable even for minutes can have large economic impacts).

Threats to availability are perhaps the most visibly disruptive types of cyber incidents because they can cause immediate loss of service. The most notorious are Denial-of-Service (DoS) attacks, including Distributed Denial-of-Service (DDoS) attacks. In a DDoS attack, an attacker harnesses a large number of compromised machines (a botnet) or otherwise uses techniques to flood a target server or network with traffic, overwhelming its capacity and rendering it unable to respond to legitimate users. These attacks have grown in scale; in recent years, some DDoS attacks have peaked at terabits per second of malicious traffic. They can be motivated by anything from hacktivism and vandalism to more strategic goals (for instance, as a diversion while another attack is carried out, or as an extortion attempt where the attacker demands ransom to stop the attack). Ensuring availability means having defenses like DDoS protection services, load balancers, or network filtering that can absorb or block malicious traffic surges. Techniques such as rate limiting, traffic anomaly detection, and having distributed infrastructure (so that no single point is overwhelmed) are common ways to mitigate DDoS threats (Osazuwa, 2023).

Apart from direct attacks, availability can be compromised by malware. Ransomware is a prime example: it encrypts a victim's data, effectively locking the rightful user out , which is a direct hit to availability of data (and often also an integrity attack, since the data is altered by encryption). Ransomware incidents in the past decade have affected hospitals, city governments, and businesses worldwide, causing critical services to halt until systems could be restored, sometimes from backups. These incidents highlight how an attacker doesn't always need to steal or leak your data to harm you; simply denying you access to your own data can be

catastrophic. Other malware might delete files or crash systems (like wiper malware that intentionally destroys data, often used in cyberwarfare scenarios). Even without malware, software or hardware failures can cause downtime. A bug in software might cause a system to hang or repeatedly crash under certain conditions, or a faulty update might render a service unusable , thus, robust testing and phased rollouts are important to preserve availability. Similarly, hardware failures (like a failed disk, power supply, or network cable) are mundane but inevitable events that systems must be designed to withstand (Tchernykh et al., 2019).

Ensuring availability therefore involves both preventative measures and redundancy. Preventative measures include regular maintenance (patching software to prevent crashes or exploitation, replacing aging hardware before it breaks, etc.) and proactive monitoring (detecting when system performance is degrading or when components might be failing, so one can intervene before a total outage). Redundancy is the principle of eliminating single points of failure: critical systems should have backup components or failover mechanisms. For example, important servers might be clustered so that if one node goes down, others can take over the load. Data might be replicated across multiple storage systems or data centers, so that if one location is lost (due to a disaster or an attack), the data is still available elsewhere. Cloud computing has made it easier for even smaller organizations to achieve high availability by distributing workloads across multiple geographic regions and using services that automatically balance and recover. However, cloud services themselves can have outages, so even then, cross-cloud or hybrid solutions are sometimes used for extreme availability requirements (Khan & Khan, 2019). A well-known guideline in industry is to avoid having any "single point of failure" , any component whose failure would bring down the entire service.

Another facet of availability in cyber defence is the concept of resilience. Resilience is the ability of a system to recover quickly and continue operating even after an incident has occurred. This goes hand-in-hand with availability: rather than just trying to prevent every possible disruption (which is impossible), assume that disruptions will happen and plan for how to minimize impact and recover. Incident response planning and disaster recovery planning are thus key. Organizations often develop Business Continuity Plans that detail how operations will continue in the face of various crises (cyber attacks, natural disasters, etc.), which often includes backup communication channels, alternative systems, and manual workarounds to keep essential functions going. Regular drills and simulations (like disaster recovery tests, where an organization practices restoring IT systems from backups) help ensure that when a real incident hits, the team can restore availability with minimal delay (Filiz, 2023).

One challenge with availability is that it can sometimes conflict with confidentiality and integrity in terms of priorities. Consider encryption: using strong encryption on data could, in some scenarios, impact availability if the encryption keys are lost (then the data becomes permanently inaccessible). Or if encryption/decryption processes introduce latency, they might reduce system responsiveness. Administrators sometimes face tough choices during incidents: for example, if a system is possibly compromised (integrity in question), is it better to take it offline immediately (impacting availability) to prevent further damage, or keep it running to maintain service while investigating? In many cases, critical infrastructure systems are designed to fail safe in favor of availability or safety. A classic example is that in industrial systems, if certain control signals are lost, the system might default to a safe mode (which might mean stopping a process to avoid hazard) , that's an availability impact accepted for safety reasons. In contrast, in some environments, availability must be maintained at almost any cost (for example, a life-critical medical device should not just shut down completely even if it detects some security issue; it might attempt to keep a degraded but working mode). The **balance** between these aspects depends on context, as we will discuss more in the next section (Aminzade, 2018).

Attacks on availability do not always target obvious production systems. Sometimes they target backups or auxiliary systems in order to hamper recovery. For instance, some ransomware attackers first try to find and encrypt or destroy backup files and systems before locking the primary data, so that the victim cannot easily restore and thus is more likely to pay a ransom. This is why it is often said in IT that backups are useless without offline or off-site copies (so attackers can't reach them) and without regular testing (to ensure the backups actually work for restoration). A comprehensive cyber defence for availability will ensure that backup mechanisms themselves are robust and secure. Additionally, monitoring network and service health in real time is crucial , sophisticated operations centers have dashboards and automated alerts to detect outages or performance degradation the moment they occur (or even before, if predictive monitoring is possible), so that engineers can quickly address issues before they escalate (Tchernykh et al., 2019).

In terms of metrics, availability is often measured as a percentage of uptime over a period. For example, "five nines" availability (99.999%) is a benchmark for high-availability systems, which corresponds to only a few minutes of downtime per year. Achieving such high levels often requires significant investment in redundancy, rapid failover capabilities, and efficient processes. Not every system needs that level of availability, some internal systems might tolerate a bit of downtime for maintenance, etc., but mission-critical public services often aim for at least 99.9% or more. Cloud service providers typically advertise high availability and geographically distributed architectures to support it, but they also lay out in contracts (Service Level Agreements) what compensation occurs if availability drops below certain thresholds.

Emerging technologies can also contribute to availability. For example, edge computing can enhance availability by distributing computing tasks closer to users, so that even if connectivity to a central server is lost, some functionality remains at the edge. Similarly, the adoption of Software-Defined Networking (SDN) and intelligent routing can help dynamically reroute traffic during outages or attacks, keeping services reachable (Osazuwa, 2023). The use of AI in managing infrastructure can also potentially predict and auto-correct issues that might lead to downtime. On the flip side, these new technologies introduce their own complexities and potential vulnerabilities (SDN controllers themselves must be highly secure and available, for instance, or they become an Achilles' heel).

In conclusion, availability is about ensuring continuous, reliable access to systems and data for legitimate users. For cyber defense, this means defending against attacks that would take systems offline or make data inaccessible, as well as engineering systems to be robust against accidents and failures. Availability is often what separates a theoretical secure system from a practically usable system; it's a reminder that security is not just about keeping bad actors out, but also about keeping services running. A comprehensive cybersecurity strategy therefore dedicates significant attention and resources to availability: from network design and server architecture to incident response and disaster recovery planning. In the next section, we will examine how the three elements of the CIA triad, confidentiality, integrity, and availability, interact with each other, and the necessity of balancing these priorities in real-world cyber defence scenarios.

BALANCING AND INTERDEPENDENCE OF THE CIA TRIAD

The principles of confidentiality, integrity, and availability are conceptually distinct, but in practice they are deeply interdependent. A robust cyber defence must address all three simultaneously, and a weakness in any one can undermine the others. It is often said that the CIA triad is only as strong as its weakest link; neglecting any of the three aspects can leave a glaring vulnerability that attackers may exploit. For instance, an organization might invest heavily in confidentiality, encrypting data, enforcing strict access controls, and maintain good integrity checks on data, but if it ignores availability by not protecting against DDoS attacks or not having reliable backups, a simple outage could cripple its operations. Conversely, an organization might build very resilient, highly available systems but misconfigure an access control (a confidentiality lapse), leading to a breach of sensitive data. Thus, balance is key. Achieving the right balance, however, is not trivial and often involves trade-offs, cost considerations, and risk assessments (Aminzade, 2018).

One way to conceptualize balancing the triad is through risk management. Organizations perform risk assessments to identify threats and vulnerabilities affecting confidentiality, integrity, and availability, then prioritize mitigations based on the potential impact and likelihood of those risks. If a company processes medical data, the risk of confidentiality breaches (leaking patient records) is extremely high impact (due to privacy laws and ethics), so it will allocate significant resources to encryption, access logging, and monitoring for unauthorized access. If the same company also operates life-critical medical equipment, availability and integrity of those systems become paramount because lives could depend on them being operational and accurate. This might mean building in extra redundancy, even if it's expensive, and perhaps accepting slightly lower confidentiality on certain system telemetry if that data needs to be widely available to keep systems running in emergencies. A purely theoretical approach that maximizes all three at once might not be feasible due to resource constraints or technical limits, so practical cyber defence finds an acceptable equilibrium (Filiz, 2023). The equilibrium can differ between sectors: for example, the military, as mentioned, often errs on the side of confidentiality (secrecy), whereas public cloud service providers heavily emphasize availability and integrity (nobody will use a cloud service that isn't reliable or corrupts customer data, even if it promised perfect confidentiality).

There are scenarios where efforts to improve one element inadvertently impact another. A common example is system usability (availability's practical side) vs security (often associated with confidentiality/integrity). If a system is locked down with too many security prompts, forced password changes, complex procedures, users may find ways to circumvent them (like writing down passwords or using unofficial channels), which ironically can reduce security. This highlights that human factors play a role in balancing CIA too. Security policies must be practical or people will create workarounds that endanger all three principles. An overly restrictive policy might ensure confidentiality on paper but lead to frustrated users finding alternative methods to share data (potentially outside monitored channels, thus risking an integrity or confidentiality breach). Therefore, a human-centric design that considers ease of use can actually enhance overall security by keeping the system both secure and accessible in the intended way.

Another angle to balancing the triad is during incident response. When an attack occurs, defenders might have to prioritize one goal over others in their immediate response. For example, if a database is suspected to be compromised (integrity in question), the team might decide to take it offline to prevent further damage (thus sacrificing availability until integrity can be verified). Alternatively, if a system is under a heavy DDoS attack, one might temporarily restrict certain functionalities or access from certain regions (affecting availability for some users) in order to keep the core service up for most users, thereby maintaining broader availability at the expense of some. These decisions often need to be made under pressure and with limited information. Preparing in advance with a clear understanding of what's most critical to protect helps. This is why critical systems often have predefined **incident response plans** that outline, for various scenarios, which services can be sacrificed and which cannot, as well as communication plans and failover steps. Those plans are essentially a playbook of how to balance CIA when things go wrong (Cirnu et al., 2018).

The interdependence of CIA also means that improving one aspect can reinforce the others. For instance, implementing strong authentication and access control (a confidentiality measure) not only keeps data secret but can also prevent unauthorized changes (supporting integrity) and misuse of resources (which could hamper availability). Encrypting data (confidentiality) can indirectly enhance integrity too, because encrypted data that an attacker can't understand is also data they cannot easily manipulate in a meaningful way. Regular data integrity checks and backups (integrity measures) obviously help with integrity, but they also boost availability , if something goes wrong, you have backups to restore availability. Likewise, high availability architectures improve integrity and confidentiality indirectly by reducing the window of opportunity and the chaos that attackers could exploit during downtimes or failovers. When systems are designed to continue operating, it means security controls within them also continue to function, logs continue to be collected (useful for integrity and accountability), etc. In contrast, in a poorly designed system, a crash might lead to turning off security controls or missing logs, which then opens doors for further compromise. Thus, a holistic approach to security architecture considers all three aspects together rather than siloing them (Osazuwa, 2023).

Research and industry practice have started to emphasize concepts like resilience and zero trust that inherently require balancing CIA. *Resilience*, as mentioned, is about continuing operations under adverse conditions , a resilient system might degrade gracefully but not fail outright. To achieve this, it often must have integrated security that does not become a single point of failure. For example, if a network segment is compromised (confidentiality/integrity breach), a resilient architecture contains the damage (so availability elsewhere is preserved), and there are processes to restore both security and service quickly. Zero Trust Architecture (ZTA) is a modern security paradigm that essentially says no user or device is inherently trusted, even if inside the network perimeter. Every access is verified, and movement within the network is tightly controlled. Implementing zero trust can strengthen confidentiality and integrity massively (as it becomes very hard for an attacker to escalate privileges or move laterally), but it can pose availability and performance challenges (because every action might require authentication or verification, adding overhead). Adopting zero trust thus requires careful engineering so that security checks are efficient and do not bottleneck the system. It's a balancing act: maximize verification (security) while minimizing latency (availability impact). Many organizations are gradually moving to this model, finding that advances in technology (like faster authentication mechanisms, behavioral analytics, etc.) can reduce the friction so that security is improved without noticeable loss of availability.

The CIA triad's balance is also tested by emerging trends. We are incorporating IoT devices into networks by the billions, many of which are resource-constrained and sometimes lack built-in strong security. These

devices often perform critical functions (like in smart homes, healthcare monitors, industrial sensors). Ensuring confidentiality and integrity on them (through encryption, firmware validation, etc.) is challenging due to limited computing power, yet their availability is also crucial (a sensor that goes offline or reports wrong data can cause bigger system failures). Researchers are actively working on lightweight cryptographic protocols and integrity checks suitable for IoT, as well as management frameworks to keep those devices updated and monitored (Guguelot et al., 2023). Meanwhile, cloud computing concentrates a lot of data and services on shared infrastructure. Cloud providers invest heavily in all three: confidentiality (through tenant isolation, encryption options), integrity (through rigorous internal controls and audits), and availability (through redundancy across data centers). Outages in major cloud platforms have wide ripple effects, so the balance there is almost a contractual obligation. Cloud customers, however, must understand their responsibilities too, like configuring their cloud storage permissions correctly (to avoid confidentiality breaches) and using the provided tools to set up backups and multi-zone deployments (to ensure availability). The phrase "shared responsibility model" in cloud indicates that the cloud operator handles some aspects (e.g., physical data center security, infrastructure uptime), but the customer must correctly utilize the service (for instance, a misconfigured cloud database left open to the public is a confidentiality failure on the customer's part, not the provider's). Balancing CIA in the cloud context requires collaboration and clear delineation of these responsibilities (Tchernykh et al., 2019).

It is worth noting that not all data or systems require the same level of protection for all three elements. This realization allows more nuanced balancing. Data classification is a practice where data is categorized (e.g., public, internal, confidential, secret, top secret) and security controls are tuned accordingly. Public data (like a company's marketing material on its website) doesn't need confidentiality (it's meant to be public), but its integrity and availability are still important (you don't want your website defaced or frequently down). For such data, one might primarily focus on availability and integrity controls and not worry about confidentiality beyond preventing unauthorized early access or modifications. On the other hand, personal customer data or trade secrets need strong confidentiality and integrity, whereas a brief downtime might be acceptable occasionally if it means better protection (some organizations might deliberately take sensitive systems offline when not in use to reduce attack surface). By classifying assets and understanding their value and role, security teams can allocate resources in a balanced way that meets the actual needs. This targeted approach prevents over-engineering (wasting effort securing trivial data) and under-engineering (failing to secure vital data) (Alhassan & Adjei-Quaye, 2017).

In summary, the CIA triad elements reinforce each other, and effective cyber defense treats them as a unified whole. Balancing them involves understanding context, potential impact, and organizational priorities. There is no one-size-fits-all solution; instead, the balance is achieved through risk management, thoughtful architecture, and continuous adjustments. As threats evolve and organizations change (new technologies, business models, etc.), the balance may need re-tuning. What remains constant is the need to avoid neglecting any one of the triad's components. Cybersecurity practitioners must remain vigilant that in shoring up defenses, they don't create blind spots. In the next section, we turn to the future: how emerging challenges and technologies may influence the role of confidentiality, integrity, and availability in cyber defense, and what adaptations might be necessary.

EMERGING CHALLENGES AND FUTURE DIRECTIONS

As the digital landscape rapidly evolves, so do the challenges in maintaining confidentiality, integrity, and availability. The core principles of the CIA triad remain as relevant as ever, but the tactics and technologies to uphold them must adapt to new contexts. One of the significant shifts in recent years is the sheer scale and complexity of systems that need protection. The rise of the Internet of Things (IoT) means potentially millions of devices, from smart home appliances to industrial sensors, are connected to networks. Many of these devices have limited processing capabilities and sometimes rudimentary security. This creates new vulnerabilities: attackers might compromise a simple IoT device (like a thermostat or camera) and use it as a foothold to attack confidentiality (steal data from the network), integrity (inject false sensor readings), or availability (as part of a botnet in a DDoS attack). Defending the CIA triad in IoT environments requires lightweight yet effective security measures and possibly new architectural approaches. For example, network segmentation is often recommended: isolate IoT devices on their own network segments so that even if compromised, they cannot freely communicate with more sensitive parts of the network (Cirnu et al., 2018).

Additionally, ensuring integrity of IoT data might involve using blockchain or distributed ledgers to log device transactions in an immutable way (as some research like Guguelot et al. (2023) suggests, using decentralized blockchain techniques to enhance security and privacy of IoT data). Confidentiality in IoT may rely on new encryption schemes tailored for constrained devices, as well as cloud-assisted security where heavy computations are offloaded.

Another burgeoning challenge is the advent of quantum computing. Quantum computers, in theory, will be capable of breaking certain cryptographic algorithms that currently secure much of our confidential communications. Specifically, widely used public-key encryption schemes (like RSA and elliptic curve) could be broken by a sufficiently powerful quantum computer running Shor's algorithm, and even some symmetric schemes would need larger key sizes to remain safe. This is a looming threat to confidentiality: an adversary might harvest encrypted data now (which they cannot read today) and store it, anticipating that in a decade or less, quantum machines could decrypt it, jeopardizing confidentiality of past communications. In response, the field of post-quantum cryptography is developing new algorithms believed to be resistant to quantum attacks. NIST, for example, is in the process of standardizing post-quantum cryptographic algorithms. Organizations will need to migrate to these new forms of encryption over the next several years to stay ahead of the threat (Whyte, 2024). Quantum computing also affects integrity: digital signature algorithms will also change (since many current signature schemes would be breakable by quantum computers). On the flip side, quantum technology offers tools like quantum key distribution (QKD), which provides a method of sharing encryption keys with security guaranteed by the laws of physics (any eavesdropping on the key exchange is detectable). QKD could be a powerful way to enhance confidentiality for highly sensitive communications (currently it's limited by distance and infrastructure needs, but progress is being made). Planning for a post-quantum world is now an important part of future-proofing the CIA triad.

Artificial Intelligence (AI) and Machine Learning are double-edged swords in cyber defense. They offer new capabilities for defenders; for example, machine learning models can analyze network traffic or user behavior to detect anomalies that might indicate attacks (thus helping protect integrity and availability by catching attacks early, or confidentiality by spotting data exfiltration). AI can also optimize system configurations or predict component failures, improving availability. However, attackers also use AI, and AI systems themselves become targets. As noted earlier, poisoning attacks on machine learning training data are a novel threat to integrity. Attackers might also use AI to craft more convincing phishing emails (threatening confidentiality by fooling people into giving away info) or to find vulnerabilities in software faster. The presence of AI means cyber defenses must consider the integrity of algorithms and models: ensuring that an AI system guiding security decisions isn't itself compromised or biased by malicious input. There is ongoing research on explainable AI in security, so that human analysts can understand and verify why an AI flagged something, which aids the integrity of the incident analysis process. The future likely holds a continuous back-and-forth between AI-augmented attackers and AI-augmented defenders, with the CIA principles remaining the goal posts each side is concerned with (Osazuwa, 2023).

Supply chain security has become a prominent concern as well. Organizations rely on a multitude of third-party software, libraries, hardware components, and services. A vulnerability or deliberate backdoor in any of these can compromise confidentiality, integrity, or availability. High-profile incidents like the SolarWinds breach (where attackers inserted malicious code into a widely used IT monitoring product, leading to a massive supply chain compromise) show how fragile trust can be in the supply chain. Ensuring integrity of software updates and software components is an enormous challenge when the chain of custody spans multiple vendors and international contexts. The concept of Zero Trust can extend here: rather than inherently trusting any vendor, organizations are moving to strategies like verifying hashes of software, using reproducible builds, segmenting networks to limit the blast radius of a compromised component, and continuously monitoring for abnormal behavior even in trusted software. In hardware, there's focus on authenticating hardware components and firmware integrity (since firmware malware can be hard to detect but very damaging). In the future, we may see more formal verification of critical software and hardware to mathematically prove aspects of their integrity, as well as more threat intelligence sharing within industries to quickly alert about compromised products (Covert et al., 2020).

With all these developments, one thing is clear: the human element will remain crucial. Attackers often choose the path of least resistance, and frequently that is not breaking advanced cryptography or bypassing redundant servers, but simply tricking or coercing a human who has legitimate access (through social engineering or

phishing) or making use of poorly trained personnel mistakes. Thus, even as technology advances, user education and organizational culture around security are vital. Employees and users need to understand why security measures exist, so they are more likely to follow them correctly. They also need to be aware of the common attack tricks so they can avoid falling prey. Building a culture that values security will support confidentiality (workers more careful with sensitive data), integrity (people following proper procedures so data remains accurate), and availability (teams prepared to handle incidents without panic, and not inadvertently causing downtime through negligence). In the future, perhaps more user-friendly security tools, like passwordless authentication, better security UX design, will reduce the friction and errors, making it easier for humans to do the right thing security-wise.

The security community is also rethinking models beyond CIA. Some propose adding a fourth letter for Safety or Serviceability (leading to models like CIAS, where "S" might stand for safety or service continuity), particularly as cyber attacks can have kinetic effects (e.g., affecting safety of physical processes). Another addition seen is Privacy as a distinct goal, separate from confidentiality in that it deals with data being used in ways that respect individuals' rights (one could argue privacy is a broader social concept built on confidentiality and integrity). While these expanded models gain traction in discussion, the CIA triad remains the core teaching and thinking tool. It is very likely to persist as the foundational layer in cybersecurity frameworks, even as we overlay new concerns on top of it (Covert et al., 2020). The triad's strength is its simplicity and generality: no matter what new technology arises, one can ask of it – can we keep its data confidential? can we ensure its outputs and behaviors have integrity? can we keep it available when needed? These questions will be as applicable to quantum computing networks or AI-driven autonomous systems as they were to mainframes and early internet servers.

Going forward, organizations are advised to adopt a holistic, adaptive security posture. This means continuously assessing and improving their security controls in light of new threats, and not treating security as a one-time project but an ongoing process. Techniques like continuous monitoring, threat hunting, and incorporating real-time threat intelligence feeds are becoming standard. By staying agile and informed, defenders can tweak their measures to strengthen any weakening link in confidentiality, integrity, or availability before it fails catastrophically (Osazuwa, 2023). The notion of "cyber resilience" encapsulates much of this future direction: it's not just about keeping attackers out (which may eventually prove impossible in all cases) but about ensuring the organization can continue to function and protect its most critical assets even under attack or after compromise. That involves quick detection (to minimize integrity or confidentiality breaches), robust response and containment (to restore availability and confidence), and learning lessons to prevent recurrence.

In conclusion, while emerging technologies and threats will change the tactics of cyber defense, they do not change the fundamental objectives represented by the CIA triad. Confidentiality, integrity, and availability will remain at the heart of what we strive to protect in any information system. The role of these principles in cyber defense will, if anything, become more pronounced as systems become more interconnected and impactful on the real world. Cyber defense professionals will need to be well-versed in balancing these principles under new conditions, whether that's securing a network of self-driving cars (where integrity and availability could be life-and-death, alongside confidentiality of user data) or deploying new cryptographic infrastructure for the quantum era. The CIA triad's continued relevance is assured, but its implementation will continuously evolve. By keeping an eye on future trends and investing in research, training, and robust design, the cybersecurity community aims to preserve these core principles against whatever challenges lie ahead.

CONCLUSION

Confidentiality, integrity, and availability form the bedrock of cyber defense. Throughout this paper, we have evaluated how each element of the CIA triad contributes to protecting information systems and how they interplay in practice. Confidentiality safeguards sensitive information from unauthorized access, a role that is increasingly vital in an era of large-scale data breaches and strict privacy regulations. Integrity ensures that information and systems can be trusted, guarding against the ever-present risk of data tampering, corruption, or sabotage that could otherwise lead to incorrect decisions and undermined credibility. Availability guarantees that the services and data on which organizations and individuals rely are accessible when needed, highlighting that without reliable access, even the most secure and accurate data is of little value. Together,

these principles provide a comprehensive framework for identifying security needs and guiding the implementation of controls and policies.

A key insight from this review is that effective cyber defense is not about choosing between confidentiality, integrity, and availability, but about achieving an appropriate balance of all three. Over-focusing on one to the neglect of others can create vulnerabilities. True security requires a holistic approach: technical solutions (like encryption, access controls, redundancy, and monitoring) combined with processes (risk management, incident response, disaster recovery planning) and people-oriented measures (training, culture, clear policies). The CIA triad serves as a reminder to cover all bases. In evaluating security postures, organizations often find it useful to assess how well each of the three dimensions is addressed. If gaps are found, for example, maybe strong firewalls and encryption are in place (protecting confidentiality) but backup routines are unreliable (threatening availability), those gaps must be remedied to avoid one weakness compromising the entire system.

We also saw that the threat landscape is dynamic. Cyber adversaries are constantly evolving their techniques, whether it's launching massive DDoS attacks to cripple availability, developing advanced malware to quietly corrupt or steal data, or exploiting human trust to bypass confidentiality protections. In response, cyber defense strategies must be adaptive. The traditional CIA model is sometimes challenged by new conditions (for instance, the potential arrival of quantum computing or the mass deployment of IoT devices), but rather than making the model obsolete, these challenges call for innovation in how we uphold the model's principles. For example, the development of post-quantum cryptography is fundamentally about preserving confidentiality and integrity of communications in the future; the push for robust IoT security frameworks is about ensuring integrity and availability in highly distributed, resource-limited environments. The core mission, to protect information's secrecy, correctness, and accessibility, remains constant even as the methods expand.

Importantly, the human factor remains a critical thread running through all three components of the CIA triad. Human mistakes and misjudgments can lead to confidentiality breaches (like a misconfigured database or falling for a phishing scam), integrity lapses (inadvertently altering or deleting important data), and availability issues (such as accidentally unplugging a server or failing to apply a crucial patch). In fact, a portion of this paper's humanized narrative, including minor errors and informalities, serves to illustrate that security documentation and policies are ultimately interpreted and implemented by people, not flawless machines. It is humans who design systems, execute procedures during an incident, and use (or misuse) the technology. Therefore, fostering an environment where people are aware of security risks, feel responsible for following best practices, and are empowered to report problems or suggest improvements is as important as any technical control. Cyber defense is as much a management and cultural challenge as it is a technical one.

In reviewing the role of confidentiality, integrity, and availability, we reaffirm that the CIA triad is more than an academic concept, it is a practical tool that has stood the test of time in guiding security efforts. The triad's strength lies in its simplicity and universality: almost any security issue can be mapped to one or more of these fundamental objectives. This helps in diagnosing what went wrong in an incident (e.g., "Was it a breach of confidentiality, an attack on integrity, or a denial of availability?") and in planning defenses ("Do our measures cover all three areas adequately?"). As we move forward, it is likely that new security frameworks will incorporate CIA alongside other considerations (like safety, privacy, resilience), but those extended frameworks will still rely on the core understanding that without confidentiality, integrity, and availability, there is no security.

In conclusion, the CIA triad continues to play an indispensable role in cyber defense. It provides a clear lens through which to evaluate and fortify the security of systems amidst a landscape of ever-changing threats. Cyber defenders must persist in safeguarding confidential data against breaches, ensuring the integrity of information and systems against tampering, and keeping critical services available even under duress. By doing so, they protect not just abstract data, but the trust and functionality that underpin our digital society. The task is ongoing and challenging, attackers will exploit any lapse in any of these areas, so we must strive for excellence in all three. The recommendations for future practice include adopting a balanced, risk-informed security strategy, staying abreast of technological changes (such as quantum-safe cryptography and AI-driven defense tools), and perhaps most fundamentally, cultivating a security-aware culture that values and supports the mission of protecting confidentiality, integrity, and availability. Only through such

comprehensive and human-conscious efforts can we build a more secure and resilient digital future for everyone.

REFERENCES:

1. Alam, T. (2019). *Blockchain and its role in the Internet of Things (IoT)*. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(1), 151-156.
2. Alhassan, M., & Adjei-Quaye, A. (2017). *Information security in an organization*. International Journal of Computer (IJC), 11(1), 100-116.
3. Almarri, S., & Aljughaiman, A. (2024). *Blockchain technology for IoT security and trust: A comprehensive SLR*. Sustainability, 16(23), Article 130.
4. Aminzade, M. (2018). *Confidentiality, integrity and availability – finding a balanced IT framework*. Network Security, 2018(5), 9-11.
5. 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.
6. Cîrnu, C. E., Rotuna, C. L., Vezeanu, A. V., & Boncea, R. (2018). *Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture*. Studies in Informatics and Control, 27(3), 359-368.
7. Covert, Q., Francis, M., Steinhagen, D., & Streff, K. (2020). *Towards a triad for data privacy*. In Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS) (pp. 4379-4387).
8. Filiz, M. (2023). *Integrating cybersecurity risk management into strategic management: A comprehensive literature review*. Research Journal of Business and Management, 10(3), 98-108.
9. Guguelot, V., Safavat, S., Shetty, S., & Rawat, D. (2023). *A review of IoT security and privacy using decentralized blockchain techniques*. Computer Science Review, 50, 100-117.
10. Osazuwa, O. M. C. (2023). *Confidentiality, integrity, and availability in network systems: A review of related literature*. International Journal of Innovative Science and Research Technology, 8(12), 1946-1955.
11. Tchernykh, A., Schwiegelsohn, U., Talbi, E., & Babenko, M. (2019). *Toward understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability*. Journal of Computational Science, 36, 100581.
12. Whyte, S. (2024). *Quantum cryptography and its implications in cybersecurity: Securing communication in the quantum era*. International Journal of Computer Science and Information Technology, 9(3), 16-28.