Muhammad Ahmad, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

A Review of Cryptographic Solutions and Forensic Readiness in IoT and Network Security

Muhammad Ahmad[1], Hua Zhou[2], Tanzeela Bibi[3], Haider Ali[4]

[1,2,3]School of Electronics and Information Engineering, Nanjing University of Information Science &Technology, Nanjing, 210044, China

[4]School of Hydrology and Water Resources Nanjing University of Information Science and Technology, Nanjing, 210044, China

Abstract- In today's digital environment, the swift advancement of interconnected technologies has raised significant worries about data safety, privacy, and reliability. The Internet of Things (IoT), networking systems, and cloud services produce and transfer large quantities of sensitive information, leaving them susceptible to cyber threats and other security risks. This research offers a detailed evaluation of how cryptography, network protection, and digital forensics work together, highlighting their combined impact on securing communication, safeguarding data integrity, and ensuring effective investigation methods. The approach to research relies on a thorough examination and combination of available literature, with a focus on major developments in cryptographic methods, network defense strategies, and forensic analysis frameworks. Particular focus is given to Homomorphic Encryption (HE), which allows processing to occur directly on encrypted information without the need for decryption, thus increasing privacy in unreliable settings such as cloud services and IoT environments. Moreover, the research includes new strategies in blockchain-centered forensics, featuring automated cost management that aligns with regulations, mapping wallet interactions, and utilizing non-fungible tokens (NFTs) as reliable audit references to enhance transparency and responsibility. The results show that cryptographic methods ensure safe data transfer, while network security strategies defend systems against unauthorized access, misuse, and cyber intrusions. At the same time, digital forensics offers a scientifically supported method for finding, preserving, and examining digital proof, tackling key evidentiary issues in today's cyber landscape. The integration of blockchain forensics and NFTs further boosts auditability, traceability, and trust, especially within decentralized finance (DeFi) setups and intricate digital transactions. In summary, the alignment of cryptography, network protection, and digital forensics creates a strong and forward-thinking security framework that improves data safety, helps with regulatory adherence, and enhances the overall durability of contemporary digital systems.

Keywords: Cryptography; network security; internet of Things; digital forensics; homomorphic encryption; blockchain forensics; non-fungible tokens; data security; cybersecurity.

I. INTRODUCTION

The emergence of cybercrime in the field of digital forensics has drastically changed the nature of criminal behavior by bringing in new types of harm that are frequently challenging to identify, look into, and prosecute using conventional legal frameworks. Because of this, the admissibility of digital evidence as a trustworthy form of proof has grown in significance. In this regard, the incorporation of digital forensics into contemporary legal frameworks shows how flexible and dynamic they are, emphasizing their ability to handle new issues while upholding long-standing legal precept [1]. The conventional forensic model focused on "computer-technical" aspects is no longer adequate to address the challenges posed by contemporary cybercrime, prompting the need for a shift to a diverse cyber-expertise framework.

An organized classification that includes telecommunications networks, infrastructure, software, cryptography, and coverage knowledge is crucial for preserving the chain of protection and validating evidence within 5G and decentralized settings. Audit findings reveal a notable "Instructional Gap" and a lack of "Forensic Logic" among professionals, marked by insufficient

analytical thinking and an overdependence on automated scripts [2]. Cryptography, network protection, and the Internet of Things are three related fields that have become important in today's digital world. Crptography is about protecting communication by encrypting and decrypting private information, while network protection is aimed at keeping networks and data safe from unauthorized access, misuse, and theft.

The Internet of Things, often referred to as IoT, refers to how devices connect with each other and the information they generate and share [3]. In today's linked world, Cryptography, security of networks, and the Internet of Things (IoT) are closely connected and vital for ensuring the safety and confidentiality of information. Network security focuses on protecting networks and information from theft, abuse, and unauthorized access, while cryptography involves securing communications by encoding and decoding private information. IoT, on the other hand, describes how devices like smart home appliances are connected to one another and the data they produce and exchange. When combined, these three domains are essential for protecting the enormous volumes of data that IoT devices produce and distribute [4]. As shown in Fig. 1, the encryption process converts plaintext into ciphertext before transmission.

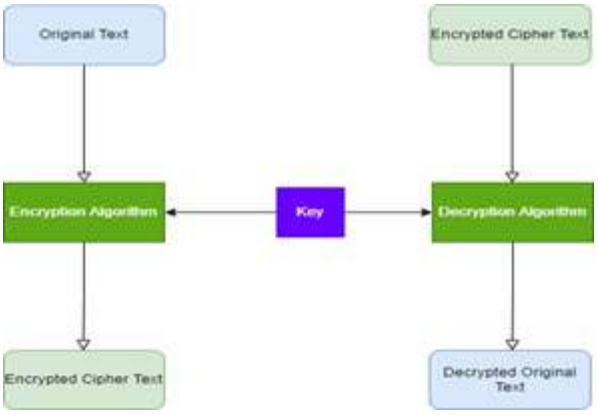

Fig.1 Encryption and Decryption

The flow of the information between the sender and reciever is illustrated in Fig. 2,

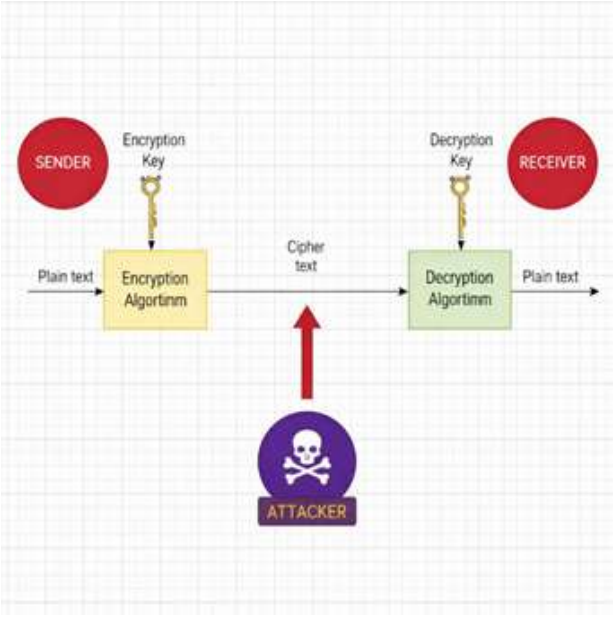

Fig.2 Sender & Receiver (Cryptography)

II. BACKGROUND AND RELATED WORK

Lately, there has been a significant increase in the number of IoT gadgets along with the amount of information they produce, resulting in a greater demand for secure data transmission and protection. Cryptography is essential in this regard as it offers secure channels for communication during data exchange among devices within an IoT framework. The rise The increase in IoT devices has likewise raised the amount of data produced and exchanged by these devices. This development has also led to a rise in security threats and vulnerabilities associated with IoT devices and their systems. Thus, cryptography, network security, and IoT must advance together to keep pace with the changing threat environment [5]. A key difficulty in protecting IoT devices arises from the variety of hardware and software systems utilized in these devices.

This variety complicates the application of a uniform security measure across all devices. Nevertheless, methods For example, both symmetric key encryption and asymmetric key encryption may be utilized to establish a safe communication link between devices, irrespective of their platform [6]. A significant obstacle in protecting IoT devices is their restricted resources and functions. In contrast to

standard computing gadgets, IoT gadgets often have restricted processing power, memory, and storage capacity. This limitation obstructs the use of conventional security methods like encryption and authentication. To overcome this issue, researchers have suggested utilizing lightweight cryptography, such as elliptic curve cryptography, which better fits devices with limited resources [7]. In Fig.3, show the IoT application flowchart, how work the life cycle actually.

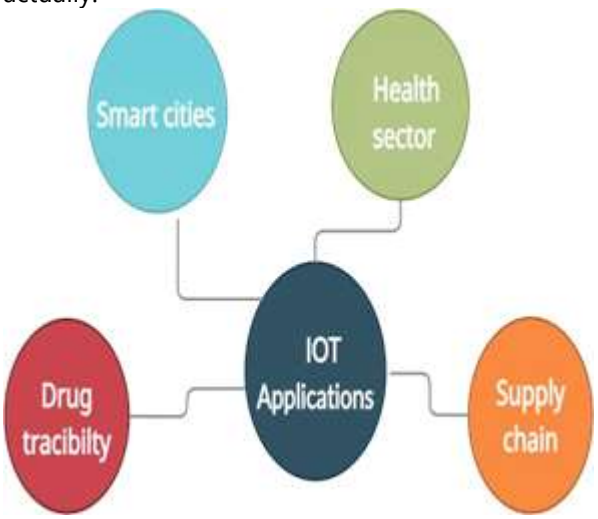

Fig.3 IoT applications

III. STAGES OF SECURITY

Network security is a crucial factor in an IoT environment. As more devices link to networks, the likelihood The increase in unauthorized access and data breaches is concerning. To tackle this issue, various security measures such as firewalls, intrusion detection systems, and VPNs can be used to protect networks from unauthorized entries [8]. A further essential element of safeguarding IoT devices involves the safe setup and oversight of these gadgets. This means confirming that merely permitted devices are allowed to connect to a network and that these devices are manageable and updatable in a secure manner. One method to achieve this is by utilizing Secure boot processes ensure that only authorized firmware is able to run on a device. An alternative approach is to use secure provisioning methods such as the Device Identity Composition Engine (DICE), allowing devices to connect to a network securely and confirm their identities [9].

In the past few years, there has been an increasing fascination with the application of blockchain technology in the internet of Things (IoT). Blockchain serves as a shared and decentralized record that can help protect and handle the information produced by IoT devices. This can be beneficial for maintaining data accuracy and stopping unwanted access to it [10]. Cryptography, network safety, and the Internet of Things are three essential fields that are linked and important in today's digital age. With the increasing number of IoT devices and the volume of data they generate, the need for secure communication and data protection has increased greatly. Cryptography, network safety, and blockchain technology are some of the key methods that can be used to ensure the protection and reliability of information in an IoT setting [11].

One of the widely used techniques for protecting networks is encryption. It allows for the secure transfer of data by converting it into a code that only authorized users can understand. Many encryption methods have been developed, each with its own strengths and weaknesses. Some of the commonly used encryption methods include RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), and DES (Data Encryption Standard) [12]. A key element of network protection is the application of firewalls. Firewalls serve as a shield between a network and external entities, observing and regulating traffic that comes in and goes out. They can be deployed in different forms, such as physical firewalls and program-based firewalls [13]. Besides encryption and firewalls, the security of a network can be improved by using IDPS. These systems observe network data for indications of harmful activity and can take measures to stop an attack from happening [14].

A crucial element of network protection is access management. This means making sure that only those with permission can enter a network and utilize its resources. This can be accomplished by implementing authentication and authorization methods, like using usernames and passwords or employing biometric measures [15]. One of the first and most common techniques for protecting networks is deploying firewalls. Firewalls serve as a

protective layer separating a network from external threats, preventing unapproved access while permitting only permitted data to flow. Firewalls may be either hardware, software, or a mix of the two [16].

Another key element of network protection is implementing encryption. Encryption refers to the method of transforming readable text into coded text, which prevents anyone without the correct decryption key from understanding it [17]. Encryption serves to safeguard information while it is being transmitted, like when it moves across the web, and also protects data that is stored, such as when it resides on a device [18]. Systems for detecting and preventing intrusions (IDPS) are a crucial component of network protection. These systems aim to identify and stop any unauthorized access to a network [19]. They might depend on signature recognition, which looks for known patterns of harmful behaviors, or anomaly recognition, which spots unusual activities that vary from normal conduct [20]. A new and innovative approach to improving network security includes using artificial intelligence and machine learning. These techniques can improve the identification and avoidance of breaches, as well as spotting and managing emerging and evolving threats [21].

Principles of Security:

Network security is a vital part of information protection aimed at safeguarding networks, gadgets, and information from unauthorized entry, use, revealing, disruption, change, or ruin. There are multiple key components of network safety that must be considered when developing and implementing safety measures.

Confidentiality: This aspect guarantees only personnel with proper authorization are allowed to reach sensitive information. Encryption can help to maintain confidentiality. [22] and access controls [23].

Integrity: This aspect guarantees that information cannot be changed or altered without prior warning. Integrity can be preserved without by employing hashing algorithms and digital signatures [24,25].

Availability: This aspect guarantees that systems and services can be reached by permitted users whenever they need to. Accessibility can be guaranteed through the use of backups, failover mechanisms, and recovery plans for emergencies [26,27].

Authenticity: This feature ensures that the identities of users and devices can be verified and relied upon. Verification can be achieved through methods such as passwords and biometric systems [29].

Non-repudiation: This feature ensures that all parties engaged in a conversation cannot refute their involvement. Non-repudiation is achievable with the help of digital signatures and various other proof-based instruments [30]. The relationships among the CIAAN security principles are illustrated in Fig.4,

Fig.4 Non-Linear Graph Representing the CIAAN Security Model (Confidentiality, Integrity, Availability, Authenticity, and Non-Repudiation)

IV. MEASUREMENTS OF NETWORK SECURITY

This element guarantees that only people with permission can reach private information. Protecting confidentiality can be maintained by using encryption, restricting access, and employing various protective methods [31].This aspect ensures that information is not changed or adjusted without proper authorization. Data integrity can be preserved through the use of digital signatures, hashing techniques, and several other protective practices [32]. This feature ensures that permitted

users can reach the network and resources whenever it is necessary. Redundancy, load balancing, and other techniques can enhance availability [33]. This element guarantees that access to a network is permitted only to those who have the right permissions. Verification can be accomplished with the help of user identification numbers, passwords, and various other types of ID methods [34]. This feature guarantees that the sender of the message cannot thereafter claim not to have sent it. Timestamps, digital signatures, and other security measures can be used to achieve non-repudiation [35].

Types of Network Security:

Numerous varieties of network security exist, each possessing distinct characteristics and benefits. Among the most widely recognized types of network security are:

Firewalls: Firewalls serve as a protective wall between a network and external entities, preventing unauthorized entry while permitting only approved data flow. They can be implemented as hardware, software, or a mix of the two [36].

Encryption: Encryption involves transforming understandable text into an unreadable format, known as ciphertext, which cannot be accessed by individuals lacking the correct decryption key. This technique can be employed to safeguard data while it moves, such as when transmitted online, as well as to secure data that is stored, like when kept on a device [37].

Intrusion detection and prevention systems(IDPS):

IDPS are designed to recognize and prevent unauthorized access to a network. They can utilize signature detection that looks for known patterns of harmful behavior, or anomaly detection that identifies unusual activities that stand out from normal behavior [38].

Virtual Private Networks (VPNs): VPNs facilitate a protected, encrypted link between multiple devices via the internet. They are helpful for linking remote employees to an organization's network or for securing data while it travels across public networks [39].

Access Control: Access control systems regulate and oversee entry to a network or system. This may involve methods for authentication and authorization, like usernames and passwords, along with physical access measures, including security cameras or biometric readers [40].

Network Segmentation: Network segmentation means dividing a network into smaller sections, with each section having its specific security protocols and rules. This method can lessen the effects of a security breach and improve the overall protection of the network [41].

V. SECURITY ADVANTAGES

Network security offers numerous benefits that assist in safeguarding networks, devices, and information from unauthorized entry, utilization, sharing, interruption, alteration, or annihilation. Some of the main benefits of network security are:

Protection of sensitive information: Network security works to safeguard private details, like financial records and personal details, from unauthorized entry and exposure. This measures can aid in avoiding data leaks and maintaining the image of a company [42].

Prevention of unauthorized access: Network security helps prevent unauthorized access to a network, which can support protection against cyber risks and different forms of harmful activities [43].

Maintaining the availability of networks: Network security plays a crucial role in keeping networks accessible, making certain that permitted users can reach the network and utilize its resources whenever they require them. [44].

Compliance with industry and government regulations: Network security assists organizations in meeting numerous governmental and industry standards, including HIPAA, PCI-DSS, and SOX [45].

Protection of intellectual property: Network security can assist businesses in preventing unwanted access to and disclosure of their intellectual property, including trade secrets and private data [46].

Cost-effective: Because it can stop expensive data breaches, lost productivity, and reputational harm, implementing network security can be economical [47].

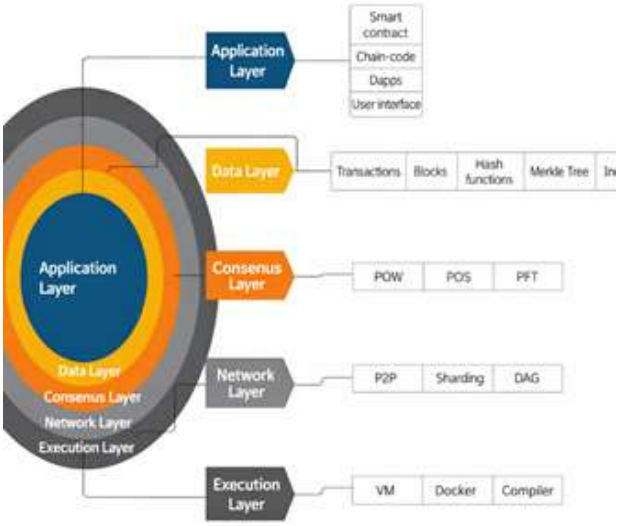

Fig.5 Network Security Layers

The blockchain layered architecture, detailing the interaction between layers and their components, is shown in Fig. 5

Network Security Disadvantages:
Although network security offers numerous advantages, there are certain drawbacks that businesses should be aware of. The following are some of the main drawbacks of network security:

High implementation costs: Establishing and upholding network safety can be expensive, needing considerable spending on equipment, programs, and staff [48].

Complexity: Network security can be complicated, needing certain knowledge and skills to properly implement and maintain [49].

Limited scalability: Network security solutions are frequently difficult to scale, making it challenging to adapt to changes or expansion in an organization's network architecture [50].

Reduced network performance: Network performance can occasionally be negatively impacted by network security measures, leading to poor network speeds and decreased productivity [51].

False positives: Network security systems might cause false alerts, leading to unwarranted warnings and piling on more tasks for security staff [52].

Limited effectiveness: The efficacy of network security solutions may be constrained, particularly in light of the rise of sophisticated persistent threats and zero-day vulnerabilities [53].

VI. SECURITY LIMITATIONS WITH VPN

Encryption is one of the main technologies used in VPN network security. The data that is sent via the VPN connection is protected by encryption, which renders it unintelligible to anyone who intercepts it. AES, RSA, and IKE are the encryption algorithms most frequently employed in VPNs [54]. Using secure protocols is another crucial component of VPN network security. These protocols, including IKEv2 and OpenVPN, are used to create and manage VPN connections and guarantee secure data transmission.

To guarantee that only authorized users can use the VPN, authentication techniques are used in addition to encryption and secure protocols. Passwords, biometrics, and two-factor authentication (2FA) are a few examples of this. Lastly, defenses against typical threats like malware, phishing, and DDoS attacks are part of VPN network security. Firewalls, systems for detecting and preventing intrusions, and antivirus applications are a few examples of this [55]. The usual VPN configuration is shown in Fig 6, which also emphasizes possible security risks when using a VPN gateway to connect several devices, including tablets, laptops, and PCs.

.

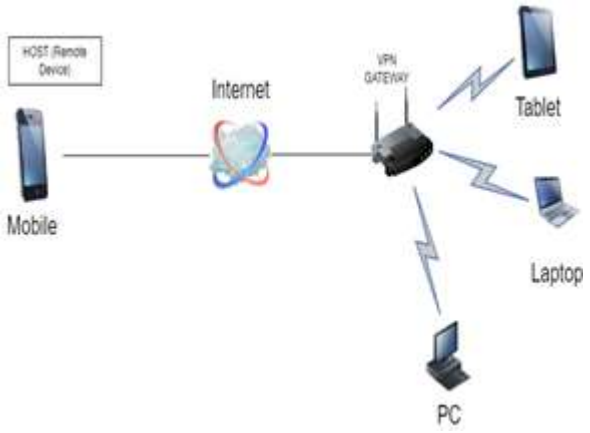

Fig.6 Configurations of VPN

VII. CONCLUSION

In conclusion, in today's highly connected digital world, encryption, network security, and IoT security are essential elements for protecting data and preserving privacy. These domains must constantly change to handle new threats, such as viruses, sophisticated cyberattacks, and illegal data access, given the exponential rise of IoT devices. Encryption, firewalls, Intrusion Detection and Prevention Systems (IDPS), access controls, and, increasingly, AI and ML approaches to identify anomalies and react in real time are just a few of the strategies and tools that must be combined for effective network security. Protecting networks, devices, and sensitive data against unwanted access, misuse, disruption, alteration, or destruction is all part of network security, which is intrinsically complex.

To guarantee complete resilience, the design and implementation of these safeguards must be guided by the critical security principles of confidentiality, integrity, availability, authenticity, and non-repudiation. Furthermore, network security and digital forensics play closely related roles. Digital forensic techniques enable investigators to track down the source of attacks, retrieve stolen data, and produce useful evidence for court cases in the event of a security breach. By combining proactive network defense with reactive forensic investigation, an organization's total cybersecurity posture is strengthened, enabling them to both prevent and successfully respond to threats. In the end, maintaining strong security necessitates not only technology solutions but also ongoing monitoring, risk assessment, and forensic preparation to safeguard data, devices, and users from changing cyber hazards as IoT networks grow and cyber-attacks get more complex.

VII. CONFLICT STATEMENT

There are advantages and disadvantages of using cryptography in network security and the Internet of Things. Although cryptography offers safe key management, encryption, and authentication, it can also raise system complexity, computational overhead, and battery consumption problems for IoT devices with limited resources. In practice, security may be challenging due of these conflicts. By making it possible to investigate breaches, track down the sources of attacks, and retrieve compromised data, digital forensics plays a crucial part in addressing these issues and assisting companies in efficiently responding even in situations when cryptographic safeguards are limited.

IX. FUNDING

Currently no funding

REFERENCES

1. Meenakshi John Jatin Kumar, "Cyber - Crime and Cyber Criminals: A Global Perspective," International Journal of Science and Research (IJSR), vol. 12, no. 4, pp. 176-178, Apr. 2023.
2. P. T. Ramazhamba and H. S. Venter, "Emerging Digital Technologies for 4IR (EDT4IR) Research Centre," Applied Sciences, vol. 16, no. 2, p. 799, 2026.
3. A. Anorboyev, "Modernizing Digital Forensics Education: Integrating Specialized Cyber-Expertise into Legal and Investigative Curriculum," Assyfa Learning Journal, vol. 4, no. 1, pp. 17-32, 2026.
4. A. S. Tanenbaum, Computer Networks, 5th ed. (Upper Saddle River, NJ: Prentice Hall, 2010).
5. A. Jain and K. Venugopal, "A survey on security issues in internet of things," in 2016 International Conference on Advances in Computing,

Communications and Informatics (ICACCI), 2016, pp. 1753–1759.
6. R. J. Anderson and M. G. Kuhn, "Low-cost attacks on tamper-proof devices," in Advances in
7. Cryptology CRYPTO'96, 1996, pp. 1–11.
8. Sadeghi, A. R., & Waidner, M. (2013). Secure provisioning and management of internet of things devices. IEEE Communications Magazine, 51(8), 26-33.
9. Y. Mao, C. Wang, Q. Wang, and K. Ren, "Secure and efficient data sharing in IoT via blockchain," in 2017 IEEE International Conference on Smart Cloud (SmartCloud), 2017, pp. 657–662.
10. Raza, M. A., & Imran, M. (2019). A survey of lightweight cryptography for internet of things (IoT). IEEE Communications Surveys & Tutorials, 21(4), 2841-2867.
11. P. L. Dandekar and R. K. Srivastava, "Blockchain technology in IoT: a review," in 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 623–628.
12. Ochoa, M., & Camacho, D. (2016). An overview of internet of things security. IEEE Communications Surveys & Tutorials, 18(4), 2233-2269.
13. Chen, X. (2016). Firewall design principles and practices. New York, NY: Springer.
14. Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.
15. Liu, Y. (2018). Intrusion detection and prevention systems: A literature review. Journal of Computer Science and Technology, 33(3), 477-487.
16. Stallings, W. (2017). Cryptography and network security. Pearson Education.
17. Chen, P., Jha, S., & Liu, L. (2004). Firewall design and deployment. IEEE Communications Magazine, 42(3), S12-S18.
18. Stallings, W. (2005). Cryptography and network security: principles and practice (4th ed.). Prentice Hall.
19. Kang, B., Shin, K., & Lee, D. (2008). Intrusion detection and prevention systems: technologies and deployment. Communications of the Korean Institute of Information Scientists and Engineers, 28(3), 12-20.
20. Buczak, A. L., Guven, E., & Yener, B. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.
21. Stallings, W. (2005). Cryptography and network security: principles and practice (4th ed.). Prentice Hall.
22. Chen, P., Jha, S., & Liu, L. (2004). Firewall design and deployment. IEEE Communications Magazine, 42(3), S12-S18.
23. Barker, E., Burr, W., Dodson, D., Polk, W., & Ylonen, T. (2002). Secure hash standard (SHS). FIPS PUB 180-4.
24. Menezes, A., Van Oorschot, P., & Vanstone, S. (1996). Handbook of applied cryptography. CRC press.
25. Kang, B., Shin, K., & Lee, D. (2008). Intrusion detection and prevention systems: technologies and deployment. Communications of the Korean Institute of Information Scientists and Engineers, 28(3), 12-20.
26. Schneier, B. (2000). Secrets and lies: digital security in a networked world. Wiley.
27. Salah, A., El-Sayed, M., & El-Sayed, A. (2013). Passwords: security measures and management techniques. Journal of Network and Computer Applications, 36(1), 1-14.
28. Jain, A., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.
29. Kamat, R., & Tiwari, R. (2018). Non-repudiation in digital forensics: a survey. IEEE Access, 6, 81651-81664.
30. Stallings, W. (2005). Cryptography and network security: principles and practice (4th ed.). Prentice Hall.
31. Bellare, M., & Rogaway, P. (1993). Authenticated encryption: relations among notions and analysis of the generic composition paradigm. Journal of Cryptology, 13(1), 85-125.
32. Takahashi, S., & Koga, Y. (2002). Availability and dependability of computer systems. IEEE Transactions on Dependable and Secure Computing, 1(1), 2-17.
33. Zhang, J., & Lee, W. (2011). Authentication and access control. IEEE Communications Surveys & Tutorials, 13(4), 524-540.
34. Chow, R. (2002). Non-repudiation in electronic commerce. ACM Computing Surveys, 34(4), 437-471.

35. Chen, P., Jha, S., & Liu, L. (2004). Firewall design and deployment. IEEE Communications Magazine, 42(3), S12-S18.
36. Stallings, W. (2005). Cryptography and network security: principles and practice (4th ed.). Prentice Hall.
37. Kang, B., Shin, K., & Lee, D. (2008). Intrusion detection and prevention systems: technologies and deployment. Communications of the Korean Institute of Information Scientists and Engineers, 28(3), 12-20.
38. Papadimitriou, C., & Vakali, A. (2011). Virtual private networks: technologies and solutions. IEEE Communications Surveys & Tutorials, 13(1), 56-76.
39. Zhang, J., & Lee, W. (2011). Authentication and access control. IEEE Communications Surveys & Tutorials, 13(4), 524-540.
40. Perez, A., et al. (2018). Network segmentation and microsegmentation: best practices and use cases. Network Security, 2018(9), 1-8.
41. Chen, P., Jha, S., & Liu, L. (2004). Firewall design and deployment. IEEE Communications Magazine, 42(3), S12-S18.
42. Kang, B., Shin, K., & Lee, D. (2008). Intrusion detection and prevention systems: technologies and deployment. Communications of the Korean Institute of Information Scientists and Engineers, 28(3), 12-20.
43. Takahashi, S., & Koga, Y. (2002). Availability and dependability of computer systems. IEEE Transactions on Dependable and Secure Computing, 1(1), 2-17.
44. Zhang, J., & Lee, W. (2011). Authentication and access control. IEEE Communications Surveys & Tutorials, 13(4), 524-540.
45. Chow, R. (2002). Non-repudiation in electronic commerce. ACM Computing Surveys, 34(4), 437-471.
46. Perez, A., et al. (2018). Network segmentation and microsegmentation: best practices and use cases. Network Security, 2018(9), 1-8.
47. Chen, P., Jha, S., & Liu, L. (2004). Firewall design and deployment. IEEE Communications Magazine, 42(3), S12-S18.
48. Kang, B., Shin, K., & Lee, D. (2008). Intrusion detection and prevention systems: technologies and deployment. Communications of the Korean Institute of Information Scientists and Engineers, 28(3), 12-20.
49. Takahashi, S., & Koga, Y. (2002). Availability and dependability of computer systems. IEEE Transactions on Dependable and Secure Computing, 1(1), 2-17.
50. Zhang, J., & Lee, W. (2011). Authentication and access control. IEEE Communications Surveys & Tutorials, 13(4), 524-540.
51. Chow, R. (2002). Non-repudiation in electronic commerce. ACM Computing Surveys, 34(4), 437-471.
52. Perez, A., et al. (2018). Network segmentation and microsegmentation: best practices and use cases. Network Security, 2018(9), 1-8.
53. Fang, X. (2020). Virtual Private Network (VPN) security: a comprehensive review. Journal of Network and Computer Applications, 149, 102451.
54. Shah, A. (2019). Virtual private network (VPN) security: A review. Journal of Network and Computer Applications, 123, 1-13.
55. Siponen, M. (2020). Authentication methods in virtual private networks: a comprehensive review. Journal of Network and Computer Applications, 145, 102364.
56. Wang, X. (2018). Virtual private network security: a review of threats and solutions. Journal of Network and Computer Applications, 114, 39-48.