STM JOURNALS

Journal of
Network Security

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 13, Issue 3, 2025
September–December
DOI (Journal): 10.37591/JoNS

https://journals.stmjournals.com/jons

Review JoNS

Network Security and Risk Technologies

Muskan Sharma[1,*], Krati Sharma[2], Khushi Sharma[1],
Navya Khandelwal[1]

Abstract

This research work delves into the dynamic domain of network security risk, providing a comprehensive analysis of corruption of data. The study explores strategic models aimed at strengthening network defenses in response to the continually changing threat environment. In the past, network security has relied on various technologies to mitigate risks, which include Firewalls, Virtual Private Networks (VPNs) and Encryption Protocols. The research scrutinizes the role of technologies such as homomorphic encryption for safeguarding data privacy and the emergence of Extended Detection and Response (XDR) platforms for holistic threat management. Automation, self-healing networks, and advancements in biometric authentication methods are also discussed as integral components of a resilient security infrastructure. Future of network security risk technologies are growing rapidly and are witnessing advancement in technologies which include AI-Powered Threat Intelligence, 5G Security, Enhanced extended detection Response (XDR), Biometric Authentication Advances and Self-Healing Networks.

Keywords: Data, AI, XDR, management, IoT

INTRODUCTION

Securing networks is essential for protecting computer systems and data against unauthorized access, cyberattacks, and interruptions. It includes applying various strategies to ensure confidentiality, integrity, and availability of information within the network environment. Key components include firewalls, encryption, intrusion detection systems, and secure authentication protocols. By employing these measures, organizations can mitigate risks and ensure a resilient and secure network infrastructure.

The vulnerabilities are weak points in computer devices or software which can present opportunities for attackers. Weaknesses could range from physical protection to antivirus updates. It protects the usability and integrity of companies' infrastructure by preventing proliferation.

Network security technology includes a range of techniques and tools developed to defend networks against unauthorized access, data leaks, and various cyber threats. Key technologies commonly used in this domain are firewalls, intrusion detection and prevention systems (IDPS), virtual private networks (VPNs), encryption tools, antivirus programs, and access control systems. Together, these tools help protect networks and the sensitive data they handle, from cyberattacks and malicious entities. At the physical layer, effective network security also demands mechanisms for detecting failures and attacks, along with smart strategies for countermeasures [1].

As technology evolves, future network security risks may include advancements in artificial

***Author for Correspondence**
Muskan Sharma
E-mail: 2023pietcsmuskan108@poornima.org

[1]Student, Department of Computer Science and Engineering, Poornima Institute of Engineering and Technology, Jaipur, Rajasthan, India
[2]Associate Professor, Department of English and Soft Skills, Poornima Institute of Engineering and Technology, Jaipur, Rajasthan, India

Received Date: May 12, 2025
Accepted Date: August 21, 2025
Published Date: September 17, 2025

Citation: Muskan Sharma, Krati Sharma, Khushi Sharma, Navya Khandelwal. Network Security and Risk Technologies. Journal of Network Security. 2025; 13(3): 26–34p.

intelligence, quantum computing threats to encryption, sophisticated phishing attacks, IoT vulnerabilities, and potential exploits in emerging technologies. Staying vigilant and adopting proactive security measures will be crucial to mitigating these evolving risks.

The necessity of a strong security system is underscored by the emergence of complex threats like ransomware, distributed denial-of-service (DDoS) assaults, and advanced persistent threats (APTs). These dangers provide serious implications to national security, reputation, and financial stability in addition to endangering data. This study examines the hazards that network infrastructures entail and assesses the methods used to reduce those risks. It looks at new threats, evaluates their effects, and identifies creative ways to bolster network defenses. The study emphasizes the necessity of ongoing investigation and cooperation to combat changing cyberthreats.

LITERATURE REVIEW

The 2006 work by Sotillo tackles the security issues related to IPv6 adoption [2]. There are new dangers and vulnerabilities that arise with the switch from IPv4 to IPv6 that must be addressed. In the context of the new protocol, this study probably examines a number of IPv6 security topics, including intrusion detection, packet filtering, and address setup. "Distinguishing Between Data Security and Network Security", by Kartalopoulos was presented at the IEEE International Conference on Communications in 2008 ICC'08. In this 2008 study, Kartalopoulos explores the differences between network security and data security [1]. Comprehending this distinction is essential to formulating all-encompassing security plans.

The study can go over how network security entails securing communication channels and network architecture, whereas data security concentrates on preserving data availability, integrity, and secrecy. It is possible that Farrow covers a variety of network security technologies and strategies in his work [3]. It may provide insight into the operation and application of devices such as firewalls, intrusion detection systems, and encryption techniques.

Comprehending these instruments is vital for proficiently safeguarding networks from cyber hazards. The white paper by Warfield examines how implementing IPv6 may affect security [2]. Organizations moving to IPv6 must take into account any security issues related to the new protocol. This study may examine vulnerabilities specific to IPv6, including protocol translation problems, address space growth, and auto-configuration techniques, and provide suggestions for reducing the risks.

The paper "Grid of Security" method by Flauzac *et al*. probably offers a fresh viewpoint on network security [4]. To improve overall security posture, this strategy can entail integrating several security mechanisms into a unified architecture that resembles a grid. The approach's ability to support quick incident response, proactive threat detection, and adaptable security measures to counteract changing cyberthreats may be covered in the paper by Florea and Craus [5].

In general, a variety of subjects pertaining to network security are covered in the evaluated literature, such as the difficulties with IPv6 security, the difference between data and network security, network security tools, and creative methods for bolstering network security posture. Every article adds significant knowledge to the area and offers a thorough grasp of the tactics and complexity involved in protecting contemporary networks (Figure 1).

Types of Network Security

- Firewall.
- Access Control.
- Remote access VPN.
- Network Segmentation.
- E-mail security.
- Data loss prevention (DLP).
- Zero Trust Network Access (ZTNA).

Figure 1. Diagram of network protection.

Key elements of network security risk include (Figure 2):

1. *Threats:* Malicious activities or events that exploit vulnerabilities in a network. Examples include malware, phishing attacks, and denial-of-service (DoS) attacks.
2. *Vulnerabilities:* Flaws within the network infrastructure that may be targeted by potential threats. These issues can result from obsolete software, improper configurations, or insufficient security protocols.

Over the years, various technologies have been employed to enhance network security and mitigate risks. Some past technologies include:

1. *Firewalls:* Conventional firewalls have been a core element of network security for many years, managing the flow of network traffic by enforcing established security policies.
2. *Virtual LANs (VANs):* Used to segment networks into smaller, isolated sections, reducing the scope of potential security breaches.

Predicting future technologies is always challenging, but several trends and areas of development are likely to shape the future of network security (Figure 3). As per the last knowledge update in January 2022, here are some potential directions for future technologies in network security:

- *Quantum-Safe Cryptography:* As quantum computing advances, increasing attention is being given to creating cryptographic algorithms that can withstand quantum-based attacks, aiming to maintain secure communication in the future.
- *AI-Driven Security Operations:* Increasing integration of artificial intelligence and machine learning to enhance threat detection, automate responses, and analyze vast amounts of security data for proactive risk management.

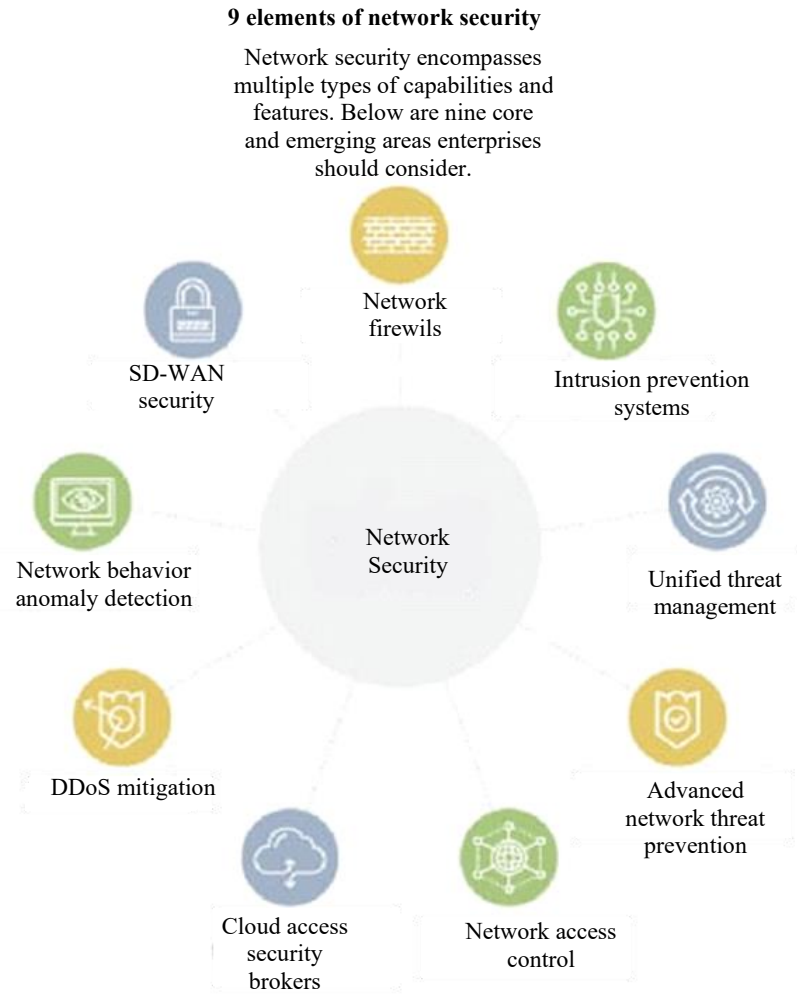

Figure 2. Flowchart of 9 elements of network security.

Essential Tools for Network Security [3]

- *Nmap Security Scanner:* A free, open-source tool used for network discovery and security assessment.
- *Nessus:* Recognized as one of the top free tools for scanning networks for vulnerabilities.
- *Wireshark (formerly Ethereal):* An open-source network protocol analyzer compatible with both UNIX and Windows platforms.
- *Snort:* A lightweight intrusion detection and prevention system that excels in analyzing traffic and logging packets in IP networks.
- *Netcat:* A basic yet powerful utility that enables reading and writing of data over TCP or UDP connections.

Background

- *Barker [6]:* Outlined key practical aspects of network security, including detecting intrusions, analyzing traffic, and monitoring network activity.
- *Flauzac [4]:* Introduced an innovative method for deploying distributed security through a collaborative and controlled model known as the "grid of security".

It is essential to recognize that network security is a constantly evolving field, with new technologies potentially transforming its landscape. To remain resilient, organizations must stay updated on industry developments and innovations to effectively enhance their security strategies moving forward.

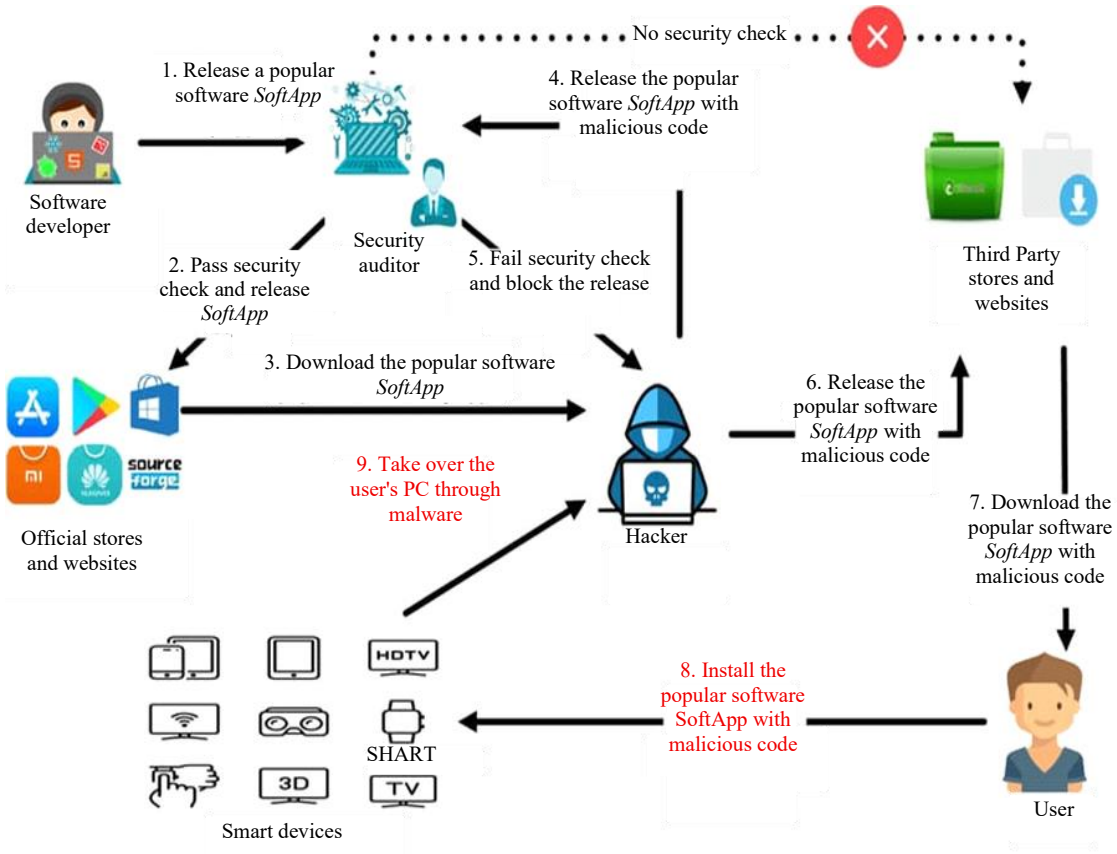

Figure 3. Essential tools for network security.

IMPACT OF NETWORK SECURITY AND RISK

Additionally, network security plays an important role in protecting against malware, phishing attacks, and other forms of cyber attackers. It helps organization with all requirements, builds trust with all the customers, and supports the whole stability of digital ecosystems [7].

With the increasing interconnectedness of the devices and system through the Internet of Things (IoT) shows the importance of network security. Vulnerabilities in one device or system should potentially compromise all entire networks, emphasizing the need for the comprehensive security measures that can be taken.

The potential damage that may arise from any consequences related to the unauthorized exposure, alteration, destruction, or loss of information, as well as the unavailability of information systems [8]. In nutshell, impact of network security and risk extends beyond immediate threat, influencing the overall safety, reliability, and resilience of digital infrastructure in the interconnected world.

ADVANTAGES

The advantages of network security and effective risk management are as follows:

Data Protection

Network security safeguards the information, preventing unauthorized data access or data breaches, which is important for protecting personal data. Through the proper implementation of network security measures of your business can make sure that the data is securely protected and that your online activities are safe from hazards, controlling incoming and outgoing network traffic with predetermined security rules and identifying all problems in your network and strategies for avoiding them.

Business Continuity

By minimizing all risk cyberattacks, network security ensures continuity of the business operations, reducing downtime and potential financial losses. Recognizing and evaluating the particular security risks and potential threats to your business and its essential infrastructure is crucial. Performing a business impact analysis helps determine the effects of various disruptions and outlines the recovery process along with potential business losses.

Customer Trust

The strong network security measures build trust with customers or clients, assuring them that their data is handled securely for long-term relationships. Customers place their trust in you to handle their data, and it is our duty to ensure its security and confidentiality. The right security software ensures so that sensitive information remains confidential, safeguarding your customer trust.

Regulatory Compliance [9]

Many industries have specific regulatory requirements regarding data protection. Implementing network security measures helps organizations comply with these regulations. It also helps in avoiding legal issues and penalties.

Enhanced Productivity

Securing networks against malware and phishing attacks reduces downtime and enabling employees to focus on their tasks without any interruptions.

Resource Optimization

By prioritizing risks based on their impact and likelihood or organizations can allocate resources efficiently to mitigate high threats.

Regulatory Compliance

Comprehensive risk assessments help organizations comply with legal and regulatory requirements and to avoid penalties and maintaining operational legitimacy.

Strategic Decision-Making

Risk analysis provides actionable insights that inform strategic planning, decision-making, fostering long-term resilience.

DISADVANTAGES

The disadvantages of network security and effective risk management are as follows:

Cost

Although it implements and maintains robust network security measures, implementing network security can be costly, particularly for smaller organizations with limited financial resources. These solutions are often available as standalone software or can be integrated into existing enterprise resource planning (ERP) systems. However, both the planning and deployment processes can be time-consuming and expensive for organizations.

Complexity

As modern networks expand in size and sophistication, managing security becomes increasingly challenging. This complexity can introduce vulnerabilities if not properly managed. Cybercriminals often exploit outdated systems, human error, and misconfigurations to identify weak points. Additionally, IT professionals may struggle to detect threats effectively when they are responsible for managing multiple security tools simultaneously.

Need for Skilled Professionals

Managing large and complex networks is not a simple task. It requires well-trained experts capable of addressing security issues as they arise. Employing a competent network administrator is essential to ensure smooth operations. This individual must possess the appropriate training to meet organizational security needs and respond to emerging threats.

Poor Administration [10]

Even after successful installation and setup of security systems, there is a risk of administrative negligence. It is the administrator's responsibility to continuously monitor the system for suspicious activity or potential breaches. However, relying too heavily on automated systems or becoming complacent can create opportunities for cyberattacks. Therefore, it is crucial for administrators to remain vigilant at all times.

The implementation of new security measures or risk analysis process can disrupt regular operations or particularly during system integration or employee training.

Over-Reliance on Tools

Organizations may become overly reliant on automated tools and fails to account for human factors, which remain critical in managing security and risks.

False Positives and Negatives

Intrusion detection systems and firewalls can produce false positives, blocking legitimate traffic, false negatives, allowing malicious activity to go undetected. These issues can disrupt operations or compromise security.

Reduced Performance

Security protocols, such as encryption and multi-factor authentication, may slow down network performance and create delays in accessing resources and impacting productivity.

SCOPE

Network security and risk management include safeguarding systems, networks, and data from intrusions, vulnerabilities, and illegal access. To protect against cyber dangers, it entails putting in place safeguards including intrusion detection systems, firewalls, encryption, and access controls. In order to maintain data integrity and business continuity, risk management also include identifying and reducing possible hazards. This entails locating weaknesses, assessing the possible consequences, and putting precautions in place to reduce or eliminate risks [11].

It is anticipated that emerging technology in network security will tackle the ever-evolving and complex cyber threats. The following are some areas of interest and possible developments:

1. *Security Defined by Software (SDSec):* Just like Software-Defined Networking (SDN), SDSec permits dynamic and programmable security rules. Future developments in SDSec will make it possible for enterprises to expand security measures across dispersed networks effectively and respond swiftly to evolving threats.
2. *Behavioral Biometrics [12]:* Phishing and identity theft are possible using conventional authentication techniques like passwords and tokens. Behavioral biometrics provide a more seamless and safe method of authentication.
3. *Compliance and Regulations:* Businesses have to go by a number of industry-specific laws and compliance guidelines, such GDPR, HIPAA, PCI DSS, and SOX, that control data security and privacy. To prevent repercussions on the legal and financial fronts, network security measures must be compliant with these criteria.
4. *Incident Response and Recovery:* To quickly lessen the effects of security breaches or cyberattacks, organizations require strong incident response and recovery procedures in addition

to preventive measures. These include locating occurrences, minimizing damage, looking into the underlying reasons, and getting things back to normal.

5. *Third-Party Risk Management:* A lot of businesses depend on outside suppliers, vendors, and service providers, whose networks and systems could be dangerous. Monitoring security standard compliance, setting contractual duties, and evaluating the security posture of external partners are all essential components of effective third-party risk management.
6. *Employee Awareness and Training:* Security breaches are still largely caused by carelessness and human error. Therefore, in order to inform staff members about the best security practices, phishing schemes, social engineering techniques, and incident reporting protocols, firms need to engage in employee awareness programs and cybersecurity training.
7. *Internet of Things (IoT) [10]:* Protecting interconnected devices from unauthorized accesses and exploitation.

CONCLUSION

Technologies for network security and risk management are essential in today's linked world for protecting digital infrastructure from ever changing cyberthreats. In order to guarantee the confidentiality, integrity, and availability of data, this study emphasized the significance of putting in place thorough security measures, such as firewalls, intrusion detection systems, encryption, and sophisticated risk assessment frameworks. Organizations must implement a proactive, multi-layered protection strategy that integrates technology, policy, and ongoing monitoring as cyber threats get increasingly complex. Additionally, cutting-edge technologies like blockchain, AI, and machine learning promise to improve real-time risk detection and mitigation.

Future research should concentrate on incorporating risk technologies that give networks resilience and agility, as well as creating adaptive security models that can change as threat landscapes do. Network security and risk technologies should be given top priority so that we can create a safer digital environment for people, companies, and governments.

Acknowledgment

I would like to sincerely thank Dr. Krati Sharma, whose advice, support, and insightful comments were crucial to the completion of this study. Additionally, I am grateful to Poornima Institute of Engineering and Technology for offering the tools and assistance I needed for this research.

My friends and coworkers deserve special recognition for their encouraging words and helpful criticism, which inspired me to pursue excellence. For their constant understanding and support throughout my research, I am also thankful to my family and friends. Lastly, I would want to thank all of the experts and researchers whose work has made this study possible. Their input has been enlightening and inspirational, influencing the course and results.

REFERENCES

1. Kartalopoulos SV. Differentiating data security and network security. In 2008 IEEE International Conference on Communications. 2008 May 19; 1469–1473.
2. Sotillo S. Ipv6 security issues. Scanning. 2006; 4: 1–6.
3. Farrow R. Securing the Web: fire walls, proxy servers, and data driven attacks. InfoWorld. 1995 Jun 19; 17(25): 103–4.
4. Flauzac O, Nolot F, Rabat C, Steffenel LA. Grid of security: A new approach of the network security. In 2009 IEEE Third International Conference on Network and System Security. 2009 Oct 19; 67–72.
5. Florea R, Craus M. A game-theoretic approach for network security using honeypots. Future Internet. 2022 Nov 30; 14(12): 362.
6. Barker K. The security implications of IPv6. Netw Secur. 2013 Jun 1; 2013(6): 5–9.

7. Sabillon R, Cavaller V, Cano J. National cyber security strategies: global trends in cyberspace. International Journal of Computer Science and Software Engineering (IJCSSE). 2016 May 1; 5(5): 67–81.
8. Vargas H, Lozano-Garzon C, Montoya GA, Donoso Y. Detection of security attacks in industrial IoT networks: A blockchain and machine learning approach. Electronics. 2021 Oct 30; 10(21): 2662.
9. Hyder MF, Farooq MU, Ahmed U, Raza W. Towards enhancing the endpoint security using moving target defense (shuffle-based approach) in software defined networking. Eng Technol Appl Sci Res. 2021 Aug 21; 11(4): 7483–8.
10. Javanmardi S, Shojafar M, Mohammadi R, Nazari A, Persico V, Pescape A. FUPE: A security driven task scheduling approach for SDN-based IoT–Fog networks. J Inf Secur Appl. 2021 Aug 1; 60: 102853.
11. Liu Y. Computer Network Information Security in the Big Data Era. In: The International Conference on Cyber Security Intelligence and Analytics. Cham: Springer International Publishing; 2020 Feb 28; 153–160.
12. Olakanmi OO, Odeyemi KO. Versa: Verifiable and secure approach with provable security for fine-grained data distribution in scalable Internet of things networks. Int J Inf Secur Priv. 2021 Jul 1; 15(3): 65–82.

