STM JOURNALS

Journal of
Network Security

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 14, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoNS

https://journals.stmjournals.com/jons

Review JoNS

Cybersecurity Early Detection Algorithms for Threats

Maniyar Dhruvi Nitinbhai*

Abstract

Cybersecurity plays a vital role in protecting digital systems, networks, and data from unauthorized access, misuse, and cyberattacks in an increasingly interconnected world. As reliance on internet-based technologies continues to grow, the frequency and sophistication of cyber threats have also increased, making effective cybersecurity strategies essential. Cybersecurity encompasses a comprehensive framework that integrates technological solutions, organizational processes, and human awareness to ensure the confidentiality, integrity, and availability of information. Key protective measures include secure networking practices, encryption techniques, intrusion detection systems, and the use of artificial intelligence for threat detection and prevention. In addition, cybersecurity is not a static solution but a continuous risk management process involving threat identification, vulnerability mitigation, system monitoring, and incident response. The dynamic nature of cyber threats requires constant adaptation of tools, policies, and user training. Despite advancements in defensive technologies, securing complex environments such as the Internet of Things remains a significant challenge. Ultimately, cybersecurity aims to establish a resilient digital ecosystem that supports secure communication, trustworthy digital transactions, and reliable information exchange for individuals, organizations, and governments. By proactively managing risks and evolving alongside emerging threats, cybersecurity strengthens trust, stability, and operational continuity in modern digital infrastructures.

Keywords: AI, machine learning, cloud security, internet security, IT security, privacy, supply chain security

INTRODUCTION

Cybersecurity refers to the systematic approach used to defend computer systems, digital devices, and online technologies from cyber threats, such as hacking, malicious software, and phishing attacks. It is commonly known as information security (INFOSEC) and focuses on maintaining the confidentiality, integrity, and availability of digital information [1]. Cybersecurity aims to protect systems, networks, and data from potential damage and misuse. It involves the use of advanced security tools, well-defined policies, and safe online practices to minimize risks. Effective cybersecurity measures help prevent data theft, system failures, and unauthorized access, thereby ensuring the secure operation of digital environments [2].

TYPES OF CYBER SECURITY

Cybersecurity consists of multiple specialized domains (Figure 1) that work together to protect digital systems, networks, and data from cyber threats. Each type addresses a specific area in the digital environment.

Network Security

The main objective of network security is to safeguard computer networks from threats, such as hacking, unauthorized access, and data breaches [3]. This protection is achieved through the implementation of various security mechanisms, including firewalls and intrusion detection systems.

***Author for Correspondence**
Maniyar Dhruvi Nitinbhai
E-mail: dhruvimaniyar06@gmail.com

Student, Deparment of Information Technology, Shree Swaminarayan College of Computer Science, Bhavnagar, Gujarat, India

Received Date: January 02, 2026
Accepted Date: January 12, 2026
Published Date: February 20, 2026

Citation: Maniyar Dhruvi Nitinbhai. Cybersecurity Early Detection Algorithms for Threats. Journal of Network Security. 2026; 14(1): 31–37p.

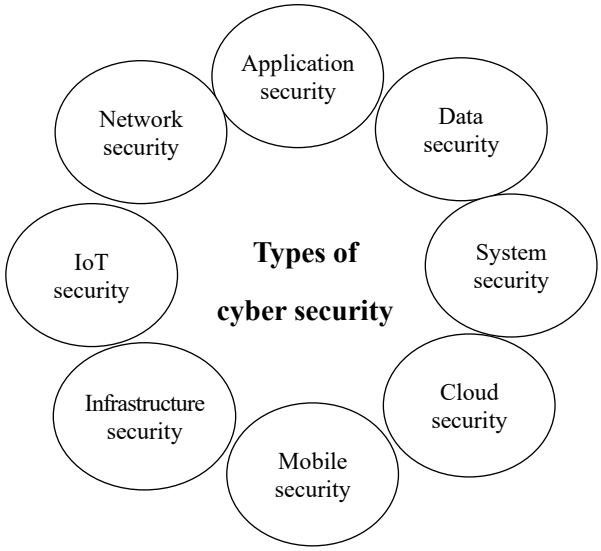

Figure 1. Types of cybersecurity.

Public Wi-Fi networks that are commonly available in places such as cafés, airports, and shopping malls pose significant security risks. Such networks allow cybercriminals to track users' online behavior and potentially access sensitive personal data [4]. When payment gateways or online transactions are used in unsecured public networks, there is a high risk of exposure to financial information. Because these networks lack strong security controls, it is advisable to use a secure private connection or a VPN to protect internal systems and ensure safe internet usage.

Application Security

- This area focuses on protecting software applications by reducing security weaknesses that attackers may misuse. This includes practices such as writing secure code, applying timely updates and patches, and using firewalls designed specifically for applications [5].
- Most mobile applications used on smartphones are generally protected and operated according to the security policies and guidelines set by official platforms, such as the Google Play Store.
- Currently, Google Play hosts approximately 3.55 million apps, the Apple App Store offers approximately 1.64 million, and the Amazon App Store provides nearly 483 million applications. Despite this vast availability, not every application can be considered safe or reliable.
- Certain applications appear trustworthy; however, after installation, they may secretly gather user information and share it with external organizations without proper consent.
- To reduce security risks, applications should always be downloaded from trusted and official app stores rather than from third-party websites that offer Android Package Kit (APK) files [6].

Data Security

Data Protection: Focuses on protecting sensitive information from:

- Unauthorized access
- Unintended disclosure
- Alteration
- Deletion

Incident Response

Incident response is a systematic approach for identifying, analyzing, and addressing security incidents.

User Awareness

Educating users about the significance of information security is essential. This involves informing individuals about potential threats, such as phishing attacks, and teaching them effective ways to safely handle sensitive data [7].

Encryption

Encryption is the process of converting information into an unreadable format known as ciphertext to ensure confidentiality and protect it from unauthorized access.

Cloud Security

- Cloud security involves safeguarding data, applications, and cloud-based infrastructure, while controlling access and ensuring compliance. This protection is often provided in partnership with cloud service providers, such as Amazon Web Service (AWS), Microsoft Azure, and Google Cloud, which help mitigate potential threats.
- In recent years, storing data in clouds has become increasingly popular. When managed correctly, it ensures data privacy and enables users to access information from any device using valid credentials [8].
- Many cloud platforms offer free tiers for limited usage, with additional storage or services available through paid plans. These providers supply a range of offerings, including storage, computing resources, and security solutions.

Internet of Things Security

- The Internet of Things (IoT) security focuses on protecting internet-connected devices, including smart gadgets, sensors, medical equipment, and wearable technology, from cyber threats. The goal is to prevent these devices from becoming entry points for hackers who can access networks and sensitive data.
- Device Authentication and Encryption ensure that only authorized devices can connect to the network while also encrypting data transmitted between IoT devices and servers to maintain confidentiality and integrity [9].
- Firmware and Software Updates are essential to address security vulnerabilities. Regular updates help reduce the risk of hackers exploiting outdated or insecure firmware in IoT devices.
- Network Segmentation separates IoT devices from other critical systems, thereby minimizing the impact of potential attacks on a broader network. Additionally, IoT security frameworks and standards, such as zero-trust architecture (ZTA), encourage best practices such as strong passwords, secure APIs, and endpoint protection to strengthen device security.

MAJOR ATTACK OF CYBERSECURITY

Malware Attack

- Malware is malicious software designed to infiltrate and damage computer systems. It includes Trojans, rootkits, and spyware.
- Cybercriminals often use techniques, such as payload obfuscation, polymorphic malware, and zero-day exploits, to bypass security systems and endpoint defenses.

CYBERSECURITY TRENDS IN 2025

Rise of AI and Machine Learning

Many cybersecurity solutions incorporate AI and machine learning to quickly identify and counteract threats that humans cannot respond to in time. These technologies help to detect unusual patterns, prevent malicious activities, and anticipate potential attacks, making them highly effective in safeguarding sensitive data.

Increase in Ransomware Attacks

Hackers are increasingly using ransomware that locks users out of their systems until a ransom is paid. To prevent such attacks, both individuals and organizations must take proactive measures and implement strong security protection [10].

How to Safe

- Stay informed about cybersecurity practices.
- Watch out for emails or messages that seem suspicious.
- Activate two-step verification on your accounts.
- Regularly update your software and applications.
- Create and maintain strong, unique passwords.

ADVANTAGES AND DISADVANTAGES OF CYBERSECURITY

Cybersecurity is essential in the modern digital era, where an increasing dependence on technology has led to an increase in cyber threats. It protects systems, networks, and data, but also involves certain limitations, such as cost, complexity, and ongoing maintenance (Table 1). The advantages and disadvantages of this method are described in detail below.

Advantages of Cybersecurity

- *Centralization:* The server manages and restricts access, resources, and data to ensure security.
- *Scalability:* Any component can be enhanced or updated as required.
- *Flexible:* New technology can be seamlessly incorporated into the system.

Disadvantages of Cybersecurity

- Exceeds expected levels.
- May lead to network congestion.

CRYPTOGRAPHY IN CYBERSECURITY

In cybersecurity, cryptography protects information by converting readable data (plaintext) into an unreadable format (ciphertext). This process helps to ensure data confidentiality, integrity, authenticity, and non-repudiation. Key cryptographic methods include encryption to safeguard the data, digital signatures to verify authenticity, and hashing to maintain data integrity. These techniques are essential components of secure technologies such as TLS/SSL protocols, VPN encryption, and password protection mechanisms. Table 2 presents the data for the period 2020–2025.

ROLE OF BLOCK CHAIN IN CYBERSECURITY

Cybersecurity is the practice of safeguarding computer systems, networks, and digital information from cyber threats that aim to gain unauthorized access and manipulate or destroy data, often for financial gain or data theft. With the rapid growth in the use of digital technologies, strengthening security mechanisms has become essential for protecting sensitive information.

Table 1. Advantages and disadvantages of cybersecurity.

S.N.	Advantages	Disadvantages
1	Centralization—Access, resources, and data security are controlled through the server.	Dependability—When the server goes down, operations cease.
2	Scalability—Any element can be upgraded when needed.	Lack of mature tools is relatively new technology, and the needed tools are lacking.
3	Flexibility—New technology can be easily integrated into the system.	Lack of scalability—Network operating systems are not very scalable.
4	Interoperability—All components work together.	Higher than anticipated costs.
5	Accessibility—The server can be accessed remotely and across multiple platforms.	May cause network congestion.

Table 2. Tabular format data in 2020–2025.

Metric	2020 data	2021 data	2022 data	2023 data	2024 data	2025 Projection/data
Global annual cost of cybercrime	-	~$6 trillion	~$8 trillion	~$8 trillion estimated	~$8 trillion estimated	$10.5 trillion
Global average cost per data breach	-	-	~$4.35 million	~$4.45 million	~$4.88 million	$4.44 million
Ransomware attacks (global volume)	304.64 million	623.25 million	493.33 million	317.59 million	-	Rising incidence, involved in 44% of breaches
Malware attacks (global volume)	5.6 billion	5.4 billion	5.5 billion	6.06 billion	6.54 billion	369 million detections across India alone
Average time to identify a breach	-	-	-	~200 days	~194 days	~240 days (detect and contain)
Unfilled cybersecurity jobs	-	~3.5 million	-	-	~4.02 million	~4.8 million
Phishing incidents (reported)	-	-	-	-	-	Over 1 million in Q1 2025 alone

Cyber threats can be carried out through various forms of malware, including viruses, Trojan horses, and rootkits. In addition, cyberattacks can take many forms, such as phishing, man-in-the-middle attacks, distributed denial-of-service (DDoS) attacks, SQL injection, and ransomware attacks.

Possible Blockchain Use: A Case for Cybersecurity

- *IoT security:* As adoption of AI and IoT technologies continues to grow, protecting data and connected systems from cyber threats has become a critical concern. Blockchain can enhance IoT security by enabling secure device-to-device encryption, efficient key management, and strong authentication mechanisms, thereby ensuring safer communication within the IoT ecosystems.
- *Integrity of software downloads:* Blockchain technology can be applied to verify the authenticity of software installations and downloads, thereby reducing the risk of malware infections. By storing the cryptographic hash values of legitimate software on the blockchain, downloaded files can be validated by comparing their hashes with stored records.
- *DNS security:* The domain name system (DNS) functions as a directory that translates domain names into IP addresses. Hackers often target DNS to alter these mappings and disrupt websites. Using blockchain's decentralized and tamper-resistant nature, DNS records can be stored securely, minimizing the risk of manipulation and improving overall system reliability.

HACKING IN CYBERSECURITY

Hacking is a concept in cybersecurity that involves exploiting system vulnerabilities to gain unauthorized access. It can be performed for malicious purposes by black hat hackers or for defensive and ethical purposes by white hat hackers, the primary goal of which is to identify weaknesses and strengthen system security.

The hacking activities include phishing, malware attacks, and password cracking. Malicious hacking often causes financial damage, resulting in losses worth billions of dollars.

Types of Hacking

- *Black hat hackers:* Individuals who intentionally breach computer systems without authorization for malicious purposes such as stealing sensitive information, gaining personal profit, or disrupting operations.

- *White hat (ethical) hackers:* Security professionals who are legally employed by organizations to penetrate systems in a controlled manner to identify weaknesses and strengthen defenses against potential cyberattacks.
- *Grey hat hackers:* Hackers who operate between legal and illegal boundaries; they may access systems without permission, but their actions are generally aimed at exposing vulnerabilities rather than causing harm, even though their approach is often controversial.

AI IN CYBERSECURITY

Artificial Intelligence in cybersecurity leverages machine learning techniques and advanced algorithms to process large volumes of data, identify unusual patterns, automate security actions, and anticipate potential threats more quickly and accurately than human analysts. It plays a vital role in defending against modern cyberattacks such as malware, phishing, and system intrusions. Cybercriminals also use AI to design more advanced and complex attacks.

The major uses of AI in cybersecurity include real-time threat monitoring, user behavior analysis, vulnerability assessment, and automated incident handling, which together strengthen proactive defense while addressing AI-driven attacks.

Cyber threats are rapidly increasing and often surpass traditional security measures, owing to the continuously evolving tactics of attackers. Consequently, the role of AI in cybersecurity has become increasingly important. AI helps organizations identify high-priority incidents, detect attacks instantly, respond automatically to security breaches, manage system vulnerabilities, and improve overall network protection (Figure 2).

Detection

Just as a pet dog can recognize the familiar scent of each family member, AI in cybersecurity identifies normal behavior patterns within the data. When something unusual occurs, such as repeated failed login attempts or unexpected file downloads, the system raises an alert, signaling a potential security threat.

Prediction

Similar to an experienced security guard, who can anticipate where a crime may happen next, AI systems analyze historical attack data to forecast future cyber threats. By studying previous incidents, AI can recognize trends and predict the most likely targets or attack methods.

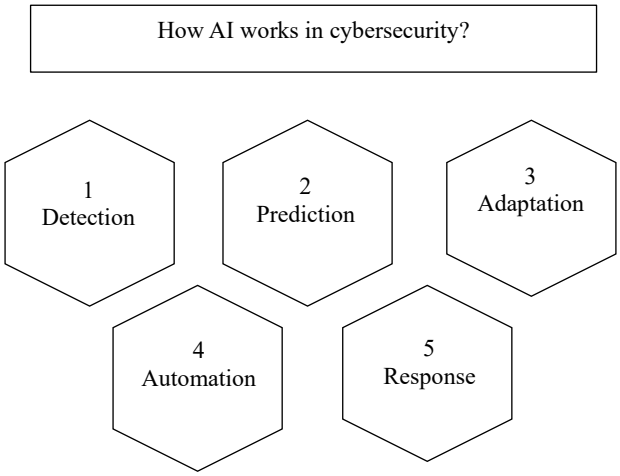

Figure 2. How AI works in cybersecurity.

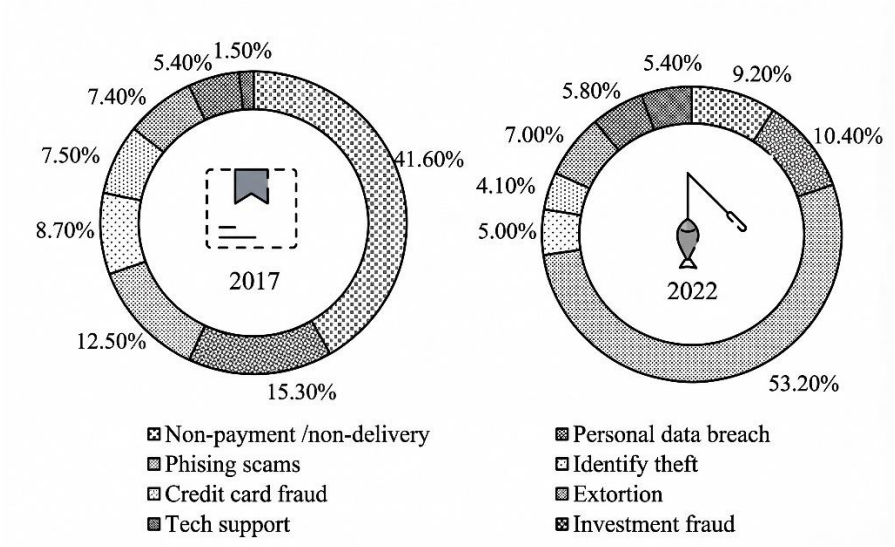

Figure 3. Cybercrimes.

Adaptation

A trained guard dog improves its ability to protect the house by learning from past experience. If it encounters a new trick used by intruders, it adjusts its responses accordingly. Similarly, AI-driven cybersecurity systems continuously learn from earlier attacks and adapt their defenses to better protect against future threats (Figure 3).

CONCLUSION

Cybersecurity is not a war that ends with a final win; it is a continuous and necessary process, as digital threats continue to evolve. Addressing these challenges requires multilayered security measures, continuous monitoring, informed users, robust cybersecurity regulations such as the Digital Personal Data Protection Act (DPDPA), and strong collaboration to protect critical infrastructure, sensitive data, and personal privacy from malicious entities. Although complete security is impossible, a high level of protection can be achieved through proactive risk management and technological advancements.

REFERENCES

1. Fang D, Huang G, Chang S, Yang H, Hu L, Ye D. Shorter lattice-based verifiable encryption using bimodal Gaussian. Cybersecurity. 2025;8(1):67. doi:10.1186/s42400-024-00351-4.
2. Yang Y, Li Z, Ding Y, Hu M. MAT-FHE: Arbitrary dimension matrix multiplication scheme for floating point over fully homomorphic encryption. Cybersecurity. 2025;8(1):48. doi:10.1186/s42400-024-00303-y.
3. Vijayaraghavan SKJ. Policy as code: A paradigm shift in infrastructure security and governance. World J Adv Res Rev. 2025;26(1):3399–3405. doi:10.30574/wjarr.2025.26.1.1441.
4. Hamidi MS, Singh B. Analysis of cyber security challenges in developing countries. Nanotechnol Percept. 2024;20(S3):604–610.
5. Asaad RR, Saeed VA. Cyber security threats, vulnerability, challenges and proposed solution. Appl Comput J. 2022:227–244. doi:10.52098/acj.202260.
6. Russell D, Gangemi GT. Computer Security Basics. Sebastopol (CA): O'Reilly Media Inc.; 1991.
7. Cybersecurity and Infrastructure Security Agency. Framework for improving critical infrastructure cybersecurity. Washington (DC): CISA; 2014.
8. Hamidi MS, Singh B. Designing a novel cybersecurity framework to prevent cyberattacks with reference to least developing countries. Nanotechnol Percept. 2024;20:159–165.
9. Chisty NMA, Baddam PR, Amin R. Strategic approaches to safeguarding the digital future: Insights into next-generation cybersecurity. Eng Int. 2022;10(2):69–84. doi:10.18034/ei.v10i2.689.
10. Baer N. Infrastructure as code: Transforming IT operations through declarative configuration management. J Multidiscip. 2025;5(7):448–454.

