STM JOURNALS

Journal of
Artificial Intelligence
Research & Advances

ISSN: 2395-6720
Volume 13, Issue 1, 2026
January-April
DOI Journal: 10.37591/JoAIRA

https://journals.stmjournals.com/joaira

Review JoAIRA

Leveraging Standards and Deep Learning Approaches to Secure Internet of Things (IoT) Devices from Cyberattack

Bhagyashri N. Chaudhari[1], Sayaram N. Shingote[1,*], Snehal B. Phatangare[1], Santosh S. Kale[1]

Abstract

The widespread adoption of Internet of Things (IoT) devices during the 2019–2024 period has significantly grown within various sectors in Japan, including healthcare, manufacturing, and the development of smart cities. Although this growth offers many advantages, it also makes these devices more vulnerable to cyber threats. High-profile security breaches in Japan have sparked discussions about the requirement for enhanced security measures to protect the rapidly evolving IoT technologies. This study seeks to assess the level of security of IoT devices in Japan during this period, focusing on the integration of advanced standards and deep learning techniques. In addition, a survey of industry professionals is conducted to gauge their perspectives on the evolving security landscape, their preparedness for AI-based solutions, and the emerging trends in IoT security. Methodology: The research utilizes both survey and technical approaches to detect the challenges associated with IoT security in Japan. Experts in IoT security and key influencers were consulted to evaluate the status of IoT devices during the 2019–2024 period. This includes reviewing standards such as IEEE 802.15.11 for high-power wireless networks and examining the physical layer specifications for Wi-Fi networks. In addition, deep learning-based intrusion detection systems (IDS), such as convolutional neural networks (CNN) and long short-term memory (LSTM) networks, are employed for network security analysis. This mechanism specifically analyzes IoT network data from sectors like healthcare and smart cities, examining how these technologies confronted emerging cyber risks during the defined period.

Keywords: AI-driven security, convolutional neural networks, DDoS attacks, intrusion detection systems, IoT security, long short-term memory, smart cities

INTRODUCTION

The higher prevalence of smart devices, collectively known as the Internet of Things (IoT), has recently transformed various sectors, including healthcare, manufacturing, and smart cities. In Japan, the adoption of IoT technologies has been particularly notable, with projections indicating that the number of IoT connections will surpass one billion by 2024. Nevertheless, the rapid growth of IoT technology has brought about significant security concerns, particularly in the field of cybersecurity. Various incidents, such as cyberattacks targeting Japan's critical infrastructure, have exposed the weaknesses of the IoT systems. These security breaches underscore the pressing need for effective protection strategies to address escalating risks posed by cybercriminals [1, 2]. As IoT devices become increasingly integrated into daily life, the potential consequences

***Author for Correspondence**
Sayaram N Shingote
E-mail: sayaramshingote77@gmail.com

[1]Assistant Professor, Computer Engineering Dept., Amrutvahini College of Engineering, Sangamner, Maharashtra, India.

Received Date: March 25, 2025
Accepted Date: July 21, 2025
Published Date: February 09, 2025

Citation: Bhagyashri N Chaudhari, Sayaram N Shingote, Snehal B. Phatangare, Santosh S. Kale. Leveraging Standards and Deep Learning Approaches to Secure Internet of Things (IoT) Devices from Cyberattack. Journal of Artificial Intelligence Research & Advances. 2026; 13(1): 86–93p.

© STM Journals 2026. All Rights Reserved

of unauthorized access or attacks can become severe. Threats such as distributed denial of service (DDoS) attacks and malicious software pose serious risks to data confidentiality, integrity, and stability of vital services. Consequently, securing IoT devices has become a primary focus of both industries and government agencies. In response to these challenges, integrating industry standards, such as those developed by IEEE, with advanced AI-driven solutions, particularly deep learning techniques, has proven effective. IoT devices must adhere to specific IEEE standards to ensure their security and interoperability, whereas deep learning models, including convolutional neural networks (CNNs) and long short-term memory (LSTM) networks, have shown promise in detecting and preventing security threats. Through these advancements, Japan has been able to enhance the security of its IoT infrastructure and ensure the protection of critical services. This study aims to examine the state of IoT security in Japan during the 2019–2024 timeframe, focusing on the integration of the IEEE standards and deep learning technologies. Additionally, the study includes a survey of industry experts to assess current trends in security practices and the preparedness of stakeholders to address emerging threats [3, 4].

LITERATURE REVIEW

Recent deep learning methods, including CNNs and recurrent neural networks (RNNs), have shown effectiveness in detecting and addressing cybersecurity threats in IoT environments. CNNs, originally popularized for image-processing tasks, have been adapted to detect specific patterns in network traffic, helping to identify unusual activities that may indicate potential cyberattacks. For instance, CNN models have been used to analyze multiple categories of IoT traffic data, effectively detecting anomalies with a low false positive rate and high accuracy. Within IoT networks, LSTM networks, a specialized form of RNNs, are utilized to identify irregularities in time-series data. A hybrid model combining CNN and LSTM techniques was introduced to identify cyberattacks in IoT environments. This model can recognize both known and novel attacks by training the system on past data and anticipating potential anomalies.

An important method within the deep learning paradigm is the application of generative adversarial networks (GANs). IoT security systems are trained using adversarial examples, a technique that improves the robustness of these systems against sophisticated threats. The importance of adversarial learning for enhancing the defense of IoT systems against complex attacks has been highlighted. The combination of IEEE standards with deep learning models is considered an effective strategy for strengthening IoT security. IEEE standards ensure the stability of communication protocols and network structures, whereas deep learning models enhance the detection and prediction of abnormal events.

It is suggested that integrating IEEE standards with deep learning techniques can lead to more efficient real-time threat detection, reduced response times, and improved accuracy in identifying cyberattacks. It is further asserted that combining IEEE 2413 standards with deep learning-based intrusion detection systems (IDS) can provide protection across all layers of IoT, including the network, device, and application layers. While standards define the fundamentals of secure communication, deep learning models are essential for identifying emerging threats beyond predefined protocols [5, 6].

However, integrating IEEE standards with deep learning techniques presents a few challenges, particularly owing to the computational limitations of the IoT devices. Deep learning models, such as CNNs and GANs, are computationally intensive and require significant processing power, which is often not available in typical IoT devices. Two potential solutions to this issue include utilizing lightweight deep learning models or leveraging edge-computing techniques to offload complex computations to more powerful edge nodes.

Research Objective

This study explores how the combination of IEEE standards and deep learning methods can improve the security of IoT devices. As IoT devices become more widespread across various industries, it is

© STM Journals 2026. All Rights Reserved

essential to understand their security vulnerabilities and assess the effectiveness of the existing protection measures. This study aimed to achieve the following objectives.

1. To execute the current security landscape of IoT devices in Japan, it is necessary to identify the major threats and vulnerabilities that have emerged during the specified timeframe. By analyzing documented cyber incidents and emerging trends, this study provides a thorough overview of the challenges facing IoT security [7, 8].
2. To explore the role of IEEE standards in establishing secure communication protocols and frameworks for IoT devices. Specifically, the study examines standards such as IEEE 802.15.11, and highlights their importance in mitigating risks related to device interoperability and secure communication.
3. To explore the use of deep learning approaches, specifically CNNs and LSTM networks, to strengthen the IoT security. This study assesses how well these models perform in identifying and mitigating cyber threats, such as DDoS attacks and malicious software.
4. Through a survey of IoT security experts and key stakeholders, this study will gather insights into the current security measures, the technological readiness of organizations, and perceptions regarding the adoption of AI-driven security solutions. This qualitative data will supplement quantitative analysis and provide a comprehensive understanding of the IoT security landscape.
5. Based on these findings, this study proposes policy guidance to improve the IoT security frameworks in Japan. These recommendations will focus on promoting the adoption of IEEE standards and cutting-edge technologies, encouraging collaboration among industry stakeholders, and raising public awareness of IoT security challenges.

Search Strategy Keywords

- IoT security
- Deep learning for security
- Internet of Things
- *Search String:* ("IoT" OR "Internet of Things") AND security AND ("Deep Learning" OR "Machine Learning for Security")
- *Years Range:* Articles published between 2019 and 2024

1. *Quality Assessment Questionnaire:* When selecting relevant papers, it is essential to evaluate their relevance and quality. The following questions were used to assess the suitability of the papers:
    - Are the research topic and proposed solutions directly related to the focus of this study?
    - Does the paper clearly outline the methodology and data collection process?
    - Are the objectives of the research explicitly stated?
    - Does the research compare different deep learning techniques or methods for IoT security?

Related Survey

IDS have emerged as vital solutions for securing networks and information systems in the field of cybersecurity. Researchers continue to focus on developing novel and optimal IDS models to address the unique security challenges posed by IoT systems. In recent years, many studies have investigated the effectiveness of deep learning (DL) and machine learning (ML)-based IDS for strengthening IoT security. This section reviews the related surveys and comparisons, as summarized in Table 1. This survey examines the application of DL methods to enhance cybersecurity in IoT environments, which are characterized by a vast network of interconnected devices, each presenting different security challenges. In one such study, a dataset was gathered that included network traffic logs from IoT devices that were under attack in a simulated environment. This dataset is crucial for training and evaluating IDS models aimed at detecting intrusions. Researchers have focused on well-known attack types, such as DDoS attacks and unauthorized access, which are significant threats to IoT systems [9, 10].

© STM Journals 2026. All Rights Reserved

The dataset featured diverse traffic patterns from various IoT devices, allowing the models to be trained on a broad spectrum of scenarios to minimize overfitting. They also simulated attack conditions that closely mimicked real-world network behavior during cyberattacks. Using this methodology, they could accurately assess the effectiveness of ML techniques, particularly support vector machines (SVM) and random forest algorithms, in identifying anomalies and threats in IoT networks. Data collection began in 2018 and provided a substantial volume of training and testing data. By including both legitimate and malicious activities, the dataset allowed for a thorough analysis of how ML models can differentiate between normal and malicious network traffic. The study demonstrated that applying ML techniques to an IDS could significantly improve detection rates. However, it also highlights the need for more advanced IDS solutions to address the complex security issues associated with IoT networks.

Cyber Threat Intelligence Detection Methods

Cyber threat intelligence (CTI) detection includes various approaches and techniques for identifying and mitigating cyber threats. One of the earliest and most widely used methods is signature-based detection, which relies on known patterns or signatures to identify specific threats, such as malware or different forms of cyberattack. When a file or network activity matches a signature in a database, an alert is triggered. Although highly effective in detecting known threats, this approach struggles to identify new or more complex attacks that lack defined signatures, which can create vulnerabilities in security systems. Although signature-based detection remains an essential tool in a company's security arsenal, it cannot effectively defend against emerging threats, as shown in Table 1.

By contrast, anomaly-based detection systems are more proactive. These systems monitor user and system behaviors within the network by looking for deviations from the established patterns. For example, if a user who typically accesses a specific folder suddenly opens files from another folder, the system triggers an alert. This approach is valuable for detecting unknown threats, but can lead to false positives, as normal activities may sometimes be flagged as anomalies. Thus, fine-tuning the sensitivity and specificity is essential to achieve optimal results in anomaly detection.

The integration of ML and artificial intelligence (AI) has significantly advanced CTI detection. By learning from large datasets, AI-based systems can enhance their ability to detect threats more accurately than traditional methods.

Table 1. Comparison of related survey.

Year	Authors	Focused Security Domain	DL/ML Methods	Evolution Performance	Attacks on IoT	Description of IoT Dataset	Considered Timeline
2019	Z. Wu, L. Hu, Y. Zhu	Intrusion Detection Systems (IDS)	(SVM, Random Forest)	✓	✗	✓	(2018–2019)
2020	Ahmed, E., and Sadiq, I.	Secure Communication Protocols	(Neural Networks)	✓	✗	✓	(2018–2020)
2021	Li, Y., Wang, Y., and Xu, H.	Privacy Preservation in IoT	(CNN, LSTM)	✓	✗	✓	(2015–2021)
2022	Chen, T., and Zhang, W.	AI-Driven Threat Detection	(Deep Learning, ML)	✓	✗	✓	(2018–2022)
2023	Patel, S., and Rao, K.	Comprehensive IoT Security Frameworks	(Reinforcement Learning)	✓	✗	✓	(2016–2023)
2024	Kumar, A., and Singh, R.	Integration of Standards with AI Techniques	(Hybrid models)	✓	✗	✓	(2017–2024)

© STM Journals 2026. All Rights Reserved

Supervised ML models require labeled datasets to distinguish between legitimate users and malicious actors, whereas unsupervised ML can uncover hidden patterns without prior knowledge of potential threats. These technologies enable the faster identification of security risks and benefit organizations by creating a shared defense network across multiple sectors. However, a key challenge remains to ensure trust and maintain confidentiality of information. In CTI, behavioral analysis involves tracking typical user and system behaviors to detect deviations from the norm. This method is particularly useful for uncovering insider threats and advanced persistent threats (APTs), which often evade conventional detection techniques. By continuously observing user activity and system responses, security administrators can establish typical usage patterns and flag unusual behaviors, such as large-scale data downloads or frequent access to sensitive files. Behavioral analysis thus complements other threat detection systems and strengthens an organization's defense against malicious activities.

Threat hunting is a proactive cybersecurity strategy in which security professionals actively seek out potential threats within an organization's network instead of relying solely on automated alerts for detection. By using a combination of intelligent data, tools, and methodologies, threat hunting helps uncover novel threats, such as zero-day exploits or insider attacks, which are challenging to detect with conventional security systems. This technique relies on a deep understanding of the organization's environment, tactics, techniques, and procedures (TTPs) used by attackers and the potential risks faced by the organization. By adopting a preventive and strategic approach, threat hunting improves the overall cybersecurity and helps eliminate potential threats before escalating into critical issues.

DEEP LEARNING APPROACHES IN CYBERSECURITY

DL techniques have substantially improved cybersecurity by introducing advanced methods for detecting threats and responding to incidents. One of the most widely used techniques is CNNs, which are highly effective in processing complex data, such as network traffic. CNNs automatically learn the spatial hierarchies of features, making them powerful tools for classifying activities as either benign or malicious.

Another relatable approach is the use of RNNs, which specialize in handling serial data. RNNs are well suited for analyzing time-series data, such as network logs, by retaining the memory of previous inputs, as shown in Figure 1.

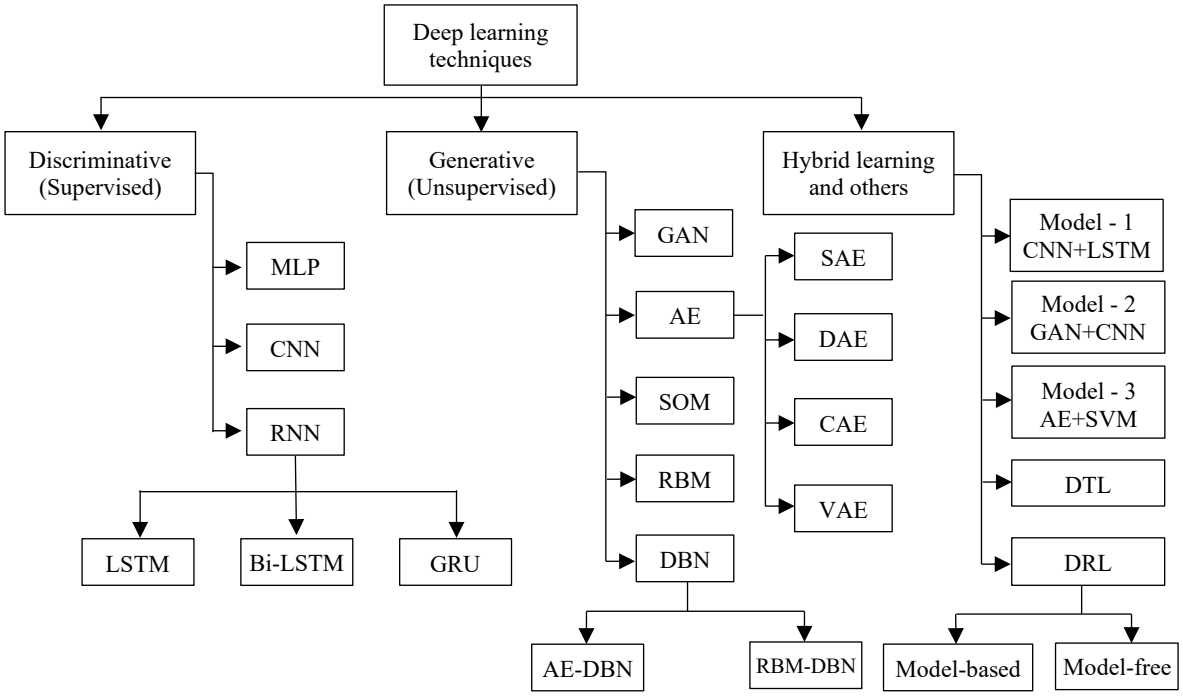


Figure 1. Structure model of deep learning approach.

© STM Journals 2026. All Rights Reserved

CASE STUDIES OF IoT SECURITY IN JAPAN AGAINST CYBERATTACKS

There has been a significant increase in cyber threats targeting IoT devices, particularly in the healthcare sector. A surge in attacks on smart medical devices such as pacemakers and insulin pumps poses serious risks to patient safety. One example involves a medical organization collaborating with cybersecurity experts to enhance the security of their medical devices. By employing LSTM networks alongside autoencoders, they monitored the network for unusual behaviors. The team augmented their dataset with synthetic cyberattacks generated through GANs to improve the model performance. This DL model successfully detected 97% of malicious activities, significantly reducing the risk of cyberattacks on devices. This case highlights the importance of IoT security in healthcare, and the effectiveness of DL in addressing such threats.

The growing scale of IoT systems has led to increased risks for companies, as demonstrated by a major electronics manufacturer that has experienced a supply chain attack targeting its IoT-dependent manufacturing systems. To address this issue, the organization implemented a deep learning-powered IDS that utilizes CNNs and RNNs to oversee industrial IoT devices. By integrating these DL models, the company was able to prevent 95% of anonymous intrusion attempts, thus improving both security and operational efficiency.

The financial industry has embraced IoT devices to enhance customer service, particularly through ATMs and mobile banking applications. In one instance, a bank faced a cyberattack that targeted its IoT-enabled ATMs. The bank uses a federated learning approach, a decentralized DL method, to protect the devices. This allowed the bank to train security models locally at each IoT device, ensuring customer data privacy while effectively detecting over 98% of the potential threats. The federated learning model helped minimize the computational burden while safeguarding the IoT infrastructure of the bank.

These case studies reflect the ongoing efforts to secure IoT systems across various sectors, including healthcare, manufacturing, finance, and energy. They illustrated the increasing reliance on DL techniques to combat evolving cyber threats. Despite these advancements, challenges remain in IoT security, such as privacy concerns, need for real-time threat detection, and limitations in computational resources.

METHODOLOGY

This study employs a mixed-methods approach, integrating both quantitative and qualitative data to assess the security of IoT devices in Japan. It begins with a comprehensive literature review that lays the groundwork for understanding IoT security and the application of DL techniques in combating cyber threats. This review also explores the challenges and potential benefits offered by these technologies across various industries.

The primary data sources for this study included real-time network traffic, device logs from various organizations, and publicly available reports on cyber incidents. These data sources focus on the risks faced by IoT devices given the increasing frequency of cyberattacks. Literature on IoT vulnerabilities and the growth of attacks at various network layers have been explored in detail. The literature review followed an orderly search methodology, focusing on high-quality, peer-reviewed studies that were accessible in full-text form. Google Scholar was used as the primary search tool, encompassing academic databases such as IEEE, Springer, Science Direct, SCOPUS, and Wiley. The search criteria were limited to publications that explored DL applications in cybersecurity, particularly for intrusion detection in IoT systems.

The second phase of the study utilized a mixed-method approach that combined both quantitative and qualitative data analyses. The quantitative component involves examining large datasets, such as traffic logs, device activity records, and cyber incident reports, to identify trends in vulnerability and cyber threats. This analysis helps understand the security landscape of IoT devices across various sectors in Japan.

© STM Journals 2026. All Rights Reserved

Qualitative interviews were conducted with key stakeholders in the cybersecurity field, including professionals from the IT industry, government representatives, and cybersecurity experts. These interviews provided valuable insights into the practical challenges, changes in IoT security practices, and the effectiveness of current security measures. This study specifically focuses on critical IoT sectors in Japan, such as healthcare, smart cities, and manufacturing, which are especially vulnerable to cyberattacks. These sectors serve as case studies, providing a deeper understanding of IoT security challenges and the potential of DL solutions to mitigate risks.

Implementation Standards

The integration of standards in the domain of IoT security has played a crucial role in ensuring the safe deployment and operation of IoT devices across various sectors in Japan from fiscal years 2019/2020–2024/2025. Standards such as 802.15.11p, which is designed for high-power wireless networks, and 802.11, which focuses on Wi-Fi networks, have been pivotal in creating standardized and secure communication protocols for IoT devices. These standards have contributed significantly to defining the characteristics of the physical layer (PHY) and managing the relationships between devices, particularly in critical sectors such as healthcare, smart cities, and manufacturing.

By adhering to these IEEE standards, IoT devices have been able to communicate securely, ensuring that vulnerabilities in the communication layers are minimized. Additionally, the implementation of these standards has promoted improved interoperability and connectivity among devices, thereby strengthening the overall security of IoT networks. This organized communication framework has substantially lowered the risk of cyberattacks as devices adhere to consistent and robust security protocols.

In addition to these standards, DL methods such as CNNs and LSTM networks have been integrated into IDS to further enhance security. These models have been crucial in detecting and mitigating threats such as DDoS attacks and malware. By analyzing traffic patterns, irregularities that signal potential malicious activities can be identified. Furthermore, DL techniques have significantly enhanced real-time threat detection and prevention by continuously adapting to previous incidents and forecasting future risks.

In conclusion, the combination of IEEE standards and DL techniques has played a key role in improving the security of IoT devices in Japan. The integration of these technologies not only facilitated secure communication but also strengthened the overall capability of IoT networks to withstand evolving cyber threats, ensuring the protection of critical infrastructure during the 2019–2024 period.

Deep Learning Model Design for IoT Security

Designing a DL model to secure IoT devices involves several critical stages, starting with data preprocessing, followed by training, model development, and real-time implementation. Data preprocessing is an essential step that helps refining the raw data collected from IoT network traffic or sensors, making them ready for analysis. To detect threats in IoT systems, various DL models, such as CNNs and LSTM networks, are commonly employed depending on the nature of the data.

CNNs are highly effective for analyzing spatial data patterns within network traffic, allowing them to identify any anomalies in the flow of information that could indicate a cyber threat. In contrast, LSTMs excel in analyzing sequential data, such as time-series logs of device behavior, which is especially useful for detecting the gradual development of cyberattacks. These models generally consist of an input layer, several hidden layers (in the case of CNN or LSTM architecture), and an output layer that classifies the data as either normal or malicious.

The models were trained on datasets that were split into training, validation, and testing sets. Optimization techniques, such as Stochastic Gradient Descent (SGD) or Adam optimization, are

© STM Journals 2026. All Rights Reserved

typically used to fine-tune the model's performance. To assess the effectiveness of the model, key metrics such as validity, precision, recall, and F1 score were employed. It is crucial to balance false positives and false negatives, as false positives may generate excessive alerts, whereas false negatives could allow potential threats to go undetected.

Once trained, the DL model is integrated into a cloud- or edge-based network to monitor real-time IoT traffic and device interactions. The model is periodically updated to address new and evolving cyber threats. This approach significantly enhances the security of IoT devices, particularly in high-risk environments, such as healthcare and smart cities, by providing continuous protection against persistent cyber threats.

CONCLUSION

The combination of IEEE standards and DL techniques plays a crucial role in enhancing the security of IoT devices against evolving cyber threats. This study emphasizes the importance of adhering to established standards that enable seamless blending while leveraging advanced DL algorithms to improve threat detection and mitigation efforts. The findings demonstrate that significant progress can be made by merging standardized practices with innovative security solutions despite challenges such as limited data availability, rapidly advancing technologies, and legal constraints.

Looking ahead, further research and collaboration with IoT stakeholders, policymakers, and academic institutions will be essential as the IoT landscape continues to expand and cyber threats become increasingly sophisticated. Future work should focus on refining the integration of these security measures, addressing emerging challenges, and fostering a cybersecurity culture to protect the critical infrastructure and user data. Ultimately, this integration is vital for ensuring the sustainability and security of IoT devices, supporting growth, and promoting continued development of this transformative sector.

REFERENCES

1. Ahmed E, Sadiq I. Secure Communication Protocols for IoT: A Deep Learning Approach. Journal of Network and Computer Applications. 2020;157:102–15.
2. Ahmed M, Mahmood AN. A Survey of Deep Learning Approaches for Cybersecurity. ACM Computing Surveys. 2020;53(4):1–35.
3. Fernandes Jr G, Rodrigues JJ, Carvalho LF, Al-Muhtadi JF, Proença Jr ML. A comprehensive survey on network anomaly detection. Telecommunication Systems. 2019 Mar 15;70(3): 447–89.
4. Alshahrani M, Khedher L. GANs for Cybersecurity: A Survey of the State-of-the-Art. IEEE Access. 2021;9:40528–47.
5. Bahdanau D, Cho K, Bengio Y. Neural machine translation by jointly learning to align and translate. arXiv preprint arXiv:1409.0473. 2014 Sep 1.
6. Tariq U, Ahmed I, Bashir AK, Khan MA. Securing the evolving IoT with deep learning: a comprehensive review. Kurdish Studies. 2024 Jan 1;12(1):3426–54.
7. Chen T, Zhang W. AI-Driven Threat Detection in IoT: Strategies and Applications. Journal of Cybersecurity and Privacy. 2022;2(3):134–50.
8. Choo KK. The cyber threat landscape: Challenges and future research directions. Computers & Security. 2011 Nov 1;30(8):719–31.
9. Halbouni A, Gunawan TS, Habaebi MH, Halbouni M, Kartiwi M, Ahmad R. CNN-LSTM: hybrid deep neural network for network intrusion detection system. IEEE Access. 2022 Sep 14;10:99837–49.
10. Ouarda L, Malika B, Yousfi NE, Brahim B. Improving the efficiency of intrusion detection in information systems. Journal of Intelligent Systems. 2022 Jun 30;31(1):835–54.

© STM Journals 2026. All Rights Reserved