Deep Models against Deep Threats: A Review of Deep Learning for Cyber Attack Mitigation

Mr. Shashi Maurya[1], Dr. Neha Gupta[2] , Dr. Rahul Kumar[3]

[1] Research Scholar, Dr. K. N. Modi University (DKNMU), Newai, Tonk Rajasthan, India

[2] Associate Professor, Dr. K. N. Modi University (DKNMU), Newai, Tonk Rajasthan, India

[3] Associate Professor, Sir Padampat Singhania University (SPSU). Udaipur, India

DOI: https://doi.org/10.47772/IJRISS.2026.10190024

Received: 23 January 2026; Accepted: 29 January 2026; Published: 14 February 2026

ABSTRACT

The speed of the advancement of digital technologies has led to a remarkable rise in the scale, complexity, and sophistication of cyber-attacks. Traditional security approaches based on extensive use of static rules and signature-based detections are simply not adequate for contemporary threats such as zero-day exploits, advanced persistent threats (APTs), and adversarial attacks. As a radical shift in approach, deep learning has emerged, providing intelligent, adaptive, and automated features for cyber defenses. This review paper provides an inclusive overview of deep learning technologies to mitigate various forms of cyber-attacks. Various deep learning architectures are investigated in this paper, such as convolutional neural networks (CNN), recurrent neural networks (RNN), long short-term memory (LSTM), autoencoders, generative adversarial networks (GANs), and graph neural networks (GNN), and the applications of each technology in intrusion detection, malware classification, phishing detection, anomaly detection, and network traffic analysis. In addition, we discuss mainstream datasets, metrics for evaluation, and methodology as they relate to cyber security. Issues such as limited data, adversarial robustness, and usability, will be critically discussed. We also discuss new directions such as hybrid models, privacy-preserving learning, and federated defenses. By aggregating recent research, this review highlights the promise of deep models to serve as robust defenders against deep and evolving cyber-attacks, which serves as impetus for next-generation intelligent cybersecurity systems.

Keywords: Deep Learning, Cybersecurity, Cyber Attack Mitigation, Intrusion Detection, Malware Detection, Anomaly Detection, Neural Networks, Adversarial Attacks, GANs, Privacy-Preserving Learning..

INTRODUCTION

The rapid advancement of digital transformation has significantly transformed how people, organizations, and governments live and function, generating a hyper-connected environment based on cloud computing, Internet of Things (IoT) devices, mobile platforms, and key digital infrastructures [1]. While the digital transformation has led to record levels of innovation and productivity, it has also created a complex and dynamic threat landscape [2]. Cyber attacks increasingly happen, are more sophisticated and harder to detect, and encompass a diverse array of attacks targeting personal data, financial systems, and national infrastructure. The adversaries of today utilize advanced evasion methods, automated exploit tools, and even artificial intelligence which bypasses modern protections, making cybersecurity an issue of global priority [3].

For decades, security methodologies that have been proven effective—signature-based intrusion detection systems, rule-based firewalls [4], and heuristic malware scanners—have supported network protection. These techniques are typically signature-based or rely on historical attack methodologies, meaning they aren't effective against zero-day exploits, polymorphic malware threats, or adaptive adversaries that continually

change in response to conventional protections [5]. Additionally, the amount of data generated by modern networks is so great that it is almost impossible for human analysts or static systems to analyze and understand security events in real-time. This has created the demand for intelligent, automated, scalable solutions capable of discovering new threats and changing attack patterns on their own – without explicit programming or manual feature engineering [6].

Deep learning [7] has emerged as an attractive alternative to solving these problems. As a subset of machine learning, deep learning is able to automatically learn hierarchical representations from large, complex datasets. Traditional machine learning approaches require manual feature extraction. In contrast, deep neural networks can analyze raw data (for example, network traffic, executable files, log records or text) to identify hidden patterns, which would indicate malicious activity. Architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, Generative Adversarial Networks (GANs) and Graph Neural Networks (GNNs) have also been shown to be successful in intrusion detection, anomaly detection, malware classification, and phishing detection, among other tasks [8]. These architectures technically model non-linear relationships, as well as subtle deviations from normal behavioral patterns, making them particularly well-suited for discovering complicated, and previously unseen, attack vectors.

In addition to their power to predict emerging cybersecurity threats, deep learning models represent a new level of adaptability in the field. The continual training of models on new data allows them to change and adapt to newly discovered cybersecurity threats, letting organizations create a proactive, rather than reactive, defense strategy. Furthermore, the rapid advancement of modern computational power and the abundance of massive security datasets have allowed deep learning systems to be not just theoretical proposals but also a practical possibility in cyber-vulnerability environments. However, with all of the promise that deep learning models and systems hold, integrating deep models into a cybersecurity workflow presents new challenges. Issues including explainability, robustness to adversarial attacks, unavailability of data, and performance in real-time, must be dealt with to ensure that deep-learning systems can be trusted for critical security activities [9].

This review article explores the relationship between deep learning and cybersecurity, specifically examining how deep models can be used to aid in defending against deep and evolving cyber threats. It expands on the latest key developments in deep model techniques, applications across different security domains, datasets used, and evaluation methods. It will also examine the challenges that currently exist and highlight potential future research directions that could include hybrid models, privacy-preserving learning, and federated defense.

A. Objectives of the Review

The main purpose of the present review paper is:

- To investigate and analyze the usages of deep learning in identifying and resolving cyber-attacks and different types of (e.g.: malware, phishing, intrusion detection, anomaly detection)
- To analyze research on various deep learning architecture and methodologies in cyber security studies (e.g.: CNNs, LSTMs, RNNs, Autoencoders, GANs, GNNs)
- To discuss challenges and limitations to applying deep learning for mitigating cyber attacks, including issues such as scarcity of data, adversarial attacks, explainability, and real-time deployment requirements-
- To synthesize future research directions and trends, such as hybrid models, privacy-preserving approaches, and federated learning, to aid better cybersecurity defense.

In this way, the article provides a valuable resource for turn researchers, cyber security analysts, and cyber security professionals searching for practical deep learning approaches to detect and respond to cyber-attacks, thereby enhancing the cyber security and resilience of digital systems and networks.

Cyber Security and Treats

Cybersecurity [10] is defined as the techniques, processes, and technology used to protect computers, networks, applications, and information from unauthorized access, destruction, or disruption. In today's increasingly connected world, digital systems can be found in almost every sector or industry; made a fundamental building block in finance, health, government, and critical infrastructure. As technology use and reliance expand, so too do the importance and value of cybersecurity since a breach of a digital system can be costly across multiple areas, including finance, operations, and reputation. Cybersecurity seeks to promote the confidentiality, integrity, and availability of information to foster trust in online systems [10].

The cyber-threat landscape is changing and fluid. Malware is one of the most prevalent, destructive types of cyber- attacks. Malware includes many types of viruses, worms, spyware, adware, ransomware, Trojans, and other types of malicious software which can spread - often from downloaded objects, e-mail attachments, and/or infected devices [11]. Phishing/social engineering attics are also common threats, as they rely on human psychology and deception to obtain sensitive information such as passwords, financial information, or personal credentials often using spoofed emails, convoluted links to bogus websites, and/or hacked messages as trusted messaging. Network intrusions are also a significant threat, and they involve unauthorized access to computer networks with the intent to monitor, steal, or disrupt data, using methods like SQL injection, man-in-the-middle attacks, and distributed denial-of-service (DDoS) attacks.

In addition to these conventional risks, advanced persistent threats (APTs) have emerged as highly sophisticated targeted attacks which go undetected for substantial amounts of time while slowly exfiltrating sensitive information [12]. Insider threats remain a major concern due to the possibility of employees or contractors misusing privileges either intentionally or unintentionally compromising it. In addition, zero-day exploits, which are attacks on vulnerabilities which have no patch and have not yet been discovered, are particularly dangerous because they can bypass completely traditional defenses [13].

With the rise and complexity of these attack vectors, traditional defenses such as signature-based anti-virus and static firewalls are insufficient [14]. A good contemporary cyber security strategy must employ intelligent, adaptive and automated techniques to detect new and advanced attack patterns in real-time. Deep learning has begun to be identified as a viable technique for countering these new types of threats. Deep learning can analyze vast amounts of data, pinpoint subtle anomalies, and provide proactive defensive mechanisms against life-threatening cyber threats.

Role of Deep Learning in Cybersecurity

Cyber threats [15] have evolved in sophistication, demonstrating the limitations of traditional security mechanisms that rely on static rules and signatures for detection. Traditional security techniques are less effective with respect to detecting zero-day attacks, polymorphic malware, and advanced persistent threats that change to evade defenses. Deep learning, which is a form of artificial intelligence, envisions a different paradigm in cybersecurity by allowing systems to automatically learn complex patterns from large amounts of multidimensional data without manual feature engineering. More formally, deep learning assists cybersecurity by adapting to new threats while providing some automated or semi-automated defenses against cyber threats [16].

There are multiple aspects of cybersecurity where deep learning provides vital functionality. For example, both Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks [17] are models applied within intrusion detection systems, where the model analyzes incoming network traffic and classifies the traffic as benign versus malicious by calculating the likelihood based on anomalous behavior. Malware detection benefits from CNNs and Autoencoders to classify the status of files as malicious by extracting complex features from binaries or even representing binaries in an image-like analysis context. Phishing detection and spam filtering are just two other examples where natural language processing (NLP) [18] and the

use of deep learning models analyze text, URLs, or email structure to classify a message into a category for malicious correspondence.

A further important application of deep learning in cybersecurity is anomaly detection. Autoencoders and Generative Adversarial Networks (GANs) [19] are able to model typical behavior of a system and identify significant deviations from that predicted behavior which may indicate malicious behavior even if there are no historical examples. Graph Neural Networks (GNNs) [20] are increasingly being applied in detection, especially situational ones that leverage complex relationships between multiple devices, specializing in detecting coordinated attacks or malware moving across devices. Beyond detection, deep learning can also assist with defensive mechanisms by way of predictive analytics, automating threat intelligence, and response strategies based on adaptive mechanisms.

In general, deep learning improves the utility of cybersecurity systems in terms of scalability, adaptability, and accuracy. The ability of machine learning of processing very large amounts of data, accurately learn hierarchy of features, and generalizable for unobserved threats in a valuable rationale for why deep learning will become a tool of choice in increasingly sophisticated cyber-attacks. As threat actors continue to evolve, deep learning will be the key to means of achieving the cyber resilience, intelligence, and real-time mitigation required for specifically responding to complex threats.

METHODOLOGY

The aim of this review paper is to give a structured survey of the recent work in the field of deep learning methods of detection and defence against cyberattack across networks, systems, and digital platforms. To achieve this objective, we conducted a systematic literature review, to permit the inclusion of high quality, suitable, and recent literature contributions. The methodology involved a structured search, definition of inclusion or exclusion criteria, and a phased selection process to find the most significant studies in the field while ensuring coverage of previous academic research. Given the methodology this article ensured that a thorough study of contemporary methods, issues, and updates in the application of deep learning in the cybersecurity field could occur.

A. Databases/Resources

The literature review involved content gathered from significant, and credible academic databases and resources, which are known to contain high quality publications related to artificial intelligence, deep learning, and cyber defence in cybersecurity. These included, but were not limited to, IEEE Xplore, SpringerLink, Elsevier (ScienceDirect), Wiley Online Library, ACM Digital Library, and Google Scholar. We also reviewed major AI and cybersecurity conference proceedings, such as NeurIPS, ICML, AAAI, and IEEE Symposium on Security and Privacy to include the latest advancements and trends in the usage of deep learning method for cyber defence.

B. Inclusion Criteria

The studies reviewed were included based on the following criteria for inclusion: the focus of study was the detection or mitigation of cyber attacks, with deep learning techniques used in the study such as CNNs, RNNs, LSTMs, Autoencoders, GANs, or Graph Neural Networks (GNNs). Studies that examined data of network traffic, or system logs, or malware binaries, or intrusion patterns, or anomalous behaviour were included. Only studies published from 2018 were included, with the exception of a limited number of earlier seminal papers that were cited to provide additional historical context. None of the studies that used only traditional machine learning (non-deep learning) technologies, or that were not related to cybersecurity were included.

C. Keywords Used

A keyword-based search strategy was used with Boolean operators (AND, OR) to locate relevant studies. Previous studies were located with keywords including, but possibly not limited to, "deep learning for cyber attack detection", "intrusion detection systems using CNN/RNN/LSTM", "malware classification using deep learning", "anomaly detection (Autoencoders or GANs)", "Graph Neural Networks for cybersecurity", etc. These strategies helped to ensure all currently and potentially pioneering applications of deep learning in cyber defence were covered.

D. Stepwise Selection Process

In the first phase of our search, 50 articles from the chosen databases and conference proceedings were identified during scoping searches. Title and abstract evaluations were conducted, followed by the application of inclusion/exclusion criteria, narrowing Article Count to 30 articles that reported on the relevant topic of deep learning in cybersecurity disciplines. After conducting a full-text review, 15 excellent-quality studies have made it into the current paper. The studies represented a state-of-the-art methodology, applying CNNs, RNNs, LSTMs, Autoencoders, GANs, and GNNs for cyber attack detection, malware classification, intrusion detection, and anomaly detection.

E. State-of-the-Art and Emerging Trends Focus

The body of literature selected reflects the state-of-the-art in deep learning for cybersecurity and noted the emerging research themes, including explainable AI (XAI) for interpretable and trustworthy security, federated learning for collaborative model training with privacy preservation, multi-modality fusion of network, system, and behavioral data, and cross-platform detection with level of generalizability across different networking environments. Through our use of systematic review methodology, this paper provides a broad understanding of methods, challenges, and future opportunities to improve the role of deep learning models in mitigating cyber threats.

Table 1: Selection Process of Literature Review

Stage	Number of Papers	Description
Initial Collection	50	Articles retrieved using targeted keywords and citation tracking from major academic databases and conference proceedings.
Shortlisting	30	Screened for relevance, focus on deep learning techniques, and alignment with cyber attack detection and mitigation topics.
Final Review	15	In-depth review of the most influential studies employing CNN, RNN, LSTM, Autoencoders, GANs, and GNN architectures for cybersecurity applications.

.

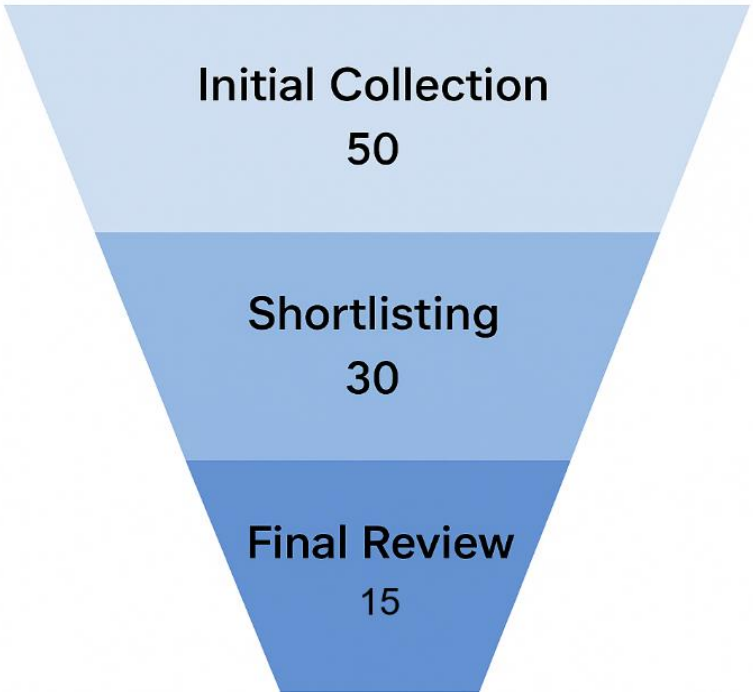

Figure 1. Funnel Diagram for Literature Review

LITERATURE REVIEW

Olanrewaju-George and Pranggono (2025) [21] had released a new IoT Intrusion Detection System (IDS) a few weeks ago, which used Federated Learning (FL) with directed and undirected deep learning terminology. The experiment was centered on the N-BaIoT dataset across 9 devices, and Olanrewaju-George and Pranggono demonstrated that a federated AutoEncoder (AE) model outperformed all other models, demonstrating the benefits of distributed learning and security and privacy-oriented learning to address problems in ICS and physical systems.

Markkandeyan et al. (2025) [22] investigated the issue of malware and software piracy within an IoT environment, and developed a hybrid deep learning framework with Adaptive TensorFlow networks, Improved Particle Swarm Optimization (IPSO), Enhanced LSTM (E-LSTM) and suspicious behavior observation. Across the GCJ dataset and Maling dataset, the study found that it outperformed contemporary models.

In the last study Imtiaz et al. (2025) [23] presented an explainable IDS named XIoT that used CNN models from spectrogram of traffic seen in the network to enable explainable decision. They found consistent and high accuracy performance (99.21-99.61%) on KDD CUP99, UNSW-NB15, and Bot-IoT dataset , and strong performances against a number of well aimed attack possibilities.

Hossain et al. (2025) [24] proposed a privacy-preserving IDS for 5G-V2X vehicular networks by utilizing Self-Supervised Learning (SSL). In this method, network traffic was pre-trained on unlabeled data and subsequently fine-tuned using few labeled data to improve accuracy from 3% to up to 9%, presenting a privacy-preserving method for intelligent vehicular communication.

In their research on the detection of anomalies, Dash et al. (2025) [25] developed SSA-LSTMIDS, as a model based on Long Short-Term Memory (LSTM) neural networks. The authors performed tuning using Particle Swarm Optimization (PSO), JAYA, and Salp Swarm Algorithm (SSA) and claimed that they produced a model that was accurate and precise while also obtaining a notable recall and F-score on the NSL-KDD, CICIDS, and Bot-IoT datasets with minimizing false positives as the main aggregation.

Guo (2025) [26] researched IoT access control with Blockchain using smart contracts and representing both Transition Systems (TS) and Computation Tree Logic (CTL), guaranteeing decentralized access management with secure, scalable, and fault tolerant strategies.

Sriram et al. (2025) [27] designed a decentralized event management system using Blockchain on Sui. This system included NFT tickets for events with a ZkLogin option for privacy, and the system incorporated low-cost utilities while improving the each events' transparency and eliminating single points of failure.

Viji et al. (2025) [28] researched blockchain in libraries and library services. Utilizing blockchain with digital skills in libraries allows for tamper-proof provenance records, digital rights management, and facilitating interlibrary loans while providing operational and security benefits where archival preservation was concerned.

Abdellatif et al. (2025) [29] provided a decentralized-learning scheme for smart grids based on the concepts of multicloud and blockchain, developed a decentralized-learning scheme for smart grids with centralized learning, federated learning, and active federated learning combined with trust-based strategies to choose participants. Their experimental evaluation shows great performance and scalability.

Mohajan and Jahan (2025) [30] developed a Dynamic Access Control Scheme (DACS) on blockchain with concepts from Zero Trust. With trust-related metrics and smart contracts, they demonstrated that the prototype built on Ethereum was capable of protecting a distributed system using continuous and dynamic risk-based monitoring.

Arif et al. (2024) [31] focused on AI-enabled threat detection in the cloud and shifting the paradigm from rule-based models to AI models and address concerns like bias in the inputs of the algorithms, privacy and the human-AI collaboration to secure everything that is under an adaptive security model.

Ofoegbu et al. (2024) [32] facilitated a real-time cyber threat detection solution by leveraging big data analytics and machine learning in real-time that increased anticipatory security and incidents response speed in the enterprise space.

Olabanji et al. (2024) [33] examined artificial intelligence based user behavior in the use of cloud computing, finding that hybrid levels of AI prediction working with traditional tools were the most balanced and effective user security.

Labu and Ahammed (2024) [34] showcased AI techniques using Random Forest for fraud detection were the best of the techniques they explored (83.94%) when it came to finding subtle high-risk financial transactions than Naïve Bayes and KNN.

Ismail et al. (2024) [35] proposed a blockchain-ML hybrid system for IoT sensor networks, using identity authentication to lightweight and lightGBM malicious node detection. Ultimately, when compared to traditional ML or AI modeling, the hybrid blockchain-ML showed greater accuracy and effectiveness in decision-making.

Table 2. Literature Review Findings

Author Name (Year)	**Main Concept**	**Findings**	**Limitations**
Olanrewaju-George & Pranggono (2025) [21]	Federated Learning for IoT IDS using supervised and unsupervised deep learning	Federated AutoEncoder model achieved best detection performance on N-BaIoT dataset, emphasizing privacy-preserving distributed IDS	Focused on a single dataset; scalability to diverse IoT environments not fully explored
Markkandeyan et al. (2025) [22]	Hybrid deep learning with IPSO and Adaptive TensorFlow for IoT	Outperformed traditional methods on GCJ and Maling datasets using E-LSTM and	Computational complexity and real-time deployment considerations not detailed

	malware detection	behavior detection modules	
Imtiaz et al. (2025) [23]	Explainable IDS (XIoT) using CNN on network spectrograms	Achieved 99.21–99.61% accuracy on KDD CUP99, UNSW-NB15, and Bot-IoT; improved transparency via explainable AI	Limited discussion on adaptability to evolving attack patterns
Hossain et al. (2025) [24]	Self-Supervised Learning for 5G-V2X privacy-preserving IDS	Pre-training on unlabeled data improved accuracy by 9% while maintaining privacy	Focused only on vehicular networks; generalizability to broader IoT contexts not tested
Dash et al. (2025) [25]	SSA-LSTMIDS: LSTM optimized with PSO, JAYA & SSA for anomaly detection	High detection accuracy and reduced false positives on NSL-KDD, CICIDS, Bot-IoT	Optimization overhead and adaptability to streaming data not addressed
Guo (2025) [26]	Blockchain-based decentralized IoT access control using TS and CTL	Formalized smart contract behavior ensuring secure, scalable, fault-tolerant access	Real-world deployment and performance evaluation not covered
Sriram et al. (2025) [27]	Blockchain-based decentralized event management on Sui	NFT ticketing, zkLogin, and low-cost tools improved transparency and reduced failure points	Application limited to event management; scalability to other domains untested
Viji et al. (2025) [28]	Blockchain in libraries for provenance and rights management	Enabled tamper-proof provenance, decentralized resource sharing, improved archival security	Lacked quantitative evaluation of system performance
Abdellatif et al. (2025) [29]	Blockchain-based decentralized learning for smart grids with multicloud support	Supported centralized, federated, and active federated learning with trust-based selection; improved scalability	Implementation complexity and interoperability challenges remain
Mohajan & Jahan (2025) [30]	Blockchain + Zero Trust for dynamic access control (DACS)	Ethereum prototype showed effective protection with trust metrics and continuous monitoring	Real-time performance under large-scale conditions not evaluated
Arif et al. (2024) [31]	Survey of AI-based threat detection in cloud	Identified shift from rule-based to AI, highlighted issues of bias, privacy, and human-AI collaboration	Lacked empirical validation; conceptual in nature
Ofoegbu et al. (2024) [32]	Big data analytics + ML for real-time threat detection	Demonstrated improved anticipatory security and rapid response in enterprises	Industry case studies may not generalize to all domains
Olabanji et al. (2024) [33]	AI-based user behavior analysis in cloud	Hybrid AI–traditional models offered balanced and effective security	No detailed evaluation of computational costs or latency
Labu & Ahammed (2024) [34]	Fraud detection using AI methods	Random Forest achieved 83.94% accuracy, outperforming Naïve Bayes and KNN in identifying subtle financial fraud	Focused on accuracy; lacked real-time deployment insights
Ismail et al. (2024) [35]	Blockchain–ML hybrid for IoT sensor networks	Integrated lightweight authentication with lightGBM	Applicability to large-scale, heterogeneous IoT

		detection, showing higher accuracy and efficiency	networks not fully explored

Research gaps Discussion

The literature reviewed highlights notable progress in leveraging deep learning, federated learning, self-supervised learning, blockchain, and hybrid AI for applications including intrusion detection, access control, fraud detection, and threat analysis in IoT and cloud environments. Nevertheless, multiple avenues for further research exist. Several proposed models prove effective with respect to performance results on a specific benchmark dataset, but do not garner further validation in heterogeneous environments, at scale, or in operational contexts, all of which contribute to challenges for practical deployment. Federated and self-supervised models may provide some relief of concerns over privacy, however, scalability, communication overhead, and monitoring and interacting with evolving attacks is still a gap in the research. Blockchain-based solutions present useful attributes—decentralization and trust—but do not address interoperability, implementation complexity, or resource constrained runtime performance in rapidly evolving situations. Explainable AI methods can enhance security and human-in-the-loop decision making, but are not currently integrated with security models, nor are they fully represented in the current literature. Finally, the majority of efforts focused on increases in accuracy and did not research energy efficiency or latency, both of which are significant issues for IoT and edge systems. These existing gaps present a case for research and development of a comprehensive, adaptive, explainable security frameworks to work in a variety of operational, real-world, distributed environments.

CONCLUSION

. In this review, we have provided a broad examination of deep learning in cybersecurity covering several distinct areas, including, e.g., intrusion detection, malware classification, phishing detection, anomaly detection, and threat prediction. We made explicit reference to the most recent literature so as to illustrate how models such as CNNs, RNNs, LSTMs, Autoencoders, GANs, and GNNs can be advantageous for uncovering and alerting to sophisticated attack patterns/behaviors, whilst providing a relatively high degree of confidence for unknown threats. . While these approaches have shown significant improvement in detection performance and responsiveness to live threats, we have also identified critical areas for further development, including interpretability, adversarial robustness, data quality, profiling, and cross-domain adaptation. Future studies should prioritize the development of explainable AI systems, federated learning and privacy-preserving learning, a multimodal approach to learning, and transfer learning as we attempt to create transparent, scalable, and resilient cybersecurity systems. In summary, the implementation of deep learning methods for studying security systems can ultimately lead to a more proactive and intelligent approach to cyber defense.

REFERENCES

1. Li, P., Xu, C., Xu, H., Dong, L., & Wang, R. (2019). Research on data privacy protection algorithm with homomorphism mechanism based on redundant slice technology in wireless sensor networks. China Communications, 16(5), 158–170.
2. Al Rasyid, M. U. H., Prasetyo, D., Nadhori, I. U., & Alasiry, A. H. (2015). Mobile monitoring of muscular strain sensor based on Wireless Body Area Network. In 2015 International Electronics Symposium (IES) (pp. 284–287). IEEE.
3. Nelson, J., et al. (2021). Wireless Sensor Network with Mesh Topology for Carbon Dioxide Monitoring in a Winery. In 2021 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNeT) (pp. 30–33). IEEE.
4. Wang, H., Yang, G., Xu, J., Chen, Z., Chen, L., & Yang, Z. (2011). A novel data collection approach for Wireless Sensor Networks. In 2011 International Conference on Electrical and Control Engineering (pp. 4287–4290). IEEE.

5. Arumugasamy, S. (2024). An intrusion detection approach in wireless sensor network security through CNN-BiLSTM model. Journal of Theoretical and Applied Information Technology, 102(2).
6. Hu, R. (2016). Key Technology for Big Visual Data Analysis in Security Space and Its Applications. In 2016 International Conference on Advanced Cloud and Big Data (CBD) (p. 333). IEEE.
7. Wang, X., Herwono, I., Cerbo, F. D., Kearney, P., & Shackleton, M. (2018). Enabling cyber security data sharing for large-scale enterprises using managed security services. In 2018 IEEE Conference on Communications and Network Security (CNS) (pp. 1–7). IEEE.
8. Diaba, S. Y., Shafie-Khah, M., & Elmusrati, M. (2023). Cyber security in power systems using meta-heuristic and deep learning algorithms. IEEe Access, 11, 18660-18672.
9. Bhuvaneshwari, A. J., & Kaythry, P. (2023). A review of deep learning strategies for enhancing cybersecurity in networks: deep learning strategies for enhancing cybersecurity. Journal of Scientific & Industrial Research (JSIR), 82(12), 1316-1330.
10. Torre, D., Mesadieu, F., & Chennamaneni, A. (2023). Deep learning techniques to detect cybersecurity attacks: a systematic mapping study. Empirical Software Engineering, 28(3), 76.
11. Hussen, N., Elghamrawy, S. M., Salem, M., & El-Desouky, A. I. (2023). A fully streaming big data framework for cyber security based on optimized deep learning algorithm. IEEE Access, 11, 65675-65688.
12. Udayakumar, R., Joshi, A., Boomiga, S. S., & Sugumar, R. (2023). Deep fraud Net: A deep learning approach for cyber security and financial fraud detection and classification. Journal of Internet Services and Information Security, 13(3), 138-157.
13. Kanagala, P. (2023). Effective cyber security system to secure optical data based on deep learning approach for healthcare application. Optik, 272, 170315.
14. Dey, S., Sarma, W., & Tiwari, S. (2023). Deep learning applications for real-time cybersecurity threat analysis in distributed cloud systems. World Journal of Advanced Research and Reviews, 17(3), 1044-1058.
15. Szynkiewicz, W., Niewiadomska-Szynkiewicz, E., & Lis, K. (2023). Deep learning of sensor data in cybersecurity of robotic systems: overview and case study results. Electronics, 12(19), 4146.
16. Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. SN Computer Science, 2(3), 154.
17. Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep learning based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA Journal of Automatica Sinica, 9(3), 377-391.
18. Jahwar, A. F., & Ameen, S. Y. (2021). A review on cybersecurity based on machine learning and deep learning algorithms. Journal of Soft Computing and Data Mining, 2(2), 14-25.
19. Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 34(8), 3779-3795.
20. Li, G., Sharma, P., Pan, L., Rajasegarar, S., Karmakar, C., & Patterson, N. (2021). Deep learning algorithms for cyber security applications: A survey. Journal of Computer Security, 29(5), 447-471.
21. Olanrewaju-George, B., & Pranggono, B. (2025). Federated learning-based intrusion detection system for the Internet of Things using unsupervised and supervised deep learning models. Cyber Security and Applications, 3, 100068.
22. Markkandeyan, S., Ananth, A. D., Rajakumaran, M., Gokila, R. G., Venkatesan, R., & Lakshmi, B. (2025). Novel hybrid deep learning-based cyber security threat detection model with optimization algorithm. Cyber Security and Applications, 3, 100075.
23. Imtiaz, N., et al. (2025). A deep learning-based approach for the detection of various Internet of Things intrusion attacks through optical networks. Photonics, 12(35), 1–39.
24. Hossain, S., Senouci, S. M., Brik, B., & Boualouache, A. (2025). A privacy-preserving self-supervised learning-based intrusion detection system for 5G-V2X networks. Ad Hoc Networks, 166, 103674.
25. Dash, N., Chakravarty, S., Rath, A. K., Giri, N. C., AboRas, K. M., & Gowtham, N. (2025). An optimized LSTM-based deep learning model for anomaly network intrusion detection. Scientific Reports, 15(1), 1554.
26. Guo, Z. (2025). Blockchain-enhanced smart contracts for formal verification of IoT access control mechanisms. Alexandria Engineering Journal, 118, 315–324.

27. Sriram, S., Tharaniesh, P. R., Saraf, P., Vijayaraj, N., & Murugan, T. (2025). Enhancing digital identity and access control in event management systems using Sui blockchain. IEEE Access.
28. Viji, C., Jagannathan, J., Rajkumar, N., Mohanraj, A., Nachiappan, B., & Kovilpillai, J. A. J. (2025). Leveraging blockchain technology to enhance library security. In Enhancing Security and Regulations in Libraries with Blockchain Technology (pp. 181–200). IGI Global.
29. Abdellatif, A. A., Shaban, K., & Massoud, A. (2025). Blockchain-enabled distributed learning for enhanced smart grid security and efficiency. Computers and Electrical Engineering, 123, 110012.
30. Mohajan, A., & Jahan, S. (2025). Embedding security awareness into a blockchain-based dynamic access control framework for the zero trust model in distributed systems.
31. Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future horizons: AI-enhanced threat detection in cloud environments—Unveiling opportunities for research. International Journal of Multidisciplinary Sciences and Arts, 3(1), 242–251.
32. Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Real-time cybersecurity threat detection using machine learning and big data analytics:
33. Olabanji, S. O., Marquis, Y., Adigwe, C. S., Ajayi, S. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-driven cloud security: Examining the impact of user behavior analysis on threat detection. Asian Journal of Research in Computer Science, 17(3), 57–74.
34. Labu, M. R., & Ahammed, M. F. (2024). Next-generation cyber threat detection and mitigation strategies: A focus on artificial intelligence and machine learning. Journal of Computer Science and Technology Studies, 6(1), 179–188.
35. Ismail, S., Nouman, M., Dawoud, D. W., & Reza, H. (2024). Towards a lightweight security framework using blockchain and machine learning. Blockchain: Research and Applications, 5(1), 100174.