Deep Learning-Based Intrusion Detection Systems For Network Security in IoT System

Neibo Augustine Olobo [1], Waliu Adebayo Ayuba [2], Ayogoke Felix Omojola [3], Izevbigie Hope Iyobosa [4], Aderemi Ibraheem Adebayo [5], Abiamamela Obi-Obuoha [6], Unuigbokhai Peter Afegbai [7]

[1] *Joseph Sarwuan Tarka University Makurdi*
P. M. B. 2373, Makurdi, Benue State, Nigeria

[2] *Northeastern University*
360 Huntington Ave, Boston, MA 02115, US

[3] *D. Serikbayev East Kazakhstan Technical University*
19 D. Serikbayev street, Ust-Kamenogorsk, 070004, Kazakhstan

[4] *Ulster University*
Louisa Ryland House, 44 Newhall Street, Birmingham, B3 3PL, UK

[5] *University of Ilorin*
P. M. B. 1515, Ilorin, Kwara State, Nigeria

[6] *National Center for Artificial Intelligence and Robotics*
Plot 790, Alimoh-Abu Street, Behind VIO Yard, Wuye District, Abuja, Nigeria

[7] *Auchi Polytechnic*
Along Benin-Okene Road, P. M. B. 13, Auchi, Edo State, Nigeria

DOI: 10.22178/pos.112-12

LCC Subject Category: L7-991

Received 25.11.2024
Accepted 28.12.2024
Published online 31.12.2024

Corresponding Author:
Neibo Augustine Olobo
neibo.augustine@gmail.com

Abstract. The Internet of Things (IoT) has revolutionised various sectors, including healthcare, education, agriculture, and military applications, by enabling seamless communication and data collection among interconnected devices. However, IoT networks' open and decentralised nature exposes them to many security threats and vulnerabilities. Intrusion Detection Systems (IDS) have been developed to address these challenges by identifying and mitigating malicious activities targeting these networks. Despite their importance, many organisations struggle to detect and prevent novel and sophisticated attacks effectively. This paper presents a comprehensive survey of the security issues inherent in IoT environments, emphasising the role of deep learning and machine learning techniques in enhancing IDS capabilities. By analysing existing vulnerabilities and evaluating various methodologies, we highlight the critical need for robust security measures that ensure IoT systems' reliability, privacy, and integrity. Through our findings, we advocate for integrating advanced analytical techniques in IDS to bolster defences against evolving threats in the IoT landscape.

Keywords: Intrusion Detection System; network security; deep learning; machine learning; vulnerabilities; malicious attacks; data privacy; security measures.

INTRODUCTION

The Internet of Things (IoT) refers to the interconnected network of devices that can communicate and exchange data over the Internet without direct human intervention. These devices, from household appliances to industrial sensors, collect and analyse data, facilitating automation and improving efficiency across various sectors such as

healthcare, agriculture, education, and the military [1]. The rapid proliferation of IoT devices has led to significant technological advancements and transformed how data is utilised in decision-making processes. Despite the numerous benefits associated with IoT, its inherent vulnerabilities pose substantial security risks. IoT systems' open architecture often exposes them to diverse threats, including unauthorised access, data breaches, and denial-of-service attacks [2]. The increasing number of devices connected to the Internet enhances the attack surface, making it challenging for traditional security mechanisms to safeguard these networks effectively. Therefore, there is an urgent need for robust security frameworks that can protect against malicious activities in IoT environments [3]. Intrusion Detection Systems (IDS) play a crucial role in network security by monitoring traffic and identifying suspicious activities. Traditional IDS methods often rely on predefined signatures of known threats, which limits their effectiveness against novel or unknown attacks [4]. As attackers continuously evolve their techniques, there is a growing interest in leveraging advanced analytical methods, intense learning and machine learning to enhance IDS capabilities. These techniques can analyse vast amounts of data and identify complex patterns indicative of potential intrusions [5].

Deep learning, a subset of machine learning, employs neural networks with multiple layers to learn data representations. This ability to extract intricate features from large datasets makes deep learning suitable for detecting anomalies in IoT networks [6]. On the other hand, machine learning algorithms can adapt to new threats by learning from historical data, improving their detection accuracy over time [7]. Integrating these methodologies into IDS can significantly enhance their effectiveness in identifying and mitigating threats in dynamic IoT environments. Moreover, ensuring data privacy is paramount in IoT systems, where sensitive information is often collected and transmitted. Security measures must not only focus on detecting intrusions but also on safeguarding the privacy and integrity of data [8]. Organisations can better protect their IoT infrastructure from potential threats by adopting a holistic approach combining advanced detection techniques and strong privacy protocols. As IoT continues to expand, addressing its security challenges becomes increasingly critical. The development of sophisticated IDS utilising deep learning and machine learning techniques presents a promising solution to enhance the security of IoT networks. This paper will explore the vulnerabilities of IoT environments, evaluate existing IDS methodologies, and advocate for integrating advanced analytics to bolster network security.

Literature Survey

The security of Internet of Things (IoT) networks has become a critical concern as the number of connected devices continues to proliferate. These devices, ranging from smart home appliances to industrial sensors, are often vulnerable to cyber threats. This literature survey examines the existing research on Intrusion Detection Systems (IDS) that leverage machine learning and deep learning techniques to enhance IoT security. Intrusion Detection Systems are essential for identifying unauthorised access and malicious activities within IoT environments. Traditional IDS primarily rely on signature-based methods, which can effectively detect known threats but struggle with new or evolving attacks [4]. This limitation has prompted researchers to explore more adaptive approaches, particularly those based on anomaly detection, which can identify unusual patterns in network traffic. Anomaly-based detection has become a more effective method for identifying previously unknown threats. Authors [9] proposed an anomaly detection framework that utilises machine learning algorithms to analyse network traffic. Their study demonstrated that unsupervised learning techniques, such as clustering, can identify deviations from normal behaviour, thus enhancing the detection of attacks in real-time. Deep learning has emerged as a powerful tool for improving the performance of IDS. For instance, authors [10] implemented a Convolutional Neural Network (CNN) to process network traffic data and detect intrusions. Their model achieved a higher detection rate than traditional methods, showcasing deep learning's ability to capture complex patterns in large datasets. Similarly, authors [5] highlighted the effectiveness of Recurrent Neural Networks (RNNs) in identifying temporal dependencies in network data, which is crucial for detecting sophisticated cyber threats.

Machine learning algorithms such as Support Vector Machines (SVM), Decision Trees, and Random Forests have been extensively studied in the context of intrusion detection. Authors [7] reviewed various machine learning techniques, noting that ensemble methods, which combine multiple classifiers, often yield improved accuracy and reduce

false favourable rates. These methods can adapt to changing attack patterns, making them well-suited for the dynamic nature of IoT networks. Hybrid approaches that integrate multiple detection methodologies are increasingly being explored. Authors [11] developed a hybrid IDS combining deep feature extraction and machine classification learning. Their model demonstrated improved detection accuracy and efficiency, suggesting that leveraging the strengths of both deep learning and traditional algorithms can provide more robust security solutions. Despite advancements in IDS technology, several challenges remain in securing IoT environments. One major issue is the lack of labelled datasets for training machine learning models, which can hinder the effectiveness of detection systems [12]. Moreover, IoT devices' diverse and dynamic nature requires continuous adaptation of detection models to address emerging threats. Authors [13] emphasised the need for self-learning IDS to update their detection mechanisms based on real-time data automatically. As IoT networks handle sensitive data, privacy concerns are paramount. Authors [8] highlighted that security measures should also ensure user privacy, advocating for privacy-preserving techniques in IDS. Approaches such as data anonymisation and encryption can help mitigate risks while maintaining effective intrusion detection capabilities. IDS in IoT security lies in developing adaptive, intelligent systems that respond to evolving threats in real time; this includes further exploration of self-learning algorithms, the integration of federated learning for privacy preservation, and the application of explainable AI to improve transparency in detection processes [14]. The literature indicates a significant shift toward employing machine learning and deep learning techniques in IDS to bolster IoT security. While considerable progress has been made, ongoing research is essential to address existing challenges, such as data scarcity and the dynamic nature of IoT environments. Future efforts should focus on developing adaptive, privacy-conscious IDS that can effectively counteract the evolving landscape of cyber threats.

Intrusion Prevention System (IPS) Techniques

Intrusion Prevention Systems (IPS) are critical components in network security, designed to detect and respond to potential threats in real-time. While Intrusion Detection Systems (IDS) primarily monitor and alert on suspicious activity, IPS actively takes steps to prevent attacks from succeeding. Below are several key techniques used in IPS:

Signature-Based Detection. Signature-based detection is one of the most common IPS techniques. It involves identifying known threats by comparing network traffic against a database of known attack signatures. This method is effective for detecting well-documented threats but may struggle with new or polymorphic attacks that do not match existing signatures.

Anomaly-Based Detection. Anomaly-based detection focuses on identifying unusual patterns or behaviours in network traffic. By establishing a baseline of regular network activity, the IPS can flag deviations that may indicate a potential attack. This technique is beneficial for detecting zero-day attacks and other unknown threats. Machine learning algorithms often refine the anomaly detection process and improve accuracy.

Stateful Protocol Analysis. Stateful protocol analysis examines the state of network connections and protocols. It verifies that all communication follows expected patterns and protocol specifications. This technique helps identify attacks that exploit vulnerabilities in protocol implementations or establish malicious connections.

Traffic Filtering. IPS can filter traffic to block malicious packets based on predefined rules or policies; this includes blocking traffic from known malicious IP addresses, specific ports, or protocols. By actively filtering out harmful traffic, the IPS can prevent attacks before reaching their target.

Rate Limiting. Rate limiting involves restricting the number of requests a user or device can make to a server within a specified time frame. This technique helps mitigate denial-of-service (DoS) attacks by limiting the impact of excessive traffic from a single source. By controlling traffic flow, IPS can protect critical resources from being overwhelmed.

Protocol Anomaly Detection. Protocol anomaly detection focuses on identifying deviations from standard protocol behaviour. This technique analyses the structure and sequence of communication packets to detect anomalies that could indicate an attack. For example, if a client attempts to use an invalid sequence of HTTP requests, the IPS can flag this behaviour as suspicious.

Behavioural Analysis. Behavioural analysis involves monitoring the actions of users and devices

within a network. By establishing profiles for expected behaviour, the IPS can detect irregularities that may indicate insider threats or compromised accounts. This technique often employs machine learning to adapt to changing behaviour patterns over time.

Integrated Threat Intelligence. Many modern IPS solutions leverage threat intelligence feeds that provide information about emerging threats, vulnerabilities, and attack patterns. IPS can enhance its detection capabilities by integrating real-time threat intelligence and proactively defending against known threats.

Sandboxing. Sandboxing is a technique where suspicious files or applications are executed in a controlled environment to observe their behaviour without risking the leading network. If malicious activity is detected within the sandbox, the IPS can block the application before it can cause harm.
Response Actions. Once a potential threat is detected, the IPS can take various response actions, including: a) Blocking the offending IP address; b) Terminating suspicious sessions; c) Alerting administrators; d) Redirecting traffic for further analysis.

Intrusion Prevention Systems are crucial in safeguarding networks by detecting and preventing threats. By utilising a combination of signature-based, anomaly-based, and behavioural analysis techniques, along with integrated threat intelligence and practical response actions, IPS can provide comprehensive protection against a wide array of cyber threats. As the threat landscape evolves, ongoing advancements in IPS technologies will be essential for maintaining robust network security.

RESULTS AND DISCUSSION

Intrusion Detection System (IDS) Techniques

Intrusion Detection Systems (IDS) are essential for identifying and responding to suspicious network activities. Security systems categorise them based on their detection methods, architecture, and the type of environment they are designed to protect. Below are key techniques used in IDS:

Signature-Based Detection. Signature-based detection involves monitoring network traffic and comparing it against a database of known attack signatures. This method effectively identifies established threats but may not detect new or unknown attacks without defined signatures.

Advantages*:* High accuracy for known threats; low false favourable rates,

Disadvantages: Ineffective against zero-day attacks and evolving threats.

Anomaly-Based Detection. Anomaly-based detection identifies deviations from established baselines of normal behaviour. This method can detect unknown threats by analysing network traffic patterns and user behaviours.

Advantages: Capable of detecting new and unknown attacks; adaptive to changes in network behaviour.

Disadvantages*:* Higher false favourable rates; requires continuous baseline updates.

Stateful Protocol Analysis. This technique examines the state of network connections and ensures that all communications comply with established protocol standards. Analysing the context of the traffic can detect anomalies related to protocol behaviour.

Advantages*:* Effective in detecting attacks that exploit protocol vulnerabilities.

Disadvantages*:* Complexity in implementation; potential for missed detections if protocols are not well-defined

Behavioural Analysis. Behavioural analysis monitors user and device activities to establish patterns of normal behaviour. It can detect irregularities that may indicate compromised accounts or insider threats.

Advantages*:* Useful for identifying insider threats; adaptable to user behaviour changes.

Disadvantages*:* It may require extensive data collection and analysis, which can be resource-intensive.

Traffic Analysis. Traffic analysis involves monitoring and analysing data flows to identify unusual patterns, such as unexpected spikes in traffic or unusual port usage. This method can help detect potential DoS attacks or data exfiltration.

Advantages*:* Can identify attacks based on traffic patterns without inspecting packet contents.

Disadvantages*:* Limited visibility into encrypted traffic; may miss sophisticated attacks.

Hybrid Detection Methods. Hybrid detection systems combine various techniques, such as signature-based and anomaly-based methods. This

approach aims to leverage the strengths of each method while mitigating their weaknesses.

Advantages*:* Increased accuracy and coverage for threat detection; adaptability to evolving threats,

Disadvantages*:* Increased complexity; potential for higher resource consumption

Machine Learning and AI Techniques. Machine learning and artificial intelligence are increasingly integrated into IDS to enhance detection capabilities. These systems can learn from historical data, identify patterns, and adapt to new threats.

Advantages*:* Capable of processing large datasets and identifying complex patterns; adaptive to changing environments.

Disadvantages*:* It requires large amounts of data for training, and there is potential for model bias.

Distributed IDS. Distributed IDS involve deploying multiple sensors across various locations within a network. These sensors collect and analyse data in real-time, allowing for centralised monitoring and analysis.

Advantages*:* Enhanced coverage and scalability; adequate in large and complex networks,

Disadvantages: Increased complexity in management and data correlation; potential latency issues

Host-Based Intrusion Detection Systems (HIDS). HIDS are deployed on individual devices or servers to monitor system-level activities. They analyse files, monitor file integrity, and examine system calls to detect suspicious behaviour.

Advantages*:* Provides detailed visibility into system activities; effective for detecting insider threats.

Disadvantages*:* Limited to the host's perspective; may be bypassed by sophisticated attacks.

Network-Based Intrusion Detection Systems (NIDS). NIDS monitor network traffic at various points within a network. They analyse packet flows and can detect anomalies or known attack signatures across the entire network.

Advantages*:* Broad visibility into network traffic; can identify attacks that span multiple hosts.

Disadvantages*:* Limited insight into encrypted traffic; may struggle with high traffic volumes.

Intrusion Detection Systems are vital for maintaining network security by identifying potential threats before they can cause harm. By employing various detection techniques, including signature-based, anomaly-based, and machine-learning approaches, organisations can enhance their ability to detect and respond to intrusions. Ongoing advancements in IDS technologies will continue to play a crucial role in addressing the evolving threat landscape.

Comparative Assessment of Various IPS and IDS Techniques

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are vital for maintaining network security. While both aim to identify malicious activities, they operate with different functionalities and techniques. This comparative assessment evaluates various IPS and IDS techniques based on key criteria such as detection methods, effectiveness, resource requirements, and adaptability.

1) Detection Methods

Technique	Description	Type	Effectiveness
Signature-Based Detection	Identifies known threats by matching signatures against traffic.	IDS / IPS	High for known threats; low for unknown attacks.
Anomaly-Based Detection	Detects deviations from normal behaviour to identify unknown threats	IDS / IPS	Effective for zero-day attacks; higher false favourable rates.
Stateful Protocol Analysis	Monitors the state of network connections to verify protocol compliance.	IDS / IPS	Effective for protocol-ba-sed attacks; complexity in implementation.
Behavioural Analysis	Monitors user and device behaviour to detect irregularities.	IDS	Effective for insider threats; requires extensive data
Machine Learning-Based Detection	It uses algorithms to learn from data and	IDS / IPS	Adaptable and scalable; data-intensi-ve for training.

Technique	Description	Type	Effectiveness
	identify patterns.		
Traffic Analysis	Analyses data flows for unusual patterns without inspecting packet contents.	IDS	Effective for identifying broad attacks; limited visibility into encrypted traffic.

2) Effectiveness and Accuracy

Signature-based techniques excel at detecting known threats with high accuracy but fail to address novel attacks. This technique generally has a low false positive rate.

Anomaly-based techniques can identify previously unknown threats by flagging unusual behaviour, although they often result in higher false favourable rates due to benign anomalies being misclassified as threats.

Machine Learning Approaches offer the advantage of evolving detection capabilities, improving over time with new data. However, they require substantial computational resources and high-quality datasets to be effective.

3) Resource Requirements

Technique	Resource Usage	Notes
Signature-Based Detection	Low to moderate	Requires regular updates of signatures
Anomaly-Based Detection	Moderate to high	Needs continuous monitoring and data analysis
Stateful Protocol Analysis	High	Resource-intensive due to detailed protocol inspection
Behavioural Analysis	High	Requires extensive historical data for accurate profiling
Machine Learning-Based Detection	Very high	Needs significant processing power for training and real-time analysis

4) Adaptability

Signature-based systems are less adaptable as they rely on predefined signatures. Regular updates are necessary to keep pace with emerging threats.

Anomaly-based and Machine Learning Techniques are more adaptable, as they learn from ongoing traffic patterns and can adjust to new attacks; this makes them suitable for dynamic environments.

Behavioural analysis also shows adaptability, particularly for detecting insider threats that may evolve.

5) Implementation Complexity

Technique	Resource Usage	Notes
Signature-Based Detection	Low to moderate	Straightforward deployment.
Technique	Resource Usage	Notes
Anomaly-Based Detection	Moderate to high	Requires extensive baseline data and continuous refinement.
Stateful Protocol Analysis	High	Complex due to protocol specifics and state tracking.
Behavioural Analysis	High	Involves detailed profiling and continuous learning.
Machine Learning-Based Detection	Very high	Complex model training and tuning are needed.

CONCLUSIONS

The choice between IPS and IDS techniques depends on organisational needs, resources, and the specific threat landscape. Signature-based methods provide reliable detection for known threats but are limited to new attacks. Anomaly-based and machine-learning techniques offer more adaptability and can identify unknown threats but often come with higher resource demands and complexity.

For organisations looking to implement adequate security measures, a hybrid approach that combines multiple techniques may provide the best balance of security, adaptability, and efficiency. By leveraging the strengths of different methods, organisations can create a more robust defence against evolving cyber threats.

As cybersecurity threats evolve, so must the methods employed to detect and prevent these attacks. The future of Intrusion Detection Systems

(IDS) and Intrusion Prevention Systems (IPS) will likely be shaped by advancements in technology, increased data availability, and the growing complexity of networks. Below are several key areas for future work and recommendations for enhancing IDS and IPS effectiveness.

1) Integration of Artificial Intelligence and Machine Learning

Recommendation: Invest in research to improve the application of AI and machine learning algorithms in IDS/IPS. These technologies can help systems learn from evolving patterns in network traffic and adapt to new threats.

Future Work: Develop more sophisticated models that reduce false positives and increase detection rates by leveraging deep learning techniques.

2) Real-Time Threat Intelligence Sharing

Recommendation: Foster collaboration among organisations to share threat intelligence in real-time; this can enhance the effectiveness of IPS/IDS by providing up-to-date information on emerging threats.

Future Work: Create standardised frameworks and protocols for sharing threat intelligence, enabling seamless integration across different platforms and organisations.

3) Privacy-Preserving Techniques

Recommendation: Incorporate privacy-preserving methods into IDS/IPS frameworks to protect sensitive data while maintaining detection capabilities.

Future Work: Explore federated learning and other decentralised models that allow for collaborative training of detection models without compromising user privacy.

4) Focus on IoT and Edge Security

Recommendation: As IoT devices proliferate, develop specialised IDS/IPS solutions tailored for IoT environments, addressing their unique vulnerabilities and constraints.

Future Work: Research lightweight detection mechanisms that can operate efficiently on resource-constrained devices without sacrificing security.

5) Improved User Behavior Analytics

Recommendation: Enhance behavioural analysis techniques to detect insider threats and anomalous user behaviour better; this could involve more granular monitoring of user actions.

Future Work: Implement advanced analytics that combines user behaviour with contextual information to improve anomaly detection accuracy.

6) Automated Response Mechanisms

Recommendation: Develop automated response capabilities that enable IPS to take immediate action upon detecting threats, minimising the response time and potential damage.

Future Work: Research the implications of automated responses on network operations and create robust frameworks that ensure accuracy and reliability.

7) Standardisation and Compliance

Recommendation: Advocate for industry standards and best practices for IDS/IPS deployment to ensure consistency and effectiveness across different environments.

Future Work: Work with regulatory bodies to align IDS/IPS solutions with compliance requirements while ensuring that security measures do not hinder operational efficiency.

8) Continuous Learning and Adaptation

Recommendation: Implement continuous learning mechanisms that allow IDS/IPS systems to evolve based on new data and threat landscapes.

Future Work: Explore self-learning models that can autonomously adapt their detection strategies based on real-time data analysis.

The future of IDS and IPS lies in embracing new technologies and methodologies that enhance their detection capabilities and adaptability. By focusing on AI integration, collaborative threat intelligence, and tailored solutions for specific environments like IoT, organisations can strengthen their defences against increasingly sophisticated cyber threats. Continuous research and development in these areas will create resilient and adequate security systems that protect sensitive data and maintain network integrity.

REFERENCES

1. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516. doi: 10.1016/j.adhoc.2012.02.016

2. Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30. doi: 10.1016/j.clsr.2009.11.008

3. Alam, M., & Khan, I. R. (2022). Cyber-physical attacks and IoT. In *Chapman and Hall/CRC eBooks*, 79–104. doi: 10.1201/9781003241348-5

4. Sommer, R., & Paxson, V. (2010). Outside the closed world: on using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316. doi: 10.1109/sp.2010.25

5. Djergou, A. A., Maleh, Y., & Mounir, S. (2022). Machine Learning Techniques for Intrusion Detection in SDN: A survey. In *Lecture notes in networks and systems,* 460–473. doi: 10.1007/978-3-030-91738-8_42

6. Dina, A. S., Siddique, A., & Manivannan, D. (2023). A deep learning approach for intrusion detection in the Internet of Things using focal loss function. *Internet of Things, 22*, 100699. doi: 10.1016/j.iot.2023.100699

7. Bertino, E., & Islam, N. (2017). Botnets and Internet of Things security. *Computer, 50*(2), 76–79. doi: 10.1109/mc.2017.62

8. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal, 4*(5), 1250–1258. doi: 10.1109/jiot.2017.2694844

9. Wanda, P., & Jie, H. J. (2020). A survey of Intrusion Detection system. *International Journal of Informatics and Computation, 1*(1), 1. doi: 10.35842/ijicom.v1i1.7

10. Selem, M., Jemili, F., & Korbaa, O. (2024). Deep learning for intrusion detection in IoT networks. *Research Square*. doi: 10.21203/rs.3.rs-4306367/v1

11. Smys, N. D. S., Basar, N. D. A., & Wang, N. D. H. (2020). Hybrid Intrusion Detection System for Internet of Things (IoT). *Journal of ISMAC, 2*(4), 190–199. doi: 10.36548/jismac.2020.4.002

12. Haripriya, L., & Jabbar, M. (2018). Role of Machine Learning in Intrusion Detection System: review. *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 925–929. doi: 10.1109/iceca.2018.8474576

13. Cao, Y., Wang, Z., Ding, H., Zhang, J., & Li, B. (2023). An intrusion detection system based on stacked ensemble learning for IoT network. *Computers & Electrical Engineering, 110*, 108836. doi: 10.1016/j.compeleceng.2023.108836

14. Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access, 10,* 93104–93139. doi: 10.1109/access.2022.3204051