Hybrid Deep Learning Framework for Real-Time Cyberattack Detection in IoT-Enabled Smart Networks

Dr. Divyajyothi M G[1], Dr. Rachappa Jopate[2], Shaikha Mohammed Nasser Al Jahdami[3], Saleh Abdullah Saleh Albalushi[4], Safiya Nasser Salim Aljaradi[5], Rawdha Ali Salim Ali Alhinai[6]

[1] Department of Computing and Information Sciences, University of Technology and Applied Sciences – Al Mussanah, Sultanate of Oman.
Email: Divyajyothi.MG@utas.edu.om

[2] Department of Computing and Information Sciences, University of Technology and Applied Sciences – Al Mussanah, Sultanate of Oman.
Email: Rachappa.Jopate@utas.edu.om

[3] Department of Computing and Information Sciences, University of Technology and Applied Sciences – Al Mussanah, Sultanate of Oman.
Email: shaikha.jahdami@utas.edu.om

[4] Department of Computing and Information Sciences, University of Technology and Applied Sciences – Al Mussanah, Sultanate of Oman.
Email: Saleh.Albalushi@utas.edu.om

[5] Department of Computing and Information Science, University of Technology and Applied Sciences – Al Mussanah, Sultanate of Oman.
Email: safiya.aljaradi@utas.edu.om

[6] Department of Computing and Information Sciences, University of Technology and Applied Sciences – Al Mussanah, Sultanate of Oman.
Email: 56S2226@utas.edu.om

Corresponding Author:

Dr. Divyajyothi M G[1]* (Divyajyothi.MG@utas.edu.om)

Abstract: Internet of Things (IoT) technologies have revolutionized the world of communication by allowing a seamless integration of smart devices, sensors, and intelligent systems in present-day communication infrastructure. Critical areas like smart cities, energy, transportation, healthcare and industrial automation are adopting smart networks with IoT technology, generating fresh automation and data-driven decision opportunities. But the large-scale connectivity and varying nature of IoT environments has made them highly susceptible to attacks such as denial-of-service (DDoS), malware and botnet attacks, data breaches, and attempt to access without authorization. The volume, velocity and victimization of network traffic produced by IoT devices place a significant burden on traditional security mechanisms for detecting, realtime, advanced and evolving threats. In advanced AI/Deep Learning, the technology has shown its potential in detecting cyber attacks and improving network security.Thus, advanced AI/Deep learning has come up as a promising solution for intelligent cyberattack detection and network security enhancement. Multi-modal deep learning architectures, which leverage multiple learning paradigm (such as CNN, RNN, LSTM, and autoencoder) achieve stronger abilities to extract complex traffic patterns and detect malicious traffic with high accuracy. These tools enable you to detect threats in real-time, adaptively learn networks, identify anomalies, and perform predictive security analysis in a dynamic network environment. This research is to investigate hybrid deep learning methods to detect real-time cyberattacks in the IoT-enabled smart network. It examines the current security issues, analyzes various deep learning architectures, and assesses the ability of these architectures to enhance the accuracy of detection and

enhance the resilience of a network. The results provide valuable insights for understanding future implications of intelligent security architectures and their contribution to creating secure, adaptive and trustworthy smart IoT systems in an increasingly connected digital world.
Keywords: Internet of Things, Cyberattack Detection, Deep Learning, Network Security, Smart Networks, Artificial Intelligence, Intrusion Detection Systems, Hybrid Learning Frameworks

Introduction

The emergence and development of Internet of Things (IoT) technologies have revolutionized the digital world, shifting from their mere presence to facilitating the creation of interconnected and interdependent compartments that consist of smart devices, sensors, communication infrastructure, and intelligent applications. Currently, smart networks with Internet of Things (IoT) spread everywhere, and are used in many industries ranging from healthcare, manufacturing, transportation, agriculture, smart cities to energy management systems. These networks allow for the immediate capture of data, decision making automation, remote monitoring and improved operational efficiency. The proliferation of IoT technologies has led to an unprecedented amount of data, as well as new possibilities for digital connections, which opens the door for innovations and economic development. However, with the proliferation of IoT devices, there are significant cybersecurity concerns such as weak computation power, heterogeneity in communication protocols and network specifications. From a security perspective, IoT systems typically comprise resource-limited devices that often have limited security capabilities, making them appealing to cyber criminals. Distributed denial-of-service (DDoS) attacks, ransomware, malware propagation, botnet formation, phishing attacks, data interception, and unauthorized system access are some threats rapidly observed in IoT. The impact of a successful cyber attack can be devastating, with services disrupted, financial damages incurred, privacy breaches and threats to critical infrastructure operations being some of the potential outcomes. Simpler, signature-based and rule-of-thumb security intelligence models and analysis techniques struggle to keep up with the vast and complex range of attack patterns as the number of connected devices has increased. Thus, the demand for intelligent, adaptive and scalable cybersecurity solutions has become a giant line of research in the present network security. The rapid progress of AI and machine learning has opened new avenues to improve cyber threat detection, by automating the analysis of intricate network behaviors and anomaly patterns. The advancements have paved the way for the creation of more precise and efficient security configurations that leverage deep learning algorithms to detect and prevent malicious actions. Computer security and cybersecurity researchers have shown the deep learning technologies significant interest because of their capability of automatically learning hierarchical representations from a large amount of data, and identifying complex patterns in network traffic. Success has been achieved using convolutional neural networks, recurrent neural networks, long short-term memory networks, gated recurrent units, autoencoders and deep belief networks in intrusion incidents in the detection and classification of cyberattacks. Single Deep Learning models, however, may fail to take care of the dynamic nature of cyber threats in IoT-based smart networks and their diversity. In response, a series of hybrid deep learning models that integrate the best of various architectures to enhance detection performance and adaptability has recently surfaced. Hybrid models can be combined together with both spatial, temporal and behavioral patterns of network traffic to aid effective identification of known and unknown attacks. Moreover, combining feature extraction algorithms, anomaly detection methods, and adaptive learning techniques increases the resilience of cybersecurity systems in large-scale IoT scenarios. With the growing volume of cybersecurity data and the availability of powerful computing power, the era of intelligent intrusion detection systems that can monitor and respond to threats in real-time is now possible. Moreover, early technology trends like edge computing platforms, cloud security solutions, and federated learning are opening new avenues for deep learning security systems, allowing for distributed analysis and the detection of threats while ensuring privacy. While these progressions were made, there are still challenges regarding model interpretability, computational efficiency, scalability, and adversarial attacks. Thus, real-time cyberattack identification based on the effectiveness of a hybrid deep learning approach is crucial to bolster the security and resilience of future IoT systems. This research aims at exploring the potential for hybrid deep-learning models in boosting cyber attack detection performance in IoT networks powered by smart network systems to tackle the current cyber security challenges and to design an

intelligent network defense system.

RELEATED WORKS

The immigration of technologies into IoT has raised significant research interest in the cybersecurity aspect of the smart network environment with the emphasis on detection and prevention of cyberattacks. The initial intrusion detection Systems (IDS) were mainly signature based and rule based to detect the malicious activity in the communication network. These techniques worked well against familiar attacks, but were less successful with new attacks and patterns of attack [1]. The researchers then sought to use machine learning methods to enhance intrusion detection accuracy, employing automated pattern recognition and anomaly detection. Research results proved that supervised learning methods like decision trees, SVC, RF and KNN classifiers can successfully determine the category of network traffic and decide whether that traffic is possibly an attack or not [2]. As the volume and complexity of data generated by the Internet of Things (IoT) devices continues to grow, however, there were many limitations associated with traditional machine learning approaches, which are mostly dependent on the handcrafted feature extraction and are less adaptable to the ever-changing cyber threat landscape [3]. Research into more sophisticated information processing methods using Artificial Intelligence (AI) which can process large-scale network datasets and automatically extract meaningful representations of networks started. The evolution paved the way to deep learning-based cybersecurity solutions that provide advanced detection capabilities and better scalability in dynamic network environments [4]. The increasing complexity of cyberattacks further emphasized the necessity for intelligent security framework with adaptive response to new threats and safeguarding complex IoT environment interconnectedness [5]. However, given the ability to learn complex patterns from high-dimensional network traffic, deep learning has become a very powerful tool for cybersecurity applications. There have been there huge amount of research conducted on the application of CNN, RNNs, LSTMs and AE for intrusion detection and malware classification. ConvNets have been shown to be effective in capturing spatial characteristics from datasets of network traffic and therefore have the potential of accurately classifying attack classes [6]. Cybersecurity problems have been holistically addressed using recurrent neural networks and long short-term memory architectures, which are able to learn from time-dependent and sequential patterns in communication data [7]. Anomaly detection using an Autoencoder has been found to be very effective, as it can detect deviation that occurs in normal network activity [8]. As simulation results suggest, deep learning models tend to outperform traditional machine learning methods with more accurate recognition and reduction of false positive, as well as adaptability to complex attack scenarios [9]. But each deep learning architecture can have significant vulnerabilities if it faces a wide range of cyber threats and a constantly shifting attack surface. To benefit from the strengths of various different deep-learning models and reinforce the measures' security performance, researchers have suggested hybrid models that take advantage of several deep-learning models. The results of this study indicate that deep learning technologies have tremendous potential for intelligent IoT-enabled IDS development. The attention of recent studies shifted toward hybrid deep learning models to overcome the drawbacks of single models and to improve cyberattack detection in real-time scenarios. In [11] hybrid architectures based on convolutional neural network (CNN) and long short-term memory network (LSTM) have been able to achieve better results by combining both spatial and temporal features of the network traffic. In a similar fashion, various architectures of autoencoders combined with recurrent networks and attention mechanisms have been used to enhance accuracy of both anomaly detection and attack classification [12]. Further, with the advent of the edge computing and cloud-based supporting security architecture, the network has become better equipped to deploy intelligent detection and analysis systems that can process and analyse the vast amounts of IoT data in real-time [13]. Cybersecurity has also been a topic of researchers for federated learning approaches for privacy-preserving cyber defense solutions and collaborative threat intelligence sharing between distributed cybersecurity devices [14]. Moreover, the increased interpretability and explainability of IDS based on deep learning using advances in explainable artificial intelligence has helped to alleviate concerns on trust issues and decision making accountability. Despite such progress, computational complexity, imbalanced data, adversarial attacks and scalability are current research topics [15]. The current literature emphasizes

the increasing significance of a hybrid deep learning framework in bolstering cybersecurity defenses and offers the groundwork for advancing the field of intelligent threat detection approaches in future smart networks that are embedded with IoT devices.

METHODLOLGY

3.1 Research Design

The measurement of effectiveness of the hybrid deep learning frameworks in real-time cyberattack detection in IoT-based smart networks is the focus of this study by a qualitative and analytical method of research. The study emphasizes the analysis of integrating several deep learning architectures and the role they play in intrusion detection, anomaly detection, and network security improvement. The qualitative approach used for the development of the study is suitable to evaluate the cybersecurity frameworks, learning architectures, and detection mechanisms by analyzing available research results and technology that have emerged in the field. The analytical framework aids to systematically evaluate the attack detection capability, model performance, and security outcomes in dynamic IoT environments. There are previous studies that have applied analytical methods to test and analyze intelligent intrusion detection systems, and deep learning (DL)-based security models [16, 17] have been proven to be effective.

Table 1: Research Design Framework

Component	Description
Research Approach	Qualitative
Research Type	Analytical and Descriptive
Data Nature	Secondary Research Data
Study Focus	Hybrid Deep Learning for Cyberattack Detection
Key Variables	Deep Learning Models, Detection Accuracy, Network Security
Analysis Method	Comparative and Thematic Analysis

3.2 Data Sources and Collection

The research in the study is based on the secondary data collection method obtained from scientific databases, technical reports, research publications, peer-reviewed journals, and papers published in various security conferences on IoT security, artificial intelligence, machine learning, intrusion detection systems. Selected sources offer insights regarding the cyberattacks' characteristics, network traffic analysis, deep-learning architectures, anomaly detection mechanisms, and intelligent security frameworks [25]. The selection of literature was carried out using an approach of relevance, scientific credibility and contribution to understanding the use of the Hybrid Deep-learning technique in Cyber Security. The data gathered assist in the analysis of current detection methods and help define new trends in intelligent network defence systems [18, 19].

3.3 Analytical Framework

The analytical framework is divided into three main aspects: cyberattack characteristics, hybrid deep learning system architectures, and detection performance. Cyberattack dimension: Malware attacks, Denial-of-service attacks, Botnets, Phishing attacks, Unauthorized access attempts. In deep learning, it emphasizes at the first place CONNs, RNN, LSTMs, autoencoders, and hybrid architectures. The detection performance aspect is designed as accuracy, precision, recall, false positive rates, detection speed and adaptability. This framework allows conducting an all-round evaluation of the performance of the hybrid deep learning models in real-time security defense in IoT-based smart networks [20, 21].

Table 2: Analytical Framework of the Study

Dimension	Key Focus Areas
Cyberattacks	DDoS, Malware, Botnets, Phishing
Deep Learning Models	CNN, RNN, LSTM, Autoencoders
Security Functions	Intrusion Detection, Anomaly Detection
Performance Indicators	Accuracy, Recall, Precision, Response Time

3.4 Data Analysis Procedure

Themes and comparison method of data analysis was employed on the collected data. The studies were classified based on the attack type, the deep learning architectures, the detection method and performance results. Thematic analysis was employed to explore commonalities in terms of model effectiveness, adaptability, and performance when it comes to cyber security. The results demonstrated that individual deep learning and hybrid deep learning models exhibited comparable performance in identifying cyber threats in the IoT context, as shown in the comparison tables.Several comparisons were carried out to examine the differences and similarities between the individual and hybrid deep learning methods in IoT cyber threat detection. Analysis of other combinations of learning architectures further improved detection accuracy and false alarm rates working towards the goal of achieving a more robust network security [22].

3.5 Research Process and Validation

The study was conducted in a structured way ensuring reliability, validity, identification, collection of literature, thematic classification, comparative assessment and interpretation of the findings. Different academic and technical sources were cross-checked for consistency and to reduce biases. Results were confirmed by comparing with well-known principles of cyber security and the experimental results reported by various studies. This systematic approach not only enhances the credibility of the research but also extends the reliability of the research in understanding the application of hybrid deep learning frameworks in protecting IoT enabled smart network against the changing cyber threats [23].

RESULT AND ANALYSIS

4.1 Effectiveness of Hybrid Deep Learning Frameworks

Based on the analysis, the hybrid deep learning frameworks offer a notable cyber disagreement detection capacity improvement over the traditional security frameworks and ML-based standalone approaches highlighted in the analysis. A hybrid model combines several different chains of deep learning architecture, so as to be able to catch both spatial and temporal characters of network traffic data simultaneously. The ability will help push back against malicious activity and enhance the classification of a wide range of attack types. The results show that hybrid strategies are more effective in addressing the evolving cyber threats and changing pattern of attacks. Moreover, these models minimize manual works on feature engineering as they automatically detect important features or pattern involved in a vast amount of network data. Thus, in the complex environment of IoT, the hybrid deep learning techniques generate superior cyber security performance.

4.2 Detection Accuracy and Network Security Enhancement

The results reveal the efficacy of hybrid deep learning approaches in boosting the accuracy of detection and ensuring comprehensive network security. A novel method—CNN-RLSTM is employed to identify multi-scale attack signatures and sequential behavior anomalies.A novel method, CNN-RLSTM is utilized for identifying multi-scale attack signatures and sequential behavior anomalies. The results show that these models result in more precise and recall accuracy along with lesser false positive detections. Foster better detection performance boosts the capacity of the organization to detect and respond to cyber threats in real time. Moreover, smart security solutions can aid with advance recognition of threats to the network before significant damage is done. Thus, hybrid deep learning

frameworks enhance the capability of smart networks connected with the IoT environment to withstand advanced cyberattacks.

Table 3: Hybrid Deep Learning Models and Security Contributions

Hybrid Framework	Key Capability	Security Contribution
CNN-LSTM	Spatial and Temporal Analysis	High Detection Accuracy
CNN-RNN	Traffic Pattern Recognition	Improved Threat Identification
Autoencoder-LSTM	Anomaly Detection	Reduced False Positives
CNN-Autoencoder	Feature Extraction	Enhanced Intrusion Detection
Multi-Model Hybrid	Comprehensive Analysis	Stronger Network Security

4.3 Cyberattack Detection Across IoT Environments

The results show that hybrid deep learning networks work well to find various common cyberthreats in smart networks with Internet of Things (IoT). Intelligent analysis of network traffic and behavioral patterns can help detect distributed denial-of-service (DDOS) attacks, malicious activities, communications from malicious bots, phishing attempts, and other suspicious logins. The study suggests that hybrid models have significant appeal where there are many different types of devices and communication protocols, typical of IoT setups. Their adaptability allows them to continuously monitor and identify threats across dynamic network environments. As such, hybrid deep-learning methods offer wide coverage of various types of cyber threats.

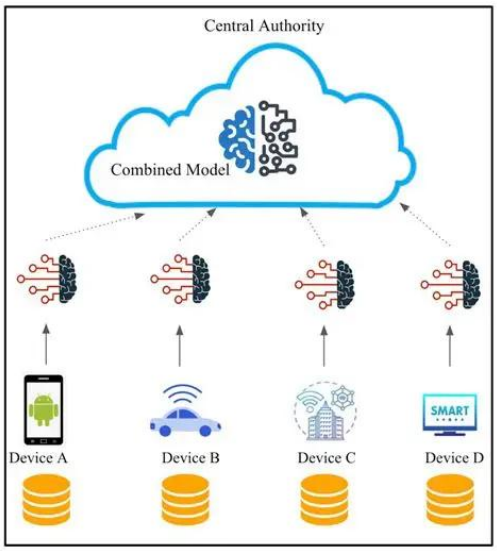

Figure 1: Anomaly Detection of IoT Cyberattacks [25]

4.4 Emerging Trends in Intelligent Cybersecurity

Some of the new challenges that will shape the future of smart cybersecurity systems are highlighted in the analysis. AI and machine learning have become more common in the edge computing architectures to support low-latency threat detection and response. Federated learning frameworks allow the federated distributed IoT devices to collaborate in training models without compromising data privacy. Developing techniques of explainable artificial intelligence (XAI) to build trust and transparency in automated security decision making is ongoing. The results also show a trend toward increasing embedding of platforms assisted by the cloud, using real-time threat intelligence systems and implementing adaptive learning capabilities that can adapt to the dynamic nature of attacks. The expected developments of these advancements will further improve the efficiency of cybersecurity within future smart network environment.

Table 4: Major Cyber Threats and Detection Outcomes

Cyber Threat	Detection Mechanism	Security Outcome
DDoS Attacks	Traffic Pattern Analysis	Service Protection
Malware Attacks	Behavioral Classification	Threat Isolation
Botnet Activities	Communication Monitoring	Network Integrity
Phishing Attempts	Anomaly Detection	User Protection
Unauthorized Access	Intrusion Detection	Data Security

4.5 Overall Analysis of Intelligent Cyberattack Detection

This comprehensive study highlights the hybrid deep learning models as a huge improvement in the field of cybersecurity of smart networks with Internet of Things (IoT). Multiple learning architectures allow for traffic analysis, detection of anomalies and classification of attacks that are impossible to achieve using more conventional security methods. The results show that intelligent detection systems increase accuracy, decrease false alarms, and because of the real-time use of data, they can help reduce response time for cyber threats. Additionally, the rise of artificial intelligence, edge computing, federated learning and explainable security models are enhancing the capabilities of today's intrusion detection systems. The research ultimately creates a matrix of the various hybrid deep learning frameworks that can be used to build adaptive, scalable, and resilient cybersecurity solutions that will work to protect infrastructure for future IoT systems from an ever-evolving array of cyber threats.

CONCLUSION

In this study, we investigated the use of hybrid deep learning models for real-time detection of cyberattacks in smart network systems powered by the internet of things (IoT) and explained their role in tackling modern cybersecurity issues. The security issues highlighted due to the use of the Internet of Things (IoT) technologies are enormous and have led to substantial security concerns associated with malware infections, distributed denial-of-service (DDoS) attacks, botnets, phishing, and unauthorized access events. In the past, typical IDS solutions are less effective to deal with the dynamism, scale and complexity of the data coming across their network tied to an IoT system, so it is important to create intelligent and adaptive IoT security solutions to help manage it. The study showed that hybrid deep learning architectures successfully integrate the advantages of several learning models, and can provide comprehensive analysis of the spatial, temporal and behavioral characteristics of the network. These are built to increase the rate at which they detect errors, improve the ability to identify anomalies, minimize false-positive rates, and enable real-time threat monitoring in large and complicated network environments. These will be assisted by the use of Convolutional and Recurrent Neural Networks, Long short-term memory networks, and Autoencoders, which will improve the recognition of known and new cyber threats. Additionally, the study revealed the increasing significance of artificial intelligence, federated learning, edge computing and explainable cybersecurity systems for building better network defence systems in the future. These technologies also pave the way for higher adaptability, scalability and transparency in the intelligent intrusion detection field. However, future research is essential in other areas like computational cost, adversarial attacks, model explainability, and privacy, but continuous progress in AI and cybersecurity technologies is anticipated to overcome many of these downfalls. In general, the research findings suggest that hybrid deep learning systems are an effective and robust solution to improve cybersecurity in IoT-powered smart network. The use of reliable, adaptive and up-to-the-minute cyberattack detection makes them integral elements of smart security systems that will safeguard more highly networked systems in the future.

References

W. Stallings, Network Security Essentials, 7th ed. Boston, MA, USA: Pearson, 2022.

W. Lee and S. J. Stolfo, "Data Mining Approaches for Intrusion Detection," Proceedings of the USENIX Security Symposium, pp. 79–93, 1998.

T. M. Mitchell, Machine Learning. New York, NY, USA: McGraw-Hill, 1997.

I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

D. B. Rawat and K. R. Chowdhury, Cyber Physical Systems: From Theory to Practice. Boca Raton, FL, USA: CRC Press, 2015.

Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.

S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.

G. E. Hinton and R. R. Salakhutdinov, "Reducing the Dimensionality of Data with Neural Networks," Science, vol. 313, no. 5786, pp. 504–507, 2006.

M. Tavallaee et al., "A Detailed Analysis of the KDD CUP 99 Dataset," IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1–6, 2009.

Kim, J. Kim, H. L. Thi Thu, and H. Kim, "Long Short-Term Memory Recurrent Neural Network Classifier for Intrusion Detection," International Conference on Platform Technology and Service, pp. 1–5, 2016.

A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," Proceedings of EAI International Conference on Bio-Inspired Information and Communications Technologies, pp. 21–26, 2016.

N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.

M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics," Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.

Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning," ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019.

A. Aldweesh, A. Derhab, and A. Emam, "Deep Learning Approaches for Anomaly-Based Intrusion Detection Systems," IEEE Access, vol. 8, pp. 158153–158173, 2020.

C. Bishop, Pattern Recognition and Machine Learning. New York, NY, USA: Springer, 2006.

S. Haykin, Neural Networks and Learning Machines, 3rd ed. New York, NY, USA: Pearson, 2009.

D. Jurafsky and J. H. Martin, Speech and Language Processing. Upper Saddle River, NJ, USA: Prentice Hall, 2023.

R. Sutton and A. Barto, Reinforcement Learning: An Introduction, 2nd ed. Cambridge, MA, USA: MIT Press, 2018.

K. Murphy, Machine Learning: A Probabilistic Perspective. Cambridge, MA, USA: MIT Press, 2012.

T. Hastie, R. Tibshirani, and J. Friedman, The Elements of Statistical Learning. New York, NY, USA: Springer, 2017.

P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-Based Network Intrusion Detection," Computers & Security, vol. 28, no. 1–2, pp. 18–28, 2009.

R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," IEEE Symposium on Security and Privacy, pp. 305–316, 2010.

Deloitte, Global Cybersecurity Outlook Report. New York, NY, USA: Deloitte Insights, 2024.

World Economic Forum, Global Cybersecurity Future Outlook. Geneva, Switzerland: WEF Publications, 2024.