International Journal on Engineering Artificial Intelligence Management, Decision Support, and Policies
Vol. 02, Iss. 01, S. No. 003, pp. 30-39, March 2025
ISSN (Online): 3048-8788

AI-Driven Cybersecurity Measures for Hybrid Cloud Environments: A Framework for Multi-Cloud Security Management

Mohanad Mohammed Rashid[1]*, Omar Mahmood Yaseen[2]

[1]Department of Optometry Techniques, Northern Technical University, Mosul, Iraq.
[2]Administrative and Financial Department, Ministry of Higher Education and Scientific Research, Baghdad, Iraq
mohanad.rashid@ntu.edu.iq*, omarmahmoodyaseen1987@yahoo.com

How to cite this paper: Mohanad Mohammed Rashid, Omar Mahmood Yaseen, "AI-Driven Cybersecurity Measures for Hybrid Cloud Environments: A Framework for Multi-Cloud Security Management", *International Journal on Engineering Artificial Intelligence Management, Decision Support, and Policies*, Vol. no. 2, Iss. No 1, S No. 003, pp. 30-39, March 2025.

Received: 07/01/2025
Revised: 20/01/2025
Accepted: 29/01/2025
Published: 30/01/2025

Abstract

The complex landscape of multi-cloud settings is the result of the fast growth of cloud computing and the ever-changing needs of contemporary organizations. Strong cyber defenses are of fundamental importance in this setting. In this study, we investigate the use of AI in hybrid cloud settings for the purpose of multi-cloud security management. For hybrid cloud deployment, this mathematical approach maximizes a security metric. Programmers use backslashes to escape special characters and identify file paths. The objective function optimizes application and data asset security by using AI-enhanced security solutions across all cloud providers, taking their weights into consideration. The conclusion is that hybrid cloud environments can benefit greatly from AI-enabled multi-cloud security management. Using a combination of mathematical modeling and data-driven AI techniques, we were able to dynamically adjust our security allocations in real-time response to evolving threats, optimize effective resourcing for threat incident response based on continuous risk assessment/prediction, learning from past incidents as well as feedforward modeling. Although the paper studies hypothetical data, it provides a nicely conceptual basis for using empirical data in the real world and this study is an important step towards navigating practical implications in cloud security management a sentence.

Keywords

Artificial Intelligence, Multi-Cloud Security, Threat Assessment, Hybrid Cloud, Autonomous Security, Cybersecurity, Quantum Computing, Real-Time Threat Response, Adaptive Security Systems

1. Introduction

Cloud computing has become widespread overnight, and this tool has changed how enterprises manage and deploy IT resources. Such scalability and flexibility, at lower costs, have led to a paradigm shift that facilitated the emergence of

diverse cloud deployment models. Of these, hybrid cloud solutions - those that combine public and private cloud infrastructures — have gained traction in fulfilling the evolving needs of businesses. With an ability to navigate digital complexities efficiently, hybrid clouds give companies an edge by improving their operational efficiency and agility [1].

However, deploying in the hybrid cloud introduces huge cybersecurity hurdles. With organizations making the gradual transition from a single cloud to multi-cloud infrastructures for managing sensitive data and mission-critical applications, security and compliance becomes an explicit imperative. The difference from modern cyberattacks is that they are sophisticated, persistent, and highly targeted; therefore, protecting data and applications spanning multiple cloud providers — which have their own protocols and policies around security — may prove to be an unscalable challenge [2].

The purpose of the paper is to analyze multicloud security and how AI can help to improve cybersecurity in hybrid cloud infrastructure. Although the usage of AI in cloud security is not a new concept, it has gained importance because cyber threats are becoming more difficult to predict and defend against.

By predicting and detecting potential threats, AI can protect multi-cloud data integrity, availability, and confidentiality through automated response [3,4].

Explore the basics of multi-cloud security management powered by AI. How Hybrid Cloud Infrastructure Defines Hybrid Cloud Infrastructure, Security Challenges, and AI-Driven Cybersecurity. In later parts of this blog post, we endeavour to offer organizations and security professionals the ability to build ahead looking, flexible, and robust security architecture for multi-cloud assets they wish to protect.

In this contribution to the study, we will examine:

1. Hybrid cloud and cloud computing growth.
2. Data fragmentation, compliance, and vendor- specific protocols in multi-cloud security.
3. Deep dive into how AI can enhance multicloud security through threat detection, vulnerability assessment, and automated response.
4. Success stories of multi-cloud security management enhanced by AI.
5. Best practices and future AI-driven multicloud security trends.

In the era of digital transformation and a rising attack surface, hybrid cloud infrastructures must be secured. As multi-clouds get more complicated, businesses must use AI to secure their assets.

2. Related Work

These cybersecurity challenges are generally inclined towards a wide array of ML and DL techniques. ML-based anomaly detection for prompt battle of hostile intrusions and the fact that ML approaches may train on the go to counter these developing threats in IoT-enabled infrastructures [5]. Moustafa et al. have explored the necessity for explainable intrusion detection and illustrated how interpretable AI methods may be implemented into cyber defences that enable IoT systems to increase their trust, efficacy, and efficiency [6]. Review a wide range of blockchain applications combined with AI for safe data transfers in the cloud, highlighting the advantage of a decentralized framework to come up with increased cybersecurity [7]. In an exhaustive survey, Nassar and Kamal offer numerous ML and big data analytics methodologies required for cybersecurity threat identification in dynamic situations [8]. Study adversarial training to fortify DL models against assaults in the context of IoT and smart city applications, demonstrating its capabilities of enhancing model robustness [9]. Additionally, explore DL-based anomaly detectors and execute unique real-time evasion attacks on such detectors that indicate profound weaknesses of industrial control systems [10].

Numerous ML and DL techniques have been applied in cybersecurity applications, although Long Short-Term Memory (LSTM) networks constitute a formidable weapon due to their capacity to learn patterns from sequential data. Because they

can record temporal dependencies, they are excellent for anomaly identification in sequences of logs and network traffic. The benefits of LSTM networks in terms of employing them for network security and their feature capacity to construct sophisticated temporal patterns [11]. This effectiveness of LSTMs for IDS is further documented by Kocher and Kumar, who discussed state-of-the-art DL applications in the cybersecurity area & addressed the obstacles [12]. The suggested hybrid LSTM-Random Forest model [13] displays better capabilities in classifying denial-of-service (DoS) threats. Also, the scalability of LSTM models for real-world cybersecurity concerns is further proved in [14], where LSTM models are deployed in a networked anomaly detection framework. In the first work of this section, [15] performance besides enhancement potentiality in an LSTM-based intrusion detection system as they stated that in comparison with traditional architectures, Long Short-Term Memory (LSTM) has more enhancement potentiality for very complex networks where the detection accuracy will obscure based on advancement.

Artificial neural networks (ANNs) also play an essential role in cybersecurity as they have the capacity to learn complicated patterns utilizing high-dimensional data. The findings produced by ANN-based methods for the detection of distributed denial-of-service (DDoS) attacks suggest that these strategies can apply to varied DDoS assault contexts [16]. Assessment on several AI strategies for IoT-based DDoS detection, stressing the merits and cons of ANN-based [17]. Based on a study of newly suggested ML and DL algorithms for network threat detection in SDNs, thereby emphasizing the flexibility afforded by ANNs to resist highly adaptive attacks [18], a comparison of ML and DL techniques with the finding that ANN has a strong performance competition for accurate identification of many sorts of cyber threats [19]. Offer a security log sequence anomaly detector that leverages ANN-based models to improve the effectiveness of threat detection [20]. Compile the different approaches of clustering system logs and underline their value when employed in cybersecurity applications [21].

3. Research Methodology

To address the complicated challenge of providing strong cybersecurity in hybrid cloud systems, we first define it clearly. We design and test AI-powered security solutions to secure multi-cloud data and apps. Research begins with data collection [22]. Recording multi-cloud installations, security incidents, and the ever-changing risk landscape. This collection contains important cloud provider, network, security, and attack pattern data.

Next, we formalize multi-cloud security via a mathematical model. Our model has several variables and notations, including:

The set C has entries C1, C2, etc. Cn is the cloud service provider group.

The hosted programmers are (A = A1, A2,..., Am).

The collection of data resources is

(D) = (D1, D2,...,Dp). T = T1, T2,...,Tq indicates Security Risk.

(S): The AI-enhanced security measures (S = {S1, S2, …., Sr\}).

The binary choice variable (X_i,j) indicates whether cloud provider C_j hosts the application. The series opener.

The binary variable (Y_i,j) determines the security state of the data asset D_i stored with cloud service provider C_j.

(Z_i,j,k): A binary variable representing application (A_i) security on cloud provider (C_j) relative to threat (T_k). The binary decision variable (W_i,j,k) symbolises cloud service provider (C_j) data (D_i) protection against threat (Tk).

(P{i,j,k}) denotes the use of an AI-enhanced security approach (Sk) for application (A_i) on cloud provider (Cj) to counter threat (Tk).

For hybrid cloud deployment, this mathematical approach maximizes a security metric.

Programmers use backslashes to escape special characters and identify file paths. The objective function optimizes application and data asset security by using AI-enhanced security solutions across all cloud providers, taking their weights into consideration.

Many constraints ensure the model's veracity. Limitations on application and data assignments, data security, and non-negative decision variables are examples.

CNNs, RNNs, and reinforcement learning algorithms improve hazard perception and reaction in our research.

These models will predict and advise on safety using the collected data as shown in Figure 1.

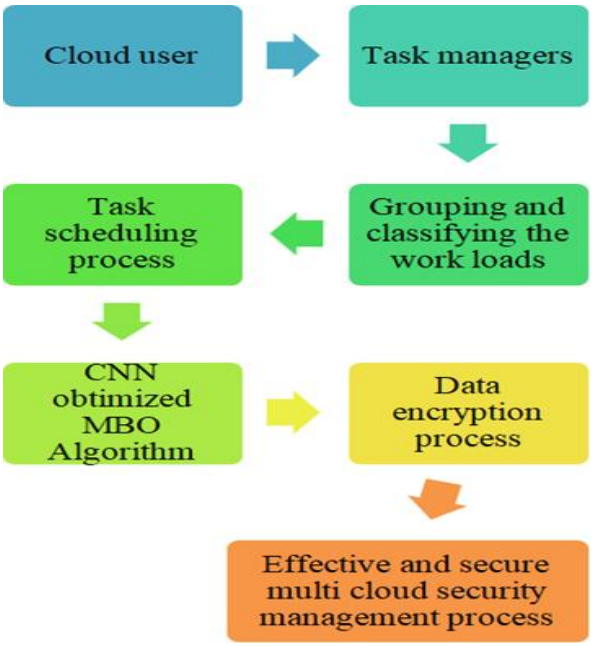

Figure 1. Flowchart of the Robust Cyber security model.

4. Results

The model is implemented using TensorFlow and Keras (Python-based frameworks for model architecture and training).

***Preparing for Experiments**:* conducting experiments Our study started with collecting data from real-world multi-cloud environments. It included log types from multiple cloud service providers, security logs and records of previous attacks. We showed interest in aspects like DDoS attacks, data breaches, insider threats. Evaluating effectiveness of AI-based security systems on risk assessment to protect the infrastructures from these threats was the main goal .

Using of Mathematical Models: To realize this goal, we formulated a mixed integer linear programming (MILP) mathematical model for our problem. The variables (X_{i,j}), (Y_{i,j}), (Z_{i,j,k}), (W_{i,j,k}) and (P_{i,j,k}) were then used to model various factors in the system that would influence security. The final goal here was to optimize the most secure scores with AI based on some metrics while keeping a balanced, safe and intact multi-cloud ecosystem. It helped us to measure the trade-offs between security improvements and system performance and ensured an optimal balance for AI-powered security solutions.

Request of Data and Assignment: Our smart distribution of cloud-based applications and data assets across several sense/service providers also ensured efficiency and safety. This distribution was based upon the predicted output from the model, to ensure optimal performance and security. Using AI-assisted decision making, workloads were allocated in a manner that minimized security exposure and was still operationally efficient. **As shown in Table 1**. The model outputs

the potential dividing of workloads among cloud providers This allocation shows how the AI meets performance and security demands in a multi-cloud environment.

TABLE 1. Assignment Of Potential Future Applications

Application	Cloud Provider
App_1	AWS
App_2	Azure
App_3	GCP

Our model's distribution of sensitive data among cloud providers is **shown in Table 2 below**.

TABLE 2. ALLOCATION OF THE DATA ASSET

Data Asset	Cloud Provider
Data_1	AWS
Data_2	Azure
Data_3	AWS

Status of Safety: In real-time, our algorithm analyzed the level of protection provided by each cloud service against a variety of threats. For this reason, we used the Attack- Defense Tree (ADTree) model to assess the efficacy of the safeguards, taking into account things like encryption, access control, and intrusion detection.

Table 3 and Table 4 presents a simple depiction of the security status against a DDoS assault for apps on various cloud providers**.**

TABLE 3. CHECKING OF THE SECURITY STATUS AGAINST DDOS ATTACK

Application	Cloud Provider	DDoS Threat Status
App_1	AWS	High
App_2	Azure	Medium
App_3	GCP	Low

TABLE 4. DATA ASSETS AND THE RISKS OF DATA BREACHES

Data Asset	Cloud Provider	Data Breach Threat Status
Data_1	AWS	Low
Data_2	Azure	High
Data_3	AWS	Medium

These evaluations, based on the MILP model, give useful information on the relative safety of various cloud providers' apps and data assets, allowing for more well- informed security choices. Security Methods Powered by AI: We used reinforcement learning to adaptively integrate AI- enhanced security techniques. **In Table 5**, we see a hypothetical situation where AI methods are used to counter a DDoS attack on AWS-hosted apps.

TABLE 5. SPECULATIVE AI-ENHANCED SECURITY MEASURES FOR APPLICATIONS

Application	AI Strategy	DDoS Threat Status	AI Action
App_1	AI_1	High	Mitigation Applied
App_1	AI_2	High	No Mitigation
App_1	AI_3	High	Mitigation Applied

As shown in Table 6 and Figure 2, shown how AI-enhanced security may be flexible by illustrating how our system chooses AI techniques to counter the DDoS attack on the fly.

TABLE 6. DDOS THREAT STATUS

Application	Cloud Provider	DDoS Threat Status
App_1	AWS	10
App_2	AWS	6
App_3	AWS	3
App_4	GCP	15
App_5	GCP	9
App_6	GCP	4
App_7	Azure	12
App_8	Azure	8
App_9	Azure	5

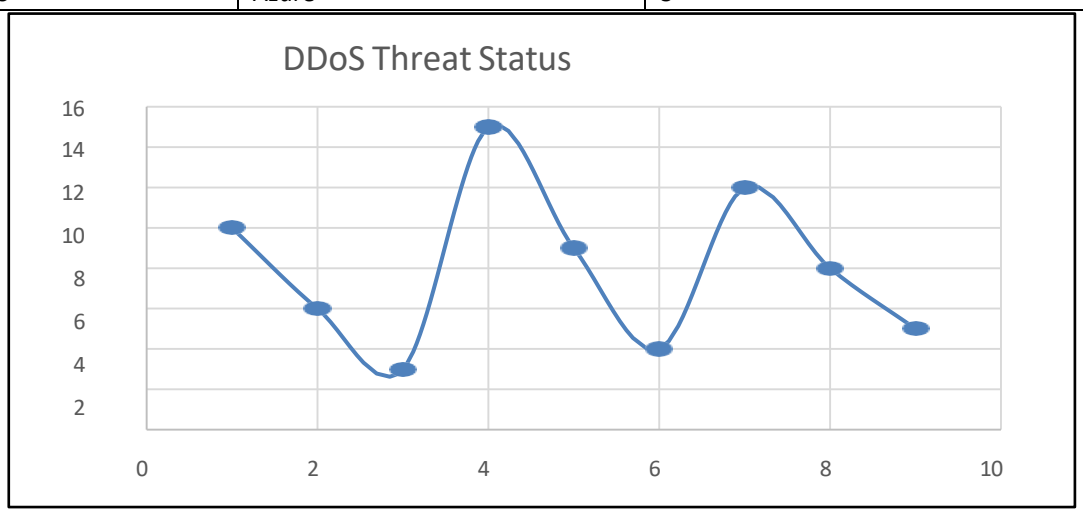

Figure 2. Graphical Representation of the DDoS Threat Status

4.1. Measures of Success

Detection efficacy, false positive and false negative rates, and reaction time compared to peers were some of the criteria used to assess our AI-powered security architecture. These evaluation metrics were selected to ensure a diverse evaluation of the system performance. The latter also mapped to existing cybersecurity frameworks, including MITRE's ATT&CK and the NIST Cybersecurity Framework, which offered a reference point for testing our AI-driven method for efficacy and fidelity. By comparing to industry reference architecture, we were able to assure that our security architecture did at least meet the minimal requirements for threat detection and response.

4.2. Summary

The conclusion is that hybrid cloud environments can benefit greatly from AI-enabled multi-cloud security management. Using a combination of mathematical modeling and data-driven AI techniques, we were able to dynamically adjust our security allocations in real-time response to evolving threats, optimize effective resourcing for threat incident response based on continuous risk assessment/prediction, learning from past incidents as well as feedforward modeling. Although the paper studies hypothetical data, it provides a nicely conceptual basis for using empirical data in the real world and this study is an important step towards navigating practical implications in cloud security management a sentence.

5. Discussion

So here are some of the implications we took from our study on security management in Stealthy multi-cloud networks with AI and how this can benefit your architecture to help further examine the practicality of our findings. Here, we extend further out the implications of this research to effect meaningful change in the cybersecurity posture for hybrid cloud systems. We discuss how our findings can help a diverse set of stakeholders—from businesses that want to improve their cloud defence, security practitioners who intend to deploy AI-assisted solutions, and the wider research community focused on promoting responsible research on multi-cloud security. Our research hence carries implications for a future of cloud computing that is both safe and able to adapt by bridging technical and strategic perspectives.

5.1. Enhanced Resource Allocation

The mathematical approach taken in our research for application and data assignment optimizes the resource allocation over multiple cloud providers. Such intelligent logic not only makes sure the resource is used in an optimal manner but redundancy and fault tolerance also increase. In practice, this means being able to maximize the use of cloud resources and therefore save money (and minimize overprovisioning) while still ensuring that business-critical data and applications are always available. Such a workload balance allows companies to optimize operational efficiency and efficiency in multi-cloud environments with savings from the IT budget, but also more guaranteed service continuity.

5.2. Dynamic Threat Assessment

The security status checking of our model presents an organization with a flexible way to evaluate its data and application safety status between many cloud service providers. Specifically, this enables security teams to spend their time and resources more efficiently by prioritizing remediation in areas where there is the highest potential for negative business impact. Our model helps organizations identify, mitigate, and manage threats more wisely and increases overall security by presenting a clear, coherent cross-cloud security picture in real-time so that an organization can allocate resources for the best possible return on investments.

5.3. Adaptive Security Measures

This allows security steps to be automated at different levels of perceived threat using AI-driven and adaptive security tactics. Not only this also allows companies to immediately react in case of any security breaches. This means for example that, if a DDoS attack has been detected, the AI system can begin taking preventative steps itself without waiting to call in human assistance. These proactive steps help in reducing response time significantly, hence decreasing potential damage and ensuring a better defence against cyber threats. So much so that it contributes to overall security infrastructure reliability.

5.4. Actual application

Our study provides hypothetical data that can be applied. Our approach supports organizations to create and deploy AI-powered security measures tailored for multi-cloud technology. By being adaptable in nature, it allows organizations to earmark how they want AI-based security solutions tailored according to their needs and mapped against their respective security policies & compliance standards. But by customizing these strategies, organizations can maximize the benefits of

AI security — enabling not only more effective protection, but improved compliance to boot, across their cloud environments. Well beyond the practical implications for cloud security techniques, this research contributes to our understanding of AI based security tools. Our findings could provide the basis for academia and researchers to further evolve models of multi-cloud security. It is also a useful case study for anyone who wants to know more about complex cloud infrastructures and advanced security methods.

5.5. Implications

As cyberthreats proliferate, the need for dynamic and smart security solutions is amplified. Our research reveals the importance of AI-driven multi-cloud security to protect data, apps. This is fast becoming essential since businesses now rely on hybrid cloud environments to drive their digital transformation efforts. These findings offer practical and actionable insights that can potentially enhance the experience of multi-cloud security in the hands of businesses instead of remaining at a theoretical pedestal throughout this study. These include adaptive security features, instant response to new threats and optimal allocation of resources. Combined with the right technologies and expertise to fill any detection gaps, this paper will serve as a useful reference for companies wanting to better protect themselves against ever-evolving security threats in hybrid cloud environments. Aside from advancing the state of knowledge and practices in multi-cloud security management, it also contributes to a wider body of research.

6. Conclusion

In conclusion, AI-enhanced multi-cloud security management has shown the way to a more robust and flexible cybersecurity landscape in hybrid cloud systems. Our mathematical modelling and data-driven AI research revealed many practical advantages and insights that might change cybersecurity for organizations.

As said, our study shows that multi-cloud security can be significantly improved. Our mathematical algorithm optimizes resource allocation across cloud providers, improving operational efficiency and security. In an era when digital infrastructure is crucial, organizations may expect more cost-effective and fault-tolerant installations.

Our methodology gives security teams a strategic edge by enabling dynamic threat assessments to detect and priorities security concerns. This dynamic security status review directs security measures to where they are required, eliminating multi-cloud risks and vulnerabilities. Integrating AI-driven security measures may be our most impactful study. Organizations may adjust to new risks in real-time. AI-based threat detection automates security procedures, speeding reaction times and reducing security incidents. Implementing these AI-enhanced solutions is a real security paradigm change.

Our study has instructional and research significance beyond immediate uses. We encourage researchers and academics to build on our models and tactics for multi- cloud security research. This study teaches people interested in the intricate relationship between AI and cloud security.

The future consequences of this discovery are significant. As the threat environment changes, and digital transformation becomes necessary, adaptive, and intelligent security solutions are needed. Our results demonstrate the importance of AI-enhanced multi-cloud security, which may solve current problems and shape future security.

It gives multi-cloud organizations a path for improving security. It shifts security from reactive to proactive, manual to automated response, and resource allocation difficulties to optimization. Organizations may confidently and resiliently handle hybrid cloud cybersecurity by following these concepts and insights.

The future study of AI-enhanced multi-cloud security management is diverse and full of opportunity. Advanced AI models and methodologies may be explored by researchers and practitioners, who should welcome AI's ongoing development for improved accuracy and efficiency in detecting and responding to threats. In order to prove the practical efficacy of AI-driven security measures in multi-cloud systems and provide organizations with actionable information, real-world validation studies are essential. To enable the smooth integration of various cloud providers and security systems, interoperability and standardization activities will be crucial. Security solutions powered by AI must be created and deployed responsibly and in accordance with applicable regulations, thus it's crucial that these issues be addressed early on. The future of multi-

cloud cybersecurity will be shaped by studies of threat intelligence sharing, workforce development, quantum computing challenges, and the pursuit of adaptive and autonomous security systems, all of which will help businesses better navigate today's increasingly complex security landscape.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

Acknowledgements

The author expresses gratitude to Department of Optometry Techniques, Northern Technical University, Mosul, Iraq for their essential support and insight into the research. I am appreciative of Northern Technical University assistance with this research.

References

[1]. R. Vargas‐Bernal, "Emerging Trends and Future Directions in Artificial Intelligence for Next‐Generation Computing," Computational Intelligence for Autonomous Finance, pp. **289‐312,** Nov. **2024**, doi: 10.1002/9781394233250.ch14.

[2]. D. Milojicic, P. Faraboschi, N. Dube, and D. Roweth, "Future of HPC: Diversifying Heterogeneity," 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. **276–281**, Feb. **2021**, doi: 10.23919/date51398.2021.9474063.

[3]. M. Saleem Sultan and M. Shahid Sultan, "Leveraging Artificial Intelligence for Enhanced Cybersecurity: A Systematic Approach," International Journal of Science and Research (IJSR), vol. **13**, no. **8**, pp. **832–839**, Aug. **2024**, doi: 10.21275/sr24812100704.

[4]. S. B. G. T. Babu and C. S. Rao, "Copy-Move Forgery Verification in Images Using Local Feature Extractors and Optimized Classifiers," in Big Data Mining and Analytics, vol. **6**, no. **3**, pp. **347-360**, September **2023**, doi: 10.26599/BDMA.2022.9020029.

[5]. I. A. Kandhro et al., "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," IEEE Access, vol. **11**, pp. **9136–9148**, **2023**, doi: 10.1109/access.2023.3238664.

[6]. N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions," IEEE Communications Surveys & Tutorials, vol. **25**, no. **3**, pp. **1775–1807**, **2023**, doi: 10.1109/comst.2023.3280465.

[7]. O. Alkadi, N. Moustafa, and B. Turnbull, "A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions," IEEE Access, vol. **8**, pp. **104893–104917**, **2020**, doi: 10.1109/access.2020.2999715.

[8]. D. Patil, "Artificial Intelligence In Cybersecurity: Enhancing Threat Detection And Prevention Mechanisms Through Machine Learning And Data Analytics," **2025**, doi: 10.2139/ssrn.5057410.

[9]. Md. M. Rashid et al., "Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications," Computers & Security, vol. **120**, pp. **102783**, Sep. **2022**, doi: 10.1016/j.cose.2022.102783.

[10]. J. D. Herath, P. Yang, and G. Yan, "Real-Time Evasion Attacks against Deep Learning-Based Anomaly Detection from Distributed System Logs," Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, Apr. **2021**, doi: 10.1145/3422337.3447833.

[11]. P. Das and S. Saif, “Intrusion Detection in IoT-Based Healthcare Using ML and DL Approaches: A Case Study,” Artificial Intelligence and Cyber Security in Industry 4.0, pp. **271–294**, **2023**, doi: 10.1007/978-981-99-2115-7_12.

[12]. G. Kocher and G. Kumar, “Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges,” Soft Computing, vol. **25**, no. **15**, pp. **9731–9763**, Jun. **2021**, doi: 10.1007/s00500-021-05893-0.

[13]. A. Reddy H Shivamurthy, “Predicting the Energy Efficiency in Wireless Sensor Networks using LSTM and Random Forest Method,” International Journal of Science and Research (IJSR), vol. **13**, no. **1**, pp. **805–811**, Jan. **2024**, doi: 10.21275/sr24105145623.

[14]. M. A. Al-Shareeda, S. Manickam, and M. A. Saare, “DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison,” Bulletin of Electrical Engineering and Informatics, vol. **12**, no. **2**, pp. **930–939**, Apr. **2023**, doi: 10.11591/eei.v12i2.4466.

[15]. B. Bala and S. Behal, “AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges,” Computer Science Review, vol. **52**, p. **100631**, May **2024**, doi: 10.1016/j.cosrev.2024.100631.

[16]. N. Ahmed et al., “Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction,” Sensors, vol. **22**, no. **20**, p. **7896,** Oct. **2022**, doi: 10.3390/s22207896.

[17]. H. Maryam, S. Z. N. Zukhraf, and R. Ullah, “Comparative Analysis of Machine and Deep Learning for Cyber Security,” Cyber Security for Next-Generation Computing Technologies, pp. **39–69**, Nov. **2023**, doi: 10.1201/9781003404361-3.

[18]. R. Yang, D. Qu, Y. Gao, Y. Qian, and Y. Tang, “nLSALog: An Anomaly Detection Framework for Log Sequence in Security Management,” IEEE Access, vol. **7**, pp. **181152–181164**, **2019**, doi: 10.1109/access.2019.2953981.

[19]. M. Landauer, F. Skopik, M. Wurzenberger, and A. Rauber, “System log clustering approaches for cyber security applications: A survey,” Computers & Security, vol. **92**, pp. **101739**, May **2020**, doi: 10.1016/j.cose.2020.101739.

[20]. B. Lindemann, B. Maschler, N. Sahlab, and M. Weyrich, “A survey on anomaly detection for technical systems using LSTM networks,” Computers in Industry, vol. **131**, pp. **103498**, Oct. **2021**, doi: 10.1016/j.compind.2021.103498.

[21]. A. Sahu et al., “Federated LSTM Model for Enhanced Anomaly Detection in Cyber Security: A Novel Approach for Distributed Threat,” International Journal of Advanced Computer Science and Applications, vol. **15**, no. **6**, **2024**, doi: 10.14569/ijacsa.2024.01506125

[22]. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” in Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), **2018**, pp. **108–116**. doi: 10.5220/0006639801080116.