***Review Article***

DeepLearning Techniques for Threat Detection in Cloud Environments: A Review

.

ABSTRACT

|  |
| --- |
| Deep learning techniques have become essential in enhancing threat detection within cloud environments, offering the ability to process large-scale data and detect complex patterns. As cloud computing continues to grow, ensuring robust security measures is critical to protecting sensitive data from evolving cyber threats. Deep learning models, particularly CNN, RNN, and Autoencoders, play a key role in identifying various threats, such as unauthorized access, data leakage, and DDoS attacks. This paper reviews research published between 2018 and 2023, comparing the effectiveness of deep learning models in cloud security. The findings indicate that deep learning models provide higher accuracy and adaptability compared to traditional methods. However, challenges such as data confidentiality, high computational requirements, and real-time detection still persist. The paper concludes by highlighting the need for hybrid models and enhanced training datasets to overcome these challenges. This review is valuable for researchers and practitioners working to implement deep learning approaches in cloud security. |

***Keywords****: Deep Learning, Threats, Cloud Security, Cyber Security*

1. **Introduction:**

Cloud computing has emerged as a phenomenon of modern Information Technology, brought into use for dynamic and flexible operation at reasonable prices. However, as reported by McGuire, the positive effect realized by organizations through the adoption of cloud services is accompanied by the steadily rising cases of cyber threats that attack cloud scenarios. All these threats are very dangerous to data and information, confidentiality, and security of the system. Cloud environments are increasingly becoming complex and dynamic to warrant advanced threats detection systems as traditional security measures cannot sufficiently address current and future cyber threats (Halbouni, 2022).

Machine learning especially deep leaning has advocated the detection of threats and the prevention of threats in the cloud since the algorithm involves the processing of large data and pattern recognition. High accuracy has been achieved by deep leaning approaches like CNN, RNN, and Auto encoder to accurately detect anomalies, threats, and probable weaknesses in cloud computing systems. These techniques can complement traditional approaches to security by offering an automated, real-time processing of network traffic, system behavior and user activity (Olateju, 2024).

Given the central role of the secure cloud environments there are significant interest in using deep learning for threat detection. Specifically, this paper seeks to present a current state of the art of deep learning methods used in cloud security, with emphasis on how these methods are enhancing the threat detection. For Deep learning models, the review discusses the advantages and drawbacks of different models, and obstacles to their adoption, before proposing ways for enhancing cloud security with these complex models. Based on the literature review exploring the role of deep learning in threat detection and its emerging trends, this research aims to provide valuable insights that contribute to the continuous enhancement of cybersecurity in cloud environments. The findings are expected to benefit researchers, security professionals, and cloud service providers (CSPs) by offering a deeper understanding of how deep learning can improve cloud security measures. (Mijwil, 2023).

1. **Cloud Security Using Deep Learning**

Cloud computing has become one of the crucial components of today’s business development because of its scalability and flexibility. But with the exponential growth of cloud services, the security of cloud environments has become a main issue (Rane, 2024). There remains hosting cloud susceptible to different types of cyber threats for instance; data breaches, DoS attacks, and threats from within the organization hence the need to adopt proper BTD solutions. Such security threats can easily go unnoticed by conventional security solutions because of the diverse and rapidly evolving nature of the cloud (Zhang et al., 2023). Advanced applications such as deep learning enhance Cloud computing threat detection by analyzing big data in real-time and tracing risky activities. These models can analyze and detect suspicious and insecure activities, violations or unauthorized access. They can learn from data, how to identify new threats and trends. Self-supervised heuristics and behavioral methodologies are capable of identifying threats completely and improve safety features to safeguard important data in intricate cloud networks (Rane, 2024).

1. **Security Threats Detection in Cloud Environment**

The adoption of cloud computing services has in recent years become widespread, and this has introduced a number of security risks pertaining to cloud structures. While organizations transmit their most sensitive processes and application workloads to the cloud, information protection, privacy, and accessibility of cloud services and data become essential priorities (Bashir et al., 2022). Security analysis concerning cloud environments is necessary to address the challenges that may threaten cloud structures and their general safety. These threats can be external, such as hackers and virus attacks, or internal, such as a disgruntled employee or misconfiguration. Machine learning and deep learning are also useful in threat detection because of their great ability to analyze vast amounts of data to distinguish abnormal cases (Sharma & Kumar, 2021). These methods can process network traffic, inspect user behavior, and system logs, discovering threats in time and minimizing the time of attacks Furthermore, leveraging artificial intelligence for real-time threat analysis ensures improved response mechanisms, particularly in dynamic and large-scale cloud environments. Cloud computing, specifically real-time analysis, is vital in the protection of all business and private clients (Aslan, 2023).

**Fig. 1. Detection in Cloud Environment**

1. **Literature Review**

This section presents an overview of recent studies that explore the application of deep learning techniques for detecting security threats in cloud environments. With the increasing complexity and volume of data being processed in cloud systems, traditional security measures are often insufficient in identifying sophisticated cyber threats. Researchers have turned to deep learning models due to their ability to analyze large datasets and detect hidden patterns that may indicate potential risks. This literature review focuses on the key contributions made in the last few years, specifically between 2018 and 2023, that highlight the role of deep learning in enhancing cloud security. These studies emphasize various deep learning techniques, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders, for improving the detection and mitigation of threats, including unauthorized access, data leakage, and DDoS attacks.

**Nassif, A. B., et al., 2021,** The research forced to look at how cloud security can utilize ML since modern threats that are becoming recurrent include unauthorized access, malware, and data breaches. Cloud environments are challenged with dynamic threats that conventional aspects of IDS cannot address in real-time environments. To address this, the study analyzed past research on ML-based approaches, using such categories as supervised learning, classification, and anomaly detection. The review showed that the decision trees, support vector machine, and deep neural network, demonstrate good possibilities to work for the anomaly’s identification and data leakage prevention. On the topic of threat detection, the authors also noted the rising trend for the integrated application of multiple ML approaches. This work highlighted on real time threat sensing and the use of hybrid machine learning in cloud security. These considerations suggest the need for future work in applying and generalizing these approaches and methods, its application in hybrid structures and stochastic modeling (Nassif, 2021).

**H, Arif., et al., 2024,** The study was centered on the application of AI techniques, especially on improving the threat identification function in cloud infrastructure, and the development of the security models that transition from the reliance on the receipt of security incident notifications and simple security gauges to the active creation of the defenses that would prevent security threats and vulnerabilities from becoming threats in the first place. This work was inspired by the rising sophistication and diversification of threats that are target cloud-based platforms and none of the traditional approaches can handle them well. The authors discussed Deep learning, reinforcement learning besides Anomaly detection, to address adversarial risks. They also focused on potential of deep learning models which can handle big amount of data and detect new threats successfully. The research also explored the issues related to deploying AI in cloud solution such as computational intensity, interpretability of the model, and security concerns. This paper can be referred as a fundamental material in terms of the promotion of self-learning based on AI structures with potential for independent recognition of new risks and improving the reliability and credibility of cloud computing security (Arif, 2024).

**Butt, U. A., et al., 2020,** The paper aims at analyzing the use of ML to improve the security of data centers in clouds. The authors’ purpose is to provide a solution to the emerging problem of threat identification and protection in weak cloud environments. Increasing cloud solutions usage results in complex threats like data loss, virus attacks, unauthorized access, etc. A variety of ML models such as supervised models; decision trees, random forests, K-NN, and unsupervised models; clustering, and anomaly detection are discussed in the study. It identifies these algorithms for assessing their capacity to identify security threats in cloud systems. The authors note that more use of ensemble learning and other hybrid models is noted due to the efficiency and better detection rates those models provide. The study establishes the need for incorporating the ML algorithms as techniques into cloud security architectures for minimizing human interaction while improving the real-time detection. It also emphasizes the desire to explore deeper the application of real-time DDos detection and mitigation (Butt, 2020).

**Shamshir band, S., et al., 2020,** aimed at the analysis of CI approaches for improving of Intrusion detection and prevention in M CC environments. This research was triggered by the susceptibility of mobile cloud systems to attacks including denial of service, unauthorized access, and malware because of the mobility of the devices and the networks. The authors therefore gave an overview of CI techniques such as artificial neural networks, fuzzy logic, genetic algorithm and some advanced deep learning intelligence such as CNNs and RNNs. The above-mentioned methods were assessed using the number of discoveries of the various types of attacks achieved by way of each method. There was great emphasis on the general possibility of the integrated systems that precipitate the use of multiple ways of increasing detection efficacy and parameters. In his work Shamshir band et al sampled deep learning as efficacious in capturing intricate attack patterns, and they area recommend that more should be done to explore the combined models and dynamic time attack detection systems to confront the emergent threats in the mobile cloud (Shamshirband, 2020).

**F. Jauro, et al., 2020,** focused on looking at the role of deep learning (DL) architectures in improving security in the next generation cloud computing paragon. As cloud infrastructures go further into areas like EC and IoT, conventional security solutions cannot adequately confront threats. This work targeted the use of the advanced techniques in DL such as CNN, LSTM and GAN for threat identification and cloud security enhancement. The paper reviewed various issues that are implemented and applied in DL solutions; privacy, computation and interpretation. Comparing DL architectures, CNNs and LSTMs showed high results in using advanced security threat patterns and diagnosing large scale data systems. Hence, the study focused on features combination from various models of DL to improve the system security. Finally, it stressed the importance of enhancing the work in the development of practical and practical results of applying DL-based security concepts for the modernized cloud structures (Jauro, 2020).

**Alsoufi, M. A., et al., 2021,** The authors’ goal was to keep up with the growing insecurity of IoT systems that are increasingly being attacked by cybercriminals. In the case of the study, the researchers focused on deep learning algorithm performance in enhancing the anomaly-based IDS in IoT systems. Considering increasing number and scale of IoT networks, traditional methods of IDS do not suffice and more sophisticated methods are needed. To this end, the authors undertook a systematic review of a pool of more than 50 articles that were published between 2010 and 2020 to assess the effectiveness of deep learning models including neural networks and auto encoders in IoT security. There is a review of how CNNs and RNNs can be used as the models for moving anomaly detection with high accuracy, particularly at large-scale data. The study focused on deep learning’s capability in learning new threats but also pointed out some of the weaknesses majoring on interpretability and scalability of the model to the bigger environment hence the call for more research in the given fields (Alsoufi, 2021).

**Kasula, V. K., et al., 2024,** The research intended to create an AI type security model that could help defend cloud infrastructure against data breaches and other security challenges. Classical models of cloud protection do not suffice to track threats in real-time and require more sophisticated ones. The study made an effort to develop an overall design of using machine learning and deep learning concepts as a tool for improving the security of a cloud system through elements like anomaly detection, pattern recognition as well as threat intelligence. The authors examined the practicability and utility of the framework through simulations in actual cloud services situations. The results also showed that the suggested AI-based algorithm outperformed the traditional security approach in detection effectiveness, minimal false alarms, and shorter response times. It is indicated that the threat detection models should be developed taking into account that they require frequent updates due to emerging security threats. This work stresses on the synthesis capability of AI that has the potential to create optimal, resilient and efficient Cloud Security Frameworks (Kasula, 2024).

**Al-Mhiqani, M. N., et al., 2020,** The research focuses on the identification of insider threats in the framework of organizational IT and cloud security and underlines the importance of incorporating ML solutions into combating ineffective traditional detection methodologies. In this paper, malicious insiders, accidental insiders and privileged insiders play an important role in the view of growing concern regarding the potential harm of the insiders. The review organizes the detection techniques such as decision tree, support vector machine and deep learning algorithms including auto encoder. It also discusses datasets that are available to the public and a private database, pitfalls concerning the quality of data, feature extraction and detection techniques’ effectiveness. To enhance threat detection goal, the authors make a point of showing that using both supervised and unsupervised learning is the best strategy. The study also reveals challenges ML can confront, such as minimal model interpretability and inadequate data quality, in addressing insider threats. Such future work should aim at scalability of the ML models to address the dynamic nature and new tactics by insiders and effective integration into real-world systems (Al-Mhiqani, 2020).

**Asharf, et al., 2020,** identify the potential of ML and DL in improving IDS in IoT networks. This research focuses on security threats from these IoT devices, devices which are invariably dynamic and resource-limited, in that the approaches to intrusion detection as described above will not suffice. The authors give a detailed explanation of the various forms of ML and DL techniques including decision trees, neural network, and deep reinforcement learning in relation to the ability to detect intrusions. In this review, CNN and RNN are considered efficient to detect IoT-based intrusion as these algorithms can handle big data and patterns of attacks. A way, the work highlights the need to select the right features and dataset when trying to achieve the best detection rates. This highlights that future recommendations major on enhancing the training and handling new attacks and the use of different hybrid models which incorporate other ML algorithms in the defense of IoT devices (Asharf, 2020).

**Lansky, J., et al., 2021,** The study aimed at enhancing the understanding of the effectiveness of DL-IDS in enhancing the possibility of identifying security violations and unlawful intrusions in computer networks. The research was initiated with a view of arresting the problems IDS is prone to in dealing with emergent and intricate threats not easily dealt with by standard techniques. It compared performance of the different types of DL models that have been used in IDS, including CNNs, RNNs, and DNNs with regard to their capacity in detecting intricate attack patterns and minimizing false alarm rates. The review compared IDS datasets and assessment criteria and revealed that DL can further improve upon detection efficiency and address complex threats. However, the study also pointed out the following limitations; large amount of labeled data is required, and the proposed models do not give much understandable information. The authors proposed the lines of future work in which scalability, interpretability, and imbalance datasets of DL-based IDS should be further addressed in order to improve the overall performance of the proposed IDS in real-world applications-related scenarios (Lansky, 2021).

**Table 1. Comparative study of related work**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Authors (Year)** | Dataset | **Algorithms or Techniques** | **Result** | **Pros** | **Cons** |
| Nassif, A. B., et al. (2021) | Public datasets like NSL-KDD, CICIDS2017, and CAIDA for cloud security. | Supervised learning, Decision Trees, Support Vector Machine (SVM), Deep Neural Networks (DNN) | Real-time anomaly detection and data leakage prevention. Hybrid ML approaches show good results. | Focuses on real-time threat sensing and hybrid ML in cloud security. | Limited direct dataset usage, requires more generalized application of ML methods. |
| Arif, H., et al. (2024) | Simulated datasets using cloud-based security environments. | Deep learning, Reinforcement learning, Anomaly detection | Promoted AI-driven security models to prevent threats in cloud infrastructure. | Highlights the potential of AI for autonomous threat identification and mitigation. | Computational intensity, interpretability issues in AI models, and security concerns. |
| Butt, U. A., et al. (2020) | Cloud-specific datasets like Cloud Sim, Cloud Security Sim. | Supervised (Decision Trees, Random Forests, K-NN), Unsupervised (Clustering, Anomaly Detection) | Improvement in real-time threat detection in cloud systems using ML models. | Emphasizes hybrid ML models for better detection rates and real-time threat mitigation. | Lacks clarity on the specifics of datasets used, focus on hybrid models but needs deeper exploration of real-time DDoS. |
| Shamshirband, S., et al. (2020) | IoT datasets such as TON\_IoT and IoT-23. | Artificial Neural Networks, Fuzzy Logic, Genetic Algorithms, CNNs, RNNs | Enhanced detection of complex attack patterns in mobile cloud environments. | Focus on integrating multiple CI techniques for higher detection efficacy. | Lacks detailed comparison of performance metrics; scalability concerns in mobile cloud environments. |
| Jauro, F., et al. (2020) | Public datasets including UNSW-NB15 and CICIDS2018. | CNNs, LSTMs, GANs | Advanced detection of complex threats in cloud security using deep learning architectures. | Focus on deep learning models to enhance security and threat identification. | Privacy, computation, and interpretability concerns for deep learning models. |
| Alsoufi, M. A., et al. (2021) | IoT anomaly detection datasets such as TON\_IoT. | Deep learning models, Neural Networks, Autoencoders | High accuracy in anomaly detection for large-scale IoT networks using deep learning models. | Highlights effectiveness of CNNs and RNNs in IoT anomaly detection. | Interpretability issues, challenges in scaling models for larger environments. |
| Kasula, V. K., et al. (2024) | Synthetic cloud datasets created using simulation tools like Cloud Sim. | Machine learning, Deep learning, Anomaly detection, Pattern recognition | AI-driven models outperform traditional security approaches in cloud security detection. | AI integration offers effective, resilient cloud security frameworks with real-time threat detection. | Frequent updates needed for dynamic cloud threats, lacks clear description of dataset. |
| Al-Mhiqani, M. N., et al. (2020) | Insider threat datasets such as CERT insider threat dataset. | Decision Trees, SVM, Autoencoders | Hybrid ML approaches improve insider threat detection. | Focuses on insider threats (malicious, accidental, and privileged). | Insufficient dataset details, scalability and data quality issues in practical use. |
| Asharf, et al. (2020) | IoT network datasets like IoT-23 and Bot-IoT. | Decision Trees, Neural Networks, Deep Reinforcement Learning, CNN, RNN | Improved intrusion detection for IoT networks using machine learning and deep learning models. | Efficient handling of big data and attack patterns using CNN and RNN. | Dataset selection and handling new attacks could be improved. |
| Lansky, J., et al. (2021) | IDS datasets including NSL-KDD and CICIDS2017. | CNNs, RNNs, DNNs | Enhanced IDS performance in detecting intricate attack patterns and minimizing false alarms. | Deep learning models show improvement in IDS detection efficiency. | Challenges with large labeled data, interpretability, and real-world scalability. |

1. **Discussion**

The application of deep learning technology to cloud threat detection now becomes a comprehensive shift in blocking advanced threats, which conventional systems in the security management domain failed to address effectively. Hence, this review provides benefits of DL models within large-scale, dynamic cloud infrastructures; flexibility and scalability. CNNs and RNNs really good in perceiving multivariate attack patterns, besides, hybrid models proved to be better with the help of several algorithms. However, shortcomings of data quality, computational intensity, etc., along with the lack of transparency of the models complicates the performance of large-scale implementation. It is essential to solve these problems, especially in deployments for which practicability and interpretability are crucial. In addition, the high frequency and variety of threat types and behaviors that require model adaptations and adequate level of training to remain pertinent to the system. This review also suggests that more close collaborations between academia and the industry are required to create new efficient, understandable, or privatized DL models. Since cloud environments are now fundamental to advanced digital environments, incorporating DL into comprehensive security will be crucial. As such, to fill these gaps future studies should incorporate emerging techniques such as federated learning and interpretable AI in DL-based cloud security systems.

Some of the gaps include: Since many extensions of hybrid models have not been systematically explored, this is an area of emphasis that has been rather neglected; Currently, there is no well-defined agenda for hybrid model capacity enhancing; Despite the fact that research is awash with hybrid models, there are no specific approaches for dealing with the plethora of types of data and data complexity that is now becoming increasingly apparent. Therefore, further research should aim at filling these gaps apart from also reviewing ways of enhancing the interpretability of models as well as reducing the complexity of computations.

On a broader level, the findings have implications of increasing the demand for the dynamic adaptive, and self-organizing cloud security driven by DL. Indeed, in the face of persistent threats, the available threats in the cyber arena, cloud protection also has to progress. This implies that there is a need for change not only at the technology level but also at the ethic and societal levels whereby requirements like privacy and open regarding matters concerning use of AI system for decision making.

DL is emblematic of the proactive and innovative possibilities for cloud security, which constitute the initial stage toward developing sophisticated, robust, and optimized protective solutions. To unlock this opportunity, attention needs to turn to the creation of broad sets of data assets, the fine-tuning of hybrid architectures, and the complex challenges of explainable AI. All these elements will be integrated into the further development of DL-based cloud security and will serve as adequate protection against constantly emerging threats.

1. **Conclusion**

This review presents DL as crucial in dealing with changed and complicated challenges within the cloud systems. Future statistics reveal that the novel DL architectures like CNN, RNNs, and even the combination of both CNN-RNN have exceptionally high performance when it comes to identifying complex and varied sophisticated threats. Such models have one significant advantage in terms of the scale of data, the complexity of attack patterns, and new threat types. It is these attributes of DL that has placed it at the center of state-of-the-Art cloud security frameworks.

However, the analysis also reveals crucial issues threatening the applicability of DL-based approaches at the same times. Some of the limitations include problems of dimensionality which the models cannot handle well, and there is little research done on explaining the decisions made by these complex structures. Furthermore, the critical importance of high-quality datasets is revealed as one of the key concerns that indicate that DL models need high quality, relevant and up to date data to detect the threats properly.

The work suggests applying DL complementing it with features like anomaly detection and real-time feedback to improve IDS and other security technologies. However, hybrid models seem to have potential over existing approaches in that they can utilize the strengths of all these different techniques to enhance the detection rate as well as make the approaches more immune to current constraints. In addition, there is the urgent need to embrace models that can accommodate the continuing expansion of data as well as the speed at which it is being generated in the cloud.

**Disclaimer (Artificial intelligence)**

Option 1:

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

Option 2:

Author(s) hereby declare that generative AI technologies such as Large Language Models, etc. have been used during the writing or editing of manuscripts. This explanation will include the name, version, model, and source of the generative AI technology and as well as all input prompts provided to the generative AI technology

Details of the AI usage are given below:

1.

2.

3.

# References

Abdulsalam, Y. S. (2021). Security and privacy in cloud computing: technical review. , Future Internet, 14(1), 11.

Alduailij, M. K. (2022). Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method., Symmetry, 14(6), 1095.

Ali, T. E. (2023). Machine learning techniques to detect a DDoS attack in SDN: A systematic review. , Applied Sciences, 13(5), 3183.

Alkadi, O. M. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks., IEEE Internet of Things Journal, 8(12), 9463-9472.

Al-Mhiqani, M. N. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations., Applied.

Alouffi, B. H. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. , Ieee Access, 9, 57792-57807.

Alsoufi, M. A. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review., Applied sciences, 11(18), 8383.

Arif, H. K. (2024). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research., International Journal of Multidisciplinary Sciences and Arts, 3(1), 242-251.

Asharf, J. M. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. , Electronics, 9(7), 1177.

Aslan, Ö. A.-O. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. , Electronics, 12(6), 1333.

Bertoli, G. D. (2021). An end-to-end framework for machine learning-based network intrusion detection system., IEEE Access, 9, 106790-10.

Butt, U. A. (2020). A review of machine learning algorithms for cloud computing security., Electronics, 9(9), 1379.

Fatani, A. D.-Q. (2021). Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system. , Sensors, 22(1), 140.

Gupta, I. S. (2022). Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions., IEEE Access, 10, 71247-71277.

Halbouni, A. G. (2022). Machine learning and deep learning approaches for cybersecurity: A review. , IEEE Access, 10, 19572-19585.

Inayat, U. Z. (2022). Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. , Electronics, 11(9), 1502.

Jauro, F. C. (2020). Deep learning architectures in emerging cloud computing architectures: Recent development, challenges and next research trend. , Applied Soft Computing, 96, 106582.

Kasula, V. K. (2024). Fortifying cloud environments against data breaches: A novel AI-driven security framework. , World Journal of Advanced Research and Reviews, 24(01), 1613-1626.

Kommisetty, P. D. (2024). AI-Driven Enhancements in Cloud Computing: Exploring the Synergies of Machine Learning and Generative AI.

Lansky, J. A. (2021). Deep learning-based intrusion detection systems: a systematic review., IEEE Access, 9, 101574-101599.

Macas, M. W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. , Computer Networks, 212, 109032.

Mijwil, M. M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. , Iraqi Journal For Computer Science and Mathematics, 4(1), 10.

Nassif, A. B. (2021). Machine learning for cloud security: a systematic review., IEEE Access, 9, 20717-20735.

Olateju, O. O. (2024). Combating the challenges of false positives in AI-driven anomaly detection systems and enhancing data security in the cloud., Available at SSRN 4859958.

Rabbani, M. W. (2021). A review on machine learning approaches for network malicious behavior detection in emerging technologies. , Entropy, 23(5), 529.

Rane, J. M. (2024). Artificial intelligence, machine learning, and deep learning in cloud, edge, and quantum computing: A review of trends, challenges, and future directions. , Future Research Opportunities for Artificial Int.

Shamshirband, S. F. (2020). Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. , Journal of Inf.

Tsimenidis, S. L. (2022). Deep learning in IoT intrusion detection. , Journal of network and systems management, 30(1), 8.

Bashir, A., Zafar, M., & Khan, H. (2022). Machine learning applications in cloud security: A comprehensive review. Journal of Cloud Security Research, 15(3), 123–135.

Sharma, P., & Kumar, R. (2021). Artificial intelligence-driven threat detection in cloud environments. International Journal of Cloud Computing and Security, 9(2), 87–99.

Zhang, L., Chen, Z., & Li, J. (2023). A deep learning-based approach to security in cloud computing environments. International Journal of Cloud Computing and Security, 11(4), 255–268.

Liu, Y., & Zhang, H. (2022). A review of machine learning and deep learning techniques for cloud security. Journal of Cloud Security Studies, 8(2), 137–150.