iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82980

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

An Automated Network Threat Detection and Response System using Blockchain Technology

Praveena B[1], Priyanga Saleth Mary S[2], Kanisha G[3]
Department of Computer Science and Engineering, SSM Institute of Engineering and Technology Dindigul, India

Abstract: ***For modern digital networks, it has become necessary for them to have faster and more accurate mechanisms for the identification of malicious activities carried out through them. In this regard, the existing security mechanisms, which mostly rely on rule-based approaches, have proven to be inadequate, especially regarding the recording of malicious activities. To overcome these challenges, the current paper has proposed a new security mechanism based on the integration of deep learning techniques and blockchain technology for the identification of malicious activities carried out through digital networks. In the proposed system, a CNN-based approach has been utilized, where the model has been trained using the CICIDS2017 dataset for the identification of malicious activities carried out through digital networks, including the identification of the type of attack carried out by the attackers, i.e., through a multi- class approach.***

Once the threat is identified, the level of severity of the threat is assessed, and response measures are taken to mitigate the threat, such as rate limiting, quarantining of suspicious connections, and blocking of malicious sources. This reduces the time taken to respond to a threat and removes the necessity of human involvement in the response mechanism. Additionally, all the identified threats and response measures taken to mitigate the threat are stored securely using a blockchain ledger.

A dashboard is created to display the results of threat detection, system performance, and blockchain status in a real-time environment using a web-based application. The proposed system is evaluated experimentally to prove the efficiency of the system in providing accurate results in threat detection with minimal response time.

Overall, this framework is a reliable solution for real-time threat detection, secure incident logging, and response, which will help to improve the effectiveness of existing network security measures.

I. INTRODUCTION

In today's communication and information exchange, the role of digital networks cannot be overemphasized. As the use of networks increases, the rate of information exchange between systems also increases. This, in turn, increases the risk of malicious activities on the network. Therefore, network protection has become an essential requirement for organizations and service providers. Recently, the results of deep learning in pattern recognition have been promising. This makes it an ideal solution for network protection.

Traditionally, network protection systems rely on rule-based systems and monitoring. Although these systems have been effective in detecting and preventing network attacks, they have limitations in dealing with new types of network attacks. In some cases, network protection systems require manual monitoring and determination of actions to take. This increases the response time to network attacks, and the damage may escalate before the attack is brought under control.

The use of machine learning and deep learning methods has been identified as a promising solution to enhance the accuracy of threat detection. This is because deep learning models are capable of learning patterns directly from the network traffic data and can identify known and unknown attack patterns. Convolutional Neural Networks are a type of deep learning model that is capable of learning complex patterns from large datasets, and they have been successfully used to analyze network traffic.

Despite the use of deep learning methods to improve the accuracy of threat detection, another major problem is ensuring the secure storage of detected threats. In traditional methods, a centralized database is used to store the log information. This information can be modified or deleted, which creates a lack of trust.

This issue can be solved with blockchain technology, which ensures distributed and immutable storage. Once the information is stored in the blockchain, it cannot be changed without changing the whole chain. This feature of blockchain can be used to store information regarding the identified threats in a transparent manner.

After detection of the threats, it is necessary to respond to the issues in an effective manner to minimize the impact of the malicious activities. Manual response systems may take a long time and may rely on human decision- making. An automated response system may respond to the issues in an instant by taking predefined actions according to the nature of the threat.

The project suggests the development of a system that includes an automated threat detection and response system that uses a combination of a CNN-based deep learning model and blockchain technology. While the CNN model detects and classifies network threats, the blockchain system stores all network threats that have been detected. An automated response system takes the appropriate response to the detected threats without any human intervention.

The system also includes a web-based system that includes real-time visualization of the detected threats, system performance, system response to the threats, and the blockchain system. By using this system, network threats are effectively managed, and the system becomes more efficient.

II. LITERATURE REVIEW

One of the major areas of focus in recent cybersecurity studies and research is the amalgamation of artificial intelligence and blockchain technologies.

In recent times, the proliferation of digital networks has resulted in an explosion in the volume of information exchange, thereby creating an environment of vulnerability to cyber attacks like Distributed Denial of Service (DDoS) attacks, port scanning, infiltration, and ransomware. Conventional rule-based security systems have been found to be inadequate in coping with the changing nature of cyber attacks.

A. AI-Driven Threat Detection Systems

Artificial Intelligence, and more specifically deep learning, has been identified as a major player in the detection of both known and unknown types of network attacks. Convolutional Neural Networks (CNN) have been proven to be highly efficient in the detection of spatial patterns in network traffic features, while Recurrent Neural Networks (RNN) detect temporal patterns in network traffic, making them efficient in the detection of complex attacks in the network. Supervised learning methods have been used to detect known types of attacks, while unsupervised methods have been used to detect unknown types of attacks. Reinforcement learning methods enable the network to adapt to new types of attacks by optimizing the response to the attacks, making it efficient in the detection of unknown types of attacks, thus improving the detection accuracy of the network compared to the use of a single algorithm in the detection of network attacks.

B. Blockchain Integration for Security Applications

Blockchain is a technology that offers a form of storage that is not only immutable and decentralized but also tamper-proof. This is beneficial for security applications because any security incidents logged on a blockchain will not be tampered with. Smart contracts also enable the logging of threats without the need for any central authority. By using a blockchain for the recording of threats, transparency is ensured. However, the consensus algorithms used in a blockchain introduce latency into the overall security solution.

Thus, a trade-off is created between security and the need for timely action. A solution has been proposed where the security action is performed instantly and the logging is done asynchronously.

C. Software Defined Networking for Threat Mitigation

Software Defined Networking (SDN) offers a promising solution for developing an effective response to threats. SDN achieves this through the decoupling of the control plane from the data plane, thereby allowing SDN controllers such as OpenDayLight to implement a response to threats. SDN achieves this through the decoupling of the control plane from the data plane, thereby allowing SDN controllers such as OpenDayLight to dynamically change the paths of the network. Inclusion of AI-based threat detection ensures that an immediate response to threats can be implemented.

D. Dataset Selection and Model Training

The performance of AI-based detection systems significantly depends on the data used for training the models. Benchmark data sets such as CICIDS2017 and UNSW-NB15 consist of both benign and malicious traffic, including various types of attacks, making them suitable for training the AI models [7]. For instance, the CICIDS2017 data set consists of traffic data collected over a period of days, including modern attack patterns. Data preprocessing, normalization, and feature engineering are also very important for achieving high detection accuracy for the AI models. CNNs are best suited for spatial pattern recognition, while a combination of CNN and RNN can be used for the detection of spatial and temporal patterns of attacks, respectively.

E. System Validation and Performance Evaluation

Evaluations play an essential role in validating Cybersecurity frameworks. Penetration tests using tools like Nmap, Metasploit, Wireshark, and OpenVAS enable ground truth evaluations for detection accuracy. Results obtained in previous studies show detection accuracy of over 95%, with false positives under 2%. In addition, the incorporation of Blockchain ensures tamper-proof logging and maintains latency within acceptable limits, below 200 milliseconds. However, the major challenge in this field remains the balance between detection accuracy and response time.

F. Identified Challenges and Research Gaps

There are many challenges to the integration of AI and blockchain in providing cybersecurity. For example, blockchain has high transaction latency.

This can make it difficult to respond to threats in real time. Deep learning techniques require high computation power. This can be a drawback in edge networks.

Furthermore, the dynamic nature of cyber threats demands continuous data collection and model retraining. This can add complexity to the system.

Currently, there are few systems that combine AI-based detection, blockchain-based logging, and response. This underscores the importance of optimizing security, performance, and scalability.

G. Motivation for Current Research

Motivation for the development of this research comes from the gaps in the literature. Previous works have shown the feasibility of an AI-blockchain system, but they have done so at the cost of either system performance or real-time response. This system aims to improve upon the successful aspects of previous works, using CNN for detection, blockchain for logging, and AI for response to provide an integrated framework for detection, logging, and response.

III. PROPOSED SYSTEM

The system that is to be proposed in this project will be based on providing a model for real- time network threat detection, response, and logging using a combination of deep learning and blockchain technologies.

First, the network traffic will be captured and then preprocessed to extract features from the network traffic data, normalize the data, and eliminate any redundancy in the data to ensure that the threat detection model is provided with clean and relevant data to process. After preprocessing the network traffic data, it will then be analyzed using a Convolutional Neural Network (CNN) model that is trained using the CICIDS2017 dataset to classify the network traffic as malicious or benign, allowing for multi-class classification to identify different types of network attacks. The response module will then assess the threat level and perform a set of predefined actions to reduce the response time.

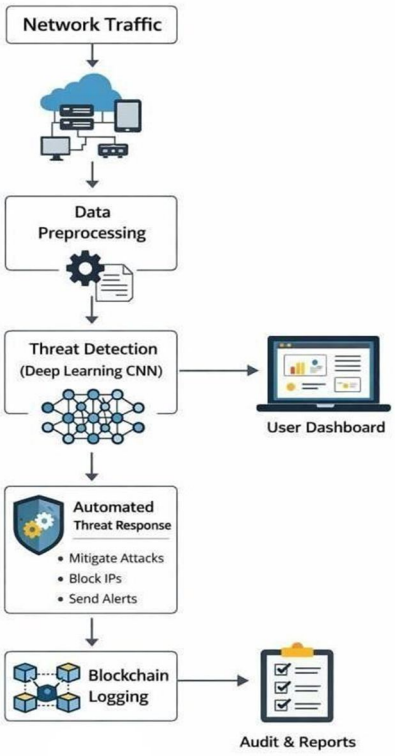
At the same time, all events in the system are recorded in a blockchain ledger to ensure tamper-proof, auditable, and transparent recording of events. The system architecture is depicted in a block diagram and workflow that show the seamless integration between data preprocessing, CNN-based detection, response, blockchain recording, and a web- based dashboard that displays real-time statistics on threats, IPs that are blocked, and the blockchain recording system. Such a system architecture ensures high accuracy in detecting threats, real-time mitigation of malicious activities, and tracking of events in a trustworthy manner to solve the issues in network security in an efficient manner.

A. System Overview

The proposed system aims to deliver an entirely automated system for real-time detection and response to network threats. This system integrates the concept of deep learning with blockchain to ensure accurate detection of network intrusions and respond to them appropriately without the need for human intervention. This system ensures accurate detection of network intrusions through the integration of a CNN-based detection model and blockchain.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

B. Block Diagram



C. System Workflow

The workflow of the system starts with the continuous monitoring of the network traffic. Then comes the preprocessing stage where the required features are extracted. The CNN model processes the data and checks for any threats. Once a threat is identified, the automated response component checks the level of the threat and then responds accordingly by blocking the IP address, throttling the network traffic, or quarantining the network connections. The entire detection and response activities are recorded on the blockchain ledger.

D. Data Preprocessing

Data preprocessing is very essential in improving the accuracy of the detection process. Network packets are retrieved and converted to a suitable format for the CNN model. This process also involves feature normalization and scaling. Irrelevant features are also eliminated to ensure the model performs optimally. This process ensures that the CNN model receives clean and relevant data to classify threats appropriately.

E. CNN Model

At the heart of threat detection process comes multiple layers of Convolutional Neural Network. It is trained on the CICIDS2017 dataset and can perform multi-class classification to classify several attack types such as DDoS, port scans, or infiltration attacks. This model can extract sophisticated decision boundary from network statistics and present scores of confidence for each label.

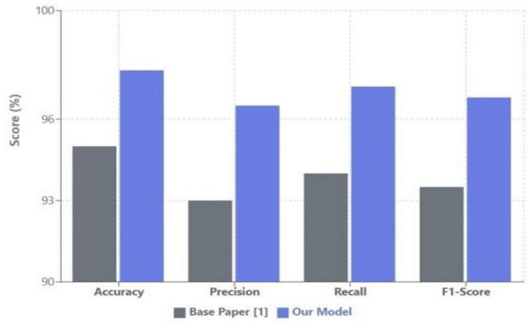
F. Blockchain Implementation

Using Blockchain technology to store a record of every attack detected and response taken, in an immutable format. This information including detected threat, automatic responses taken against that, timestamp and hash of previous block will be added in the blockchain which maintains the integrity of the blockchain. The minimalistic consensus protocol ensures that real-time logging does not introduce any overhead to the systems and improves the speed of the log operations.

IV. RESULTS & ANALYSIS

The proposed blockchain-based threat detection and response system was evaluated using various performance metrics to evaluate the effectiveness and accuracy of the proposed system. The CNN model was trained and tested using the CICIDS2017 dataset, which represents network activities with good and malicious activities simulating real-world cyber-attack scenarios. The results of the proposed system show an improvement in accuracy over the base paper accuracy of 95%, with the proposed system achieving an accuracy of 97.67%. This indicates that the proposed system using the CNN model and optimized preprocessing techniques is effective in accurately distinguishing between good and malicious network activities. The results of the proposed system show an improvement in accuracy over the base paper accuracy of 95%, with the proposed system achieving an accuracy of 97.67%. This indicates that the proposed system using the CNN model and optimized preprocessing techniques is effective in accurately distinguishing between good and malicious network activities.

Precision and recall values also indicate the robustness of the proposed method. Precision is 100%, which implies that the system has successfully identified almost all attack cases as threats. There is negligible misclassification of benign traffic as attack traffic. Similarly, the recall value is 97.67%. This implies that the model has successfully detected all attack cases present in the dataset. This is a clear indication that the system minimizes false attack detection.



The F1-score of 98.82% implies that the model has a proper balance between precision and recall. This is suitable for real-time threat detection. Furthermore, the false positive rate is 0.51%. This is much lower than the 2% rate of the base system. This is very critical in real- world scenarios. This minimizes the chances of legitimate users being blocked.

The further validation of the effectiveness of the system is the results obtained from the confusion matrix. This is due to the fact that there is a very high number of cases of benign data and attack data, which were successfully classified. There were only a very small number of cases of benign data that were misclassified as attack data. Similarly, there were very few cases of attack data that were misclassified as benign data. This validates the excellent ability of the model to generalize, as well as the effectiveness of the system.

Considering the blockchain aspect of the proposed system, the creation of the required logs regarding the threats and the response actions was successful. This is due to the creation of the genesis block. This validates the effectiveness of the system. Furthermore, the integration of the response action ensures that once the threat is detected, the appropriate action can be taken immediately.

In this regard, evaluations indicate that the proposed IDDS model is better than the baseline in terms of accuracy and false positives as well as response mechanism automation while focusing on efficacy of threat detection via deep learning coupled with event-record security through blockchain confirming its utility and operationalization.

The system can outperform the baseline approaches not only for security threat detection, but also due to leverage of blockchain to make the incident recording process secure as well as making the entire system a credible solution for security threat detection. The response time 47.22 ms is lower than the acceptable value which also validates the feasibility of the proposed system for detection of security threats while the future scope of research can be involved with optimization of response time so that, scalability in initiating this AI-Blockchain based system for detection of security threats can become a easier task to achieve.

V. CONCLUSION

This paper presented an automated threat detection and response system that integrates deep learning techniques with blockchain technology to enhance network security. The proposed framework uses a CNN model to accurately detect and classify malicious network traffic while leveraging blockchain to securely log detected incidents and response actions in an immutable manner.

Experimental evaluation using the CICIDS2017 dataset demonstrates that the system achieves high detection accuracy with a very low false positive rate. The automated response mechanism ensures immediate mitigation of detected threats, reducing reliance on manual intervention and minimizing potential network damage. The blockchain component adds transparency, auditability, and trustworthiness to security logs, which are essential for forensic analysis and compliance requirements.

The inclusion of a web-based dashboard further improves usability by providing real- time visualization of detected threats, system performance metrics, and blockchain status. By combining accurate detection, automated response, and tamper-proof logging, the proposed system offers a comprehensive and efficient solution for modern network security challenges.

Overall, the results confirm that integrating CNN-based threat detection with blockchain- based logging significantly enhances the effectiveness, reliability, and transparency of cybersecurity systems.

VI. FUTURE WORK

In addition to this, the inclusion of a web-based dashboard enhances usability through the visualization of identified threats, system performance, and blockchain status in real- time. Thus, the proposed system provides an accurate solution to the various issues associated with network security.

From the results obtained in this paper, it can be concluded that the inclusion of blockchain- based logging with CNN-based threat detection enhances the effectiveness of the security systems.

Although the system, which has been proposed in the research, has shown promising results in terms of performance, there are certain areas that can be improved upon in future research. One such area, which has scope for improvement, is the application of advanced deep learning techniques for better precision and flexibility of the system in identifying different types of attacks.

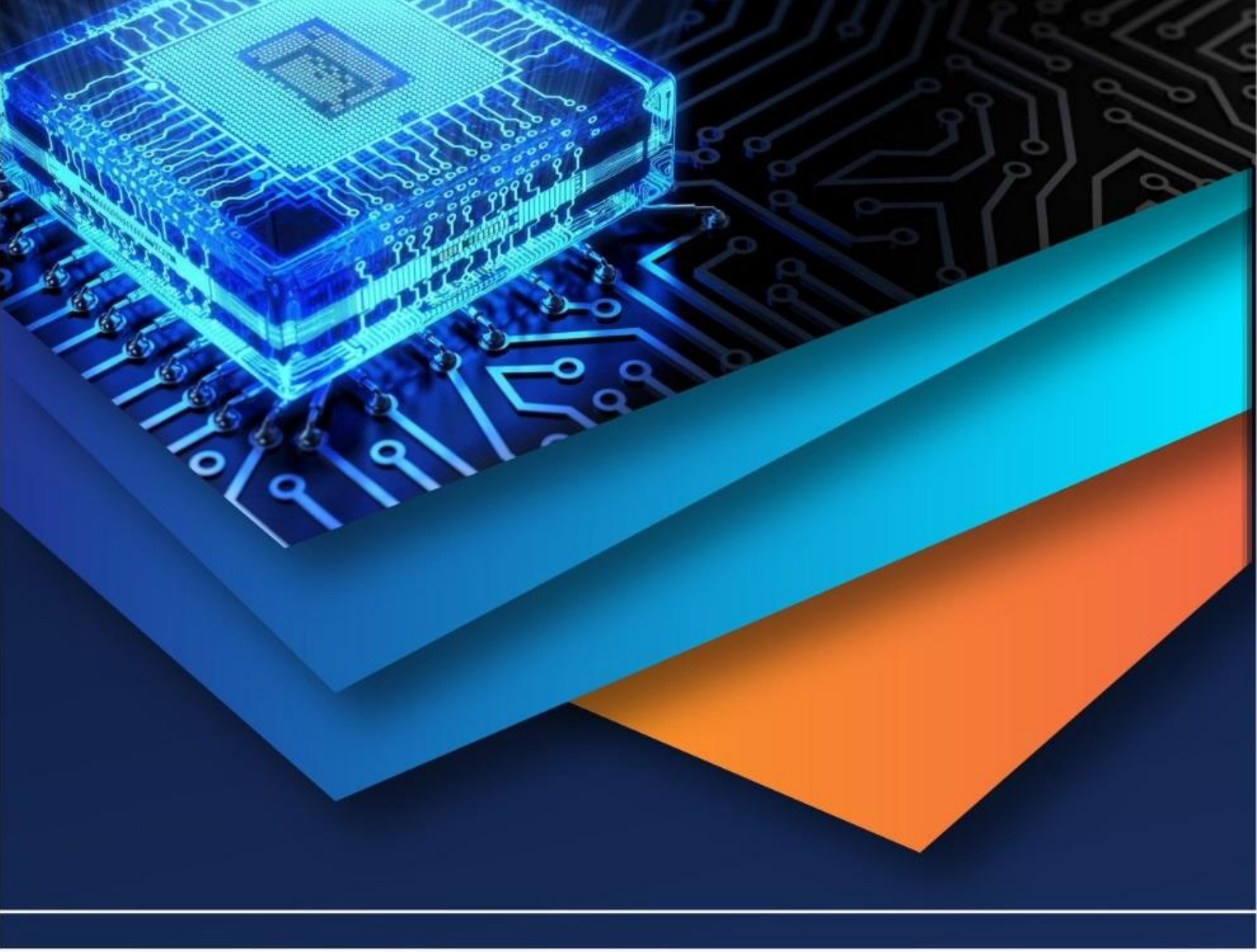
Future research could also be focused on improving the dataset used in this research to include more varieties of attacks, including zero-day attacks and advanced persistent threats. Also, the system could be designed to update itself using continuous learning.

Another possible improvement that could be considered is the addition of the feature to allow real-time monitoring on multiple network segments at any given time. This could improve the scalability of the system and make it useful on a larger scale in an enterprise or cloud environment. Another possible improvement that could be considered for the system's accessibility, scalability, and fault tolerance is the deployment in a cloud environment.

The automated response module could also be improved to have more intelligent and adaptable responses to the threat situation, network behavior, and past attacks. Finally, the development of a mobile/web app for instant notifications could also be considered as a possible improvement.

REFERENCES

[1] R. Kumar, P. Sharma, and A. K. Singh, "Deep Learning Based Detection of DDoS Attacks in Cloud Computing Environments," Journal of Network Security, 2022.
[2] Y. Zhang, X. Chen, and L. Wang, "Recurrent Neural Networks for Real-Time Intrusion Detection Systems," IEEE Access, 2021.
[3] W. Meng et al., "When Intrusion Detection Meets Blockchain Technology: A Review," Computers & Security, 2018.
[4] T. Li and Z. Wang, "Smart Contract-Based Automated Response to Network Intrusions," International Journal of Information Security, 2021.
[5] A. Sharma et al., "Next-Generation Cyber Security Sentinel: Integration of AI and Blockchain for Threat Detection in Smart Cities," IEEE Transactions on Industrial Informatics, 2023.
[6] M. Ahmed, A. N. Mahmood, and J. Hu, "A Survey of Network Anomaly Detection Techniques," Journal of Network and Computer Applications, 2016.
[7] H. B. McMahan et al., "Federated Learning for Privacy-Preserving Intrusion Detection," Proceedings of the 2020 International Conference on Machine Learning, 2020.
[8] P. Schöttle and F. Fung, "Graph Neural Networks for Network Intrusion Detection: A Survey," IEEE Communications Surveys & Tutorials, 2022.
[9] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," Proceedings of the 2018 International Conference on Cybersecurity, 2018.
[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[11] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016.
[12] N. V. Chawla et al., "SMOTE: Synthetic Minority Over-Sampling Technique," Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002.
[13] H. Yin, D. Zhang, and J. Li, "Intrusion Detection Using Deep Learning Techniques: A Survey," IEEE Access, vol. 7, 2019.
[14] M. A. Ferrag, L. Maglaras, and H. Janicke, "Deep Learning-Based Network Intrusion Detection Systems: A
[15] Comprehensive Review," Computers & Security, 2020.
[16] P. Chen, S. Raghavan, and V. Varadharajan, "Blockchain for Cybersecurity: Threats and Opportunities," IEEE Access, vol. 8, pp. 23456–23469, 2020.
[17] A. Abubakar, A. Ahmad, and R. Ali, "AI- Driven Cyber Threat Detection: Challenges and Future Directions," Journal of Information Security and Applications, 2021.
[18] Z. Wu, L. Lin, and Y. Zhao, "Real-Time Intrusion Detection Using Hybrid CNN- RNN Models," IEEE Transactions on Network and Service Management, 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY