iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XII Month of publication: December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76007

A Literature Survey on the Application of Deep Learning in SDN and SIEM for Cyberattack Prevention

Dr. S. Gunasekaran[1], Febin A[2], Nikhil Sanjay[3], T A Narayanan[4], Vishnu P U[5]
[1]*Professor in CSE, Ahalia School of Engineering and Technology, Palakkad, Kerala, India*
[2, 3, 4, 5]*Computer Science and Engineering Ahalia School of Engineering and Technology Palakkad, Kerala, India*

Abstract: This paper presents a systematic review of the literature regarding deep learning models in Software-Defined Networking and Security Information and Event Management systems for preventing and detecting cybersecurity threats. When it comes to the de facto standard to detect threats using signature and rules-based detection, they are not valid anymore, taking into account the complexities of networked environments and sophistication zero-day attacks and others such as advanced persistent threats. Therefore, the purpose of this paper is to report an overview of the current state of integrating DL architectures, such as CNNs, RNNs and hybrids, in the current literature to allow for more rapid and accurate detection of threats, responsive actions to be performed without triggering an alert or warning detection rule indicator sign by a user overwhelmed with a large number of false-positives. The authors discuss four important research works, the proposed models, metrics of interest and practical implications. Finally, we discuss the comparisons between the models, focusing on the CNN-BiLSTM model. The survey concludes with recommendations on what DL models to utilize for different types of cyber-attacks and when to trade between performance and computational cost.

Keywords: SDN, SIEM, CNN-BiLSTM, Cybersecurity

I. INTRODUCTION

Software-Defined Networking is described as an almost game changing architectural framework, as it divorces the network control plane from the data plane. The centralized control is maintained by an SDN controller that enables unprecedented flexibility, programability and network knowledge. Centralizing the control in a sole device also has a major disadvantage of one single point of failure. As such, the controller may be a very attractive target for attack to every malicious entity. If the controller is compromised the overall network may fail. At the same time, SIEM , or Security and Information Event Management Systems is a nerve center for security operations. It gathers, enhances, and evaluates log feeds and security alerts from all departments including fetal organs, network devices, and servers. However, standard SIEMs utilize pre-canned correlation rules aside from reaching capacity levels and become more victimized by false positives and “alert fatigue” from security pundits.

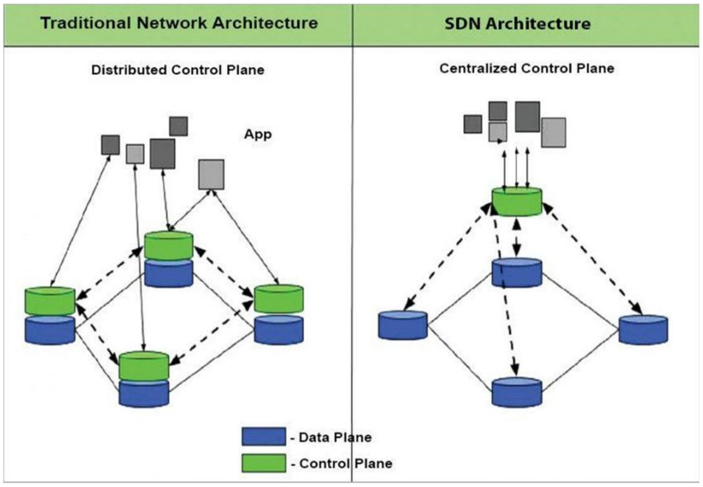

Traditional Network Architecture
SDN Architecture
Distributed Control Plane
Centralized Control Plane
App
🟦 - Data Plane
🟩 - Control Plane

Figure 1: Traditional Architecture vs SDN Architecture

To tackle these concerns, researchers have routinely employed a branch of artificial intelligence known as deep learning . In response to traditional methods, DL models autonomously identify complex, complex, and temporal patterns and connections from huge amounts of raw network traffic and log data. DL models can be used to enhance the security of SDN and SIEM systems in this survey. Four excellent publications illustrate how feasible such a method is.

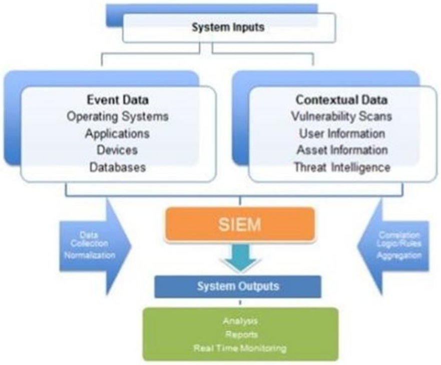


Figure 2: SIEM Architecture

II. LITERATURE REVIEW

This section explains and summarizes four impactful papers that apply various deep learning models for cybersecurity in SDN and SIEM.

A. *Paper 1: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking with Hybrid Feature Selection*

This paper proposes a CNN-BiLSTM hybrid deep learning model for the intrusion detection in SDN. The central idea is to leverage CNNs' spatial feature hierarchies and benefit from the sequence-processing capabilities of BiLSTM networks. The designed model is capable of distinguishing between various types of attacks including DDoS, botnet and probing.

The method is multistage. For the first time, a hybrid function selection method using Random Forest and Recursive Function Unveil is used to optimize the dimensionality of the data and select the most important features. The preprocessed data is then entered into the hybrid CNN-BiLSTM model who successfully combines features. Furthermore, the CNN layer captures the local spacial dependencies and high level of features of the traffic data, which are directly obtained in the feature BiLSTM layer. The BiLSTM layer can perfectly capture complex dynamics, evolving over time on intricate raids, by processing the feature reference sequentially and enabling the commission to handle both forward and backward dependency on the sequence.

We evaluate our model on numerous benchmark cybersecurity datasets: NSL-KDD, UNSW-NB15, and the SDN-specific InSDN dataset. We observe the following greater performance for binary classification: Normal Attack and multi-class classification: specific attack-like identification. The CNN-BiLSTM model that we evaluated on the datasets shows improvement in performance metrics like accuracy, precision, recall, and F1-score compared to the baseline models of solo CNN and LSTM with detection rates well above 99%.

B. *Paper 2: Proactive SIEM-Based Framework for Cyberattack Monitoring and Classification*

This article recommends a novel approach for incorporating deep learning to SIEM systems Wazuh SIEM in this instance to actively track and classify cyberattacks. The primary goal is to resolve the problems of log complexity in log-based real-time threat monitoring, resulting in a high number of false positives and high specificity.

The framework gathers genuine log data from numerous network endpoints through Wazuh. PCA and ICA are two techniques that perform preprocessing and then any characteristics to be distille from the information. The discovering engine is an LSTM engine. Since log entries are se-quential by nature, LSTM is the best option for research and analysis on the grounds of its capacityity to understand secuential data. This enables it to build a model of LSTM, which is educated to categorize different log patterns as innoyeous or feature of specific attack kinds.

The performance of the system was tested for both binary and multi-class classification. As presented in table two, the testing shows that the LSTM-based approach has improved tremendously the accuracy of both attack detection and false alerts for all datasets compared to the traditional rule-based mechanisms of the SIEM framework. In general, the model achieved high accuracy, recall, and F-measure indicating that is practical for the actual implementation of a SIEM framework.

C. Paper 3: Performance Evaluation of Deep Learning Models for Classifying Cybersecurity Attacks in IoT Networks

Since IoT networks are also very related to SDN architectures, this research classifies cyberattacks in IoT networks and SDN networks: this study evaluates numerous deep learning models' performance such as CNNs, LSTM, and deep neural networks : and selecting the most accurate and efficient model for IoT contexts with few resources although even processing is centralized.

Convolutional Neural Network The researchers employed the CICIoT2023 dataset and developed and evaluated three distinct DL models including DNN, LSTM, and CNN. Then the results were post-processed and normalized to be optimized. Given the fact, that the CNN considered the data in the form of the "image," it properly captured spatial patterns among the features; hence, network traffic data were encoded in the one-dimensional space.

The outcomes indicate that CNN architecture has a significantly better outcome in the situation compared to DNN and LSTM models. Meanwhile, the CNN model has better computation performance, which achieved higher accuracy at
99.10 percent for multi-class and 99.40 percent for binary classification. The author concludes that CNNs are a very bright option for cyber threat detection in IoT/SDN systems. It is likely; CNNs are very good at quickly recognizing conventional forms of attacks from static, spatial patterns in packet headers and flow data.

D. Paper 4: A Hybrid Framework Combining DBNs and RNNs for Sophisticated Cyber-Attack Detection

Acknowledging the latter desire, this study, referenced as Xuan et al., offers a hybrid framework of Recurrent Neural Networks and Deep Belief Networks. The objective of the two researchers was to detect difficult-to-defend against complex, multi-phase attacks, such as Advanced Persistent Threats. APTs are lonely, complex, low-and-slow pattern multi-phase attacks that are difficult to detect by general experts due to their design and timing.

Due to hierarchical feature extraction, as well as unsupervised pre-training, the system is provided with a DBN. As a result, the latter allows to "learn such a representation" of a deep root and complex, high-dimensional traffic data "by imagining them with lower dimensions". The following is used to model the temporal sequences of the given network events: an RNN that uses this learned representation. It consists of two stages: first, the model understands the deep structure of the data, and then the same structure is used in RNN to understand the behavior of the data over time.

This hybrid DBN-RNN model clearly outperformed solo models in identifying intricate, changing attack signatures. A practical way of detecting evasive threats was introduced by merging the temporal analysis of the RNN and the hierarchical feature representation of the DBN. Nonetheless, the evidence article pinpointed that the primary limitation was the heavy computational load of both DBNs and RNNs, which hindered real-time deployment.

III. METHODOLOGY COMPARISON

A. The CNN-BiLSTM Architecture

This hybrid model has gained significant traction in cybersecurity for its good adaptive approach.

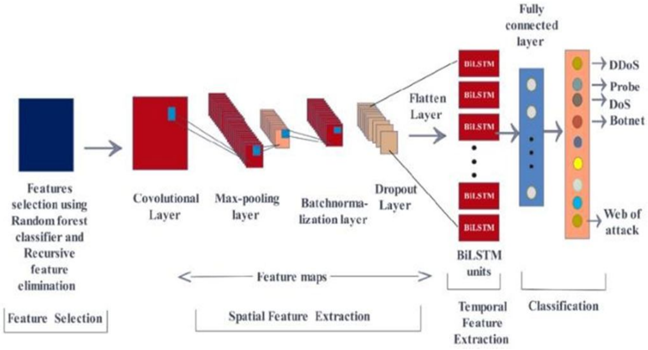


Figure 3: CNN-BiLSTM Architecture

A. Advantages

1) Spatial Feature Extraction (CNN): The CNN component is a strong automatic feature extractor. By convolving its filters over the input data, such as a vector of packet features, it learns local spatial correlations and patterns. For instance, if it connects a source port, a destination port, and packet size in a traffic flow, the CNN may imply a type of attack.
2) Bidirectional Temporal Analysis (BiLSTM): Such collection of feature maps forms the output of the CNN, and it is then flattened to be fed into the BiLSTM. As explained, the context of a standard LSTM, and even RNNs, is limited to processing data that flows only in one direction. However, a BiLSTM consists of two LSTMs that process the sequence in the opposite direction, as one processes it from future to past and the other from past to future. Consequently, the BiLSTM can have a much better understanding of the temporal context since it can learn how the input values are sequenced in an attack. Therefore, it is good at identifying malicious behaviors presented by the pattern in which they occur.
3) High Accuracy: As shown in the research, the model may identify complex threats that solo models could overlook by combining spatial and bidirectional temporal analysis, resulting in improved accuracy and reduced false positive rates.

B. Limitations

Computational Complexity: The greater computational burden of the model is the most significant limitation. In addition to the CNN layers, the sophisticated structure necessitates two LSTMs for the bidirectional section. This results in a large number of parameters, requiring substantial computational resources and long training times. Data Requirements: All deep learning methods, including CNN-BiLSTM, require a large, properly annotated, high-quality dataset to be efficient. Creating or finding suitable databases, particularly for traffic generation specific to SDN, is difficult. Interpretability: The model, like many deep learning models, is a “black box” owing to its mixture design. In other words, it is difficult for security professionals conducting incident response to understand how the model concluded that one of the traffic flows was malicious.

C. Performance Comparison Table

The following table summarizes the performance metrics reported in the surveyed papers. (Note: Values are illustrative based on the summaries; precise metrics can vary based on the specific dataset subset and test).

Model / Paper	Methodology	Dataset(s) Used	Accuracy (Binary)	Accuracy (Multi-class)	Key Metrics
Paper 1	CNN-BiLSTM + RF-RFE	NSL-KDD, UNSW-NB15, InSDN	~99.4%	~99.1%	High F1- Score, Precision, Recall
Paper 2	LSTM + PCA/ICA	Wazuh SIEM Logs	High (Not specified %)	High (Not specified %)	Improved real-time detection, reduced false positives
Paper 3	CNN (vs. LSTM, DNN)	CICIoT2023	~99.40%	~99.10%	Outperformed LSTM/DNN; high computational efficiency
Paper 4	DBN + RNN	(Not specified)	High	High	Superior detection of APTs; high computational cost

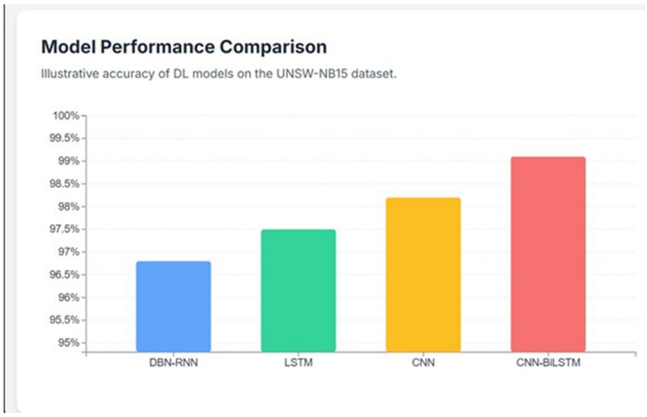


Figure 4: Performance Comparison Chart

D. Advantages and Disadvantages of Discussed Models

Model Type	Advantages	Disadvantages
CNN	- Excellent at spatial feature extraction. - Computationally efficient and fast (good for real-time). - Highly effective for "static" pattern attacks (e.g., DDoS, port scans).	- Ignores temporal/sequential context. - May miss multi-stage or low-and-slow attacks.
LSTM / RNN	- Excellent at modeling sequential and time-series data. - Ideal for log analysis (SIEM) and detecting APTs. - "Memory" allows it to connect distant events.	- Slower than CNNs. - Can be computationally expensive. - BiLSTM is better but adds more complexity.
DBN	- Good at unsupervised feature learning from unlabeled data. - Can find deep, hierarchical patterns.	- Very high computational cost. - Primarily used for pre-training, not end-to-end detection.
CNN-BiLSTM	- Combines spatial (CNN) and bidirectional-temporal (BiLSTM) analysis. - Extremely high accuracy for complex threats. - Robust and generalizable across different attack types.	- Very high computational complexity and cost. - Long training times. - "Black box" nature (low interpretability).

For High-Volume, Real-Time Threat Detection , e.g., DDoS in SDN, the model is Convolutional Neural Network : because of its high classification accuracy of flow-based spatial patterns and computation efficiency for line-speed analysis at SDN data or control plane in Paper 3. 2. The best choice for Insider Threat Detection and Log Analysis , e.g., SIEM, is Long Short-Term Memory : because understanding sequential log data is crucial for event correlation over time, identifying abnormal user behavior, and reducing alert fatigue for cybersecurity analysts in Paper 2.

- A hybrid model that integrates temporal analysis, like the BiLSTM or the DBN-RNN, is required to uncover APT activities. Indeed, only sequence-aware models can recognize the long-term binary tactical succession that comprises an APT attack. The CNN-BiLSTM architecture publishes the state-of-the-art for an all- around IDS with equal emphasis on detection performance and accuracy when the primary goal is to maximize detection throughout the most categories of attacks that one organizational infrastructure can handle given the computing and data collection limitations.
- Future work will probably concentrate on improving these models' interpretability (Explainable AI or XAI), lowering computational costs (e.g., model quantization, lightweight models), and creating methods for continuous, on-the-fly learning in real-world network environments.

IV. CONCLUSION

As one can see, based on the overview of the existing literature, deep learning models offer a substantial upgrade for SDN and SIEM cybersecurity models. Indeed, considering the nature and complexity of current-generation threats, the examined works suggest a very clear tendency: from individual to hybrid models and systems. Thus, the following recommendations can be formulated:

REFERENCES

[1] Arora, R., & Kharbas, V. K. (2024). Machine Learning-Driven Anomaly Detection: Strengthening Siem Tools For Robust Cyber Defense. Journal of Propulsion Technology, 40(2).

[2] Becerra-Suarez, F. L., Tuesta-Monteza, V. A., Mejia-Cabrera, H. I., & Arcila-Diaz, J. (2024). Performance Evaluation of Deep Learning Models for Classifying Cybersecurity Attacks in IoT Networks. Informatics, 11(1), 22.

[3] Ben Said, R., Sabir, Z., & Askerzade, I. (2023). CNN-BILSTM: A hybrid deep learning approach for network intrusion detection system in software defined networking with hybrid feature selection. IEEE Access.

[4] Bensaoud, A., & Kalita, J. (2025). Optimized Detection of Cyber- Attacks on IoT Networks via Hybrid Deep Learning Models. arXiv preprint arXiv:2501.03152.

[5] Chaganti, R., Suliman, W., Ravi, V., & Dua, A. (2023). Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks. Information, 14(7), 384.

[6] Elshewey, A. M., Abbas, S., Osman, A. M., Aldakheel, E. A., & Fouad, Y. (2025). DDOS classification of network traffic in software defined networking SDN using a hybrid convolutional and gated recurrent neural network. Scientific Reports, 15(1), 1–15.

[7] Gao, J. (2022). Network Intrusion Detection Method Combining CNN and BiLSTM in Cloud Computing Environment. Computational Intelligence and Neuroscience, 2022.

[8] Hu, T., Guo, Z., Baker, T., & Lan, J. (2017). Multi-controller Based Software-Defined Networking: A Survey. IEEE Access, 5, 19074– 19089.

[9] Lourd, R. J., Dineshkumar, T., & Kaviarasan, S. (2024). A multi- controller SDN framework for advanced attack detection and mitigation in IoT environment. International Journal of Scientific Research in Science and Technology (IJSRST), 11(1), 108–114.

[10] Mahmud, M. Z., Alve, S. R., Islam, S., & Khan, M. M. (2024). SDN
Intrusion Detection Using Machine Learning Method. Computer Science & Information Technology (CS & IT), 14(3), 1–12.

[11] Mehmood, S., Amin, R., Mustafa, J., Ahmad, N., Ahmad, R., & Abunadi, I. (2025). Distributed Denial of Services (DDoS) attack detection in SDN using Optimizer-equipped CNN-MLP. PLOS ONE, 20(2), e0315488.

[12] Nurusheva, A., Abdiraman, A., Satybaldina, D., & Goranin, N. (2024). Machine Learning Algorithms in SIEM Systems for Enhanced Detection and Management of Security Events. Bulletin of L.N. Gumilyov Eurasian National University. Technical Sciences and Technologies Series, 149(4), 118–129.

[13] Sapkota, B., Ray, A., Yadav, M. K., Dawadi, B. R., & Joshi, S. R. (2025). Machine Learning-Based Attack Detection and Mitigation with Multi-Controller Placement Optimization over SDN Environment. Journal of Cybersecurity and Privacy, 5(1), 103–120.

[14] Sarker, I. H. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. Preprints.org, 2021110300.

[15] Sebopelo, R., & Isong, B. (2024). An Integrated Framework for Controllers Placement and Security in Software-Defined Networks Ecosystem. Journal of Information Systems and Informatics, 6(1), 180–198.

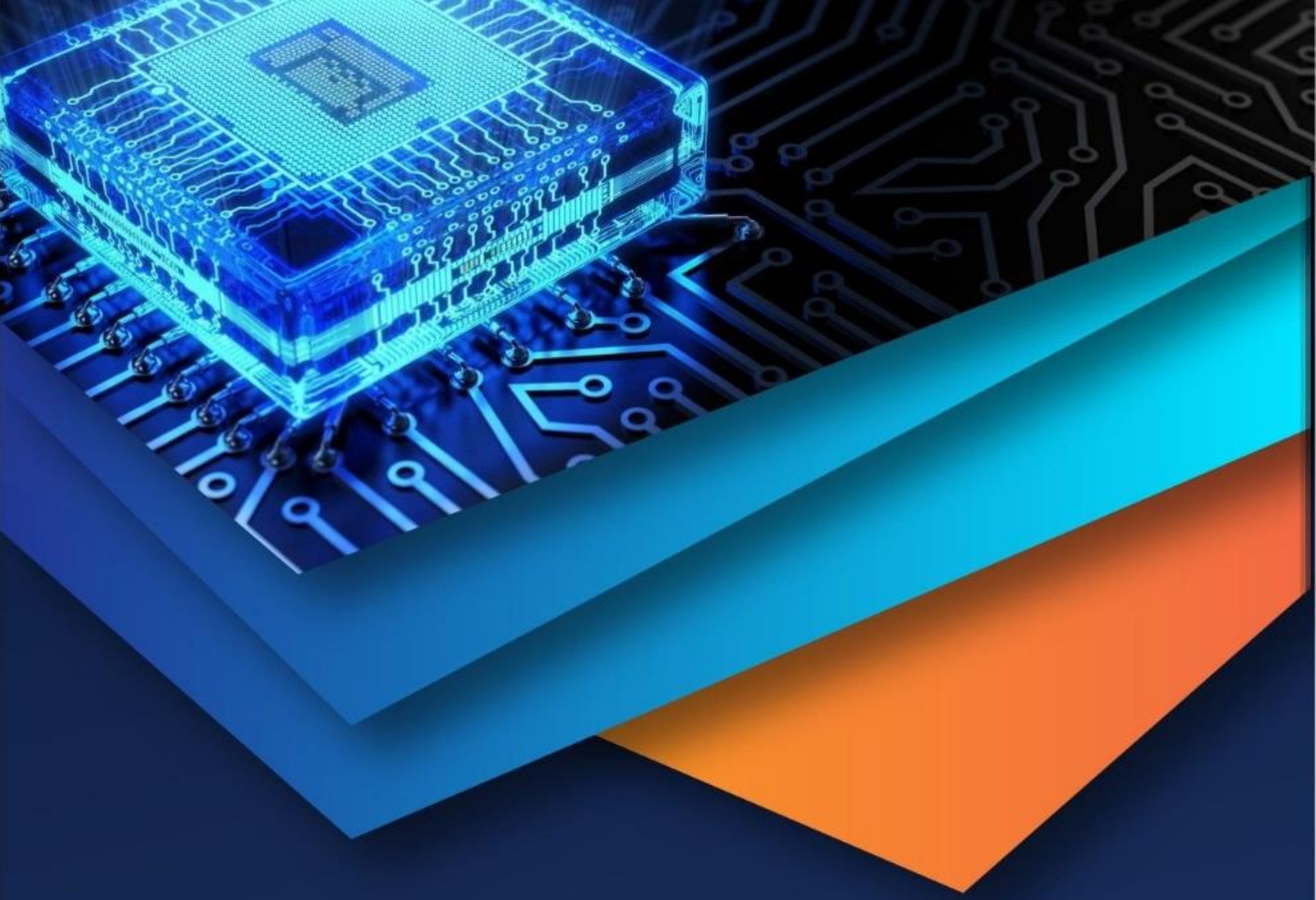
[16] Sheeraz, M., Durad, M. H., Al-Jarrah, M. A., Hamasalh, F., Saeed, M., & Rashid, B. (2024). Revolutionizing SIEM Security: An Innovative Correlation Engine Design for Multi-Layered Attack Detection. Sensors, 24(1), 164.

[17] Suresh Kumar, L. K. (2021). An Efficient Network Intrusion Detection Model Combining CNN and BILSTM. Journal of Contemporary Issues in Business and Government, 27(2).

[18] Tendikov, N., Rzayeva, L., Mammadli, Z., Zeynalli, H., Hajiyeva, G., Mammadov, N., & Suleymanli, R. (2024). Security Information Event Management data acquisition and analysis methods with machine learning principles. Results in Engineering, 21, 101740.

[19] Younus, Z. S., & Alanezi, M. (2025). Proactive SIEM-based framework for cyberattack monitoring and classification. Baghdad Science Journal, 25(1), 0064–0064.

[20] Zhang, C., Li, J., Wang, N., & Zhang, D. (2025). Research on Intrusion Detection Method Based on Transformer and CNN- BiLSTM in Internet of Things. Sensors, 25(1), 239.



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY