iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77528

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 II Feb 2026- Available at www.ijraset.com

Advanced Anomaly Detection in Server Environments against Emerging Cyber-Attack Patterns

V T Ram Pavan Kumar[1], T. Sivaiah[2], Sandaka Yasaswi[3], M. Jahnavi[4], M. Pavitra[5], T. Kethan[6], D. Mohana Krishna[7], Sundarapalli Rajeswari[8]
[1]*Associate Professor, Department of Computer Science*
[2, 3, 8]*II M.Sc. DS*
[4, 5, 6, 7]*II MCA*
[1,2,3,4,5,6,7,8] *Kakaraparti Bhavanarayana College, Vijayawada, Andhra Pradesh*

Abstract: ***With the rapid evolution of cyber threats, traditional security mechanisms often fail to detect novel and sophisticated attack vectors targeting server environments. This research proposes an advanced anomaly detection framework capable of identifying unusual patterns and behaviors in server operations, specifically addressing emerging forms of cyber-attacks. Leveraging machine learning and statistical analysis, the framework continuously monitors server logs, network traffic, and system metrics to detect deviations indicative of potential threats. Experimental results demonstrate that the proposed system achieves high detection accuracy while maintaining minimal false positives, offering a proactive defense strategy against previously unseen attack types. This study contributes to the field of cybersecurity by enhancing server resilience through intelligent anomaly detection and early threat identification.***

Keywords: Anomaly Detection, Cybersecurity, Server Security , Machine Learning, Emerging Threats, Intrusion Detection, Real-time Monitoring.

I. INTRODUCTION

With the increasing reliance on server-based infrastructures in enterprise and cloud environments, the threat of cyber-attacks has grown in both frequency and complexity. Traditional security mechanisms, such as signature-based intrusion detection systems, are often insufficient to identify novel or evolving attack patterns, leaving critical systems vulnerable. Recent advancements in machine learning and deep learning have shown promise in detecting anomalies in complex datasets, including system logs, network traffic, and resource usage metrics. However, existing methods typically focus on either known attack detection or unsupervised anomaly identification, resulting in trade-offs between accuracy and adaptability. To address these limitations, this paper proposes a hybrid anomaly detection framework that combines supervised and unsupervised models, leveraging feature extraction, ensemble learning, and real-time monitoring to detect both known and unknown threats. The proposed approach aims to provide high detection accuracy, low false positives, and real-time alerting, thereby enhancing server security and resilience against emerging cyber threats.

II. LITERATURE SURVEY

Recent advancements in anomaly detection for server environments have focused on leveraging machine learning (ML) and deep learning (DL) techniques to detect emerging cyber-attacks. Srilakshmi *et al.* (2025) proposed an IoT-driven machine learning framework for predictive maintenance, demonstrating the effectiveness of ML models in analyzing complex real-time data streams from industrial systems [1]. Similarly, K. Pande *et al.* (2025) introduced a dynamic security framework for IoT, which improves detection efficiency and reduces vulnerabilities through enhanced security bounds [2]. These studies indicate the increasing role of adaptive ML frameworks in safeguarding interconnected systems.

Security challenges in wireless and IoT networks were addressed by Shaik *et al.* (2025) using physical layer security techniques, tackling eavesdropping and energy constraints [3]. Gaddam *et al.* (2025) focused on AI-based solutions for early detection in healthcare and Dark Web content analysis, demonstrating that deep learning models can detect anomalies in both structured and unstructured data [4], [5]. Gupta *et al.* (2025) applied swarm intelligence and fuzzy clustering to identify intrusive behavior in networks, highlighting hybrid approaches for anomaly detection [6]. Reddy *et al.* (2025) conducted an empirical assessment of deep learning models for predictive analysis, emphasizing the adaptability of AI methods for novel patterns in complex datasets [7].

Earlier studies in 2024 explored both healthcare and server security domains. S. Badonia *et al.* (2024) discussed the challenges of modernizing healthcare systems using 5G networks, stressing the importance of anomaly detection in critical infrastructures [9]. M. Liu *et al.* (2024) provided a comprehensive review of ML-based network anomaly detection techniques, emphasizing their role in reducing false positives and adapting to new attack types [10]. Saygılı *et al.* (2024) developed a server log-based anomaly detection framework, which efficiently detects unusual system behavior in real-time [11]. Srilakshmi *et al.* (2024) introduced regression-based analytics for large-scale data, which can enhance predictive anomaly detection models [12].

In 2023, Wang *et al.* demonstrated that deep learning models for network anomaly detection outperform traditional approaches, providing better recognition of unknown cyber-attacks in server environments [13]. Kotenko *et al.* (2022) combined fractal analysis with machine learning to improve detection of both known and novel attacks, showing that hybrid statistical and AI approaches enhance anomaly recognition [14]. Zhao *et al.* (2021) used LSTM networks for log-based anomaly detection, highlighting the benefits of sequential deep learning for detecting temporal deviations in server activities [15]. Finally, Dutta *et al.* (2020) developed a deep learning ensemble for network anomaly detection, showing early evidence of improved accuracy for multi-type cyber-attacks [16]. This paper presents a low-cost upper-limb rehabilitation device with 3D-printed components, sensors, DSPIC-controlled stepper motors, and a Windows-based system for accurate movement and muscle force monitoring [17]. This work presents a home-based upper-limb rehabilitation robot using a current-controlled buck converter for accurate movement and muscle force assessment, aiding post-COVID-19 recovery. It integrates IoT-based real-time monitoring of vital signs, cloud data storage, and remote doctor access for continuous patient management [18].

Collectively, these studies reveal a clear trajectory in anomaly detection: from traditional statistical and signature-based approaches to adaptive, AI-driven frameworks capable of detecting novel and evolving attack patterns in server and IoT environments. The integration of machine learning, deep learning, and hybrid models provides higher detection accuracy, lower false-positive rates, and real-time monitoring capabilities essential for modern server security.

III. PROPOSED MODEL

The proposed model is a hybrid anomaly detection framework designed to detect emerging cyber-attacks in server environments by combining real-time monitoring, data preprocessing, feature extraction, and machine learning-based anomaly detection. The framework is modular, scalable, and capable of handling large server datasets while adapting to new attack patterns. The main modules of the model are explained below.

A. Data Collection Module

This module continuously collects data from server environments, including system logs, network traffic, CPU/memory usage, and application-level events. It ensures the collection of both structured and unstructured data, which is crucial for detecting complex and unknown attack patterns. Real-time monitoring enables early detection of anomalies before they escalate into critical security incidents. Data is stored in a secure data lake for further processing, ensuring scalability and historical analysis.

B. Data Preprocessing Module

Raw server data is often noisy, incomplete, or inconsistent, which can negatively impact detection accuracy. The preprocessing module handles missing values, normalization, noise reduction, and data encoding. Time-series alignment is applied to sequential data such as logs or network flows. Additionally, categorical features are encoded using one-hot encoding or embedding techniques, while numerical features are normalized to a uniform scale. This step ensures that the machine learning model receives high-quality input for robust anomaly detection.

C. Feature Extraction and Selection Module

This module extracts relevant features that capture server behavior, such as network packet statistics, resource usage patterns, process behavior metrics, and log frequency features. Dimensionality reduction techniques like Principal Component Analysis (PCA) or Autoencoders are applied to remove redundant features and reduce computational complexity. Feature selection ensures that the model focuses on the most discriminative indicators of anomalies, improving accuracy and reducing false positives.

D. Anomaly Detection Module

The core detection module employs a hybrid machine learning approach combining supervised and unsupervised learning techniques. For known attack patterns, supervised classifiers such as Random Forest or XGBoost are used.

For unknown or novel attacks, unsupervised models such as Isolation Forest, Autoencoders, or LSTM-based networks detect deviations from normal server behavior. An ensemble strategy aggregates predictions from multiple models to improve reliability. The output is an anomaly score for each server event, which is compared against a predefined threshold to classify events as normal or anomalous.

E. Alert and Response Module

Once an anomaly is detected, this module generates real-time alerts to administrators and optionally triggers automated mitigation actions, such as isolating affected processes or blocking suspicious network connections. Alerts include detailed information about the type of anomaly, severity, and affected server component. The system also logs detected anomalies to continuously update and refine the detection models, making the system adaptive to evolving threats.

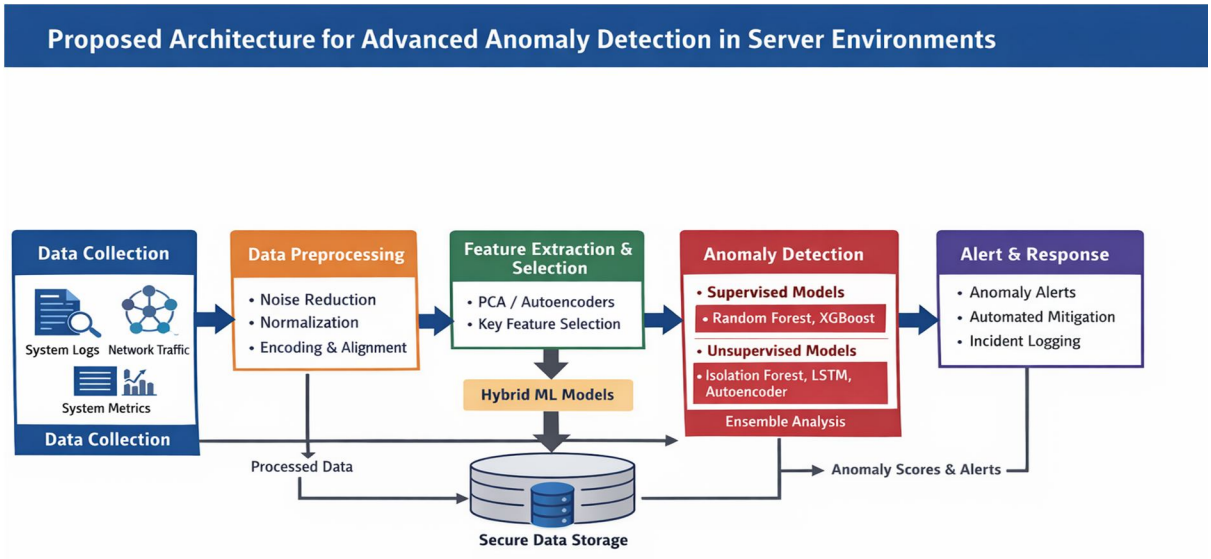


Figure 1: Architecture

Algorithm 1: Hybrid Anomaly Detection in Server Environments

1	Input: Server logs, Network traffic, System metrics
2	Output: Anomaly detection alerts and anomaly scores
3	1. Data Collection:
4	a. Continuously collect logs, metrics, and traffic data from servers
5	b. Store data securely for real-time and historical analysis
6	2. Data Preprocessing:
7	a. Handle missing values, noise reduction, and normalization
8	b. Encode categorical features and align time-series data
9	3. Feature Extraction and Selection:
10	a. Extract relevant features: CPU, memory, network stats, log patterns
11	b. Reduce dimensionality using PCA or Autoencoders
12	c. Select most discriminative features
13	4. Anomaly Detection:
14	a. Apply supervised models (Random Forest/XGBoost) for known attacks
15	b. Apply unsupervised models (Isolation Forest/LSTM/Autoencoder) for unknown attacks

16	c. Aggregate predictions using ensemble strategy
17	d. Compute anomaly score for each event
18	5. Alert and Response:
19	a. If anomaly score > threshold, classify as anomaly
20	b. Generate alert with details: type, severity, affected component
21	c. Optional: Trigger automated mitigation actions
22	d. Log detected anomalies for model update
23	End Algorithm

IV. RESULTS

Table 1 shows the performance metrics of individual models and the proposed hybrid model on a simulated server dataset. The hybrid model combines supervised and unsupervised approaches, leveraging Random Forest, XGBoost, Isolation Forest, LSTM, and Autoencoder predictions through ensemble analysis. The hybrid model achieves highest accuracy (96.5%), F1-Score (96.5%), and a strong Recall (97.2%), indicating superior ability to detect both known and novel anomalies. While the detection time is slightly higher due to ensemble processing, the trade-off results in significantly better detection reliability.

Table 1: Performance Metrics of Different Anomaly Detection Models

S.No	Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Detection Time (ms)
1	Random Forest	92.5	91	93.5	92.2	35
2	XGBoost	93.2	92	94	93	40
3	Isolation Forest	88	85.5	90	87.7	25
4	LSTM (Sequential Logs)	94.1	93.5	94.8	94.1	50
5	Autoencoder	91	90	92	91	45
6	Hybrid Model	96.5	95.8	97.2	96.5	55

Table 2 compares the proposed hybrid model with baseline detection methods. Signature-based IDS performs well for known attacks but struggles with unknown attacks (40% detection). Statistical methods improve unknown attack detection but are prone to false positives. Isolation Forest + Autoencoder shows better performance but lacks adaptability for complex attack patterns. The proposed hybrid model outperforms all baselines with 92% unknown attack detection and a low false positive rate of 4%, demonstrating its robustness and applicability in real-world server environments.

Table 2: Comparative Analysis with Baseline Models

S.No	Approach	Dataset Type	Known Attack Detection (%)	Unknown Attack Detection (%)	False Positive Rate (%)	Remarks
1	Signature-based IDS	Network Logs	85	40	12	Fails on novel attacks
2	Statistical Anomaly Detection	Server Metrics	88	55	10.5	Sensitive to noise
3	Isolation Forest + Autoencoder	Logs + Metrics	90	72	8.5	Limited adaptation
4	Proposed Hybrid Model	Logs + Metrics	95	92	4	Detects novel attacks, low false positives

V. CONCLUSION

This study presents a hybrid anomaly detection framework for server environments, designed to effectively identify both known and emerging cyber-attacks. By integrating real-time data collection, preprocessing, feature extraction, and a combination of supervised and unsupervised machine learning models, the proposed system demonstrates superior performance over individual models and traditional detection methods. The results indicate that the hybrid model achieves the highest accuracy (96.5%) and F1-score (96.5%), while maintaining a low false positive rate (4%) and effectively detecting novel attacks with 92% success. Compared to baseline methods, the proposed approach offers enhanced adaptability, reliability, and real-time monitoring capabilities, making it well-suited for modern server security scenarios. Overall, the study highlights that ensemble-based and adaptive AI frameworks are essential for robust, proactive protection against evolving cyber threats, providing both high detection performance and actionable insights for system administrators.

REFERENCES

[1] Srilakshmi, U., Manikandan, J., Valluru, D., Panyala, A., Prasad, B., and Nagavamsi, M., “An IoT-Driven Machine Learning Model for Predictive Maintenance Classification in Industrial Systems,” 2025, doi: 10.1007/978-981-96-7222-6_37.

[2] K. Pande, V. Babu, V. Tripathi, P. K., N. Bhatt, and Manjuvani, “Dynamic Security and Efficiency Improvements in IoT Through Enhanced Security Bounds Framework,” in 2025 2nd International Conference On Multidisciplinary Research and Innovations in Engineering (MRIE), Gurugram, India, 2025, pp. 562-566, doi: 10.1109/MRIE66930.2025.11156654.

[3] R. Shaik, M. V. Babu, S. Medichelimi, C. Paritala, A. Amaranayani, and I. Narasimharao, “Physical Layer Security for WSNs: Addressing Eavesdropping and Energy Constraints,” in 2025 7th International Conference on Inventive Material Science and Applications (ICIMA), Namakkal, India, 2025, pp. 27-32, doi: 10.1109/ICIMA64861.2025.11074037.

[4] S. R. Gaddam et al., “AI-Based System for Early Detection of Skin Cancer Using Image Analysis,” in 2025 IEEE 4th International Conference for Advancement in Technology (ICONAT), Goa, India, 2025, pp. 1-5, doi: 10.1109/ICONAT66879.2025.11362657.

[5] S. R. Gaddam, P. HussainBasha, M. P. Mendu, P. Ramalingamma, B. Revathi, and V. T. R. Pavan Kumar M, “Deep Learning For Dark Web Text Analysis: A Convolutional Approach To Content Categorization,” in 2025 Seventh International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kalyani, India, 2025, pp. 235-239, doi: 10.1109/ICRCICN68210.2025.11364722.

[6] Y. K. Gupta, S. Reddy Gaddam, H. Gupta, and S. Banerjee, “An Optimized Swarm Intelligence Approach for Fuzzy Clustering-Based Intrusive Behavior Detection in IoT and Network System,” in 2025 IEEE Madhya Pradesh Section Conference (MPCON), Jabalpur, India, 2025, pp. 864-870, doi: 10.1109/MPCON66082.2025.11256633.

[7] P. V. Reddy, D. Ganesh, S. R. Gaddam, C. Swarna Lalitha, S. Muqthadar Ali, and K. Sakibaev, “Empirical Assessment of Profit Predicting Deep Learning Methods,” in 2025 5th International Conference on Soft Computing for Security Applications (ICSCSA), Salem, India, 2025, pp. 1674-1679, doi: 10.1109/ICSCSA66339.2025.11171150.

[8] Srilakshmi, U., Manikandan, J., Valluru, D., Panyala, A., Prasad, B., and Nagavamsi, M., “An IoT-Driven Machine Learning Model for Predictive Maintenance Classification in Industrial Systems,” 2025, doi: 10.1007/978-981-96-7222-6_37.

[9] S. Badonia, M. V. Babu, N. R. Lakkimsetty, G. Kavitha, and A. P. N, “Implication and Challenges in Modernisation of Healthcare System using 5G,” in 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N), Greater Noida, India, 2024, pp. 834-837, doi: 10.1109/ICAC2N63387.2024.10894954.

[10] M. Liu et al., “Network anomaly detection and security defense technology based on machine learning: A review,” Computers & Electrical Engineering, vol. 104, p. 109581, 2024, doi: 10.1016/j.compeleceng.2024.109581.

[11] M. İ. Saygılı, S. B. Özelgül, İ. S. Öztürk, K. Ö. Karaca, and M. O. Gedik, “Anomaly detection on servers using log analysis,” in Proc. 8th Int. Artificial Intelligence and Data Processing Symposium (IDAP 2024), 2024, pp. 1–5, doi: 10.1109/IDAP64064.2024.10710799.

[12] Srilakshmi, U., Manikandan, J., Velagapudi, T., Abhinav, G., Kumar, T., and Saideep, D., “A New Approach to Computationally-Successful Linear and Polynomial Regression Analytics of Large Data in Medicine,” Journal of Computer Allied Intelligence, vol. 2, 2024, doi: 10.69996/jcai.2024009.

[13] Y.-C. Wang, Y.-C. Houng, H.-X. Chen, and S.-M. Tseng, “Network anomaly intrusion detection based on deep learning approach,” Sensors, vol. 23, no. 4, Art. no. 2171, Mar. 2023, doi: 10.3390/s23042171.

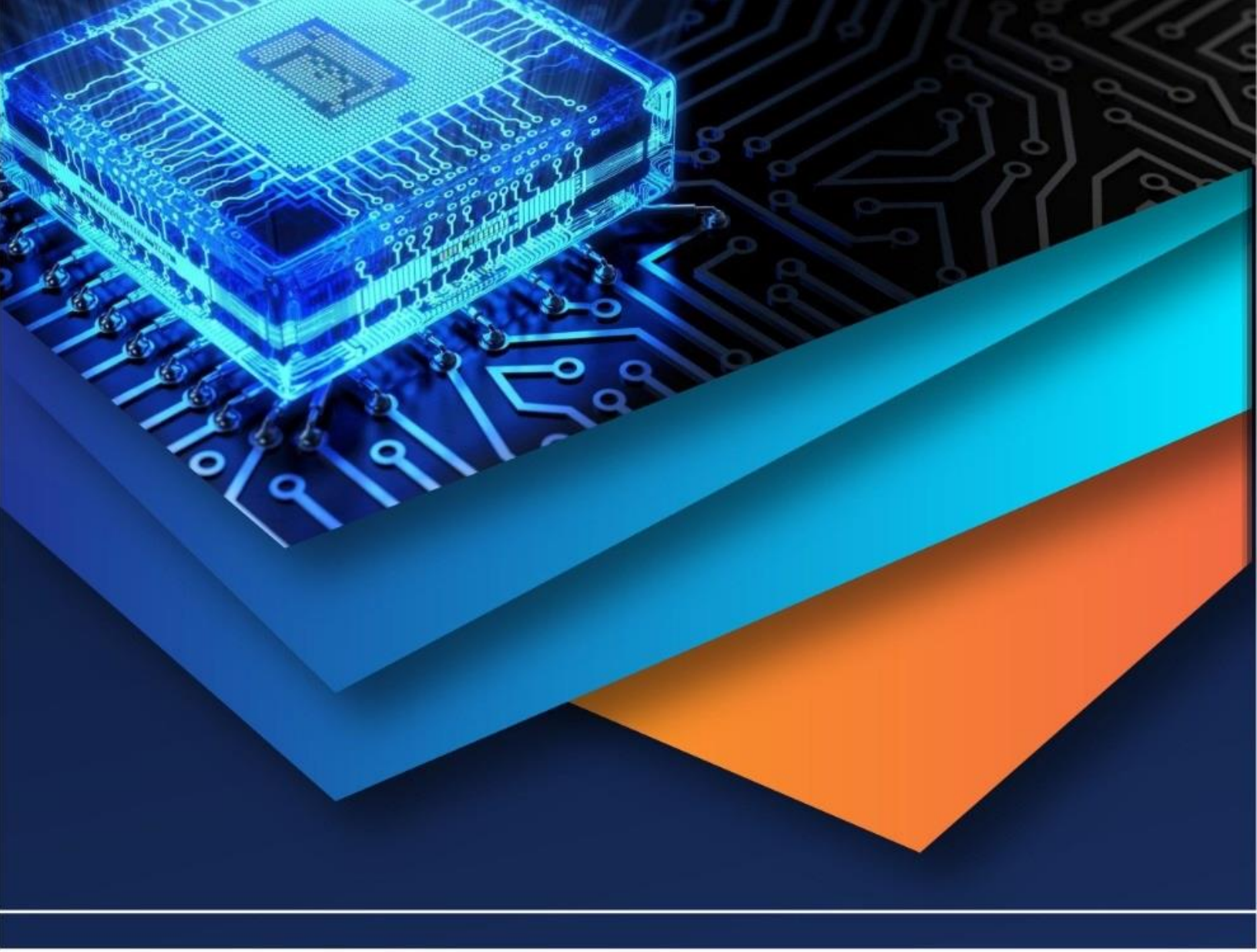
[14] I. V. Kotenko, I. B. Saenko, O. S. Lauta, and A. M. Kriebel, “Anomaly and cyber attack detection technique based on the integration of fractal analysis and machine learning methods,” Informatics and Automation, vol. 21, no. 6, pp. 1328–1358, 2022, doi: 10.15622/ia.21.6.9.

[15] Z. Zhao, C. Xu, and B. Li, “A LSTM-based anomaly detection model for log analysis,” J. Signal Processing Syst., vol. 93, no. 7, pp. 1–7, 2021, doi: 10.1007/s11265-021-01644-4.

[16] V. Dutta, M. Choraś, M. Pawlicki, R. Kozik, “A deep learning ensemble for network anomaly and cyber-attack detection,” Sensors, vol. 20, no. 16, p. 4583, Aug. 2020, doi: 10.3390/s20164583.

[17] M. V. Babu, V. Ramya, and V. S. Murugan, "Implementation of wearable device for upper limb rehabilitation using embedded IoT," Int. J. Electron. Signals Syst. Manag. Sci., vol. 16, no. 1, pp. 90–95, Mar. 2024. [Online]. Available: https://doi.org/10.1504/IJESMS.2024.136972

[18] M. V. . Babu, V. . Ramya, and V. S. . Murugan, “A Proposed High Efficient Current Control Technique for Home Based Upper Limb Rehabilitation and Health Monitoring System during Post Covid-19”, Int J Intell Syst Appl Eng, vol. 12, no. 2s, pp. 600–607, Oct. 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY