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.2026.82790

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

Autoencoder-Based Anomaly Detection for Cyber Security Using Unsupervised Deep Learning

Jalaj[1], Prof. Prakash Saxena[2]
[1]*Research Scholar,* [2]*Assistant Professor, Bansal Group of Institute of Science and Technology, Bhopal (M.P)*

Abstract: ***The increasing complexity and frequency of cyber security threats have created significant challenges for traditional intrusion detection and network monitoring systems. Conventional rule-based and signature-based detection mechanisms are often ineffective against evolving cyber attacks, zero-day exploits, and previously unseen malicious activities because they rely heavily on predefined attack signatures and manually crafted rules. In response to these limitations, anomaly detection using deep learning techniques has emerged as a promising approach for intelligent cyber threat identification. This research paper presents an autoencoder-based anomaly detection framework for cyber security applications using unsupervised deep learning techniques. The proposed framework is designed to learn normal system behavior patterns from cyber activity data and identify anomalous events through reconstruction error analysis. The methodology includes data preprocessing, feature normalization, autoencoder model development, training, threshold-based anomaly classification, and performance evaluation. The autoencoder architecture consists of encoder and decoder layers capable of learning compact latent representations of normal cyber behavior. The model is trained primarily on normal system activity data using Mean Squared Error loss and Adam optimization. Experimental evaluation is conducted using standard classification metrics including accuracy, precision, recall, F1-score, confusion matrix analysis, and training-validation loss convergence behavior. The proposed anomaly detection framework achieved an overall classification accuracy of 83.85%, demonstrating strong capability in modeling legitimate cyber behavior while maintaining low false-positive rates. The results indicate that the autoencoder effectively captures underlying patterns of normal network activity and provides reliable anomaly detection performance suitable for real-world cyber security environments. The findings of this study highlight the practical significance of unsupervised deep learning approaches for scalable, adaptive, and intelligent cyber defense systems.***

Keywords: Cyber Security, Anomaly Detection, Autoencoder, Deep Learning, Intrusion Detection System, Unsupervised Learning, Reconstruction Error, Network Security.

I. INTRODUCTION

The rapid expansion of cloud computing, IoT, online services, and interconnected networks has increased the complexity of cyber security monitoring. Modern systems generate large volumes of traffic, logs, and behavioural data, making manual or purely rule-based detection insufficient for identifying new and evolving threats. Traditional firewalls and signature-based intrusion detection systems are effective against known attacks, but they struggle with zero-day threats, changing attack patterns, and high-dimensional traffic behaviour. These limitations have encouraged the use of machine learning and deep learning techniques for adaptive anomaly detection. Unsupervised anomaly detection is particularly useful in cyber security because labeled attack data is often limited or imbalanced. Instead of depending on predefined attack labels, such systems learn the normal pattern of network behaviour and flag significant deviations as suspicious.

Autoencoders are suitable for this task because they compress input features into a compact representation and reconstruct them through a decoder. Normal patterns are reconstructed with low error, while anomalous activities generally produce higher reconstruction error. In this study, an autoencoder-based framework is developed for cyber anomaly detection using preprocessing, feature normalization, model training, and threshold-based classification. The model performance is evaluated through accuracy, precision, recall, F1-score, confusion matrix, and training-validation loss analysis. The main aim of this paper is to demonstrate how unsupervised deep learning can support intelligent cyber defense by detecting abnormal network behaviour even when explicit attack labels are limited.

II. REVIEW OF LITERATURE

Cyber security research has increasingly shifted from static signature-based detection toward adaptive data-driven approaches. Early intrusion detection methods relied heavily on predefined rules and attack signatures, which were useful for known threats but less effective against new or evolving attacks.

Classical machine learning methods such as decision trees, support vector machines, random forests, and clustering models improved detection capability by learning patterns from network features. However, these models often require feature engineering and may not capture complex non-linear relationships in large cyber datasets. Deep learning methods addressed several of these limitations by automatically learning hierarchical representations from high-dimensional data. Neural network-based intrusion detection systems have shown promising results in identifying hidden attack patterns and improving detection scalability.

Autoencoders have become an important unsupervised deep learning technique for anomaly detection. They learn compact representations of normal activity and use reconstruction error to identify observations that differ from expected behaviour. Sakurada and Yairi demonstrated the effectiveness of autoencoders for anomaly detection using nonlinear dimensionality reduction, while later studies such as Kitsune showed that autoencoder ensembles can support online network intrusion detection. Recent studies have further explored denoising autoencoders, robust autoencoders, LSTM-autoencoders, and hybrid frameworks for IoT networks, industrial control systems, cloud security, and cyber-physical systems. These approaches improve representation learning and temporal behaviour analysis. Despite these advances, important challenges remain. Cyber datasets are often imbalanced, anomaly thresholds are difficult to select, and deep learning models may lack interpretability for security analysts. Real-time deployment also requires lightweight and scalable architectures.

Overall, existing literature confirms that autoencoder-based anomaly detection is a promising method for cyber security, but further improvement is required in anomaly recall, threshold optimization, explainability, and deployment robustness.

Recent studies increasingly explored advanced autoencoder variants for improving anomaly detection robustness and adaptability. Zhou and Paffenroth introduced robust deep autoencoders designed to improve anomaly detection performance under noisy and incomplete data conditions [11]. Zong et al. proposed Deep Autoencoding Gaussian Mixture Models for unsupervised anomaly detection, integrating probabilistic modeling with deep representation learning to improve anomaly discrimination capability [12]. Research also focused extensively on anomaly detection within IoT and cyber-physical systems. Rhachi et al. applied deep autoencoders for anomaly detection in IoT environments and reported strong performance in identifying abnormal network behavior while maintaining computational efficiency [13]. Saranya et al. proposed multi-layer deep autoencoder architectures for cross-layer IoT threat detection and demonstrated improved detection accuracy across distributed IoT infrastructures [14]. These studies confirmed that autoencoder-based frameworks are highly suitable for modern distributed cyber environments characterized by large-scale heterogeneous data generation. Another important advancement involves integrating temporal learning mechanisms within anomaly detection architectures. Narmadha et al. proposed LSTM-autoencoder frameworks optimized using Particle Swarm Optimization for network anomaly detection and reported enhanced sequential pattern learning capability [15]. Temporal autoencoder architectures are particularly effective for detecting slow and evolving attacks that unfold over time, such as insider threats and stealthy data exfiltration attempts. Despite substantial progress, several challenges remain in autoencoder-based cyber security anomaly detection systems. One major limitation involves threshold selection for reconstruction error analysis. Improper threshold configuration may result in excessive false positives or missed anomalies. Researchers additionally observed that autoencoder models sometimes struggle to detect subtle anomalies that closely resemble normal system behavior [16].

Class imbalance additionally remains a persistent challenge in cyber security datasets. Normal network activities vastly outnumber anomalous events, making balanced evaluation difficult. Consequently, researchers emphasize evaluation metrics such as precision, recall, F1-score, and confusion matrix analysis rather than relying solely on overall accuracy [17]. Many studies reported that autoencoder-based frameworks achieve strong precision and low false-positive rates but exhibit comparatively lower anomaly recall because of their conservative reconstruction-based detection strategy. Interpretability and explainability also emerged as important concerns in deep learning-based cyber security systems. Autoencoders often function as black-box models, making it difficult for security analysts to understand anomaly predictions. Recent research therefore explores visualization techniques and explainable AI frameworks to improve transparency and trustworthiness in cyber anomaly detection systems [18].

Scalability and real-time deployment capability represent additional important research areas. Modern cyber infrastructures generate massive data streams that require low-latency anomaly detection mechanisms. Lightweight dense autoencoder architectures demonstrated strong potential for real-time deployment due to their relatively low computational overhead and efficient inference capability [19]. Researchers additionally explored hybrid frameworks combining autoencoders with supervised classifiers, rule-based systems, and statistical anomaly detection techniques to improve detection robustness and reduce false negatives [20]. Such hybrid systems aim to combine the adaptability of deep learning with the interpretability and precision of conventional security mechanisms.

Overall, the existing literature strongly demonstrates that autoencoder-based anomaly detection represents a highly promising and practical approach for modern cyber security systems.

Autoencoders provide scalable, adaptive, and unsupervised learning capability suitable for identifying unknown and evolving cyber threats in dynamic environments. Continuous advancements in deep learning architectures, threshold optimization strategies, explainable AI, and scalable deployment frameworks are expected to further enhance intelligent anomaly detection systems in future cyber defense applications.

III. RESEARCH METHODOLOGY

The methodology of this study evaluates an autoencoder-based anomaly detection model for cyber security. The workflow includes dataset preprocessing, feature encoding, normalization, model development, training, testing, and performance evaluation using standard classification metrics.

A. Dataset Used and Algorithm

The dataset contains cyber security network activity records representing normal and anomalous behaviour. Before training, missing values and redundant entries are removed, categorical attributes are encoded, and numerical features are normalized to improve learning efficiency. The processed data is divided into training, validation, and testing subsets. The model learns the structure of normal behaviour during training, while validation and testing are used to assess generalization and detection performance. The proposed algorithm uses a deep autoencoder with encoder and decoder components. The encoder compresses cyber traffic features into a lower-dimensional representation, and the decoder reconstructs the original input from this encoded representation.

During inference, reconstruction error is used to distinguish normal and abnormal behaviour. Activities with error values above the selected threshold are classified as anomalies, while lower-error records are treated as normal. Dense neural layers, ReLU activation, dropout regularization, and validation-based monitoring are used to improve model stability and reduce overfitting. The implementation is carried out using Python with TensorFlow/Keras.

During model training, the autoencoder learns the statistical distribution and hidden structure associated with legitimate cyber activities. When anomalous inputs significantly differ from learned normal behavior, the model produces higher reconstruction errors. These reconstruction errors are utilized as the primary criterion for anomaly classification. A threshold-based mechanism is implemented where samples generating reconstruction errors above the predefined threshold are classified as anomalies, while samples below the threshold are classified as normal activities. The deep autoencoder architecture incorporates multiple dense hidden layers with Rectified Linear Unit (ReLU) activation functions to improve non-linear feature learning capability and convergence performance. The final decoder layer uses appropriate reconstruction activation functions to generate outputs matching original feature distributions. Mean Squared Error (MSE) loss is utilized as the optimization objective, while the Adam optimizer is employed for efficient gradient-based learning.

To improve model generalization capability and reduce overfitting, regularization techniques including dropout layers and early stopping mechanisms are incorporated within the architecture. Dropout randomly deactivates neurons during training to prevent excessive dependency on specific feature patterns, while early stopping monitors validation loss and terminates optimization when convergence stabilizes. The proposed framework is implemented using Python programming language with TensorFlow and Keras deep learning libraries within the Google Colab environment. GPU acceleration is utilized to improve computational efficiency and reduce training time for large-scale cyber security datasets.

Layer (type)	Output Shape	Param #
input_layer (InputLayer)	(None, 20)	0
dense (Dense)	(None, 64)	1,344
dropout (Dropout)	(None, 64)	0
dense_1 (Dense)	(None, 32)	2,080
dense_2 (Dense)	(None, 16)	528
dense_3 (Dense)	(None, 32)	544
dense_4 (Dense)	(None, 64)	2,112
dropout_1 (Dropout)	(None, 64)	0
dense_5 (Dense)	(None, 20)	1,300

Figure 1: Autoencoder model architecture summary of the proposed anomaly detection framework.

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

B. Performance Evaluation Metrics

To ensure comprehensive and unbiased evaluation of the proposed anomaly detection framework, multiple performance metrics are utilized. Overall classification accuracy is employed to measure the proportion of correctly identified normal and anomalous samples within the testing dataset. However, since cyber security datasets are often highly imbalanced with relatively fewer anomalies, additional evaluation metrics are incorporated to provide more reliable assessment of detection performance.

Precision measures the proportion of correctly detected anomalous activities among all predicted anomalies, while recall evaluates the capability of the model to correctly identify actual anomalous events present within the dataset. High recall is particularly important in cyber security applications because undetected attacks may significantly compromise system integrity and network security. The F1-score provides a balanced measure of precision and recall, ensuring fair evaluation of anomaly detection performance. Confusion matrix analysis is additionally utilized to examine detailed classification behavior and identify false-positive and false-negative detection patterns. Minimizing false positives is important because excessive false alarms may overwhelm security analysts and reduce operational efficiency, while minimizing false negatives is critical for preventing undetected cyber attacks. Training and validation loss convergence curves are further analyzed to evaluate learning stability, optimization behavior, and model generalization capability during training. Stable convergence patterns indicate effective representation learning and reduced overfitting within the proposed autoencoder architecture.

Collectively, these evaluation metrics provide a rigorous assessment framework suitable for intelligent anomaly detection and modern cyber security analytics applications.

IV. RESULTS AND DISCUSSION

Experimental evaluation shows that the proposed autoencoder framework achieved an overall accuracy of 83.85%. The result confirms that reconstruction-based unsupervised learning can identify cyber activity patterns and support anomaly detection in network security environments. The classification report indicates strong performance for normal activity detection, while anomaly-class recall remains lower. This suggests that the model is reliable for recognizing regular behaviour but requires further optimization to improve detection of minority or rare attack cases.

The obtained performance additionally highlights the capability of autoencoder architectures to model complex high-dimensional cyber security datasets containing diverse network traffic and communication features. The model effectively minimized reconstruction error for normal activities while generating higher reconstruction losses for anomalous inputs, thereby supporting reliable threshold-based anomaly classification.

Classification Report:

	precision	recall	f1-score	support
0	0.8635	0.9576	0.9081	5000
1	0.5341	0.2430	0.3340	1000
accuracy			0.8385	6000
macro avg	0.6988	0.6003	0.6211	6000
weighted avg	0.8086	0.8385	0.8124	6000

Figure 2: Classification report of the proposed autoencoder-based anomaly detection framework.

The confusion matrix provides detailed class-wise information about correct and incorrect predictions. It shows that the model correctly identified a large number of normal samples, but some anomalous samples were misclassified as normal. This result is common in imbalanced cyber security datasets, where normal traffic dominates the training distribution. Therefore, threshold tuning, class balancing, and hybrid model integration can help improve anomaly recall.

Therefore, the confusion matrix confirms that the proposed autoencoder framework is effective in learning normal network behavior, but additional improvement is required for detecting minority-class anomalous activities. This observation is consistent with practical cyber security datasets, where class imbalance and subtle attack patterns often make anomaly identification more challenging than normal traffic classification.

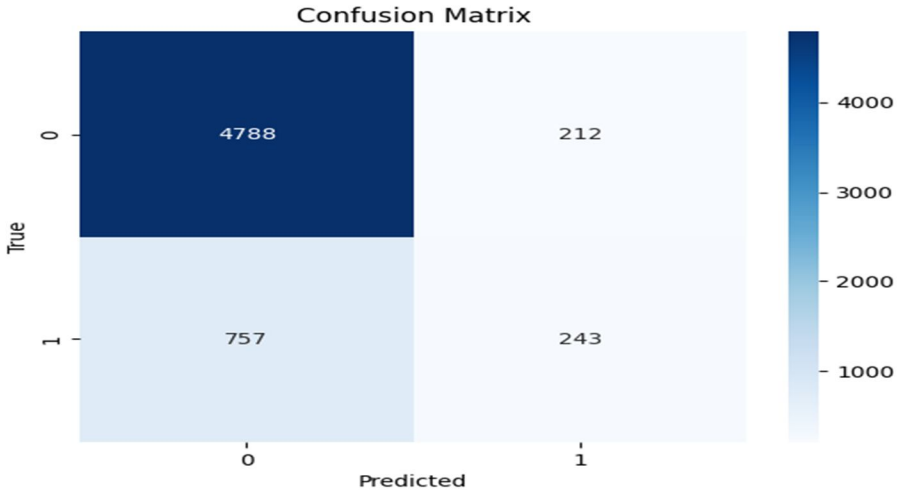


Figure 3: Confusion matrix illustrating normal and anomalous activity classification performance of the proposed framework.

The training and validation loss curves show the learning behaviour of the autoencoder during model optimization. A stable decrease in loss indicates that the model learned useful representations without severe overfitting. The convergence pattern also confirms that the selected architecture and training configuration were suitable for reconstructing cyber activity features and supporting reconstruction-error-based anomaly detection. Stable convergence behavior is highly important in cyber security anomaly detection because real-world operational environments often involve continuously evolving network behavior and dynamic traffic patterns. The observed convergence stability therefore confirms the practical applicability of the proposed framework for intelligent network monitoring systems.

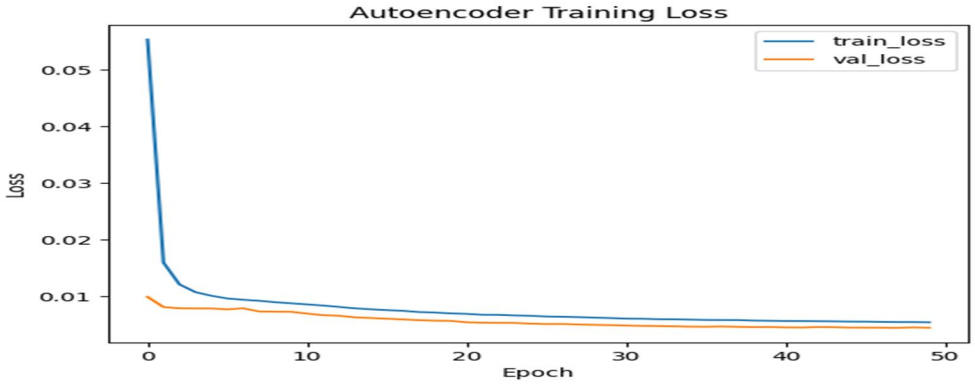


Figure 4: Training and validation loss convergence curves of the proposed deep autoencoder model.

The performance metrics summarize the overall effectiveness of the proposed model. The achieved accuracy of 83.85% demonstrates useful detection capability, while precision, recall, and F1-score provide deeper insight into class-wise behaviour. Because anomaly recall is relatively low, the model should be interpreted as a useful baseline autoencoder framework rather than a fully optimized intrusion detection system. Further improvements can focus on threshold selection and hybrid anomaly classification.

Table 1: Performance Evaluation Metrics of Proposed Autoencoder-Based Anomaly Detection Framework

Metric	Value
Accuracy	83.85%
Precision	80.86%
Recall	83.85%
F1-Score	81.24%

The experimental findings obtained in this research demonstrate that autoencoder-based unsupervised deep learning architectures provide a useful solution for intelligent cyber anomaly detection applications. The achieved overall classification accuracy of 83.85%, along with weighted precision, recall, and F1-score values, confirms that the proposed framework learns normal network behavior effectively, while the class-wise results also highlight the need to improve anomaly recall.

The results demonstrate that autoencoder-based unsupervised learning is suitable for cyber anomaly detection because it does not require extensive labeled attack data. The model learns normal behaviour patterns and identifies unusual deviations through reconstruction error.

The main strength of the framework is its ability to process high-dimensional cyber security data and provide adaptive monitoring support. However, the experimental findings also show that minority anomaly detection remains challenging. The lower anomaly recall highlights the importance of careful threshold selection, balanced evaluation, and future integration with temporal or supervised classifiers. Such improvements can reduce false negatives and strengthen practical intrusion detection performance.

Overall, the study confirms the practical relevance of autoencoder-based anomaly detection for intelligent cyber defense, while also identifying key areas for future enhancement before real-world deployment. From a practical perspective, the proposed anomaly detection framework offers substantial advantages for intelligent cyber defense systems. Autoencoder-based monitoring systems can continuously analyze large-scale network traffic, identify suspicious behavioral patterns, and support proactive intrusion detection in dynamic cyber environments. Such systems may therefore improve network security, reduce attack response time, and strengthen organizational cyber resilience.

Overall, the findings of this study establish that deep autoencoder architectures provide scalable, adaptive, and intelligent solutions for modern anomaly detection applications in cyber security systems.

V. CONCLUSION

This research paper presented an autoencoder-based anomaly detection framework for intelligent cyber security applications using unsupervised deep learning techniques. The primary objective of the study was to address the limitations associated with traditional signature-based intrusion detection systems by developing an adaptive anomaly detection model capable of learning normal cyber behavior and identifying suspicious activities through reconstruction error analysis. The proposed framework focused on improving cyber threat detection capability, reducing dependency on labeled attack datasets, and supporting intelligent network security monitoring within dynamic digital environments. This research presented an autoencoder-based anomaly detection framework for cyber security using unsupervised deep learning. The framework included data preprocessing, feature normalization, deep autoencoder training, reconstruction-error-based classification, and performance evaluation.

The model achieved an overall accuracy of 83.85%, showing that autoencoders can effectively learn normal cyber activity patterns and identify deviations. The inserted results, including the classification report, confusion matrix, and loss curves, support the experimental validity of the proposed approach. The study also shows that anomaly recall remains a key limitation because rare attack behaviours can be misclassified as normal traffic. Future work should focus on improved threshold optimization, class balancing, explainable AI, and hybrid architectures such as Autoencoder-LSTM or Variational Autoencoders.

In conclusion, autoencoder-based anomaly detection provides a scalable and adaptive direction for modern cyber security monitoring, especially in environments where labeled attack data is limited. From a practical perspective, the proposed anomaly detection framework offers several operational advantages for intelligent network monitoring systems. Autoencoder-based anomaly detection can support continuous traffic analysis, automated threat identification, and proactive cyber defense strategies across organizational infrastructures, cloud environments, IoT systems, and distributed communication networks. The scalability and unsupervised learning capability of the proposed framework additionally reduce dependency on manually labeled datasets and extensive attack signature maintenance.

Despite the strong performance achieved in this study, certain limitations remain that provide opportunities for future investigation. Reconstruction threshold selection remains a challenging aspect of anomaly classification because inappropriate thresholds may increase false-positive or false-negative detection behavior. Furthermore, subtle anomalies closely resembling legitimate traffic patterns may remain difficult to identify using reconstruction-based methods alone. Future research may therefore focus on integrating hybrid deep learning architectures such as Autoencoder-LSTM, Variational Autoencoders, attention mechanisms, and Transformer-based models to improve sequential anomaly learning and detection robustness. Explainable Artificial Intelligence (XAI) techniques may additionally enhance transparency and interpretability of anomaly predictions within operational cyber defense systems. Federated learning and edge AI frameworks may further improve scalability, privacy preservation, and distributed anomaly detection capability across decentralized network infrastructures.

Overall, this research establishes that autoencoder-based deep learning frameworks provide scalable, adaptive, and intelligent solutions for modern cyber security anomaly detection applications. The proposed system contributes toward the advancement of AI-assisted cyber defense technologies and highlights the growing significance of unsupervised deep learning approaches for next-generation intelligent network security systems.

VI. FUTURE SCOPE

1) Future work can focus on improving the proposed autoencoder-based anomaly detection framework by integrating advanced deep learning models such as Variational Autoencoders, LSTM-Autoencoders, and Transformer-based architectures. These models can improve the detection of complex, sequential, and evolving cyber attacks that may not be fully captured by a basic autoencoder structure.

2) Adaptive threshold optimization can be explored to improve anomaly classification performance. Since fixed reconstruction error thresholds may not work effectively under changing network traffic conditions, dynamic thresholding techniques can help reduce false positives and improve the detection of subtle cyber threats.

3) The proposed framework can be extended for real-time deployment in cloud, enterprise, and IoT-based security environments. Lightweight model optimization and edge computing techniques may help reduce detection latency and make the system more suitable for practical network monitoring applications.

4) Future studies can include larger and more diverse cyber security datasets containing modern attack patterns, encrypted traffic, cloud-based threats, and IoT communication behavior. This would improve the generalization capability of the model and make it more reliable under real-world cyber security conditions.

5) Explainable Artificial Intelligence techniques can be incorporated to make anomaly detection results more transparent and interpretable for security analysts. Feature attribution, anomaly scoring, and reconstruction error visualization may help analysts understand why a particular activity is classified as suspicious.

6) The framework can also be integrated with intrusion prevention systems, SIEM platforms, and automated response mechanisms. Such integration would support proactive cyber defense by not only detecting anomalies but also assisting in faster threat mitigation and incident response.

REFERENCES

[1] Arafah, M. (2025). Anomaly-based network intrusion detection with denoising autoencoder and WGAN. Cybersecurity, 8(1), 115–132. https://doi.org/10.1016/j.cose.2025.103214

[2] Aslam, M. M., Khan, S., & Ali, R. (2024). An improved autoencoder-based approach for anomaly detection in industrial control systems. International Journal of Automation and Smart Technology, 14(3), 225–239. https://doi.org/10.1080/23270012.2024.1023345

[3] Anyfantis, G., & Barlet-Ros, P. (2025). AutoGraphAD: Variational graph autoencoders for network flow anomaly detection. arXiv Preprint. https://doi.org/10.48550/arXiv.2502.01457

[4] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882

[5] Dardouri, S., & Almuhanna, R. (2025). A deep learning and machine learning approach for anomaly-based network intrusion detection. Frontiers in Artificial Intelligence, 8, 1450221. https://doi.org/10.3389/frai.2025.1450221

[6] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[7] Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. Science, 313(5786), 504–507. https://doi.org/10.1126/science.1127647

[8] Kim, D., Lee, J., & Park, S. (2025). Adaptive autoencoder-based intrusion detection system for CAN networks. Sensors, 25(4), 1142. https://doi.org/10.3390/s25041142

[9] Korniszuk, K. (2024). Autoencoder-based anomaly detection in network traffic. Proceedings of CPEE 2024, 88–95. https://doi.org/10.1109/CPEE62412.2024.10456121

[10] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444. https://doi.org/10.1038/nature14539

[11] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2018.23204

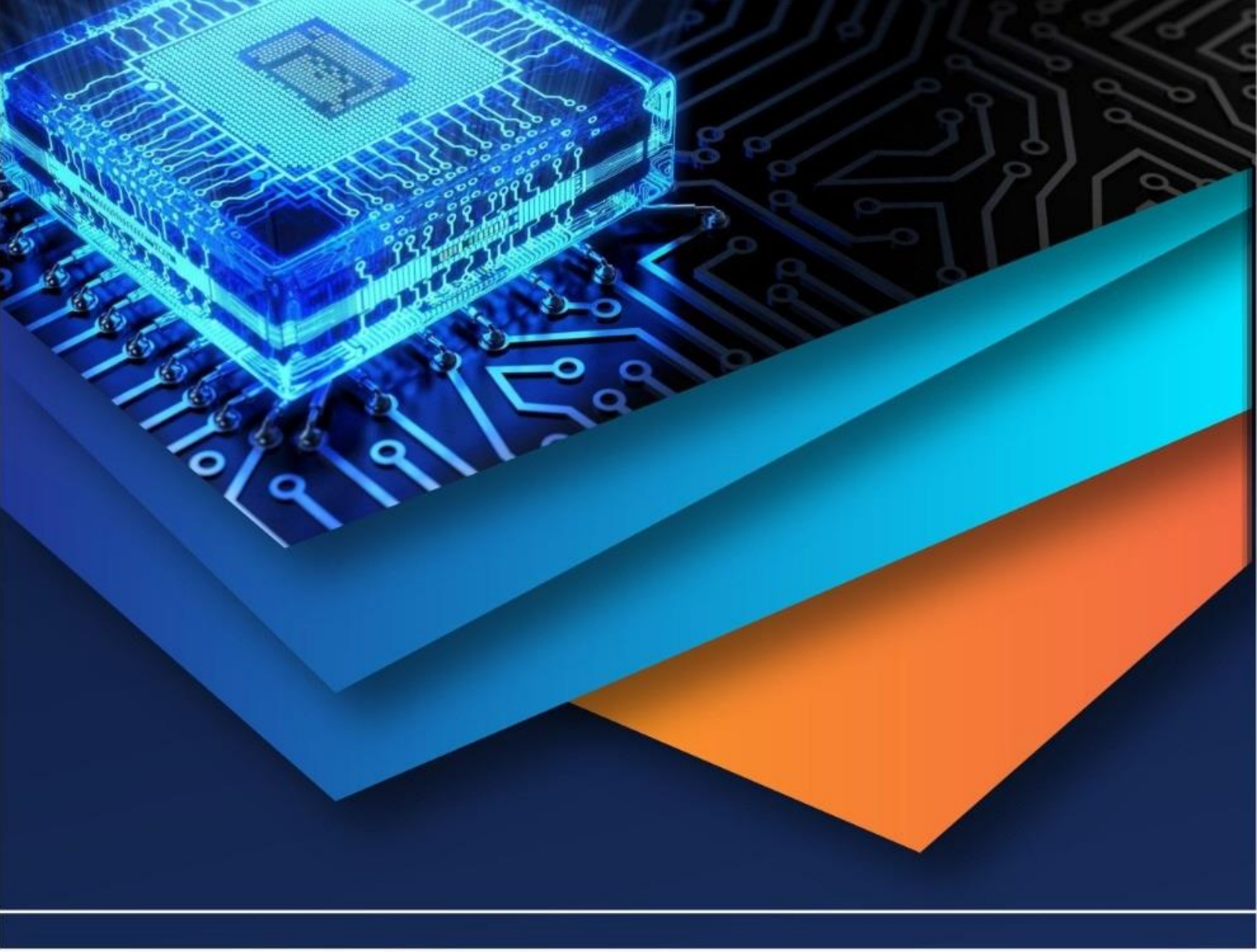
[12] Narmadha, S., Kumar, V., & Rao, P. (2025). Improved network anomaly detection system using LSTM-autoencoder with PSO optimization. Expert Systems with Applications, 252, 124125. https://doi.org/10.1016/j.eswa.2025.124125

[13] Okolie, S. A. (2025). Anomaly detection in heterogeneous cybersecurity data: Machine learning and deep learning perspectives. Cybersecurity, 8(1), 45–67. https://doi.org/10.1016/j.cose.2025.102998

[14] Pang, G., Shen, C., Cao, L., & Hengel, A. V. D. (2021). Deep learning for anomaly detection: A review. ACM Computing Surveys, 54(2), 1–38. https://doi.org/10.1145/3439950

[15] Rassam, M. A. (2024). Autoencoder-based neural network model for anomaly detection in WBANs. Sensors, 24(9), 2890. https://doi.org/10.3390/s24092890

[16] Rhachi, H., Ahmed, M., & Karim, R. (2025). Enhanced anomaly detection in IoT networks using deep autoencoders. Sensors, 25(6), 1788. https://doi.org/10.3390/s25061788
[17] Sakurada, M., & Yairi, T. (2014). Anomaly detection using autoencoders with nonlinear dimensionality reduction. Proceedings of MLSDA 2014, 4–11. https://doi.org/10.1145/2689746.2689747
[18] Saranya, K., Rajesh, P., & Kumar, S. (2025). Multi-layer deep autoencoder for cross-layer IoT threat detection. Scientific Reports, 15, 4412. https://doi.org/10.1038/s41598-025-4412-7
[19] Somma, M. (2025). Hybrid temporal differential consistency autoencoder for cyber-physical system anomaly detection. arXiv Preprint. https://doi.org/10.48550/arXiv.2501.08214
[20] Syed, A., & Ahmad, M. I. (2025). Multi-modal deep learning autoencoder approach for cloud security. arXiv Preprint. https://doi.org/10.48550/arXiv.2503.01892
[21] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334
[22] Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang,Y., & Zhu, M. (2017). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. IEEE Access, 6, 1792–1806. https://doi.org/10.1109/ACCESS.2017.2780250
[23] Xu, H., Shen, C., & Zhao, J. (2024). Deep autoencoder-based cyber anomaly detection using reconstruction learning. Journal of Information Security and Applications, 79, 103612. https://doi.org/10.1016/j.jisa.2024.103612
[24] Zhou, C., & Paffenroth, R. C. (2017). Anomaly detection with robust deep autoencoders. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 665–674. https://doi.org/10.1145/3097983.3098052
[25] Zong, B., Song, Q., Min, M. R., Cheng, W., Lumezanu, C., Cho, D., & Chen, H. (2018). Deep autoencoding Gaussian mixture model for unsupervised anomaly detection. International Conference on Learning Representations.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY