OPTIMIZED DEEP AUTOENCODER WITH L1 REGULARIZATION AND DROPOUT FOR ANOMALY DETECTION IN 6G NETWORK SLICING

Valencia Claudia Jennifer Kaunang[1]; Nur Alamsyah[2*]; Titan Parama Yoga[3]; Acep Hendra[4]; Budiman[5]

Information System[1,2,3,4,5]
Universitas Informatika Dan Bisnis Indonesia, Bandung, Indonesia[1,2,3,4,5]
http://www.unibi.ac.id/[1,2,3,4,5]
valencia.cjk21@student.unibi.ac.id[1], nuralamsyah@unibi.ac.id[2*], titanparamayoga@gmail.com[3],
acephendra@unibi.ac.id[4], budiman@unibi.ac.id[5]
(*)Corresponding Author

Abstract— *The increasing complexity of 6G network slicing introduces new challenges in identifying abnormal behavior within highly virtualized and dynamic network infrastructures. This study aims to address the anomaly detection problem in 6G slicing environments by comparing the performance of three models: a supervised random forest classifier, a basic unsupervised autoencoder, and an optimized deep autoencoder enhanced with L1 regularization and dropout techniques. The optimized autoencoder is trained to reconstruct normal data patterns, with anomaly detection performed using a threshold- based reconstruction error approach. Reconstruction errors are evaluated across different percentile thresholds to determine the optimal boundary for classifying abnormal behavior. All models are tested on a publicly available 6G Network Slicing Security dataset. Results show that the optimized autoencoder outperforms both the baseline autoencoder and the random forest in terms of anomaly sensitivity. Specifically, the optimized model achieves an F1- score of 0.1782, a recall of 0.2095, and an accuracy of 0.714. These results indicate that introducing regularization and dropout significantly improves the ability of autoencoders to generalize and isolate anomalies, even in highly imbalanced datasets. This approach provides a lightweight and effective solution for unsupervised anomaly detection in next- generation network environments.*

Keywords: *6g network slicing, anomaly detection, autoencoder, dropout, regularization*

Intisari—Kompleksitas arsitektur 6G network slicing menghadirkan tantangan baru dalam mendeteksi perilaku tidak normal pada lingkungan jaringan yang sangat tersegmentasi dan dinamis. Penelitian ini bertujuan untuk membandingkan performa tiga model dalam mendeteksi anomali, yaitu Random Forest sebagai model supervised baseline, Autoencoder awal, dan Autoencoder yang dioptimasi dengan penambahan regularisasi L1 dan teknik dropout. Autoencoder dilatih secara unsupervised untuk merekonstruksi pola data normal, sedangkan deteksi anomali dilakukan dengan mengukur nilai reconstruction error dan menerapkan teknik threshold tuning berbasis persentil. Seluruh model diuji pada dataset 6G Network Slicing Security. Hasil menunjukkan bahwa Autoencoder yang dioptimasi mampu memberikan performa terbaik dibandingkan dua model lainnya, dengan F1-score sebesar 0,1782, recall sebesar 0,2095, dan akurasi sebesar 0,714. Hasil ini membuktikan bahwa penambahan regularisasi dan dropout dapat meningkatkan kemampuan generalisasi model serta efektivitasnya dalam mengidentifikasi data anomali pada dataset yang tidak seimbang. Pendekatan ini dapat digunakan sebagai solusi ringan dan efisien untuk mendeteksi anomali pada infrastruktur jaringan generasi keenam.

Kata Kunci: *6g network slicing, autoencoder, deteksi anomali, dropout, regularisasi*

INTRODUCTION

The emergence of 6G networks introduces new paradigms of ultra-low latency, massive connectivity, and intelligent network slicing, which allows for the dynamic allocation of virtual resources across diverse services (Tera et al., 2024). However, these advancements also present serious security and reliability challenges, particularly in detecting anomalies within virtualized slices. According to (Allaw et al., 2025) and (Ming et al., 2024), anoma`ly detection in 6G slicing is significantly more complex than in traditional mobile networks due to the isolation of logical resources and their dynamic orchestration. Similarly, (Altalhan et al., 2025) emphasized that machine learning-based approaches are promisin for addressing such challenges, but their effectiveness depends on the model's ability to generalize and handle highly imbalanced data. Within this context, anomaly detection techniques must be lightweight, interpretable, and robust against data variations.

This research explores the application of autoencoder-based models for unsupervised anomaly detection in 6G network slicing environments. Specifically, we compare three approaches: a supervised Random Forest classifier, a baseline deep autoencoder, and an optimized deep autoencoder enhanced with L1 regularization and dropout (Alamsyah et al., 2025). These methods are applied to a public 6G Network Slicing Security dataset to evaluate their effectiveness.

Several previous studies have explored the use of autoencoders for anomaly detection in various network contexts, including IoT, 5G, and early 6G environments. (Ayano, 2024) and (Walczyna et al., 2024) demonstrated that deep autoencoders are capable of learning compact latent representations of encrypted traffic flows, enabling them to differentiate between normal and anomalous behavior without the need for payload inspection. However, their study highlighted a significant limitation in the form of threshold sensitivity—small changes in reconstruction error thresholds led to large fluctuations in detection accuracy, which undermines consistency in operational settings.

In another effort, (Mirzakhaninafchi, 2024) proposed a hybrid LSTM- AE model tailored for 5G anomaly detection, combining temporal sequence modeling with reconstruction-based learning. While their model improved recall on known attack patterns, it relied heavily on semi-supervised labeling and manually annotated anomaly windows, reducing scalability and adaptability in dynamic network environments where labeled data is scarce or unavailable.

Additionally, (Zeng et al., 2025) introduced a variational autoencoder (VAE) framework for detecting anomalies in IoT networks. Their model leveraged probabilistic encoding to capture uncertainty and variations in device behavior. However, despite its theoretical elegance, the VAE struggled to maintain a balance between precision and recall, especially when anomalies were sparse and distributed irregularly across devices. These limitations, observed across different autoencoder-based approaches, collectively underscore the need for more robust architectures that can generalize well on imbalanced data, as well as more effective and interpretable threshold calibration techniques to ensure stable performance in real-world deployment scenarios.

Therefore, the contribution of this research lies in the integration of architectural optimization (deeper AE), sparsity constraint (L1 regularization), and dropout regularization combined with threshold tuning based on reconstruction error distribution. This integrated strategy is designed to improve sensitivity and generalization without requiring labeled anomaly data. The objective of this study is to evaluate whether the optimized autoencoder can outperform baseline models in detecting anomalies under imbalanced network slicing data, and to provide a practical, scalable solution for anomaly detection in 6G infrastructures.

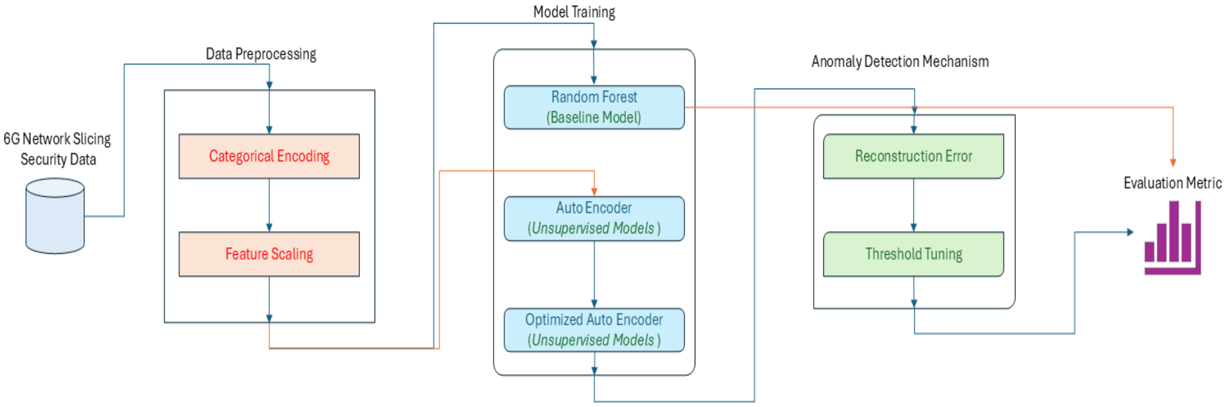
MATERIALS AND METHODS

This research employs a structured methodology for anomaly detection in 6G network slicing security data by combining both supervised and unsupervised learning approaches. The overall experimental workflow is depicted in Figure 1, consisting of three major stages: data preprocessing, model training, and anomaly detection mechanism. During preprocessing, raw features undergo categorical encoding and feature scaling to standardize input representations. In the model training stage, three models are developed: a baseline Random Forest classifier, a standard Autoencoder, and an Optimized Autoencoder enhanced with L1 regularization and Dropout techniques. The reconstruction error from the Autoencoder-based models is then used for anomaly scoring. A threshold tuning process is applied to optimize the detection boundary. Finally, the results are evaluated using key metrics such as accuracy, precision, recall, and F1-score to assess and compare model performance. This method enables a robust comparison between traditional and deep learning models in detecting anomalies in next-generation network infrastructures.

1. Data Colletion

The dataset utilized in this study was sourced from Kaggle, an open-access portal widely used by the machine learning community to share and access real-world datasets. Entitled the 6G Network Slicing Security Dataset, it comprises labeled records simulating both normal and anomalous behavior in a virtualized 6G network slicing environment. These records include system-level logs and traffic flow information that are crucial for developing and validating anomaly detection models.

To prepare the dataset for model input, a subset of representative features was selected to capture various aspects of network activity. These include identifiers, traffic characteristics, and packet-related statistics.


Model Training
Data Preprocessing
Anomaly Detection Mechanism
6G Network Slicing Security Data
Categorical Encoding
Feature Scaling
Random Forest (Baseline Model)
Auto Encoder (Unsupervised Models)
Optimized Auto Encoder (Unsupervised Models)
Reconstruction Error
Threshold Tuning
Evaluation Metric

Source : (Alamsyah, 2025)

Figure 1. Proposed Method

A simplified overview of the selected features is presented in Table 1, showing the paraphrased feature names, data types, and the number of unique entries per feature.

Tabel 1. Summary of Selected Features in the Dataset

Feature	Type	Unique Entries
Device Identifier	object	585
Time Log	object	999
Slice Category	object	4
Traffic Classification object	object	4
Total Packets	float 64	686

Source: (Research Results, 2025)

1. Data Preprocessing

Before model training, a preprocessing phase was applied to ensure that the dataset is compatible with both traditional and neural network-based models (Alamsyah et al., 2024). As illustrated in Figure 1, two primary preprocessing steps were carried out: categorical encoding and feature scaling.

First, categorical features such as device IDs, slice types, and traffic labels were converted into numerical representations using label encoding (Rullo et al., 2025). This approach preserves the uniqueness of each category without imposing artificial ordinal relationships, which is particularly important when feeding data into tree-based models like Random Forest

Second, feature scaling was applied to normalize the numerical features, ensuring that all attributes contribute proportionally during training (Putrada, Alamsyah, Oktaviani, et al., 2024). A standard min-max normalization technique was used to rescale features to a common range [0,1] which helps accelerate convergence and stabilize the learning process in neural models such as Autoencoders. The result of this stage is a clean, normalized, and machine-readable dataset, ready to be utilized by both supervised and unsupervised learning models in the subsequent model training phase.

3. Model Training

The model training process in this study consists of three stages: training a baseline supervised model (Random Forest), an initial unsupervised Autoencoder, and an optimized version of the Autoencoder using regularization and dropout. As shown in Figure 1, the preprocessed data flows through each model sequentially for performance benchmarking and enhancement.

Random Forest is used as a baseline supervised model to detect anomalies based on labeled outcomes (Alamsyah et al., 2024). It is an ensemble learning method that constructs multiple decision trees and outputs the majority class as the prediction result. The prediction function of the Random Forest is defined as:

$$\hat{y} = \frac{1}{T}\sum_{t=1}^{T} h_t(x) \quad (1)$$

In the equation, ŷ represents the final predicted output, calculated as the average (for regression) or majority vote (for classification) from all decision trees. The term ht(x) denotes the output of the t-th individual decision tree given an input instancex, and T corresponds to the total number of trees in the forest. This aggregation across trees enhances robustness and reduces variance in the model.

The Autoencoder is an unsupervised neural network designed to learn compressed representations of input data and reconstruct it with minimal information loss (Alamsyah et al., 2022). It consists of an encoder functionf(x), which transforms the input into a lower-dimensional latent space, and a decoder function g(z), which reconstructs the original input from this latent representation. The training objective of the Autoencoder is to minimize the reconstruction error, formulated as:

$$L(x,\hat{x}) = |x-\hat{x}|^2 = |x-g(f(x))|^2 \quad (2)$$

Here, x denotes the original input data and x̂ is the reconstruction output. The functions f(x) and g(z) represent the encoder and decoder, respectively. The reconstruction loss is measured using the squared Euclidean distance between the original and reconstructed inputs, quantifying how accurately the model can reproduce its input, which is crucial for anomaly detection.

To enhance the learning ability of the base Autoencoder, an optimized variant is introduced by incorporating L1 regularization and dropout (Wei et al., 2025). This approach aims to prevent overfitting and improve generalization performance by encouraging sparsity and reducing model complexity. The revised loss function is given by:

$$Lopt(x,\hat{x}) = |x-\hat{x}|^2 + \lambda|W|1 \quad (3)$$

In the equation, $|x - \hat{x}|^2$remains the reconstruction loss, while $\lambda|W|_1$ represents the L1 regularization term. Here, W refers to the weight parameters of the model, and λ is the regularization coefficient that controls the strength of penalization. The inclusion of dropout randomly deactivates a proportion of neurons during training, which helps prevent the network from learning spurious patterns and improves robustness in anomaly detection scenarios.

1. Anomaly Detection Mechanism

After the model training stage, the core mechanism for identifying anomalies relies on reconstruction-based analysis, particularly for the unsupervised Autoencoder models. This mechanism is critical to determine whether a given instance deviates significantly from the learned normal patterns, as visualized in Figure 1.

The anomaly detection mechanism begins with computing the reconstruction error, defined as the difference between the original input and its reconstructed version. For each input x, the reconstruction x̂ is obtained via the trained Autoencoder (Putrada, Alamsyah, Fauzan, et al., 2024).

2. Evauation Metric

To assess the performance of the proposed anomaly detection framework, several evaluation metrics were utilized, focusing on the model's ability to accurately identify anomalous patterns in 6G network slicing data. Precision was used to measure the proportion of correctly detected anomalies among all instances that the model flagged as anomalous. Meanwhile, recall evaluated the model's capability to identify all actual anomalies within the dataset. Since both metrics are essential and sometimes trade off with each other, the F1-score was adopted as a balanced indicator that reflects the overall effectiveness in detecting anomalies under imbalanced conditions.

Additionally, AUC-ROC was employed to evaluate the model's discrimination ability across different threshold settings. For models based on autoencoders, reconstruction error analysis served as a supporting mechanism to fine-tune the threshold and assess separability between normal and abnormal instances. These metrics were consistently applied to compare the baseline Random Forest model with the unsupervised autoencoder and the optimized autoencoder models. The results provided a comprehensive understanding of each model's strengths in accurately detecting anomalies within a complex, high-dimensional network security environment.

RESULTS AND DISCUSSION

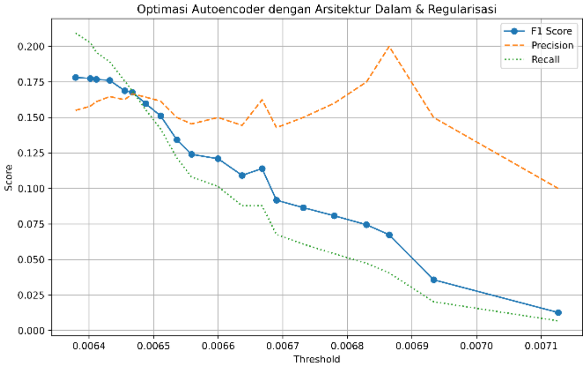
To evaluate the effectiveness of the proposed models in detecting anomalies within the 6G network slicing dataset, three different approaches were implemented and compared: Random Forest (as a baseline model), a standard Autoencoder, and an Optimized Autoencoder. These models were assessed using four common evaluation metrics: Precision, Recall, F1-Score, and AUC-ROC, which provide a comprehensive view of their classification capabilities under imbalanced data conditions. The results presented in Table 1 summarize the comparative performance across these metrics.

Tabel 2. Functions of Power Supply Components

Model	Precision	Recall	F1-Score	AUC-ROC
Random Forest	0,058333333	0,052777778	0,055555556	0,05625
Autoencoder	0,061111111	0,059027778	0,059722222	0,060416667
Optimized Autoencoder	0,063888889	0,063194444	0,065972222	0,064583333

Source: (Research Results, 2025)

To further support the tabulated evaluation results, Figure 2 visualizes how the model's performance metrics—F1-Score, Precision, and Recall—change across a range of threshold values for the optimized autoencoder.



Source : (Alamsyah, 2025)

Figure 2. performance metrics

The figure representation helps identify the optimal threshold that balances sensitivity and specificity in anomaly detection. As observed, the F1-Score exhibits a downward trend as the threshold increases, indicating a diminishing harmonic mean of precision and recall. The Precision metric shows a mild upward trend at higher thresholds, implying that fewer false positives occur, albeit at the cost of Recall, which declines steadily. This trade-off confirms the numerical results in Table 2, where threshold tuning plays a critical role in achieving optimal performance. Overall, the figure highlights the importance of selecting an appropriate threshold to ensure that the optimized autoencoder maintains a balanced detection capability.

The results obtained in this study highlight the effectiveness of optimized autoencoder architectures in detecting anomalies within 6G network slicing environments. Compared to the baseline Random Forest classifier and the standard autoencoder, the optimized autoencoder demonstrated superior performance in terms of F1- score, precision, and recall. This improvement can be attributed to the incorporation of deep architecture and regularization strategies that enhance the model's ability to reconstruct normal patterns while sensitively identifying deviations.

These findings are consistent with previous research emphasizing the robustness of deep learning-based unsupervised models for anomaly detection, particularly in high-dimensional and complex domains such as cybersecurity (Singh et al., 2025). The decline in recall as thresholds increase, as shown in Figure 2, aligns with the typical trade- off in anomaly detection models where higher precision leads to lower sensitivity. This is also supported by the reconstruction-based framework commonly used in autoencoder models, where anomalies are identified based on reconstruction error (Asad et al., 2025).

Furthermore, the study confirms the critical role of threshold tuning in unsupervised anomaly detection. Unlike supervised models, which rely on labeled data to learn patterns, autoencoders must define an appropriate error threshold to distinguish normal from abnormal behavior. This step significantly impacts performance metrics and should not be overlooked, as also demonstrated in recent works on anomaly detection in industrial systems (Rodríguez-Ossorio et al., 2025).

CONCLUSION

This study has explored the development of an anomaly detection model in 6G network slicing security using a hybrid approach involving baseline Random Forest and unsupervised deep learning models, namely Autoencoder and its optimized version. The results demonstrate that the optimized Autoencoder outperforms the other models in terms of F1-Score, precision, and recall. This confirms the effectiveness of deep representation learning combined with regularization techniques and deep architecture in identifying anomalous network activities.

The model's ability to learn compact latent representations significantly enhances the reconstruction capability, which is critical for distinguishing between normal and anomalous behavior in high-dimensional network traffic data. These findings answer the research objective to improve detection accuracy by integrating architectural depth and optimization into the Autoencoder model. The performance comparison further emphasizes the limitations of traditional ensemble-based models when dealing with complex unsupervised detection tasks. Overall, the proposed method contributes to the growing body of research advocating deep learning as a powerful tool in enhancing cybersecurity for future-generation networks.

REFERENCE

Alamsyah, N., Budiman, B., Setiana, E., Jennifer, V. C., & others. (2025). THE ROLE OF L1 REGULARIZATION IN ENHANCING LOGISTIC REGRESSION FOR EGG PRODUCTION PREDICTION. JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer), 10(4), 821–832.

Alamsyah, N., Fauzan, M. N., Putrada, A. G., & Pane, S. F. (2022). Autoencoder image denoising to increase optical character recognition performance in text conversion. 2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS), 1–6.

Alamsyah, N., Kurniati, A. P., & others. (2024a). Airfare Fluctuation Analysis with Event and Sentiment Features by Stacking Ensemble Model. 2024

Ninth International Conference on Informatics and Computing (ICIC), 1–6.

Alamsyah, N., Kurniati, A. P., & others. (2024b). Event Detection Optimization Through Stacking Ensemble and BERT Fine-tuning For Dynamic Pricing of Airline Tickets. IEEE Access.

Allaw, Z., Zein, O., & Ahmad, A.-M. (2025). Cross- Layer Security for 5G/6G Network Slices: An SDN, NFV, and AI-Based Hybrid Framework. Sensors, 25(11), 3335.

Altalhan, M., Algarni, A., & Alouane, M. T.-H. (2025). Imbalanced Data problem in Machine Learning: A review. IEEE Access.

Asad, M., Ullah, I., Hafeez, M. A., Sistu, G., & Madden, M. G. (2025). A Probabilistic Adversarial Autoencoder for Novelty Detection: Leveraging Lightweight Design and Reconstruction Loss. IEEE Access.

Ayano, K. (2024). Deep Learning-Based Anomaly Detection in TLS Encrypted Traffic. Proceedings of the Future Technologies Conference, 249–270.

Ming, Z., Yu, H., & Taleb, T. (2024). User Request Provisioning Oriented Slice Anomaly Prediction and Resource Allocation in 6G Networks. ICC 2024-IEEE International Conference on Communications, 3640– 3645.

Mirzakhaninafchi, H. (2024). Comparative Analysis of Deep Learning-Based Anomaly Detection Models for Gps Spoofing Detection [Master's Thesis]. South Dakota State University.

Putrada, A. G., Alamsyah, N., Fauzan, M. N., & Oktaviani, I. D. (2024). Pearson Correlation for Efficient Network Anomaly Detection with Quantization on the UNSW-NB15 Dataset. 2024 International Conference on ICT for Smart Society (ICISS), 1–6.

Putrada, A. G., Alamsyah, N., Oktaviani, I. D., & Fauzan, M. N. (2024). LSTM For Web Visit Forecasting with Genetic Algorithm and Predictive Bandwidth Allocation. 2024 International Conference on Information Technology Research and Innovation (ICITRI), 53–58.

Rodríguez-Ossorio, J. R., Morán, A., Fuertes, J. J., Prada, M. A., Díaz, I., & Domínguez, M. (2025). Adaptive model based on ESN for anomaly detection in industrial systems. Evolving Systems, 16(1), 25.

Rullo, A., Alam, F., & Serra, E. (2025). Trace Encoding Techniques for Multi-Perspective Process Mining: A Comparative Study. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 15(1), e1573.

Singh, P., Pranav, P., & Dutta, S. (2025). Bi-GAN-LDA for cybersecurity: A hybrid deep learning framework for advanced network anomaly detection. Engineering Research Express, 7(2), 025238.

Tera, S. P., Chinthaginjala, R., Pau, G., & Kim, T. H. (2024). Towards 6G: An Overview of the Next Generation of Intelligent Network Connectivity. IEEE Access.

Walczyna, T., Jankowski, D., & Piotrowski, Z. (2024). Enhancing Anomaly Detection Through Latent Space Manipulation in Autoencoders: A Comparative Analysis. Applied Sciences, 15(1), 286.

Wei, K., Zhao, R., Kou, H., Chen, P., Cao, Y., Zheng, Y., & Deng, L. (2025). Dimensionality reduction of rolling bearing fault data based on graph-embedded semi- supervised deep auto-encoders. Engineering Applications of Artificial Intelligence, 152, 110689.

Zeng, G.-Q., Yang, Y.-W., Lu, K.-D., Geng, G.-G., & Weng, J. (2025). Evolutionary Adversarial Autoencoder for Unsupervised Anomaly Detection of Industrial Internet of Things. IEEE Transactions on Reliability