Confluence University Journal of Science and Technology
Journal of the Confluence University of Science and Technology,
Osara, Kogi State
Journal Homepage: www.cujostech.com.ng
CUJoSTech

Network Anomaly Detection in Enhanced Machine-Type Communication IoT Applications on 5G and Beyond Networks: A Convolutional Autoencoder Approach

*[1]CHIKEZIE I. C., [1]USMAN U. A, [1]DAVID M., [1]SULEIMAN Z., [2,3]OHIZE O.H., [4]OJENIYI J.
[1]Department of Telecommunications Engineering, Federal University of Technology, Niger State, Nigeria.
[2]Department of Electrical & Electronics Engineering, Federal University of Technology, Minna, Nigeria.
[3]Department of Electrical & Electronics Engineering, Confluence University of Science and Technology, Osara, Nigeria.
[4]Department of Cyber Security Science, Federal University of Technology, Niger State, Nigeria.
*Chekwas.pg.2010285@futminna.edu.ng
DOI: https://doi.org/10.5455/CUJOSTECH.2504

Research Article

Abstract

The exponential growth of Enhanced Machine-Type Communication (eMTC) in 5G and beyond networks is fundamental to the evolving Internet of Things (IoT) landscape, connecting billions of low-power devices. This rapid growth, while transformative, significantly broadens the attack surface, introducing critical security challenges that traditional measures struggle to address. This study proposes an advanced anomaly detection framework leveraging Convolutional Autoencoders (Conv AEs) to identify unusual patterns and potential security threats in eMTC-enabled IoT data traffic. The Conv AE model was developed and rigorously evaluated using the CICIoT2023 dataset, which comprises over 46 million records of both normal and anomalous network traffic. Through binary stratified sampling and z-score normalization, a balanced and representative dataset was prepared for training and evaluation. The model was trained exclusively on normal traffic to learn benign behavior. The Conv AE architecture, comprising an encoder with 1D convolutional layers and a decoder with 1D transposed convolutions, optimizes a Mean Squared Error (MSE) loss function to reconstruct input data, flagging anomalies based on high reconstruction errors exceeding an empirically selected threshold of 0.0262. The evaluation metrics demonstrate the framework's exceptional effectiveness and efficiency. The model achieved an impressive Accuracy of 0.9892, a Precision of 0.9987, a Recall (True Positive Rate) of 0.9903, and an F1-Score of 0.9945. These results indicate a strong ability to detect anomalous events with remarkably few false positives. Furthermore, the model exhibited efficient operational performance, with a per-sample inference time of 0.0809 seconds and the ability to process a full test set of 102,578 samples in 52.87 seconds, enabling real-time anomaly detection. The False Alarm Rate (FAR) was 0.0530, and the True Negative Rate (TNR) was 0.9470, confirming the model's proficiency in distinguishing normal from malicious traffic. The high Kappa Score of 0.8000, Matthews Correlation Coefficient (MCC) of 0.8096, Geometric Mean (G-Mean) of 0.9684, AUC-ROC of 0.9895, and AUC-PR of 0.9996 further validate the model's balanced and robust performance. This research contributes a robust and efficient solution for enhancing the security and safe deployment of IoT systems within the eMTC framework on current and future generation networks. Future research may adapt this binary framework to a multi-class classification approach, enabling classification of attack types for more detailed threat insight in eMTC-enabled IoT applications on 5G and beyond networks.

Keywords: *Network Anomaly Detection, Enhanced Machine-Type Communication (eMTC), 5G IoT Security, Convolutional Autoencoder (Conv AE), Deep Learning (DL), Real-Time Threat Detection.*
Article History: *Received: 3 May 2025; Accepted: 27 June 2025; Published: 28 June 2025*

1.0 Introduction

The Internet of Things (IoT) has become a pivotal force in reshaping modern digital ecosystems, enabling intelligent interaction among physical devices and fostering real-time data exchange across numerous domains. From smart homes and healthcare to industrial automation and transportation, IoT technologies continue to transform how information is generated, communicated, and utilized. As the number of interconnected devices grows exponentially, the demand for more robust and scalable communication networks has intensified. Fifth-generation (5G) mobile communication technologies have emerged in response to this demand, offering enhanced mobile broadband, ultra-reliable low-latency communication, and massive machine-type communication (mMTC) [1, 2]. Among the variants of mMTC, Enhanced Machine-Type Communication (eMTC) has garnered particular attention for its capacity to support a high density of low-cost, low-power IoT devices over a wide coverage area with relatively low latency and power consumption.

Designed to operate efficiently within cellular infrastructures, eMTC is capable of supporting up to one million devices per square kilometer, making it well-suited for large-scale IoT deployments across smart environments. Its improved spectral efficiency, deep coverage penetration, and extended battery life for devices make it a critical component for achieving the goals of 5G-enabled IoT systems [3]. Industry forecasts underscore the magnitude of its growth. The number of eMTC-enabled IoT devices is projected to rise significantly, from approximately 26.66 billion in 2019 to 41.6 billion by 2026, reflecting a growth

rate of over 54% [4]. This remarkable expansion highlights the increasing reliance on eMTC to support the connectivity demands of modern IoT applications.

However, the widespread adoption of IoT devices within eMTC networks has introduced an expanded threat surface. These devices often operate with minimal security configurations, limited firmware update capabilities, and constrained computing resources, making them highly susceptible to exploitation. As the volume and variety of connected devices grow, so too does the potential for coordinated network disruptions, data manipulation, and service degradation. The Mirai botnet attack of 2016 serves as a notable example, where thousands of vulnerable IoT devices were hijacked and used to execute large-scale Distributed Denial-of-Service (DDoS) attacks, resulting in significant network outages and financial losses [5], [6]. In recent years, similar patterns have continued to emerge. The National Information Technology Development Agency (NITDA) in Nigeria has documented frequent incidents of network breaches and service interruptions attributed to poorly secured IoT infrastructures [7]. These disruptions, according to the Nigerian Communications Commission (NCC), have incurred financial damages exceeding $500 million annually [8]. The situation reflects a broader concern within both industry and academia regarding the inadequacy of conventional security mechanisms in addressing the evolving threat landscape in IoT networks.

1.1 Security Challenges in eMTC-enabled 5G-IoT Environments

Enhanced Machine-Type Communication (eMTC) is pivotal for the Internet of Things (IoT) within 5G networks, enabling vast connectivity and low power consumption for large-scale deployments. However, the rapid adoption of eMTC introduces significant security challenges that are increasingly critical in today's interconnected landscape, particularly in regions like Nigeria. A major concern is the expanded attack surface; eMTC can connect up to one million devices per square kilometer, creating numerous potential entry points for malicious actors. Each connected device, regardless of size, presents a vulnerability [9]. The 2016 Mirai botnet attack exemplifies this risk, as it exploited small IoT devices to launch widespread Distributed Denial-of-Service (DDoS) attacks. Managing authentication and access control in eMTC networks compounds these security issues. With millions of connected devices, ensuring proper authentication before network access becomes a daunting task. Traditional mechanisms may be too resource-intensive for low-power devices, increasing the risk of unauthorized access [10].

The dynamic nature of IoT networks, where devices frequently join and leave, necessitates scalable solutions for effective access management. DDoS attacks represent another significant threat, as eMTC's massive connectivity makes these networks particularly vulnerable. The 2020 attack on Amazon Web Services illustrates the scale of potential threats, with the large number of connected devices heightening the risk of service disruptions. This underscores the need for real-time detection and mitigation strategies. Data privacy is a pressing issue, with IoT devices generating sensitive information, such as personal health data and operational metrics. Ensuring secure transmission and storage is vital; however, many devices lack the processing power for advanced encryption, leaving them vulnerable to breaches. This challenge is exacerbated by the complexity of monitoring data flows and complying with regulations across large-scale eMTC networks. Recent incidents, such as the 2023 attack on a major European energy company exploiting poorly secured IoT sensors, demonstrate the vulnerabilities within eMTC frameworks [11]. In Nigeria, documented disruptions and data breaches have had severe economic consequences, costing approximately $500 million annually [7]. The heterogeneity of devices and protocols in eMTC networks further complicates security. The variety of devices with differing capabilities and security requirements makes it challenging to implement standardized security solutions, increasing the risk of exploitation through outdated software or inadequate configurations.

1.2 Limitations of Traditional Security Measures in eMTC Networks

As the Internet of Things (IoT) expands through Enhanced Machine-Type Communication (eMTC) in 5G networks, traditional security measures are increasingly inadequate [12]. eMTC enables massive connectivity and low-cost communication, but also presents unique security challenges that legacy approaches cannot effectively handle.

One key limitation is scale. eMTC supports millions of devices per square kilometer, generating vast amounts of network traffic that traditional firewalls and encryption methods struggle to monitor and secure in real-time [13]. This leaves eMTC networks vulnerable to advanced threats, like zero-day attacks, which evade static, signature-based defenses.

Resource limitations in IoT devices further constrain security. Many devices connected via eMTC lack the processing power for intensive cryptographic methods, such as AES-256 or RSA, resulting in weaker protections that increase the risk of data breaches [14].

eMTC's dynamic environment, where devices constantly join and leave, also complicates the use of traditional security frameworks designed for static networks. This can lead to ineffective access control and easier intrusion. Additionally, traditional security systems are often overwhelmed by Distributed Denial-of-Service (DDoS) attacks in eMTC, as they cannot manage the high traffic volumes created by millions of compromised devices, nor can they easily distinguish malicious from legitimate traffic [15].

The centralized nature of traditional security architectures creates further challenges in eMTC environments, which are distributed and often mobile. Relying on central points of control can result in bottlenecks and single points of failure, making them susceptible to targeted attacks [16]. Finally, the diversity of devices and protocols in eMTC networks complicates the application of standardized security policies, often leaving gaps that attackers can exploit [17]. Traditional anomaly detection methods often employ signature-based intrusion detection systems, which rely on predefined attack signatures. However, this approach is insufficient in detecting new, unknown threats. Anomaly-based detection systems, particularly those using deep learning, offer a solution by learning patterns of normal network behavior and identifying deviations. Convolutional Autoencoders

(CONV AEs) are especially promising, as they effectively process high-dimensional data and are well-suited for binary anomaly detection by capturing network traffic patterns in real time. This study aims to address these issues by developing an advanced anomaly detection framework based on Convolutional Autoencoders. This framework will be designed to identify unusual patterns and potential security threats in IoT data traffic, leveraging deep learning techniques to improve detection accuracy. The research will rigorously evaluate the framework using diverse datasets to ensure its effectiveness. By proactively tackling these security challenges, the study seeks to enhance the safe deployment of IoT systems within the eMTC framework, protecting sensitive data and critical infrastructure.

2.0 Review of Some Related Works

The rapid integration of the Internet of Things (IoT) across various industries has revolutionized data collection and automation but has also introduced significant security challenges, particularly for resource-constrained IoT devices that are vulnerable to sophisticated attacks. To address these issues, authors in [18] developed the N-BaIoT system, a Network Intrusion Detection System (NIDS) designed to enhance security in IoT environments. Utilizing deep autoencoders to detect anomalies, N-BaIoT was tested on a dataset comprising various BASHLITE and Mirai botnet attacks, demonstrating improved accuracy over traditional signature-based NIDS. However, its reliance on specific attack types may limit its adaptability to emerging threats.

In response to the risk of Distributed Denial-of-Service (DDoS) attacks, authors in [19] proposed a hybrid Intrusion Detection System (IDS) that combines network-based (NIDS) and host-based (HIDS) systems with federated learning and fog computing. Evaluated on a synthetic DDoS dataset, their IDS achieved an accuracy of 89.75%, showcasing its potential for privacy-preserving and real-time threat detection. However, the study did not evaluate its performance in diverse, real-world network environments, leaving questions about its scalability and effectiveness under varying conditions.

Authors in [20] investigated machine learning models for real-time anomaly detection in healthcare IoT networks using the CICIoT2023 dataset, which includes 33 attack types. After preprocessing the data and employing the SMOTE algorithm for class balancing, they evaluated several models, including Random Forest, Adaptive Boosting, Logistic Regression, Perceptron, and Deep Neural Networks across binary, 8-class, and 34-class classifications. Random Forest emerged as the most effective model, achieving up to 99.55% accuracy while maintaining reduced computational time, which is crucial for real-time applications. However, it struggled to differentiate between complex attack types such as Recon and Spoofing, indicating the need for further feature engineering to enhance detection accuracy across all categories. This study underscores the potential of machine learning in securing IoT-based healthcare systems while pinpointing areas for future improvement.

As the IoT landscape expands within 5G networks, new security concerns arise, particularly related to vulnerabilities unique to 5G systems. Authors in [21] conducted a thorough analysis of these vulnerabilities, focusing on the Core Network (CN), Radio Access Network (RAN), and User Equipment (UE) within the 5G ecosystem. They advocate for the adoption of a Zero Trust security model, emphasizing strict access controls and continuous verification to mitigate risks in each component. While the study provides a valuable theoretical framework, its lack of empirical validation in real-world 5G implementations limits insights into practical application and effectiveness.

Authors in [22] further advanced 5G IoT security with an anomaly detection model that leverages transfer learning, applying it to the NUSW-NB15 and 5G-NNID datasets. Their approach achieved an impressive accuracy of up to 99.8%, effectively adapting to various 5G scenarios and reducing the need for model retraining across different datasets. However, the limited scope of datasets and absence of real-world testing restrict its generalizability in broader and more diverse 5G environments.

Finally, authors in [12] developed an Intrusion Detection System (IDS) aimed at enhancing IoT security against Denial-of-Service (DoS) attacks through anomaly detection and machine learning (ML) classifiers. Using the IoTID20 dataset, their model achieved exceptional results, with Decision Tree (DT) and Random Forest (RF) classifiers, particularly when combined with Genetic Algorithm (GA) feature selection, attaining 100% in accuracy, precision, recall, and F1 score. The DT also excelled in training and testing efficiency, surpassing other classifiers. However, the study's focus on a single dataset (IoTID20) and reliance on GA for feature selection highlight its limitations, indicating a need for broader testing across diverse datasets and additional attack types.

The rapid advancement of 5G networks and the growing use of IoT devices, especially within the Enhanced Machine-Type Communication (eMTC) framework, call for sophisticated security measures. Deep learning models stand out as promising solutions for detecting network anomalies due to their ability to analyze vast amounts of data, identify subtle patterns, and adapt to emerging threats in eMTC-enabled IoT systems.

Convolutional Neural Networks (CNNs), originally developed for image recognition, have shown versatility in network anomaly detection. By capturing spatial hierarchies in data, CNNs can detect patterns in network traffic, distinguishing between benign and potentially harmful activities [23]. Autoencoders also play a key role in unsupervised anomaly detection. By learning to reconstruct normal data with minimal error, they can flag anomalies based on higher reconstruction errors [24].

Building upon the strengths of CNNs and Autoencoders, the Convolutional Autoencoder (Conv AE) model combines the best of both worlds. CONV AEs utilize the convolutional layers of CNNs to capture spatial patterns in the data while incorporating the encoding-decoding structure of autoencoders to learn compressed representations. This combination allows CONV AEs to effectively process high-dimensional data, such as network traffic, and detect anomalies that might be missed by traditional methods [25]. In the context of eMTC-enabled IoT networks, where traffic patterns can be complex and varied, CONV AEs offer

a powerful tool for identifying deviations that could signal security threats. One of the main advantages of using deep learning models like CONV AEs in anomaly detection is their ability to automatically learn features from the data without requiring manual feature engineering [26]. This is particularly important in the dynamic environment of eMTC-enabled IoT within 5G networks, where the diversity of devices and traffic types makes it challenging to define static features that can reliably identify anomalies.

While deep learning models demand significant computational resources and rely on diverse, high-quality data, they represent significant advancements in eMTC-enabled IoT anomaly detection. Their adaptability, scalability, and data-driven approach make them essential for securing future 5G IoT systems. As deep learning evolves, models like CNNs, Autoencoders, and CONV AEs will continue to enhance security in our increasingly connected world.

3.0 Research Methodology

This study develops a deep learning-based network anomaly detection system tailored specifically for IoT applications operating over 5G and beyond network architectures. The methodological framework is structured into two principal phases: dataset preprocessing and the development, training, and evaluation of a Convolutional Autoencoder (Conv AE) model. These phases are strategically designed to maximize the system's capacity to identify anomalous traffic patterns with high detection accuracy, a minimized false alarm rate, and balanced performance across multiple classification metrics.

To support the computational and storage requirements of this research, Google Colab Pro, a paid cloud-based platform equipped with high-performance GPUs, was employed for model development and training. In addition, Google Drive (16TB), as provided by the Federal University of Technology, Minna, served as the primary data repository and facilitated seamless integration with the Colab environment. This cloud-based infrastructure ensured scalable data handling, efficient model training, and real-time experimentation, thereby enhancing both the methodological rigor and reproducibility of the study. The subsequent subsections elaborate on each phase, beginning with the preprocessing of benchmark IoT datasets to prepare them for model input, followed by the architecture, training process, and evaluation metrics used for the Conv AE-based anomaly detection model.

3.1 Data Description and Preprocessing

The research employs the CICIOT2023 dataset, which contains over 46 million records comprising both normal and anomalous network traffic collected from diverse IoT environments. For the purposes of this study, a binary classification problem was formulated, where normal traffic is labeled as 0 and all attack traffic is aggregated under the anomalous class, labeled as 1.

To address class imbalance and ensure fair training, a binary stratified sampling strategy was employed to create a balanced, representative working dataset. Let the dataset be denoted as Equation 1:

$$\mathcal{D} = \{(x_i, y_i)\}_{i=1}^{N} \tag{1}$$

where $x_i \in \mathbb{R}^{46}$represents the feature vector, and $y_i \in \{0,1\}$ is the corresponding binary class label (0 for normal traffic, 1 for anomalous traffic).

A stratified subset $\mathcal{D}' \subset \mathcal{D}$ was drawn using Equation 2 such that:

$$\frac{|\{(x_i, y_i) \in \mathcal{D}' : y_i = c\}|}{|\mathcal{D}'|} \approx \frac{|\{(x_i, y_i) \in \mathcal{D} : y_i = c\}|}{|\mathcal{D}|}, \forall c \in \{0,1\} \tag{2}$$

where c is the class label (0 or 1), $|\cdot|$ denotes the cardinality (number of instances), $\mathcal{D}'$ is the stratified subset used for model training and evaluation.

The resulting dataset was partitioned into:

a) 70% training set $\mathcal{D}_{\text{train}}$
b) 15% validation set $\mathcal{D}_{\text{test}}$
c) 15% test set $\mathcal{D}_{\text{val}}$

All subsets preserved the original class distribution to ensure consistent evaluation and to avoid skewed results.

To improve learning convergence and ensure numerical stability, each feature x_j was normalized using z-score normalization. As expressed in Equation 3, each feature was transformed as:

$$\hat{x}_{ij} = \frac{x_{ij} - \mu_j}{\sigma_j} \tag{3}$$

where x_{ij} is the value of feature j for instance i, μ_j is the mean of feature j computed over the training set $\mathcal{D}_{train}$ and σ_j is the corresponding standard deviation of feature j. This normalization ensures that all input features contribute equally to the learning process by centering them around zero with unit variance.

It is important to note that no explicit feature selection technique was applied during preprocessing. All 46 available features in the CIC-IoT2023 dataset were retained and used as input to the Conv AE model. This decision was motivated by the desire to allow the Conv AE to autonomously learn the most informative latent representations from the full feature space, without introducing biases from manual feature elimination.

3.2 The Study's Model Architecture

The core of the anomaly detection system is a Convolutional Autoencoder (Conv AE) designed to learn the inherent patterns of normal network traffic and to detect deviations from this learned representation as potential anomalies. The model was trained exclusively on normal traffic to allow it to develop a baseline profile of benign behavior. The architecture of the Conv AE is illustrated in Figure 1.

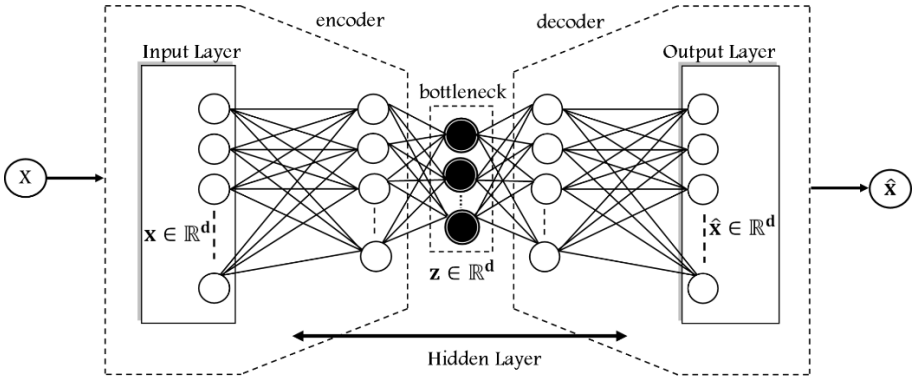

Figure 1: Architecture of the Convolutional Autoencoder (Conv AE) used in this study.

The model consists of two main components:

a) **Encoder**: This stage compresses the input feature vector $\mathrm{x} \in \mathbb{R}^{46}$ into a lower-dimensional latent representation $\mathrm{z} \in \mathbb{R}^{\mathrm{d}}$. The encoder employs a stack of **1D convolutional layers** with ReLU activation functions. The transformation at layer l is defined in Equation 4:

$$\mathrm{h}^{(\mathrm{l})} = \phi\left(\mathrm{W}^{(\mathrm{l})} * \mathrm{h}^{(\mathrm{l}-1)} + \mathrm{b}^{(\mathrm{l})}\right), \quad \mathrm{h}^{(0)} = \mathrm{x} \tag{4}$$

where $\mathrm{h}^{(\mathrm{l})}$ is the output of layer l, $\mathrm{W}^{(\mathrm{l})}$ is the weight kernel of the convolution at layer l, $\mathrm{b}^{(\mathrm{l})}$ is the bias term, $*$ denotes the convolution operation, and $\phi(\cdot)$ is the ReLU activation function.

b) **Decoder**: This stage reconstructs the original input from the latent space. The decoder uses 1D transposed convolutions, as expressed in Equation 5:

$$\hat{\mathrm{x}} = \mathrm{g}(\mathrm{z}) = \mathrm{W}^{\mathrm{dec}} * \mathrm{z} + \mathrm{b}^{\mathrm{dec}} \tag{5}$$

where $\mathrm{W}^{\mathrm{dec}}$ is the weight kernel of the transposed convolution, $\mathrm{b}^{\mathrm{dec}}$ is the corresponding bias, and $\hat{\mathrm{x}}$ is the reconstructed input vector.

3.2.1 Loss function

To train the CONV AE, the model optimizes a Mean Squared Error (MSE) loss, which measures the reconstruction fidelity between the original input x and its reconstruction $\hat{x}$. The loss function is expressed in Equation 6:

$$\mathcal{L}_{\mathrm{ConvAE}}\,(\mathrm{x}, \hat{\mathrm{x}}) = \frac{1}{N}\sum_{i=1}^{N} \|\mathrm{x}_i - \hat{\mathrm{x}}_i\|_2^2 \tag{6}$$

where N is the number of instances in the batch, x_i is the original input for instance i, and $\hat{\mathrm{x}}_i$ is the corresponding reconstruction.

3.2.2 Anomaly Scoring

During inference, the reconstruction error for each instance is computed using Equation 7:

$$\mathrm{s}_i = \|\mathrm{x} - \hat{\mathrm{x}}\|_2 \tag{7}$$

where s_i is the reconstruction error score for instance i. An instance is classified as anomalous if its reconstruction error s_i exceeds an empirically selected threshold τ, determined via validation on $\mathcal{D}_{\mathrm{val}}$.

3.3 Model Training and Evaluation

The Conv AE model was trained using the Adam optimizer with a learning rate $\eta = 0.001$ and a batch size of 128. An early stopping criterion was employed based on validation loss to avoid overfitting.

Model evaluation was conducted on the independent test set $\mathcal{D}_{\mathrm{test}}$ using a comprehensive set of performance metrics to ensure a rigorous and balanced assessment of the model's detection capability.

Given the critical importance of both detecting actual anomalies and avoiding false alarms in IoT networks, a suite of evaluation metrics was employed.

3.3.1 Accuracy

Accuracy is a fundamental evaluation metric in machine learning that measures the proportion of correctly classified instances out of the total instances evaluated. It is commonly used across various classification tasks to gauge the overall performance of a model. Equation 8 depicts the accuracy metrics.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{8}$$

where, TP is True Positive, TN is True Negative, FP is False Positive, and FN is False Negative

While accuracy is intuitive and easy to interpret, it may not always be the most suitable metric, especially when dealing with imbalanced datasets. In such cases, a model might achieve high accuracy by predominantly predicting the majority class. Therefore, complementary metrics are also employed.

3.3.2 Precision

Precision quantifies the proportion of instances predicted as anomalous that are truly anomalous. It is calculated using Equation 9:

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} \ + \ \text{False Positive}} \tag{9}$$

Precision can also be interpreted as the ability of the model to avoid false positives, indicating how confident the model is when it predicts a positive outcome.

3.3.3 Recall

Recall, also known as sensitivity or true positive rate measures the proportion of correctly predicted positive instances out of all actual positive instances. It is expressed in Equation 10:

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive} \ + \ \text{False Negative}} \tag{10}$$

In other words, It quantifies the model's ability to identify all relevant instances, making it particularly important in fields where missing a positive instance can have serious consequences.

3.3.4 F1 score

The F1 score combines the precision and recall into a single value, providing a balanced assessment of a classifier's performance. It is particularly useful when dealing with imbalanced datasets, where the distribution of classes is unequal. Equation 11 shows F1 score calculation as the harmonic mean of precision and recall.

$$\text{F1 Score} = \frac{2 \ \times \text{Precision} \ \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{11}$$

The harmonic mean gives more weight to lower values, penalizing classifiers with imbalanced precision and recall. A high F1 score indicates a good balance between correctly identifying and capturing positive instances.

3.3.5 Confusion matrix

A confusion matrix is a fundamental tool in machine learning for evaluating the performance of a classification model. It provides a comprehensive breakdown of the model's predictions compared to the ground truth labels across different classes.

In a typical binary classification scenario, the confusion matrix has four components:

a) True Positives (TP): Instances where the model correctly predicts the positive class.
b) False Positives (FP): Instances where the model incorrectly predicts the positive class (false alarms)
c) True Negatives (TN): Instances where the model correctly predicts the negative class.
d) False Negatives (FN): Instances where the model incorrectly predicts the negative class (missed detections).

3.3.6 False alarm rate (FAR)

The false alarm rate (FAR), also known as the false positive rate (FPR) or fall-out, reflects a detection system's tendency to misclassify negative cases as positive. In other words, FAR measures the rate at which false alarms occur relative to the total number of true negatives and false positives. Equation 12 shows the FAR evaluation.

$$\text{FAR} = \frac{\text{False Positive}}{\text{False Positive} \ + \ \text{True Negative}} \tag{12}$$

A high FAR indicates that the system frequently raises alerts for events that are actually not indicative of security threats, leading to unnecessary alerts and potential disruption of normal operations. Conversely, a low FAR implies that the system effectively distinguishes between normal and abnormal behavior, minimizing false alarms and ensuring that genuine security threats are detected promptly.

3.3.7 True-negative rate (TNR)

The true-negative rate (TNR), also known as specificity represents the proportion of instances where the system correctly identifies normal behavior or benign events as not malicious or anomalous, relative to the total number of true negatives and false positives.

In essence, TNR measures the system's ability to accurately recognize and classify normal activities or non-threatening events as such, without raising false alarms or incorrectly flagging them as security threats. Equation 13 shows the TNR evaluation.

$$\text{TNR} = \frac{\text{True Negative}}{\text{False Positve} + \text{True Negative}} \tag{13}$$

A high TNR indicates that the system effectively distinguishes between normal and abnormal behavior, minimizing the occurrence of false alarms and ensuring that genuine security threats are accurately detected while maintaining a low rate of false positives. Conversely, a low TNR suggests that the system may fail to adequately recognize normal behavior, leading to an increased risk of false alarms and potential disruption of regular operations.

3.3.8 False-negative rate (FNR)

The false-negative rate (FNR) represents the proportion of instances where the system fails to detect genuine security threats or malicious activities, incorrectly classifying them as normal or benign events, relative to the total number of true positives and false negatives.

In simpler terms, FNR measures the system's ability to accurately identify and classify security threats or anomalous behavior as such, without overlooking or failing to detect them. Equation 14 shows the FNR evaluation.

$$\text{FNR} = \frac{\text{False Negative}}{\text{True Positve} + \text{False Negative}} \tag{14}$$

A low FNR indicates that the system effectively detects and flags genuine security threats, minimizing the risk of undetected malicious activities and ensuring comprehensive security coverage. Conversely, a high FNR suggests that the system may overlook or miss genuine security threats, leading to vulnerabilities and potential security breaches.

3.3.9 Kappa Score

The Kappa Score (Cohen's Kappa) measures the level of agreement between the predicted and true labels, adjusting for chance agreement. It is particularly useful for evaluating classifiers under class imbalance. It is defined in Equation 15:

$$\kappa = \frac{P_o - P_e}{1 - P_e} \tag{15}$$

where P_o is the observed agreement and P_e is the expected agreement by chance.

3.3.10 Matthews Correlation Coefficient (MCC)

The Matthews Correlation Coefficient provides a balanced measure of classification quality, even when the classes are imbalanced. It is computed as shown in Equation 16:

$$\text{MCC} = \frac{\text{TP} \times \text{TN} - \text{FP} \times \text{FN}}{\sqrt{(\text{TP} + \text{FP})(\text{TP} + \text{FN})(\text{TN} + \text{FP})(\text{TN} + \text{FN})}} \tag{16}$$

An MCC value close to +1 indicates perfect classification, while a value close to 0 indicates random performance.

3.3.11 Geometric Mean (G-Mean)

The G-Mean metric evaluates the balance between classification performance on both classes, and is defined in Equation 17:

$$\text{G} - \text{Mean} = \sqrt{\frac{\text{TP}}{\text{TP} + \text{FN}} \times \frac{\text{TN}}{\text{TN} + \text{FP}}} \tag{17}$$

This metric is particularly relevant for anomaly detection tasks where maintaining high sensitivity (recall) and high specificity (true negative rate) is equally important.

4.0 Result and Discussion

The performance of the Convolutional Autoencoder (Conv AE) model was systematically evaluated to determine its suitability for detecting network anomalies in IoT applications over 5G and beyond networks. This section presents a detailed analysis of the results, highlighting both classification accuracy and operational efficiency.

4.1 Training and validation loss curves

The progression of training and validation losses offers critical insight into the Conv AE's learning behaviour. As shown in Figure 2, both loss curves demonstrate a consistent downward trend, with stable convergence achieved after sufficient training epochs. The proximity between training and validation losses suggests the model successfully avoided overfitting while maintaining strong generalisation capabilities. Based on this validation behaviour, an anomaly detection threshold of 0.0262 was derived from the 95th percentile of the validation set's mean squared error (MSE) distribution and subsequently applied for test set classification..

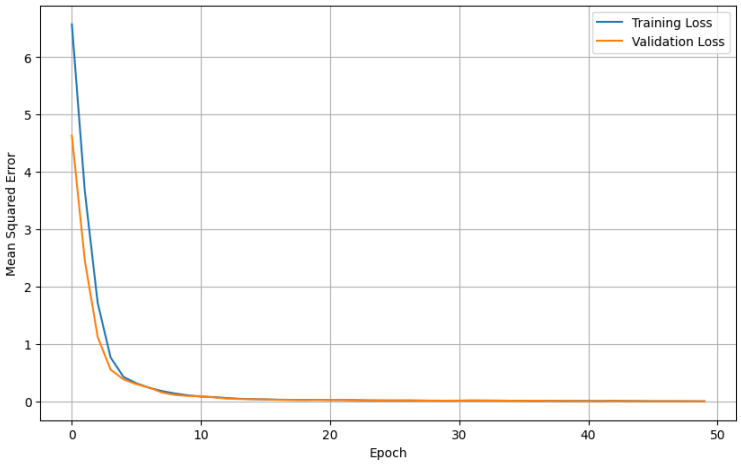

Figure 2. Loss Curves Plot for binary anomaly detection

The convergence behaviour illustrated in Figure 2 confirms that the model maintained excellent generalisation throughout training, providing a reliable basis for anomaly threshold selection.

4.2 Training and Inference Times

In high-speed IoT networks, anomaly detection models must not only achieve high accuracy but also operate with low latency and computational efficiency. The Conv AE demonstrated strong performance in this regard. As illustrated in Figure 3, the model required approximately 905.06 seconds for training. During inference, it achieved a per-sample inference time of 0.0809 seconds, with a Detection Delay of 0.0859 seconds. This is well within acceptable bounds for real-time IoT anomaly detection scenarios. Furthermore, the model processed a full test set of 102,578 samples in 52.87 seconds, highlighting its capacity to scale to large IoT deployments.

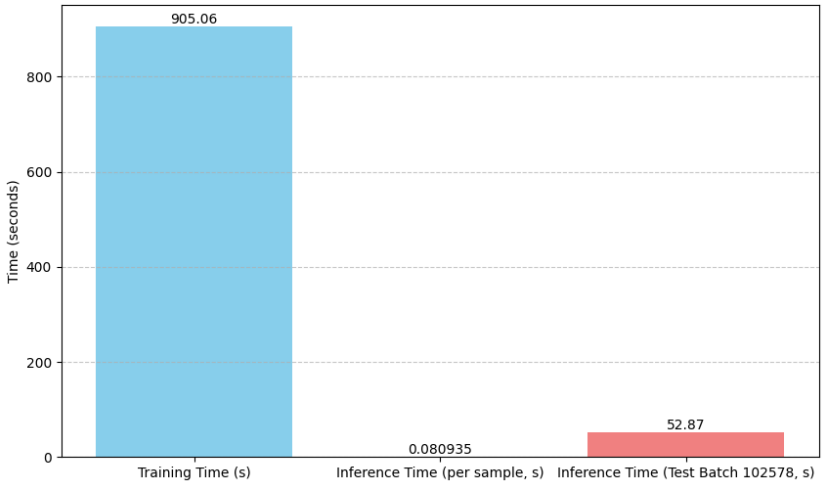

Figure 3. Training and Inference Times (including Detection Delay)

The results in Figure 3 demonstrate that the Conv AE achieves a practical balance between computational efficiency and rapid detection, supporting its deployment in time-sensitive IoT environments.

4.3. Precision, Recall and F1-Score on the Test Set

The model's anomaly detection performance was further evaluated using key classification metrics on the test set. As shown in Figure 4, the Conv AE achieved a Recall of 99.03%, indicating its strong ability to detect anomalous events. The Precision was 99.87%, suggesting that very few false positives occurred. The resulting F1-Score of 99.45% reflects an optimal balance between sensitivity and specificity, which is vital in practical IoT environments where maintaining service quality is critical.

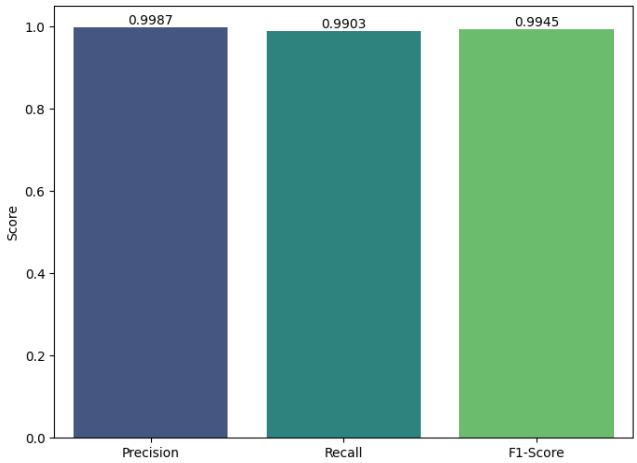

Figure 4. Recall, Precision and F1-Score on the Test Set for Conv AE

The high scores shown in Figure 4 confirm that the Conv AE can robustly identify anomalies while maintaining a low false positive rate, thereby ensuring reliable protection of IoT networks.

4.4 Confusion Matrix Analysis

A detailed breakdown of classification outcomes is provided by the confusion matrix in Figure 5. The model correctly classified 2,285 normal samples (True Negatives) and 99,189 anomalous samples (True Positives). In contrast, 128 normal samples were misclassified as anomalies (False Positives), and 976 anomalous samples were incorrectly classified as normal (False Negatives). These results translate into a False Alarm Rate (FAR) of 5.30% and a True Negative Rate (TNR) of 94.70%, reflecting the model's balanced ability to avoid both excessive false alarms and missed detections.

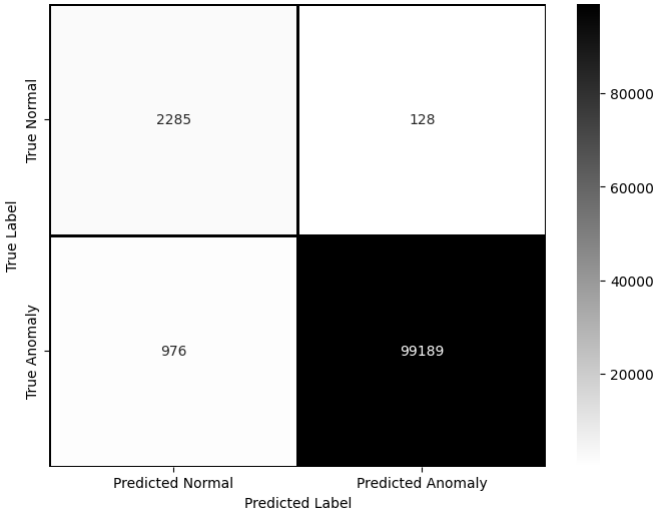

Figure 5. Confusion Matrix for the Test Set

As evidenced by Figure 5, the Conv AE achieves a strong classification balance, effectively limiting both false alarms and missed anomalies in a challenging IoT test environment.

4.5 Receiver Operating Characteristic (ROC) Analysis

The Conv AE's overall discriminative capacity is summarised in Figure 6 through the Receiver Operating Characteristic (ROC) curve. The model achieved an AUC-ROC of 0.9895, which confirms its excellent ability to distinguish between normal and anomalous network traffic. In parallel, the AUC-PR reached 0.9996, further highlighting superior performance under highly imbalanced data conditions. Complementary metrics provide additional support for the model's robustness and reliability. The Kappa score was 0.8000, the Matthews Correlation Coefficient (MCC) reached 0.8096, and the Geometric Mean (G-Mean) stood at 0.9684. Furthermore, the model maintains a lightweight profile, with a disk size of only 9.55 MB, which makes it particularly suitable for deployment in edge-based IoT environments.

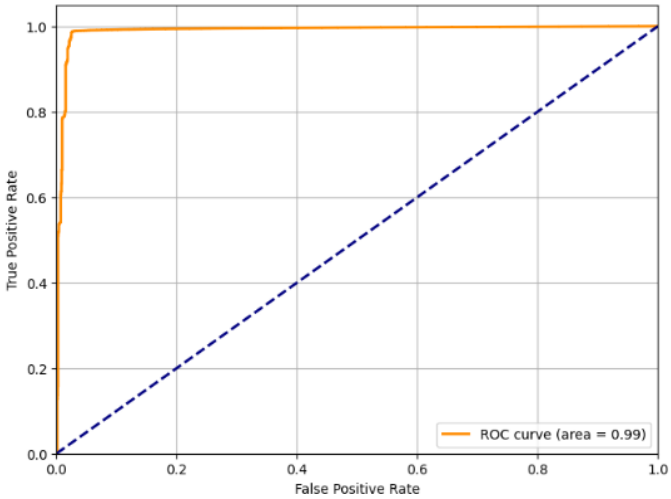

Figure 6. Receiver Operating Characteristic (ROC) Curve

The excellent AUC and supporting metrics presented in Figure 6 provide strong evidence of the Conv AE's capacity to deliver high-fidelity anomaly detection across diverse and imbalanced IoT traffic scenarios.

5.0 Conclusion

This study robustly validates the efficacy of Convolutional Autoencoders (Conv AEs) for binary anomaly detection within eMTC-enabled IoT networks operating in 5G environments. Leveraging the comprehensive CICIoT2023 dataset, comprising over 46 million records of normal and anomalous network traffic, a Conv AE model was meticulously developed. This methodology involved training the model exclusively on benign traffic to robustly learn normal behavior, utilizing an architecture with 1D convolutional layers in the encoder and 1D transposed convolutions in the decoder, optimizing a Mean Squared Error (MSE) loss function. Anomalies were precisely flagged based on reconstruction errors exceeding an empirically optimized threshold.

The research results demonstrated exceptional effectiveness and efficiency. The framework achieved high classification performance, with an Accuracy of 0.9892, Precision of 0.9987, Recall of 0.9903, and an F1-Score of 0.9945, clearly indicating its proficiency in distinguishing anomalous patterns with minimal false positives. Operational efficiency was further confirmed by a low per-sample inference time of 0.0809 seconds, enabling real-time network monitoring capabilities. Consistent performance across a comprehensive suite of evaluation metrics, including AUC-ROC of 0.9895 and AUC-PR of 0.9996, alongside a low False Alarm Rate (0.0530) and high True Negative Rate (0.9470), affirm the model's strong generalization ability and reliability in diverse traffic conditions.

The findings establish Conv AEs as a highly effective and scalable solution for bolstering the security and ensuring the safe deployment of IoT systems, critically addressing the expanding attack surface inherent in current and future generation cellular networks. This research significantly contributes to the advancement of intelligent anomaly detection techniques for critical IoT infrastructure. Future research could extend this to a multi-class classification approach for granular threat insight, thereby providing more detailed threat intelligence for eMTC-enabled IoT applications on 5G and beyond.

6.0 Recommendations

For further research, we recommend extending this Conv AE model to a multi-class classification framework. This would enable the model not only to detect anomalies but also to categorize them into specific attack types, providing network administrators with more granular threat intelligence. A multi-class Conv AE could enhance security in eMTC-enabled 5G-IoT environments by identifying and classifying specific intrusions, such as Distributed Denial-of-Service (DDoS) or botnet attacks, thereby supporting more targeted and efficient responses. Future work could test this approach across diverse real-world datasets, assessing the scalability and performance of multi-class CONV AEs in varying network conditions to refine 5G-IoT network security further.

7.0 Acknowledgments

The authors gratefully acknowledge the financial support provided by the Tertiary Education Trust Fund (TETFUND) through the Institution-Based Research (IBR) intervention, under grant number TETFUND/FUTMINNA/A/2024/061. This support was pivotal in providing the resources and dedicated research time necessary for the successful completion of this study. We also extend our sincere appreciation to the Directorate for Research, Innovation and Development (DRID), Federal University of Technology, Minna, for facilitating the grant process and for their continued administrative and institutional support.

Conflict of interest:

The authors declare no conflicting interest

References

1. Chikezie CI, Usman AU, David M, Suleiman Z, Hassan MA. 5G enabled Internet of Things: A review. Int J Converg Inform Res. 2024;2.
2. Chikezie CI, David M, Usman AU. Power allocation optimization in NOMA system for user fairness in 5G networks. In: 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON). IEEE; 2022. p. 1–4. doi:10.1109/NIGERCON54645.2022.9803107.
3. Law W, Li S, Chavez KMG. Empirical comparison of the energy consumption of cellular Internet of Things technologies. IEEE Access. 2023;11:106374–86. doi:10.1109/ACCESS.2023.3320070.
4. Rizvi S, Pipetti R, McIntyre N, Todd J, Williams I. Threat model for securing internet of things (IoT) network at device-level. Internet Things. 2020 Sep;11:100240. doi:10.1016/j.iot.2020.100240.
5. Thilakarathne NN, et al. Internet of Things (IoT) security: Status, challenges and countermeasures. Int J Adv Netw Appl. 2022;14(3):5444–54. doi:10.35444/IJANA.2022.14305.
6. Hairab BI, Elsayed MS, Jurcut AD, Azer MA. Anomaly detection based on CNN and regularization techniques against zero-day attacks in IoT networks. IEEE Access. 2022;10:98427–40. doi:10.1109/ACCESS.2022.3206367.
7. National Information Technology Development Agency (NITDA). NITDA-CERRT-1.pdf. Regul Reports Act Comput Emerg Readiness Response Team (NITDA-CERRT). Abuja, Nigeria: NITDA; 2023.
8. Nigerian Communications Commission. National Policy on Fifth Generation (5G) Networks for Nigeria's Digital Economy. 2021. p. 28.
9. Kamal AME, Zaghloul MS, Badawi WK, Abdelrassoul RA. Exploit vulnerabilities in 4G and 5G cellular access network. J Adv Res Appl Sci Eng Technol. 2024 Oct;53(2):252–62. doi:10.37934/araset.53.2.252262.
10. Miao J, Wang Z, Wang M, Feng X, Xiao N, Sun X. Security authentication protocol for massive machine type communication in 5G networks. Wirel Commun Mob Comput. 2023 Apr;2023:1–10. doi:10.1155/2023/6086686.
11. Aljohani TM. Cyberattacks on energy infrastructures as modern war weapons—Part I: Analysis and motives. IEEE Technol Soc Mag. 2024 Jun;43(2):59–69. doi:10.1109/MTS.2024.3395688.
12. Altulaihan E, Almaiah MA, Aljughaiman A. Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. Sensors. 2024 Jan;24(2):713. doi:10.3390/s24020713.
13. Nallakaruppan M, Somayaji SRK, Fuladi S, Benedetto F, Ulaganathan SK, Yenduri G. Enhancing security of host-based intrusion detection systems for the Internet of Things. IEEE Access. 2024;PP:1–1. doi:10.1109/ACCESS.2024.3355794.
14. Alluhaidan ASD, Prabu P. End-to-end encryption in resource-constrained IoT device. IEEE Access. 2023;11:70040–51. doi:10.1109/ACCESS.2023.3292829.
15. Niboucha R, Ben Saad S, Ksentini A, Challal Y. Zero-touch security management for mMTC network slices: DDoS attack detection and mitigation. IEEE Internet Things J. 2023 May;10(9):7800–12. doi:10.1109/JIOT.2022.3230875.
16. Ahmed SF, et al. Toward a secure 5G-enabled Internet of Things: A survey on requirements, privacy, security, challenges, and opportunities. IEEE Access. 2024;12:13125–45. doi:10.1109/ACCESS.2024.3352508.
17. Sadhu PK, Yanambaka VP, Abdelgawad A, Yelamarthi K. Prospect of Internet of Medical Things: A review on security requirements and solutions. Sensors. 2022 Jul;22(15):5517. doi:10.3390/s22155517.
18. Meidan Y, et al. N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Comput. 2018 Jul;17(3):12–22. doi:10.1109/MPRV.2018.03367731.
19. Caldas-Filho FL, et al. Botnet detection and mitigation model for IoT networks using federated learning. Sensors. 2023 Jul;23(14):6305. doi:10.3390/s23146305.
20. Khan MM, Alkhathami M. Anomaly detection in IoT-based healthcare: Machine learning for enhanced security. Sci Rep. 2024 Mar;14(1):5872. doi:10.1038/s41598-024-56126-x.
21. Scalise P, Boeding M, Hempel M, Sharif H, Delloiacovo J, Reed J. A systematic survey on 5G and 6G security considerations, challenges, trends, and research areas. Futur Internet. 2024 Feb;16(3):67. doi:10.3390/fi16030067.
22. Dwedar M, Bayram F, Eberhard J, Jesser A. Dynamic anomaly detection in 5G-connected IoT devices using transfer learning. In: 2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI). IEEE; 2024. p. 1–6. doi:10.1109/ICMI60790.2024.10585712.
23. Kimanzi R, Kimanga P, Cherori D, Gikunda PK. Deep learning algorithms used in intrusion detection systems – A review. 2024 Feb. doi:10.48550/arXiv.2402.17020.
24. Berahmand K, Daneshfar F, Salehi ES, Li Y, Xu Y. Autoencoders and their applications in machine learning: A survey. Artif Intell Rev. 2024 Feb;57(2):28. doi:10.1007/s10462-023-10662-6.
25. Ehsani N, Aminifar F, Mohsenian-Rad H. Convolutional autoencoder anomaly detection and classification based on distribution PMU measurements. IET Gener Transm Distrib. 2022 Jul;16(14):2816–28. doi:10.1049/gtd2.12424.
26. Ribeiro M, Romero M, Lazzaretti A, Lopes HS. Learning spatio-temporal features for detecting anomalies in videos using convolutional autoencoder. In: Anais do 14. Congresso Brasileiro de Inteligência Computacional. ABRICOM; 2020. p. 1–8. doi:10.21528/CBIC2019-140.