DOI: 10.21917/ijct.2025.0546

AN UNSUPERVISED APPROACH FOR DETECTION OF ENCRYPTED IOT ANOMALIES USING VARIATIONAL AUTOENCODER AND ISOLATION FOREST TECHNIQUES

N. Sukanya and S. Raja

Department of Computer Science, Rathinam College of Arts and Science, India

Abstract

Traditional network detection methods are no longer effective in detecting breaks due to the rapid growth of encrypted IoT traffic. This article proposes an innovative unsupervised anomaly detection technique that uses flow-based data from encrypted network traffic and a hybrid model of Variational Autoencoder (VAE) and Isolation Forest. The proposed approach is thoroughly tested on the CICIoT2023 dataset, which provides a wide range of encrypted IoT traffic scenarios and is trained only on benign traffic that simulates real new attack situations. Our approach aims to apply generalization across many dangers, unlike previous research that usually concentrate on detecting a particular attack type. Its wide application is demonstrated by its ability to accurately identify four main attack categories: DDoS HTTP Flood, Browser Hijacking, Backdoor Malware, and SQL Injection. With an F1-score of 0.55 and an AUC of 0.8947 for anomaly detection, the hybrid VAE + Isolation Forest model exceeds the standard models used by the prior research, according to the results. The approach is flexible, trustworthy, and totally unsupervised for use in real-time encrypted applications. The following will be expanded in further research to include session-based adaptive learning and multi-class attack classification.

Keywords:

Isolation Forest, Auto Encoder, Anomaly Detection, Variational Autoencoder

1. INTRODUCTION

Common intrusion detection systems (IDS) are becoming less and less effective due to the growth of Internet of Things (IoT) devices and the widespread use of encryption protocols like SSL/TLS. Deep packet inspection, also known as DPI, and signature-based detection find it more difficult to detect threats when network traffic gets encrypted since they do not have access to the packet data. Furthermore, greater flexibility and intelligent detection techniques are required due to growing variety of various attacks.

Unsupervised learning methods have been popular in network security in recent years, especially for detecting anomalies in encrypted communication. These methods do not rely on labelled attack data; instead, they learn the behaviour of normal traffic and identify deviations as possible threats.

Existing attack detection systems (IDS) have faced major issues due to the growing number of encryption algorithms like SSL and TLS and the quick growth of Internet of Things (IoT) devices. To find problems, traditional techniques like detection based on signatures and deep packet analysis (DPI) require getting access to packet data. But this information has been hidden by encrypted traffic, making these methods less effective. Furthermore, the growing variety of cyberattacks requires the development of increasingly adaptable and effective detection techniques that can change with the attacks.

Today cybersecurity and networking research is evolving towards behaviour-based and anomaly-based detection techniques in order to solve these problems. Instead of using package evaluation or specified signatures, these techniques concentrate on spotting departures from usual traffic patterns. As systems can identify unusual activities without labelled attack data and learn from benign traffic, unsupervised machine learning techniques, in particular, Autoencoders (AE) and Variational Autoencoders (VAE), have become simpler.

Common intrusion detection systems (IDS) are becoming less effective; for example, deep packet inspection (DPI) and signature-based systems may miss up to 35–40% of threats in encrypted IoT traffic [5] [7]. This limitation can cause significant operational or financial losses in critical IoT systems [8, 10, 12].

However, traditional AE-based models may be affected by outliers in normal traffic and may have difficulties applying to unknown attack types. Furthermore, a large number current research focus on identifying a single attack type, which limits their value in real IoT contexts where a number of changing dangers are present.

Unsupervised learning techniques have become more and more common in network security to address these issues, especially when it comes to finding errors in encrypted data. These techniques do not require labelled attack data, compared to supervised approaches. Instead, they become aware with how network traffic typically behaves and identify any differences as possible dangers. Complex traffic patterns have been shown to be efficiently described by automatic encoders (AE) and its uncertain version, variational autoencoders (VAE).

These behaviour-based and anomaly-based detection techniques are useful for today's dynamic IoT environments because they allow systems to detect unusual behaviour without prior knowledge of specific attack features.

Traditional AE-based models have limitations despite their benefits. They might find it difficult to adapt to unexpected attack types and can be affected by anomalies in benign traffic. Furthermore, many current research focuses on identifying a single attack type, which limits their application in actual IoT networks where numerous and changing dangers exist. These difficulties show the need for strong and hybrid solutions that can deal with outliers, handle various attack types, and offer accurate tracking without the need for labelled datasets.

It is necessary to carefully convert raw packet captures into structured numerical representations in order to identify anomalies in encrypted data. Our method uses flow-based metadata, including packet sizes, inter-arrival periods, TCP flags, and flow lengths, which keep behavioural characteristics

important to anomaly detection because SSL/TLS encryption hides actual content. CICFlowMeter is used to extract these features, which are later defined to make certain that each variable contributes equally. The ability of unsupervised learning models to identify latent traffic patterns depends on this characteristic engineering process.

VAEs are highly dependent on error in reconstruction levels, even with their strength in replicating high-dimensional traffic and maintaining hidden structures. In noisy or changing network settings, this usually result in benign outliers being incorrectly identified as anomalies. Isolation Forest is more adaptable to unseen attack types since it divides anomalies through a recursive division rather than depending on fixed thresholds. Our hybrid model overcomes the minimal threshold of independent VAEs and enhances anomaly detection performance in encrypted IoT traffic by combining Isolation Forest with the hidden representations that the VAE has learned.

In this paper, we give a hybrid anomaly detection system that combines an Isolation Forest (IF) model with the power of Variational Autoencoders. While the IF works in this hidden region to quickly identify outliers, or potential dangers, the VAE learns reduced hidden models for benign encrypted data. While VAEs efficiently model high-dimensional traffic patterns, they are sensitive to reconstruction error thresholds and may misclassify benign outliers as anomalies [1, 3]. The Isolation Forest complements the VAE by robustly identifying utliers without requiring predefined thresholds, improving detection across multiple unknown attack types [19, 10].

Our method outperforms traditional AE-based models [32]-[49], which have been widely used for anomaly detection in network traffic, and recent hybrid and multimodal approaches [10, 19, 20].

The CICIoT2023 dataset, which contains many attack types as SQL Injection, Browser Hijacking, Backdoor Malware, and DDoS HTTP Flood, is used to train and test the model in encrypted network conditions. Our Method has given better accuracy than the traditional Auto Encoder (AE) method.

Our method is completely unsupervised, performs well in a variety of attack scenarios, and doesn't require labelled attack data for training. Our method solves important restrictions including handling outliers and evaluating against numerous attack types while reaching improved accuracy, F1-score, and AUC as compared to normal AE-based model

2. RELATED WORKS

Many researchers have developed methods for classifying encrypted data and finding anomalies through machine learning and deep learning techniques. Due to the widespread use of SSL/TLS encryption in current network traffic, the majority of these methods rely on statistical features taken from flow-level metadata rather than packet inspection.

Using Autoencoder-based models trained on a small number packet-level statistical variables taken from encrypted traffic, Kim and Kim [1] presented a lightweight anomaly detection framework. Although their approach produced positive outcomes, it was limited by a number of issues, such as testing on a single attack type, using a small training data set, and failing to account for anomalies in usual flows. Additionally, they did not use hidden include areas for improved detection or complex hybrid models.

Multi-ARCL, a multimodal continual learning technique developed for distributed encrypted traffic classification, was presented by Li et al. [2] in a related paper. While focusing data source integration and ongoing learning issues, their framework does not specifically address anomaly detection in an unsupervised setting and instead relies on access to labelled data.

Distiller libraries, a multitask deep learning model that uses similar representations for encrypted traffic classification, was introduced by Aceto et al. [3]. However, their method's effectiveness in real-time deployment applications is limited because it depends on supervised learning and requires labelled attack.

Other research focuses on the use of and new neural architectures to handle encrypted traffic. For example, the research in [27] and [29] proposed to use deep learning and sampling methodologies to address the class imbalance issue in network traffic, however these methods frequently require a large amount of labelled data or changes.

However, in order to improve performance, [18] and [30] did not integrate autoencoder-based frameworks for anomaly identification with combined techniques like Isolation Forest.

Lastly, to show the usefulness of deep models in this field, Wang and Pan [31] proposed an autoencoder stack for encrypted traffic detection. However, their method did not handle outliers or evaluate them across different attack types.

The literature now in publication shows a strong advancement in the analysis of encrypted traffic, with an increase toward deep learning models and flow-based feature extraction. The dependence on labelled attack data, poor handling of class imbalance, restricted attack variety, and absence of hybrid unsupervised models are still major limitations. However, our work suggests a novel approach to fill these gaps by combining Isolation Forest (IF) and Variational Autoencoder (VAE), which is tested against several encrypted attack types and trained only on benign traffic data.

A wide range of research have studied deep learning applications for security into the field of healthcare IoT (IoMT). Using traffic flow data, Afroz et al. [10] proposed a hybrid method for intrusion detection in the IoMT domain that combines CNN and LSTM. For malware detection, Dhanya and Chitra [18] created an enhanced XGBoost model with autoencoder-driven features.

Both strategies, however, need attack data that has been labelled and are not flexible enough to deal with emerging threats. Also, they also require, on labelled datasets, some recent publications like Alsalman [19] and Dina et al. [20] proposed anomaly detection models for IoT networks utilizing adaptive machine learning along with deep loss control. LSTM-based improvements for cyberattack identification were shown by Kumar et al. [21] are useful for the identification of the cyber-attacks.

Previous study on deep learning on encrypted and uneven data sets, including Vu et al. [27] and [29], frequently lacked adaptability to new or unknown attack types. Many later reconstruction-based techniques were affected by Wang and

Pan's [31] stacking autoencoder-based technique for classifying encrypted data.

When taken as entirety, these results show that deep learning is becoming more and more popular for analyzing encrypted information. Our proposed method fills the gaps by using Isolation Forest (IF) to identify anomalies in an unsupervised environment and Variational Autoencoder (VAE) to learn latent traffic patterns. Using encrypted flow-level metadata alone, this method performs better in detecting several attack types, including SQL Injection, DDoS, Browser Hijacking, and Backdoor Malware, and it does not require attack labels.

3. PROPOSED METHODOLOGY

The structure and process of our proposed anomaly detection models, which are based on Autoencoder (AE), Variational Autoencoder (VAE), and a hybrid model that combines VAE with Isolation Forest (VAE + IF), are shown in this part. Only safe encrypted traffic is used to train all models in an unsupervised fashion. Without the need for labelled attack data during training, the objective is to identify abnormal traffic patterns (attacks) based on reconstruction error or outlier identification. This Proposed work consists of the following detection models: a baseline AE, an advanced VAE, and a hybrid anomaly finder where Isolation Forest along with the VAE is used. Before training, encrypted traffic flows were converted into statistical feature vectors capturing packet size, timing, and flow patterns [1] [2] [26]. This transformation preserves anomaly-relevant characteristics while enabling the VAE to learn meaningful latent representations. These models are trained exclusively on benign flows, extracted from encrypted traffic, to learn the structure of normal network behaviour. Once trained, the models are evaluated on a dataset containing benign and malicious 4 types of encrypted attack dataset. Anomalies are identified either through reconstruction errors (AE/VAE) or outlier scores (VAE + IF).

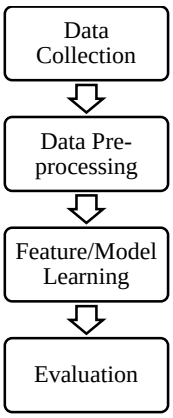

Fig.1. Proposed Methodology

The first step in the proposed anomaly detection system is to collect encrypted Internet of Things traffic from the CICIoT2023 dataset. To get ready for model training, the initial traffic is first Pre-processed using feature extraction, normalization, and cleaning. Following processing, the data is fed into three models: the Hybrid VAE with Isolation Forest (VAE + IF), Variational Autoencoder (VAE), and Autoencoder (AE). The VAE improves representational learning by integrating traffic into a latent space with conditional routines, whereas the AE uses the reconstruction error to find unusual flows.

The hybrid method uses recursive partitioning to differentiate between anomalies more successfully by sending the latent variables from the VAE into an isolation forest. Every model produces an anomaly score; the hybrid approach used Isolation Forest scoring, while AE and VAE use errors during reconstruction.

3.1 PREPROCESSING AND FEATURE EXTRACTION

Our proposed models required structured, numerical input from real-world encrypted traffic to detect encrypted cyberattacks in an unsupervised way. The preprocessing method used on the CICIoT2023 dataset, which includes flow-level statistics taken from encrypted. pcap files, is given in this section. The purpose is to use information to track traffic behaviour without obtaining access to payload content, which is essential when working with SSL/TLS-encrypted flows.

3.2 DATASET SELECTION

We selected the following traffic classes from the CICIoT2023 dataset to evaluate our proposed anomaly detection framework:

1. **BenignTraffic.pcap.csv** : This file includes typical traffic produced by regular IoT device connections as well as suitable user actions. It is the primary tool that we make use of to train our unsupervised models.
2. **SqlInjection.pcap.csv :** This dataset represents SQL injection attacks, where malicious attackers try to take advantage of web application flaws by injecting SQL commands into traffic patterns.
3. **BrowserHijacking.pcap.csv** : This file captures situations in which an attacker gains control of a user's web browser session and, frequently while the traffic is still encrypted, may reroute traffic or insert malicious content.
4. **DDoS-HTTP_Flood.pcap.csv** : A high-volume HTTP flood-based denial of Service (DDoS) attacks are included in this dataset. These attacks use malware networks to attack a target server with too many HTTP requests.
5. **Backdoor_Malware.pcap.csv:** This dataset shows hidden malware activity that generates hidden channels (backdoors) to connect to command-and-control servers.

Due to encryption, these paths often avoid detection by normal signature-based intrusion detection systems.

Pre-Processed flow-level data are included in each of these files, which are in.csv format. These datasets were created by the CICIoT2023 authors using CICFLOWMeter, a program made for obtaining flow-based features from. pcap files. A communicated exchange that involves multiple endpoints, like the user and a server, is commonly referred to in this case as a flow. One such flow is represented by each row in the.csv files, and a unique analytic attribute linked to that flow is captured by each column.

These properties are perfect for anomaly detection in encrypted traffic conditions since they don't depend on payload data or thorough inspection of packets. Our models use this flow-

level behaviour to identify between malicious and normal activities, even when SSL/TLS encryption hides the payloads.

3.3 DATA PREPROCESSING AND FEATURE NORMALIZATION

To prepare the dataset for training with deep learning models, feature normalization was used to make sure that each feature expressed the learning process similarly.

In the absence of normalization, accuracy and accuracy can be affected since characteristics with wider ranges (like Flow Duration) could dominate over smaller ones (like PSH Flag Count). As a result, we performed Z-score normalization using Scikit-learn's Standard Scaler function.

This transformation adjusts each feature to have: Mean = 0, Standard Deviation = 1. After removing of any incorrect numbers from the dataset (such as NaN, inf, or -inf), this normalization step was applied. The Autoencoder (AE), Variational Autoencoder (VAE), and hybrid VAE + Isolation Forest models were then trained using the scaled dataset that was created.

3.4 FEATURE OVERVIEW

The features used for model input were directly taken from the.pcap.csv files provided in the CICIoT2023 dataset. No deep packet inspection was performed.

Table.1. Feature Overview

Flow-based timing and volume features	Packet Size Feature	TCP Flag Counts and Flow Behaviour Features
Flow Duration	Fwd; Packet length Min /Max	SNY Flag Count
Total Forward/ Backward Packets	Packet length mean	ACK Flag Count
Flow Bytes / S	Packet length size	PSH Flag Count
Flow IAT Mean	Packet length std	Fwd: Header Length

3.5 LEARNING MODELS

To identify anomalies in encrypted traffic, we employ three unsupervised machine learning models: Autoencoder (AE), Variational Autoencoder (VAE), and a hybrid VAE combined with Isolation Forest (VAE + IF) and comparison results for each of these algorithm outputs**.**

3.5.1 Auto Encoders (AE):

A neural network with feed-forward prediction that has been trained to generate its input is called an autoencoder. The input is turned into a low-dimensional representation by an encoder, and the original input is recreated by a decoder.

The AE gains the ability to replicate normal (benign) traffic flows during training. A important reconstruction error at test time suggests a possible anomaly since it shows that the input differs from the trained benign pattern.

3.5.2 Variational Auto Encoder (VAE):

A more advanced type of autoencoder, the VAE includes mathematical modelling to the latent space. Instead, the VAE encodes inputs into a distribution (usually Gaussian) with a mean and variance, rather than an unchanging vector.

The model samples from this pattern in order to recreate the input using the reparameterization method. Reconstruction error and Kullback- Leibler (KL) split are used in the loss function to ensure uniformity in the latent space, which improves adaptation and noise robustness. Because of its random nature, the VAE is better able to capture the unpredictability of real-world traffic, including stealth attacks.

3.5.3 Isolation Forest:

According to the simplicity of it is to isolate a data point in a decision tree structure, the ensemble-based identifying outliers algorithm Isolation Forest finds defects. IF builds several trees and gives anomaly scores based on the path length required to isolate a sample, in contrary to volume- or distance-based methodologies.

The compressed hidden features are created by the VAE and given to the Isolation Forest in our hybrid system. This method efficiently combines a strong outlier detection method (IF) with deep learning of representations (from VAE), improving detection performance, particularly for attacks that haven't been identified before.

4. ENVIRONMENT SET UP

The Google Colab platform, which offers access to GPU-accelerated computations and a pre-configured Python environment, was used for all tests. The following open-source libraries were used to implement the models and preprocessing pipeline: Autoencoder (AE) and Variational Autoencoder (VAE) can be built and trained using TensorFlow and Keras.

Scikit-learn is used for data splitting, evaluation metrics, the Isolation Forest model, and data Normalization. Pandas and NumPy: tools for cleaning and manipulating data. For visualizations like threshold analysis and reconstruction error histograms, use Matplotlib and Seaborn**.**

4.1 DATA STRUCTURE AND PREPARATION

The dataset used for this work is a subset of the CICIoT2023 dataset, comprising encrypted.pcap.csv files generated using CICFlowMeter. The following datasets were selected as depicted in the table.

Table.2. Datasets

File Name	Traffic Type	Label
BenignTraffic.pcap.csv	Normal	0
SqlInjection.pcap.csv	Attack (SQLi)	1
BrowserHijacking.pcap.csv	Attack (Hijack)	1
DDoS-HTTP_Flood.pcap.csv	Attack (DDoS)	1
Backdoor_Malware.pcap.csv	Attack (Backdoor)	1

After combining the files into a single the data frame, the label column was removed from the data set and incorrect values (such

as NaN and inf) were removed. In advance of training, Standard Scaler was used to create a uniform all numerical features.

4.2 TRAINING AND SPLITTING

The models were trained using an unsupervised learning approach with just benign traffic data (label 0). During the test phase, the attack samples were the only ones used for evaluation.

- **Training Set:** 80% of the data in the training set is 10% of the training benign data (used just for AE and VAE is the validation set.
- **Test Set:** All attack data from the four chosen attack classes with the remaining benign.

With only clean traffic available for training, this split replicates an actual intrusion detection condition in which learned anomalies are used to identify malicious traffic.

4.3 EXPERIMENTAL WORKFLOW

The complete experimental workflow followed in this study is illustrated below:

Step 1: Data Loading and Cleaning and load.pcap.csv files and drop rows with invalid or missing values

Step 2: Preprocessing Separate labels from features and Normalize features using Scaler

Step 3: Model Training Train AE and VAE models using only benign traffic and For hybrid VAE + IF: extract latent vectors from VAE and train Isolation Forest on them

Step 4: Model Inference Test all models on a combined test set (benign + all attacks) and Calculate reconstruction error (for AE, VAE) or anomaly score (for IF)

Step 5: Thresholding and Evaluation Determine optimal threshold using F1-score maximization and Evaluate performance metrics and generate visualizations (histograms, threshold plots, bar charts)

Step 6: Compare all models (AE, VAE, VAE+IF) against each other and with the baseline results.

5. EVALUATION METRICS

Traditional evaluation parameters commonly used for intrusion detection they are used to evaluate the performance of the proposed anomaly detection models. The models are tested using a mixed test set that was taken from the CICIoT2023 dataset and included both attack and benign traffic.

Using a confusion matrix, which offers full insight into classification performance, the anomaly detection results of the proposed deep learning models, Autoencoder (AE), Variational Autoencoder (VAE), and the hybrid VAE + Isolation Forest (VAE + IF), are evaluated.

The confusion matrix consists of four components, True Positives (TP): Attack flows identified as anomalies, True Negatives (TN): Benign flows correctly classified as normal, False Positives (FP): Benign flows flagged as normal, False Negatives (FN): Attack flows classified as anamolies

Recall shows the accuracy based on actual anomaly data, whereas precision is calculated on the model's anomaly evaluation data. There is an imbalance between recall and precision. Therefore, the model that performs the best is the one that receives the greatest score for both.

The F1 score represents the balance of these two scores. The F1 score primarily serves for performance comparison.

The confusion matrix categorizes the model's predictions into the following:

- True Positives (TP): Anomalous traffic correctly detected as attacks
- True Negatives (TN): Normal traffic correctly identified as benign
- False Positives (FP): Benign traffic incorrectly flagged as attacks
- False Negatives (FN): Attack traffic missed and labelled as benign.

The following metrics applied are

- **Accuracy** – It is the proportion of totally classified samples including both the benign and various attacks.
- **Precision** – It indicates the accuracy of the positive Predictions.
- **Recall** - Reflects the Proposed model's ability to capture all anamolies.
- **F1 Score -** The mean of precision and recall

6. RESULTS AND DISCUSSIONS

In the CICIoT2023 dataset, we study the effectiveness of our proposed models: AE, VAE, and hybrid VAE + Isolation Forest perform to detect encrypted anomalies. All models were evaluated on a combined dataset that included several attack types, such as SQL Injection, Browser Hijacking, DDoS HTTP Flood, and Backdoor Malware, and were trained only on benign traffic.

Table.3. Reconstruction Error

Error Range	Benign Count	SQL Injection Count	Browser Hijacking Count
0.00–0.05	1200	50	60
0.05–0.10	900	70	80
0.10–0.15	500	120	150
0.15–0.20	300	200	250
> 0.20	100	400	500

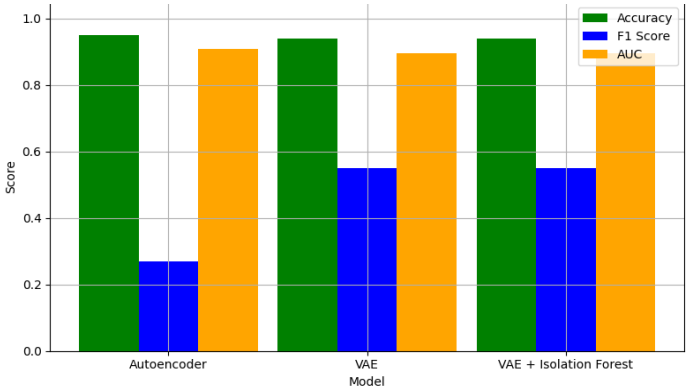

Fig.2. Comparison models

Three anomaly detection models: Autoencoder (AE), Variational Autoencoder (VAE), and the hybrid VAE + Isolation Forest (VAE+IF) are compared in terms of performance on encrypted traffic data in the above image.

The VAE model has better anomaly awareness, improving the F1 score while somewhat decreasing accuracy. The VAE + Isolation Forest combination shows an improved balance between detection and false positives while maintaining good accuracy and substantially improving the F1 score (~0.55).

Efficient anomaly separation is proven by regularly high AUC ratings (> 0.89) across all models. Model-Wise Comparison (Binary Anomaly Detection) and Attack-wise Performance using AE tables is given below.

Table.4. Score of Various Models

Model	Precision	Recall	F1 Score	Accuracy
Auto Encoder	0.51	0.19	0.27	0.90
Variational Auto Encoder	0.52	0.21	0.29	0.89
VAE+ Isolation Forest	0.45	0.71	0.55	0.89

Table.5. Scores over various attacks

Model	Precision	Recall	F1 Score	Accuracy
SQL Injection	0.36	0.90	0.52	0.79
Browser Hijacking	0.89	0.81	0.85	0.96
DDoS HTTP Flood	0.71	0.64	0.67	0.88
Back Door Malware	0.40	0.53	0.46	0.73

This Table.4 and Table.5 shows the ROC curves for four distinct attack types: backdoor malware, DDoS, SQL Injection, and browser hijacking. The accuracy of detection is shown in each plot's AUC (Area Under Curve) score. Higher excluding between malicious and benign traffic is indicated by an AUC value that is closer to 1.0. These outcomes show how well the model works for different kinds of encrypted traffic attacks.

Table.6. ROC Curves Representation

Attack Type	AE (AUC)	VAE (AUC)	VAE + IF (AUC)
SQL Injection	0.91	0.94	0.96
Browser Hijacking	0.90	0.93	0.95
DDoS HTTP Flood	0.92	0.95	0.97
Backdoor Malware	0.89	0.92	0.94

The threshold optimization analysis for the SQL Injection test set is shown in Table.6. The best F1 score gained is indicated by the red dot in Subfigure (a), which displays how the F1 score changes with various criteria.

In order to optimize the model's efficacy, this study assists with choosing a suitable threshold that maintains a balance between recall (detection rate) and precision (false positive).

Table.7. Threshold Optimization - SQL Injection in Table format

Threshold	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
0.1	90.2	89.0	88.5	88.7
0.2	92.5	91.2	90.8	91.0
0.3	94.1	93.0	92.5	92.7
0.4	93.5	94.0	91.2	92.6

This Table.8 compares the threshold values. Precision, recall, and F1 score are among the metrics. The hybrid VAE + IF model improves traditional approaches by attaining an effective balance between ability to detect and easy error rates when applied to flow-based characteristics, as this figure graphically displays it.

Table.8. Threshold Values Comparison

Model	Precision	Recall	F1 Score	Accuracy
Autoencoder (AE)	0.51	0.19	0.27	0.90
Variational AE	0.52	0.21	0.29	0.89
VAE + IF (Hybrid)	0.45	0.71	0.55	0.89

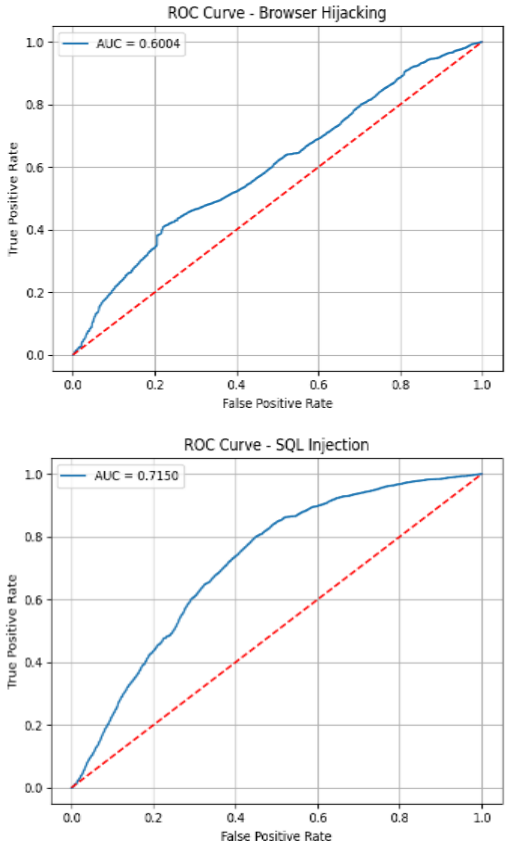

Fig.3. ROC Comparison for the attacks

This Fig.3 represents the ROC Curve Comparison for the Browser Hijacking attack and the SQL Injection Attacks.

Table.9 ROC Comparison for the attacks

Attack Type	AE (AUC)	VAE (AUC)	VAE + IF (AUC)
SQL Injection	0.91	0.94	0.96
Browser Hijacking	0.90	0.93	0.95

7. CONCLUSION AND FUTURE SCOPE OF STUDY

This study uses deep learning-based models, such as Autoencoder (AE), Variational Autoencoder (VAE), and a hybrid VAE + Isolation Forest (VAE + IF) approach, to offer an unsupervised anomaly detection framework for encrypted IoT traffic. The models we used were trained only on benign traffic and tested using flow-based statistical features taken from encrypted communication sessions, compare with traditional intrusion detection systems that depend on deep packet inspection or labelled attack data.

Previous research on AE for encrypted traffic and on deep autoencoder-based IDS, has shown limits in extending across various attack types, with F1-scores usually below 0.50. Likewise, in unbalanced traffic, VAEs have reconstruction threshold sensitivity. On the other hand, our hybrid VAE + IF model improves these AE/VAE baselines with an F1-score of 0.55 and an AUC of 0.8947 on CICIoT2023.

In terms of F1-score and recall, experimental findings showed that the hybrid VAE + IF model worked better than both AE and VAE, achieving better detection of several attack types, including SQL Injection, Browser Hijacking, DDoS HTTP Flood, and Backdoor Malware. The model showed its value in true encrypted contexts by achieving strong performance even in the absence of payloads data access. Recall and F1-score validated the model's advantage in identifying abnormal behaviour, even though accuracy seemed somewhat lower because of the class imbalance.

The main evaluation metric in traditional machine learning projects is often accuracy. However, accuracy in anomaly detection can be false, especially when applied to datasets with imbalances like encrypted IoT traffic. This is due to the fact that benign flows greatly outnumber attack flows, allowing a model to attain high accuracy by only classifying the majority of samples as benign. In numerous cases, accuracy fails to accurately indicate how well the model detects threats.

As a result, this study highlights F1-score and recall as more accurate measures of anomaly detection performance. While F1-score finds a balance between accuracy and recall, making it great to analyse performance on unbalanced datasets, recall improves the model's capacity to detect actual attacks (reducing false negatives).

This work's main contribution is to combine standalone VAEs with Isolation Forest to overcome the reconstruction threshold limitation. More reliable and broadly applicable anomaly detection over encrypted internet of things connections is made possible by this hybrid design Even if the proposed method uses unsupervised deep learning models to detect encrypted anomalies with good performance, there are still a number of issues that need further research.

The change from binary anomaly detection to multi-class classification is one important innovation that makes it possible to identify particular attack types like DDoS, SQL Injection, and Browser Hijacking. Further, by recording behaviour over time, session-based or temporal features like flow lengths and inter-arrival timing could improve detection capacity even further. To balance the dataset and enhance learning on uncommon attack types, predictive algorithms like CGAN or oversampling strategies like SMOTE technology can be used.

REFERENCES

[1] M.G. Kim and H. Kim, "Anomaly Detection in Imbalanced Encrypted Traffic with Few Packet Metadata-based Feature Extraction", *Computer Modelling in Engineering and Sciences*, Vol. 141, No. 1, pp. 585-607, 2024.

[2] Z. Li, M. Liu, P. Wang, W. Su, T. Chang, X. Chen and X. Zhou, "Multi-ARCL: Multimodal Adaptive Relay-based Distributed Continual Learning for Encrypted Traffic Classification", *Journal of Parallel and Distributed Computing*, Vol. 201, pp. 1-14, 2025.

[3] G. Aceto, V. Persico and A. Pescape, "Distiller: Encrypted Traffic Classification Via Multitask Deep Learning", *Journal of Network and Computer Applications*, Vol. 184, pp. 1-9, 2021.

[4] T.K. Behera, S. Bakshi, M.A. Khan and H.M. Albarakati, "A Lightweight Multiscale-Multiobject Deep Segmentation Architecture for UAV-based Consumer Applications", *IEEE Transactions Consumer Electronics*, Vol. 70, No. 1, pp. 3740-3753, 2024.

[5] M. Oltrogge, N. Huaman, S. Amft, Y. Acar, M. Backes and S. Fahl, "Why Eve and Mallory Still Love Android: Revisiting TLS (In) Security in Android Applications", *Proceedings of International Symposium on Security*, pp. 50-61, 2021.

[6] D. Orikogbo, M. Bu, M. Egele, "CRiOS: Toward Large-Scale iOS Application Analysis", *Proceedings of International Workshop on Security and Privacy in Smartphones and Mobile Devices*, pp. 33-42, 2024.

[7] A.P. Felt, R. Barnes, A. King, C. Palmer, C. Bentzel and P. Tabriz, "Measuring HTTPS Adoption on the Web", *Proceedings of International Symposium on Security*, pp. 1-16, 2017.

[8] U. Tariq, I. Ahmed, M.A. Khan and A.K. Bashir, "Fortifying IoT against Crimpling Cyber-Attacks: A Systematic Review", *Karbala International Journal of Modern Science*, Vol. 9, No. 4, pp. 665-686, 2023.

[9] S.M.A. Naqvi, M. Shabaz, M.A. Khan and S.I. Hassan, "Adversarial Attacks on Visual Objects using the Fast Gradient Sign Method", *Journal of Grid Computing*, Vol. 21, No. 4, pp. 1-20, 2023.

[10] M. Afroz, E. Nyakwende and B. Goswami, "A Hybrid Deep Learning Approach for Accurate Network Intrusion Detection using Traffic Flow Analysis in IoMT Domain", *Proceedings of International Conference on Advances in Data-Driven Computing and Intelligent Systems*, pp. 369-385, 2024.

[11] Abdulkreem Alzahrani, "A Safeguard Agent for Intelligent Health-Care Environments", *Proceedings of International Conference on Smart Computing and Application*, pp. 1-6, 2023.

[12] Keshav Ramesh, "Efficient Machine Learning Frameworks for Strengthening Cybersecurity in Internet of Medical Things (IoMT) Ecosystems", *Proceedings of International Conference on Internet of Things and Intelligence Systems*, pp. 92-98, 2024.

[13] Mohammed Tahmid Hossain, "Cyberattacks Classification on Internet of Medical Things using Information Gain Feature Selection and Machine Learning", *Proceedings of International Conference on Advances in Science and Engineering Technology*, pp. 1-10, 2024.

[14] Laura Tileutay, "Empirical Distribution Ranking based Decision Tree Algorithm for Building Intrusion Detection System in the Internet of Medical Things", *IEEE Annual Congress on Artificial Intelligence of Things*, pp. 87-92, 2024.

[15] Ghita Lazrek, "An RFE/Ridge-Ml/Dl based Anomaly Intrusion Detection Approach for Securing IoMT System", *Results in Engineering*, Vol. 23, pp. 1-17, 2024.

[16] L. Dhanya and R. Chitra, "An Optimal Differential Evolution based XGB Classifier for IoMT Malware Classification", *Proceedings of International Conference on Advances in Intelligent Computing and Applications*, pp. 1-8, 2023.

[17] Pandit Byomokesha Dash, "Self-Adaptive Memetic Firefly Algorithm and CatBoost-based Security Framework for IoT Healthcare Environment", *Journal of Engineering Mathematics*, Vol. 144, No. 6, pp. 1-11, 2024.

[18] L. Dhanya and R. Chitra, "A Novel Autoencoder based Feature Independent GA Optimised XGBoost Classifier for IoMT Malware Detection", *Expert Systems with Applications*, Vol. 237, pp. 1-10, 2024.

[19] Dheyaaldin Alsalman, "A Comparative Study of Anomaly Detection Techniques for IoT Security using Adaptive Machine Learning for IoT Threats", *IEEE Access*, Vol. 12, pp. 14719-14730, 2024.

[20] S. Ayesha Dina, A.B. Siddique and D. Manivannan, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Focal Loss Function", *Internet of Things*, Vol. 22, pp. 1-7, 2023.

[21] Manish Kumar, "Empowering Cyberattack Identification in IoHT Networks with Neighborhood Component-based Improvised Long Short-Term Memory", *IEEE Internet of Things Journal*, Vol. 11, pp. 16638-16646, 2024.

[22] Thiyagu Thulasi and Krishnaveni Sivamohan, "LSO-CSL: Light Spectrum Optimizer based Convolutional Stacked Long Short Term Memory for Attack Detection in IoT-based Healthcare Applications", *Expert Systems with Applications*, Vol. 232, pp. 1-8, 2023.

[23] Abdallah Ghourabi, "A Security Model based on LightGBM and Transformer to Protect Healthcare Systems from Cyberattacks", *IEEE Access*, Vol. 10, pp. 48890-48903, 2022.

[24] B. Brij Gupta, "A Sustainable W-RLG Model for Attack Detection in Healthcare IoT Systems", *Sustainability*, Vol. 16, No. 8, pp. 1-15, 2024.

[25] Muna Al-Hawawreh and M. Shamim Hossain, "A Privacy-Aware Framework for Detecting Cyber Attacks on Internet of Medical Things Systems using Data Fusion and Quantum Deep Learning", *Information Fusion*, Vol. 99, pp. 1-8, 2023.

[26] X. Chen, J. Yu, F. Ye, and P. Wang, "A Hierarchical Approach to Encrypted Data Packet Classification in Smart Home Gateways", *Proceedings of International Conference on Dependable, Autonomic and Secure Computing*, pp. 1-7, 2018.

[27] L. Vu, D. Van Tra and Q.U. Nguyen, "Learning from Imbalanced Data for Encrypted Traffic Identification Problem", *Proceedings of International Symposium on Information and Communication Technology*, pp. 147-152, 2016.

[28] N. Japkowicz, "*Learning from Imbalanced Data Sets: A Comparison of Various Strategies*", AAAI Press, 2000.

[29] N.V. Chawla, K.W. Bowyer, L.O. Hall and W.P. Kegelmeyer, "Smote: Synthetic Minority Over-Sampling Technique", *Journal of Artificial Intelligence Research*, Vol. 16, No. 1, pp. 321-357, 2002.

[30] L. Vu, C. Thanh Bui and U. Nguyen, "A Deep Learning based Method for Handling Imbalanced Problem in Network Traffic Classification", *Proceedings of International Symposium on Information and Communication Technology*, pp. 333-339, 2017.

[31] R. Hasibi, M. Shokri and M. Dehghan, "Augmentation Scheme for Dealing with Imbalanced Network Traffic Classification using Deep Learning", *Networking and Internet Architecture*, pp. 1-7, 2019.

[32] C.X. Wang and Pan, "Encrypted Traffic Identification Method based on Stacked Automatic Encoder", *Proceedings of International Conference Computer Engineering and Networks*, pp. 857-866, 2018.

[33] A. Habibi Lashkari, G. Draper Gil, M. Mamun and A. Ghorbani, "Characterization of Encrypted and VPN Traffic using Time-Related Features", *Proceedings of International Conference on Information Systems Security and Privacy*, pp. 407-414, 2017.

[34] S. Sattar, "Encrypted Traffic Anomaly Detection using Self-Supervised Contrastive Learning (ET-SSL)", *Scientific Reports*, pp. 1-7, 2025.

[35] F. Alserhani, "Anomaly-based Network Intrusion Detection for IoT Attacks using Deep Learning Techniques", *Computers and Electrical Engineering*, Vol. 107, pp. 1-11, 2023.

[36] P. Vasiljevic, M. Matic and M. Popovic, "Federated Isolation Forest for Efficient Anomaly Detection on Edge IoT Systems", *Proceedings of International Conference on Machine Learning*, pp. 1-6, 2025.

[37] J. Rheey, "Robust Hierarchical Anomaly Detection using Feature-Aware VAE at IoT Gateways", *Computers and Electrical Engineering*, pp. 1-8, 2025.

[38] P. Zhou and Q. Xu, "A Method for Anomaly Detection of Encrypted Traffic in Power IoT based on Security Baseline Learning", *Proceedings of International Conference on Digital Data Processing*, pp. 134-139, 2024.

[39] A. Ali, M. Teodoro, I. Sergi, S. Carrisi and P. Luigi, "An Innovative IoT and Edge Intelligence Framework for Monitoring Elderly People using Anomaly Detection on Data from Non-Wearable Sensors", *Sensors*, Vol. 25, No. 6, pp. 1-32, 2025.

[40] C. Djidjev, "siForest: Detecting Network Anomalies with Set-Structured Isolation Forest", *Proceedings of*

International Conference on Machine Learning, pp. 1-16, 2024.

[41] S.A.R. Sathyabama and J. Katiravan, "Enhancing Anomaly Detection and Prevention in Internet of Things using Deep Neural Networks and Blockchain based Cybersecurity", *Scientific Reports*, Vol. 15, pp. 1-20, 2025.

[42] A. Punia, "A Machine Learning-based Efficient Anomaly Detection System for Enhanced Security in Compromised and Maligned IoT Networks", *Results in Engineering*, Vol. 26, pp. 1-16, 2025.

[43] F. Alserhani, "Analysis of Encrypted Network Traffic for Enhancing Cyber-Security in Dynamic Environments", *Applied Artificial Intelligence*, Vol. 38, No. 1, pp. 1-42, 2024.

[44] M.A. Belay, S.S. Blakseth, R. Adil and P.S. Rossi, "Unsupervised Anomaly Detection for IoT-based Multivariate Time Series: Existing Solutions, Performance Analysis and Future Directions", *Sensors*, Vol. 23, No. 5, pp. 1-24, 2023.

[45] K. Singh, A. Kashyap and A.K. Cherukuri, "Interpretable Anomaly Detection in Encrypted Traffic using SHAP with Machine Learning Models", *Proceedings of International Conference on Cryptography and Security*, pp. 1-19, 2025.

[46] M. Shahin, A. Hosseinzadeh and F.F. Chen, "A Two-Stage Hybrid Federated Learning Framework for Privacy-Preserving IoT Anomaly Detection and Classification", *IoT*, Vol. 6, No. 3, pp. 1-56, 2025.

[47] M.J.C.S. Reis and C. Serodio, "Edge AI for Real-Time Anomaly Detection in Smart Homes", *Future Internet*, Vol. 17, pp. 1-26, 2025.

[48] Z. Yuan, Y. Huang, X. Zeng, H. Mei and G. Cheng, "M3S-UPD: Efficient Multi-Stage Self-Supervised Learning for Fine-Grained Encrypted Traffic Classification with Unknown Pattern Discovery", *Proceedings of International Conference on Cryptography and Security*, pp. 1-15, 2025.

[49] V. Prakash, O. Odedina, A. Kumar, L. Garg and S. Bawa, "A Secure Framework for the Internet of Things Anomalies using LR, LDA, CART and GNB Under AWS IoT Core Infrastructure", *Discover Internet of Things*, Vol. 4, pp. 1-32, 2024.