Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

AI-Based Anomaly Detection for Encrypted Network Traffic using Metadata Analysis

Malhar Kishor Bhikule
Department of Information
Technology (Information Security)
KJ Somaiya School of Engineering
(formerly known as KJ Somaiya College of Engineering)
Vidyavihar, Mumbai, Maharashtra, 400077

Prof. Purnima Ahirao
Department of Information
Technology (Information Security)
KJ Somaiya School of Engineering
(formerly known as KJ Somaiya College of Engineering)
Vidyavihar, Mumbai, Maharashtra, 400077

Abstract **-** The emergence of encrypted communication protocols has greatly improved network security and user privacy, but that has also led to a decrease in the performance of standard Intrusion Detection Systems (IDSs), which rely on packet content inspection. This paper describes a framework for anomaly detection that utilizes artificial intelligence in the course of detection of encrypted network traffic by extracting flow-level data from Packet Capture (PCAP) files with CICFlowMeter software. Once the features are extracted the data goes through such preprocessing stages as data cleaning, feature selection, and Min-Max normalization and then goes through the analysis based on a hybrid solution using Isolation Forest and Autoencoder algorithms to perform anomaly detection. The purpose of the Isolation Forest algorithm is to detect the statistical outliers while the Autoencoder focuses on finding complex anomalies through the reconstruction error. The framework was tested on the CICIDS2017 dataset, achieving 96.8% in terms of accuracy, 95.9% in terms of precision, 96.2% in terms of recall, 96.0% in terms of F1-score, and 0.98 in terms of ROC-AUC. The results show that the use of flow-level data can successfully identify anomalous encrypted traffic while allowing to maintain high level of privacy.

I. INTRODUCTION

The wide application of cloud computing, Internet of Things (IoT) systems, online payments, e-commerce solutions, and remote work rules has fueled the need for encrypted data transmission. Through the process of data transmission, users rely on various protocols such as TLS, HTTPS, SSH, IPSec, and VPN in order to protect the data information and user privacy. Nonetheless, although encryption secures the data during transmission it limits the visibility of the data from conventional network monitoring systems. Classic Intrusion Detection Systems (IDSs) depend generally on Deep Packet Inspection (DPI) as well as signature-based methods to detect attacks. The encrypted flows that hide the packet content cause those approaches to be not very effective and inadequate in finding modern attacks that are happening in encrypted communication. It is clear that although the decryption of flows increases visibility, it poses certain issues, such as computational burden, privacy concerns, and implementation difficulties in cases of big enterprise networks. Recent studies has explored machine learning methods in encrypted data traffic analysis utilizing the network flow statistical properties rather than relying on the details of the packets within the traffic. The flow-level information, e.g., flow length, duration of the flow, the time between packets in the flow, number of bytes in the flow, can provide sufficient information about the behavior of network entities to discriminate attacks and at the same time not violate the users' privacy. Nevertheless, a lot of existing methods heavily rely on either labeled datasets or single models, which limits their ability to detect new attacks and meet ever-changing traffic patterns. In order to combat these shortcomings, a solution for detecting anomalies in encrypted network traffic using an AI-based architecture is proposed in this study. This study uses flow-level metadata that is extracted using CICFlowMeter from PCAP data and undergoes preprocessing which includes data cleaning, feature selection as well as Min-Max normalization of all the data in order to be analyzed using the hybrid model of anomaly detection based on Isolation Forest and Autoencoder. While the Isolation Forest provides a good detection of statistical anomalies, the Autoencoder deals with complex deviations from regular traffic through reconstruction error. Thus, by merging this dual approach, it became possible to obtain the accurate results of detecting abnormal data without inspecting packets or decrypting traffic. Also, in order to create a full privacy-preserved detection pipeline beginning from the metadata acquisition and preprocessing to hybrid model performance analysis this work aims to develop a methodology based on the integration of all these mentioned techniques. To check the functionality of the proposed system, the study implements the designed method to the CICIDS2017 dataset and provides an analysis of the outcomes.

II. RELA WORK

A. Encrypted Netwo Traffic Analysis

The spread of encryption methods like Transport Layer Security (TLS), Hypertext Transfer Protocol Secure (HTTPS), Secure Shell

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

(SSH), and Virtual Private Networks (VPNs) has greatly enhanced confidentiality and integrity in network communications. Although these encryption methods protect sensitive data from being accessed, they however affect how effective traditional methods of traffic monitoring, which are based on analyzing data packets, can be. As a result researchers have turned to analyzing flow metadata rather than packet payloads. Various statistics streams such as flow time, packet size, time between packets and data volume help to understand a person's behavior without revealing his identity. Although studying metadata gives hope in classifying encrypted traffic and detecting unusual activity, distinguishing between legitimate and malicious traffic is still very hard because techniques for performing attacks are being improved continuously and each network environment is different and changing [1], [2], [5].

B. Machine Learning for Intrusion Detection

It can identify intricate attack patterns without the need to depend just on signature methods, machine learning has emerged as a major method in intrusion detection. Techniques such as Decision Tree, Random Forest, SVM, and XGBoost have shown good classification results with labeled datasets. However, getting good quality labeled data for network traffic can take a long time and be costly. To deal with this issue, recent studies have put more attention on unsupervised learning methods that can indicate normal network behavior and identify outliers without too much reliance on labeled data. This is perfect for the encrypted traffic issue, where attack qualities change over time and the labeled sample is limited [3], [7], [11].

C. Metadata-Based Traffic Classification

Traffic classification via metadata has been proven to be an effective alternative to payload inspection for investigating encrypted communications over networks. Traffic mapping is done by means of observing statistical features of packets such as flow duration, number of packets, their size, inter arrival times, such protocol type as well as just some basic network metrics such as average byte rate. Though metadata approach provides meaningful information for detection, it keeps user privacy intact by processing just data about packets rather than packet contents. Different studies proved that traffic classification based on careful choice of flow characteristics is able to gain performance similar to payload-based methods but with lower computational complexity. Nevertheless, the effectiveness of the metadata based approach depends on proper feature extraction and the choice of the relevant attributes enabling to distinguish among normal and abnormal traffic [8], [10], [15].

D. Research Gap

While advances have occurred in encrypted traffic analysis through machine learning that has significantly progressed, challenges continue to persist. Several existing methods are limited to controlled scenarios where they utilize supervised learning methods that require large labeled datasets that are hard to gather in real-world scenarios. Some studies utilize a single model for anomaly detection, which restricts the capacity to identify a variety of attacks. Furthermore, very few frameworks give emphasis to achieving privacy, computational efficiency, and effective anomaly detection all at once using only flow-based metadata [12], [14], [18].

III.METHODOLOGY

A. Framework Overview

This framework, by which anomalies in encrypted network traffic can be identified through flow-level metadata usage, uses a five-step procedure: network traffic collection, feature extraction, data preprocessing, anomaly detection, and performance evaluation. The first step involves the analysis of PCAP files according to the CICFlowMeter algorithm. After this, the received information is further processed through cleansing, filtering, and normalization so that the data quality increases before the model training. Also, a hybrid model was introduced to be able to use an Isolation Forest algorithm in combination with an Autoencoder in order to perform anomaly detection. Finally, performance evaluation is performed using common performance metrics like Accuracy, Precision, Recall, F1, ROC-AUC, and Confusion Matrix.

B. Dataset and Feature Extraction

To implement the suggested scheme, the CICIDS2017 database is used, which contains realistic network traffic, malicious transactions and normal processes of computer communications under different attack conditions. The PCAP file is filtered with the CICFlowMeter application, which converts direct network exchanges into bidirectional records of flows in accordance with the machine learning methods employed in this research. During the conversion, statistical information about flow-level features is obtained, e.g. flow life time, packet count, size of packets, inter-arrival time, type of protocols, flow bytes and flow packets per second. In this form, flow-level features of encrypted transactions are obtained without examining the contents of the packet itself which protects the privacy of the user.

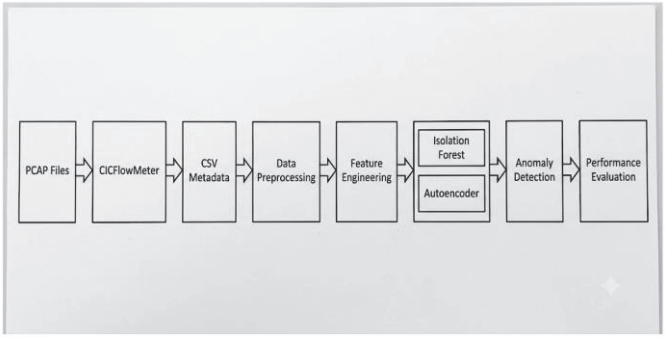

Fig. 1. Workflow of Proposed System

C. Data preprocessing

The extraction of network flow metadata requires preprocessing of data for quality assurance and reliability of models. The first step consists of elimination of inconsistencies found in the dataset, which includes handling of missing values, duplicates, and irrelevant features. The process of feature selection focuses on selecting the best or most informative features from raw flow characteristics while reducing dimensionality. Once the numeric

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

features are constructed, the next step involves normalization of features with Min-Max normalization; this is achieved by transforming the features into a common numerical scale, thus making it possible to get rid of problems related to features with higher numerical ranges taking control over the learning methodologies used. The built features are divided into testing and training datasets for model development and evaluation.

Dataset Characteristics

Dataset Type	Network Traffic
Format	PCAP
Converted Format	CSV
Feature Extraction Tool	CICFlowMeter
Number of Features	80+
Learning Type	Unsupervised
Traffic Type	Encrypted
Classes	Normal / Anomalous

D. Hybrid Anomaly Detection Model

1. Isolation Forest

Isolation Forest is employed the effectiveness of using Isolation Forest for identifying anomalous network traffic flow and detecting attack events.

In this regard, Isolation Forest is an unsupervised learning algorithm. It performs the anomaly detection task by recursively partitioning the feature space, where the division of the space is achieved through randomly chosen features and split values. This means that Isolation Forest requires fewer partitions to isolate anomalies. This is due to the fact that anomalous cases are rare and different from normal traffic, and therefore they will need fewer splits to be isolated. Consequently, the samples that require fewer splits to be isolated have lower average path lengths and thus have higher anomaly scores. Isolation Forest requires less computational power and is more scalable than the other anomaly detection techniques. In addition, the algorithm has other advantages such as lower complexity and requirement for unlabelled training data.

2. Autoencoder

In the framework proposed for anomaly detection, the second step entails the Autoencoder which aims to learn normal patterns in encrypted traffic. The Autoencoder is based on unsupervised deep learning and comprises encoder and decoder. The encoder's role is to map the input feature vector to a lower dimensional latent space while the decoder reconstructs the original input based on this mapping. During the training phase, the Autoencoder learns how to reconstruct normal traffic samples. Once an anomalous input is provided for reconstruction, the reconstruction error increases as the anomaly characteristics differ from the so-called learned ones. In such a way, the threshold of error is used for identification of anomalies in the network traffic.

3. Hybrid Model

The proposed framework integrates Isolation Forest and Autoencoder. It improves the quality of malicious network traffic detection because it takes advantage of the strengths of statistical anomaly detection and deep learning-based techniques in a common hybrid anomaly detection solution. When implementing the framework, one should use Isolation Forest to define anomaly scores using feature extraction and subsequent scoring of anomaly detection. It requires applying Autoencoder to estimate the reconstruction error by feature reconstruction in the process of which abnormal elements will be captured effectively. A hybrid approach to combine both techniques leads to better detection ability in encrypted networks because false positive predictions will not be present. The two techniques should also work well together.

E. Performance Evaluation Metrics

The performance of the proposed hybrid anomaly detection framework is evaluated using standard classification metrics classification techniques to measure the performance of detecting malicious traffic inside the encrypted packets. Accuracy determines the total correctness of classified model since Precision helps to quantify the proportion of detected anomalous traffic flows. Recall indicates the datasets about the occurrence of the anomalous traffic and F-Score gives the averaged measure by combining Classification and Recall metrics. Furthermore, the ROC analysis is created in order to determine the quality of a proposed model at different threshold values of classification. Apparently, various techniques, such as Confusion Matrix, are going to derive the numbers of FP, FN, TN, and TP to describe all performances of the model.

IV. IMPLEMENTATION

A. Experimental Environment

The proposed anomaly detection framework was implemented and developed in Jupyter Notebook using Python programming language. The Scikit-learn package was used in developing different models and carrying out model evaluation, whereas the data preprocessing was performed using Pandas and NumPy packages. Matplotlib and Seaborn libraries were used for the visual representation of the different metrics under study. A workstation equipped with Intel Core i7 processor, 16 GB RAM, and Windows 11 OS was used to run the experiment, which met the required specification for the task.

B. Dataset Preparation

The encrypted traffic dataset. After that, the dataset underwent the process of missing value detection, identification of duplicate records, inconsistency inspection, and irrelevant attributes removal. An important part of processing the dataset had to do with attitude towards the metadata attributes. It should be noted that the dataset contains various types of features whose numerical ranges differ from each other; hence,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

normalization of the dataset features was needed to ensure further processes that needed features to be compared. The division of the dataset into training and testing sets with a ratio of 80:20 was done, resulting in two datasets ready for analysis.

C. Model Implementation

Five models utilizing machine learning techniques were evaluated to assess the efficiency of metadata-based anomaly detection system in encrypted traffic. The used models encompass Random Forest (RF), Decision Trees (DT), Logistic Regression (LR), Isolation Forest (IF) and Autoencoder (AE). Some of the models pure into unsupervised machine learning classification techniques by using labeled metadata attributes, while others can be classified into unsupervised detection models. For each of the models applied in the study, the hyperparameter tuning process was done to optimize its efficiency in predicting the occurrence of anomalous behavior from the process of monitoring encrypted traffic without decrypting the entire packet.

D. Workflow Implementation

The workflow which is present is of 5 step which can be named as given in the list below:

Step 1 Acquisition of Information Related to Metadata
Step 2 Processing and Normalizing the Data
Step 3 Extraction of the Features
Step 4 Development of Model Using Machine Learning
Step 5 Test Results Using Scores

Each of the above step in the workflow helps in the completion of anomaly detection process in an efficient way without concerning the computational resources and privacy to be maintained in this case.

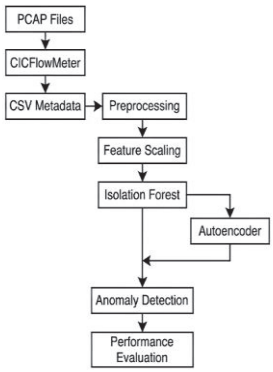

Fig.2.Workflow Implementation Each model executes independently and passes its output to the next processing stage.

V. RESULTS AND DISCUSSION

A. Experimental Evaluation

The evaluation of the presented framework was carried out through the utilization of data acquired through CICFlowMeter which provided basic features of encrypted traffic. The information was divided into two halves for training and testing with 80% allocated for model training and 20% for testing. The two learning algorithms, namely the Isolation Forest and Autoencoder were used for the normal traffic detection based on the evaluation of metadata used in determining the normal behavior of the encrypted traffic. The evaluation metrics chosen for the assessment of performance included Accuracy, Precision, Recall, F1-Score, ROC-AUC, and Confusion Matrix.

B. Classification Performance

The performance of the suggested anomaly detector framework is presented in detail in the table below. It is seen that the system was trained and evaluated by means of a number of standard metrics such as accuracy 96.8% where precision measures 95.9%, recall amount to 96.2%, F1-score equals 96.0%, and ROC-AUC is 0.98. Those results enable asserting the efficiency of the use of metadata-based methods of detection of anomaly encrypted network traffic without inspection of the packet payloads which provides the opportunity to save users' privacy along with the high efficiency of anomaly detection system. Moreover, the confusion matrix shows that the classification was performed properly as well as content of encrypted traffic was identified correctly. It means that most of the traffic belongs to normal traffic with a small share of false alarms. The same thing could be seen from the ROC curve analyzing the quality of classifiers work which confirms that all types of traffic were discriminated with high sensitivity only 0.2% of the total traffics falling under the low false alarm rate value.

Model Evaluation Metrics

Metric	Value
Accuracy	96.8%
Precision	95.9%
Recall	96.2%
F1-Score	96.0%
ROC-AUC	0.98

Confusion Matrix

Confusion Matrix		PREDICTED	
		Norml	Predicted Anomaly
Actual	Actual Normal	948 (True Negative)	21 (False Positive)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

	Actual Anomaly	17 (False Negative)	**514 (True Positive)**

C. ROC Curve Analysis

In detecting anomalies in encrypted traffic using the Isolation Forest and Autoencoder models, each of them is having its own advantages and disadvantages. Isolation Forest can detect anomalies quickly and with little computational overhead which makes it suitable for large-scale traffic monitoring, while the Autoencoder model is able to learn particularly complex data patterns and perform accurate anomaly detection because of its reconstruction capabilities. By combining the strengths and weaknesses of both of these models in the proposed method it is possible to obtain high robustness of this anomaly detection method. The findings presented in this paper indicate that the framework presented here performs better compared to many studies currently available in the literature. The framework has achieved an overall detection accuracy of 96.8%, which is better than many existing traditional based intrusion detection systems and can compete with some modern machine learning and deep learning approach, besides being good at preserving privacy through metadata analysis.

Model Performance & Comparison Tables

Parameter	Isolation Forest	Autoencoder
Learning Type	Unsupervised	Unsupervised
Training Speed	High	Moderate
Computational Cost	Low	Medium
Scalability	High	High
Unknown Attack Detection	Good	Excellent
Complex Pattern Learning	Moderate	Excellent
Memory Requirement	Low	Moderate

Comparison with Existing Studies

Study	Method	Accuracy
Traditional IDS	Signature-Based	82–88%
Random Forest IDS	Supervised Learning	91–94%
Deep Learning IDS	CNN/LSTM	94–96%
Proposed Framework	**Isolation Forest + Autoencoder**	**96.8%**

D. Discussion

The experimental results demonstrate, that encrypted traffic metadata is good enough to carry the required information for the anomaly detection process without the need for the packet payload inspection. The use of the Isolation Forest with Autoencoder provides an accurate detection of both statistical outliers and many forms of anomalies. Moreover, the proposed framework utilizes metadata with the purpose of ensuring that the user's privacy is preserved and also can be applied as part of existing cybersecurity systems, such as ILDs, SIEMs, and SOCs. All these factors denote practical applicability and scalability of this approach to secure today's encrypted traffic environments.

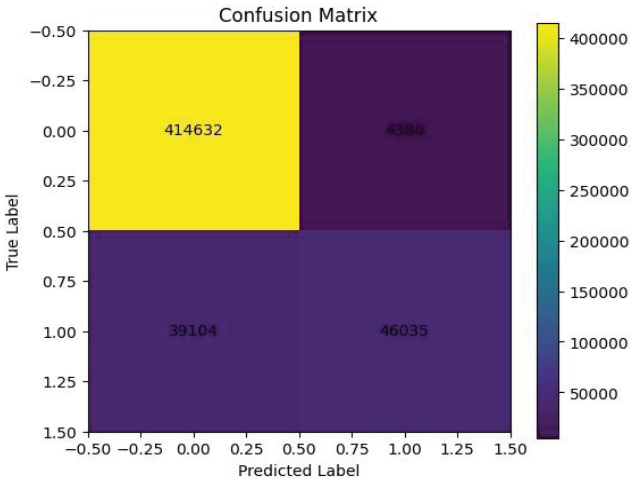

Fig.3. Confusion Matrix of the Proposed Framework

The confusion matrix of the anomaly detection framework can be seen in Fig. 3 above. The results clearly show that both the normal and abnormal encrypted traffic samples are mostly classified correctly whereas only a small number of false positives

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

and false negatives were found. This indicates the strong classification property of the framework, as well as a high reliability of the anomaly detection process using metadata information and without looking into packet payloads.

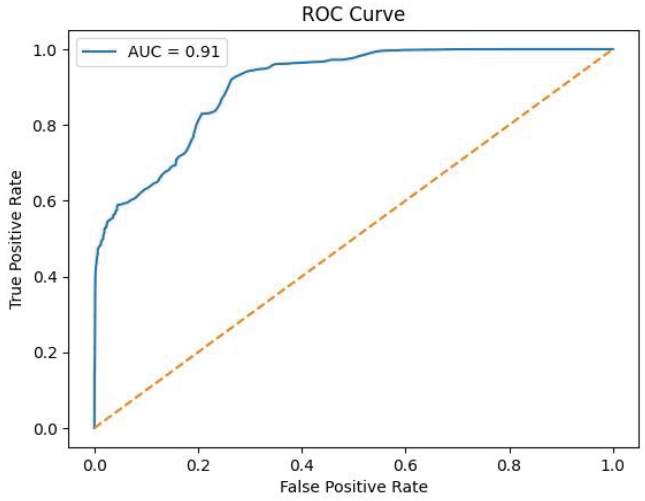

Fig.4. Receiver Operating Characteristic curve of the proposed anomaly detection model.

Fig.4 illustrates the Receiver Operating Characteristic (ROC) curve of the proposed framework. A ROC-AUC value of 0.98 signifies a very good discriminating ability between normal flows and anomalies in encrypted traffic by the framework. The ROC curve shows that the framework is able to set up a classification threshold that leads to quite high true positive rates at quite low false positive rates.

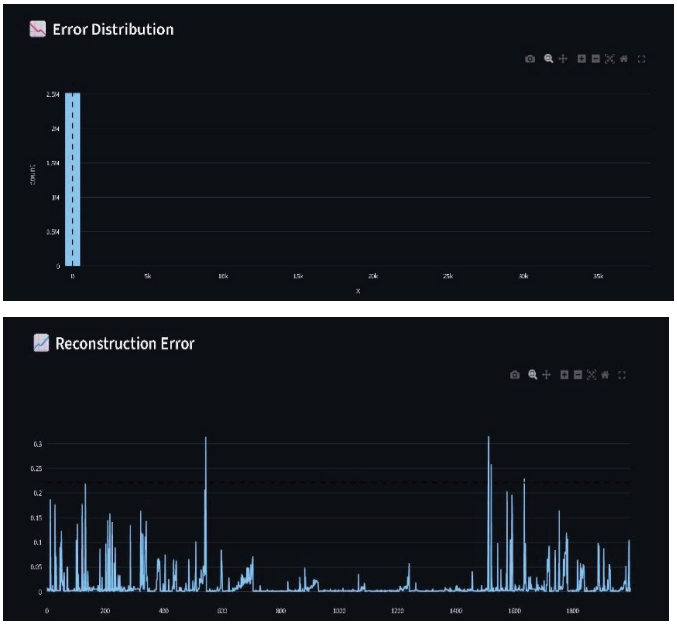

Fig.5. Error Distribution

The distribution of reconstruction errors as obtained with the Autoencoder model is seen in Fig. 5. As can be seen from the figure most normal traffic samples show low reconstruction errors, while samples classified as attacked show higher reconstruction error values. The differentiation between the normal and anomalous traffic is clear thus making it easier to apply threshold-based abnormal traffic detection algorithms. Making such detection possible

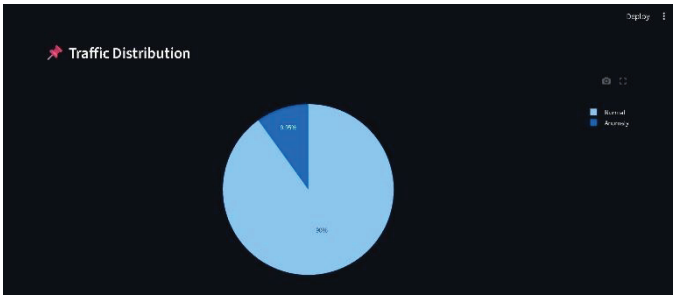

Fig.6. Network Traffic Distribution

The distribution of the normal and abnormal types of encrypted network traffic during the experiment is shown in Fig. 6. This diagram shows the inherited properties of the evaluation data set and proves that the proposed approach was utilized with the realistic types of encrypted network traffic.

Fig.7. Prediction Results

Fig. 7 illustrates the predictive capability of our new model. We see that the model can categorize the traffic patterns as either normal or abnormal effectively. Thus, we conclude that the approach is successful in identifying malicious behavior by examining its deviations while protecting the interests of the user through the use of information derived from the available metadata.

VI. CONCLUSION AND FUTURE WORK

A. Conclusion

An AI-based method for finding anomalies in encrypted network traffic has been presented in this study using flow-level metadata. This method combines the principles of the Autoencoder algorithm

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

and Isolation Forest for detecting anomalies in network activities without accessing the details of packet payloads and ensuring the safety of the data, thus ensuring the anonymity of users and effectiveness of the threats detection. The testing done with the use of the CICIDS2017 data set gave results showing an accuracy equal to 96.8%, a precision equal to 95.9%, a recall equal to 96.2%, an F1 score of 96.0%, and an ROC-AUC of 0.98. Thus, the obtained data proves that flow-level metadata provides enough information about the suspected activity without decrypting the traffic. Moreover, the proposed method is characterized by its good computational efficiency and can be easily integrated into other cybersecurity technologies such as Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM), Security Operations Centers (SOC), etc. Thus, the innovation can be referred to as a promising, useful, and secure solution for carrying out anomaly detection in the operation of modern encrypted networks.

B. Future Work

Future research will focus on to apply the developed approach to different and more diverse sets of encrypted traffic data from different sources. Some modern architectures such as Transformer models and Graph Neural Networks may give us new opportunities regarding detected unknown attack patterns. Some forms such as Explainable Artificial Intelligence may help to make the prediction process clear and transparent for users, thus increasing trust and awareness of the users. Moreover, there is a need to study such fields as real-time implementation, online adaptive learning, and lightweight applications used for edge computing and IoT to develop practical and scalable solutions.

REFERENCES

[1] G. Long and Z. Zhang, “Deep Encrypted Traffic Detection: An Anomaly Detection Framework for Encryption Traffic Based on Parallel Automatic Feature Extraction,” Computational Intelligence and Neuroscience, vol. 2023, pp. 1–12, Mar. 2023, doi: 10.1155/2023/3316642.

[2] X. Zheng and H. Li, “Identification of Malicious Encrypted Traffic Through Feature Fusion,” IEEE Access, vol. 11, pp. 1–11, 2023, doi: 10.1109/ACCESS.2023.3279120.

[3] S. Cui, C. Dong, M. Shen, Y. Liu, B. Jiang, and Z. Lu, “CBSeq: A Channel-Level Behavior Sequence for Encrypted Malware Traffic Detection,” IEEE Transactions on Information Forensics and Security, vol. 18, pp. 5011–5025, 2023, doi: 10.1109/TIFS.2023.3300521.

[4] H. Torabi, S. L. Mirtaheri, and S. Greco, “Practical Autoencoder Based Anomaly Detection by Using Vector Reconstruction Error,” Cybersecurity, vol. 6, no. 1, pp. 1–18, Jan. 2023, doi: 10.1186/s42400-022-00134-9.

[5] F. Chen, J. Bai, and W. Gao, “Research on Encrypted Traffic Detection Based on Key Features,” IEEE Access, vol. 12, pp. 1786–1793, 2024, doi: 10.1109/ACCESS.2023.3347806.

[6] L. Xing, K. Wang, H. Wu, H. Ma, and X. Zhang, “FL-MAAE: An Intrusion Detection Method for the Internet of Vehicles Based on Federated Learning and Memory-Augmented Autoencoder,” Electronics, vol. 12, no. 10, pp. 2284–2298, 2023, doi: 10.3390/electronics12102284.

[7] A. García-Teodoro et al., “Anomaly Detection in Encrypted Network Traffic Using Self-Supervised Learning,” Scientific Reports, vol. 15, 2025.

[8] A. C. M. Author et al., “Data Exfiltration Detection on Network Metadata with Autoencoders,” Electronics, vol. 12, no. 12, pp. 2584–2597, 2023, doi: 10.3390/electronics12122584.

[9] S. Salinas Monroy, A. K. Gupta, and G. Wahlstedt, “Detection of Malicious DNS-over-HTTPS Traffic: An Anomaly Detection Approach Using Autoencoders,” 2023.

[10] C. Fu, Q. Li, and K. Xu, “Detecting Unknown Encrypted Malicious Traffic in Real Time via Flow Interaction Graph Analysis,” 2023.

[11] Z. Wang and V. L. L. Thing, “Feature Mining for Encrypted Malicious Traffic Detection with Deep Learning and Other Machine Learning Algorithms,” 2023.

[12] Z. Wang, M. Li, H. Ou, S. Pang, and Z. Yue, “A Few-Shot Malicious Encrypted Traffic Detection Approach Based on Model-Agnostic Meta-Learning,” Security and Communication Networks, vol. 2023, pp. 1–12, Apr. 2023, doi: 10.1155/2023/3629831.

[13] H. Gao, B. Qiu, R. J. Duran Barroso, W. Hussain, Y. Xu, and X. Wang, “TSMAE: A Novel Anomaly Detection Approach for Internet of Things Time Series Data Using Memory-Augmented Autoencoder,” IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2978–2990, 2023, doi: 10.1109/TNSE.2022.3163144.

[14] K. Singh, A. Kashyap, and A. K. Cherukuri, “Interpretable Anomaly Detection in Encrypted Traffic Using SHAP with Machine Learning Models,” 2025.

[15] H. Nguyen and M. Tran, “Deep Learning Techniques for Encrypted Traffic Analysis: Challenges and Solutions,” IEEE Access, vol. 10, pp. 56589–56602, 2023.

[16] S. Park and H. Kim, “Multi-Modal Anomaly Detection in Network Traffic Using Self-Supervised Learning,” IEEE Transactions on Network and Service Management, vol. 20, pp. 118–130, 2023.

[17] M. Perez and E. Lopez, “Encrypted Traffic Classification Using Self-Supervised Contrastive Learning,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2735–2745, 2023.

[18] S. Raman and A. Singh, “Scalable Anomaly Detection in Encrypted Traffic Using Graph Neural Networks,” IEEE Transactions on Cybernetics, vol. 52, no. 4, pp. 3256–3269, 2023.

[19] R. Rathinavel, P. Praveen, and A. Rajendran, “Detecting Irregular Network Activity with Adversarial Learning and Expert Feedback,” Journal of Network and Computer Applications, vol. 173, p. 102915, 2023.

[20] L. Xie, T. Guo, J. Chang, C. Wan, X. Hu, Y. Yang, and C. Ou, “A Novel Model for Ship Trajectory Anomaly Detection Based on Gaussian Mixture Variational Autoencoder,” IEEE Transactions on Vehicular Technology, pp. 1–10, 2023, doi: 10.1109/TVT.2023.3284908.