SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V13I3P118

Volume 13 Issue 3, 248-259, March 2026

Original Article

EdgeGuard-QoE: A Hybrid Autoencoder-LightGBM Framework for Secure and QoE-Preserving Video Transmission in Cloud-Edge 5G Networks

Kumbha Ravi Kumar[1*], Ayyagari.Srinagesh[2]

[1*]*Department of Computer Engineering, Acharya Nagarjuna University (ANU), Nagarjuna Nagar, Guntur, Andhra Pradesh, India.*
[2]*Department of Computer Science and Business Systems, RVR&JC College of Engineering, Chowdavaram, Guntur, Andhra Pradesh, India.*

[1]*Corresponding Author : khumbaravikumar@gmail.com*

Received: 14 December 2025 Revised: 15 January 2026 Accepted: 25 February 2026 Published: 31 March 2026

Abstract - *There is an increased utilization of adaptive video streaming over cloud-edge 5G networks, which subjects latency-sensitive multimedia services to multimedia threats other than Quality of Experience (QoE). To address the problem, this paper proposes EdgeGuard-QoE (Edge-based Guarded Quality of Experience Framework), a video transmission architecture of 5G networks to provide security and Quality of Experience (QoE). The hybrid model in the framework is GWO-SAE-LightGBM (Grey Wolf Optimized Stacked Autoencoder-LightGBM) that is oriented at the use of intelligent attacks prediction and mitigation. In such a technique, stacked autoencoders recognize normal traffic behavior based on network flow traffic of varying dimensions, that is, packet size, flow duration, transmission entropy, and header anomalies, and can identify patterns of attack (DoS, Man-in-the-Middle, and packet injection). Then, a LightGBM (Light Gradient Boosting Machine) network classifier on the edge of the network detects the anomalies and puts in place adaptive security precautions to prevent the degradation of the service, which comprises light encryption and localized attack quarantine. The Grey Wolf Optimization (GWO) algorithm is used to enhance the efficiency of the hyperparameter configuration of the stacked autoencoder and LightGBM models to enhance their detection and reduce the processing downtimes. The new EdgeGuard-QoE Framework can support exceptionally high accuracy attack detection, low alarm rates, and low latency, as well as support adaptive bitrate and stable QoE. Several experimental analyses performed in the conditions of realistic cloud-edge 5G video streaming verify the correctness of hybrid frameworks when it comes to real-time secure video transmission in the next-generation cloud-edge-based 5G networks.*

Keywords - *Secure video transmission, 5G networks, Cloud-edge computing, Network, Intrusion detection, Autoencoder, LightGBM, Grey Wolf Optimization, Quality of Experience (QoE).*

1. Introduction

The blistering development of high-definition and ultra-high-definition video services using the cloud-edge 5G networks has not only changed the contemporary multimedia communication radically but has also guaranteed that contemporary innovative application infrastructures are integrated into the network. The use of live streaming, remote healthcare, autonomous surveillance, and immersive entertainment requires low latency, large bandwidth, and continuous service delivery to provide reasonable Quality of Experience (QoE). Nevertheless, cloud and edge computing and 5G infrastructure integration further increase the attack surface and, as a result, the latency-sensitive video streaming service is now vulnerable to the more advanced network-based attacks, including DDoS, Man-in-the-Middle (MitM), and packet injection attacks. Such security attacks do not only disrupt data confidentiality and integrity, but also lead to considerable deterioration of QoE effects due to delay, jitter, and packet loss and bifrate fluctuations. In turn, a reasonable trade-off between a high level of security protection and the maintenance of QoE has become the key problem of the next-generation cloud-edge 5G video-utility transmission systems.

1.1. Problem Statement

Although there has been tremendous progress in the 5G architecture and adaptive video streaming technology, the current security provisions in multimedia delivery are mostly ineffective in the cloud-edge deployment. Traditional intrusion detection and control mechanisms are highly centralized, high-computational, and reactive, which leads to higher processing latency and slower response to attacks. Furthermore, security frameworks tend to be independent of

QoE-aware video adaptation schemes and, as a result, trigger unjustified service collapse because of aggressive encryption, packet checking, or traffic congestion. The absence of this connection causes the deterioration of the video, the constant fluctuation of bitrate, and the rising incidence of interruptions in playing the video during an attack. Moreover, the existing machine learning-based detection methods are not very effective in capturing the complex, high-dimensional traffic patterns and are incapable of generalizing to dynamic and varying attack patterns in heterogeneous cloud-edge 5G networks. These constraints indicate the necessity of a lightweight, smart, and QoE-conscious security architecture that can effectively identify and counter attacks in real time without affecting video streaming performance.

The accelerated development of cloud-edge computing alongside the Fifth-Generation (5G) wireless networks has completely changed the design of adaptive video streaming systems. Cloud-edge collaboration accounts for much higher latency performance and Quality of Experience (QoE) of bandwidth-intensive multimedia services by offloading computations, performing dynamic transcoding, and caching with greater proximity to end users. The recent studies have established that one of the potential ways of dealing with the unpredictable wireless channel conditions and maintaining the high quality of the video in dense network conditions is to resort to cloud-edge cooperative transcoding and adaptive streaming mechanisms [1]. Such developments have made cloud-edge 5G networks an important enabler of real-time and immersive video applications. Cloud-edge infrastructures have also been seen to be explored beyond the performance of video delivery in efficient use of the resource, as well as energy-conscious task execution. Optimization-based scheduling schemes have also been suggested as hybrids to balance the workloads on computational nodes both in the cloud and the edge node to minimize processing delays and total energy consumption in the distributed computing environments [2]. These kinds of optimization methods are especially applicable to multimedia workloads in which video encoding, decoding, and analysis of traffic demand very high computational and timing constraints. Nevertheless, these methods enhance efficiency; the main problem is that they are aimed at optimizing performance and pay little attention to the security issues involved in processing multimedia traffic at the edge. Cloud-edge collaboration with 5G dynamic resource scheduling has become a potential solution to real-time video analytics and control systems, especially in industrial and mission-critical video applications. Recent studies have shown that edge-assisted computing models are efficient at satisfying the ultra-reliable and low-latency communication needs of industrial video streams [3]. However, the growing use of distributed edge nodes creates new weaknesses because attacked or overloaded edge nodes might seriously affect real-time video streaming and processing. This difficulty is enhanced in cases where it deals with massive deployments, especially in conditions of heterogeneous networks.

The edge caching and transcoding strategies have also been optimized using learning-based strategies to maximize throughput in video delivery. Games and meta-learning have been used to optimize trans-coding operations and caching decisions in cloud-edge hierarchies, which allow responsive caching functionality to traffic dynamics and user demands, and which have been utilized to optimize the responsiveness to traffic dynamics and user demand variation [4]. These solutions enhance bandwidth utilization and streaming performance, but they are mostly unaware of threats to network security and their effects on QoE, especially in a situation of malicious attacks on the video traffic streams. Adaptive video streaming as QoE has therefore been an area of growing interest as a key design requirement of next-generation and beyond 5G networks. High-level surveys have pointed out that the multimedia systems of the future should take into consideration network performance/application-layer adjustment/user-perceived quality together to serve the emerging service needs [5].

However, ensuring QoE when the environment is unfavorable, e.g., network congestion or active interference, is a major problem. Traditional security systems tend to be incompatible with the QoE optimization due to the add-on of latency, computation load, or aggressive congestion control. Video streaming that takes the form of an encrypted video makes the QoE monitoring and security enforcement even more difficult. In-network QoE measurement systems have been suggested to be able to deduce user experience based on encrypted traffic without breaching privacy limitations [6].

Although these methods are effective in performance assessment, they have a disadvantage in terms of detecting and alleviating advanced network attacks in real time. In addition, they are generally based on a centralized analysis, which does not fit in the cloud-edge video streaming settings with latency constraints. The new developments in cloud-edge adaptive streaming systems have identified the necessity of smart, distributed, and QoE-driven control systems. Research has determined issues that are associated with scalability, attack resistance, and real-time decision-making when using cloud-edge video delivery systems [7]. The results suggest the importance of deploying intelligent traffic analysis and security-conscious adaptation directly at the edge, where the rapid detection and localized mitigation will allow preventing the extensive service debasement. The new semantic-based and learning-based video streaming algorithms also show that more sophisticated machine learning frameworks can be used to optimize the transmission of multimedia using wireless networks [8]. Nevertheless, the majority of the current learning-based solutions are based on content adaptation and semantic compression, where security-conscious traffic intelligence is not given much attention. Specifically, optimization of the accuracy of intrusion detection, mitigation latency, and preservation of the QoE is an unresolved issue in cloud-edge 5G video streaming systems.

1.2. Motivation and Contributions

This paper is driven by the need to perform a dual role of maintaining network security and long-lasting Quality of Experience in latency-sensitive 5G video delivery, so that a new edge-centric hybrid security framework named EdgeGuard-QoE is proposed to support both safe and QoE-controlled video delivery.

With the benefit of closeness between the edge and the central computing nodes, the framework will allow quick attack identification and localized response, which will shorten the time taken to respond to the issues and decrease the impact of the services being affected. The following are the main contributions of this work:

i) an innovative GWO-based Stacked Autoencoder (SAE) model that can learn normal traffic, as well as anomalous traffic, patterns, effectively using multidimensional network flow features;
ii) an edge-deployed LightGBM classifier, to accurately classify the type of attacks and enforce security dynamically accordingly;
iii) the addition of the use of Grey Wolf Optimization (GWO) to automatically optimize model hyperparameters, improving accuracy in detection but at a lower computational cost; and
iv) a QoE-sensitive mitigation approach which maintains the adaptive bitrate stability and minimizes the latency under attack conditions. Vast experimental testing of the proposed EdgeGuard-QoE framework on realistic cloud-edge 5G video streaming conditions shows that the proposed architecture has a high detection rate, lower false alarms, and longer QoE than the current state-of-the-art solutions.

These constraints are the driving force behind the paper, where this researcher suggests a hybrid edge-based scheme, EdgeGuard-QoE, to support video transmission over cloud-edge 5G networks in a secure and QoE-preserving manner. The proposed framework combines a LightGBM classifier and is deployed at the edge to classify attacks and mitigate them precisely and adaptively, with a proposal for an intelligent anomaly detector based on optimized stacked autoencoders (GWO-SAE). With the capabilities of multidimensional network flow and minimal security enforcement at the edge, EdgeGuard-QoE can deliver high detection accuracy, low false alarm rates, and minimal processing latency with adaptive bitrate stability and perceived video quality.

The usefulness of the given framework is supported by comprehensive experimental analyses of the proposed scheme in realistic cloud-edge 5G video streaming conditions, which prove the applicability of the given framework in terms of delivering next-generation networks securely and in real-time, when it comes to delivering multimedia.

2. Literature Survey

Recent studies of the theme of cloud-edge enabled video streaming in 5G networks encompass several related areas, including adaptive video streaming, resource management, Quality of Experience (QoE) modeling, and network security. Current literature is mainly concerned with improving the streaming efficiency with the use of cloud-edge collaboration, intelligent caching, transcoding, and learning-based adaptation methods, and there is a smaller amount of literature that deals with monitoring the QoE in the presence of encrypted traffic. Security-conscious QoE protection, especially when it comes to network-layer attacks on real-time video broadcasting, is under-researched, though. This area is a literature review and categorization of previous literature into three broad topics, namely, (i) cloud-edge collaborative video streaming and resource optimization, (ii) QoE-based adaptive streaming and monitoring methods, and (iii) smart intrusion detection methods of multimedia traffic. The analysis reveals the major weaknesses of existing solutions and encourages the necessity of a unified, edge-centric design that considers the attack detection, mitigation latency, and QoE maintenance aspects in cloud-edge 5G video streaming systems.

Shi et al. introduce an extensive overview of smart methods to improve the quality of video delivery to cloud-edge-end networks, which include AI-based adaptation, edge caching, transcoding, and orchestration schemes. The survey points out that the intelligence distribution throughout the delivery pipeline is critical to gaining high QoE in the heterogeneous network conditions [9]. Nonetheless, although a significant portion of the work is devoted to the optimization of performance and the control based on learning, the issue of security is brought up as a background issue, and the ways in which the adversarial traffic patterns affect the stability of QoE are discussed insufficiently. This inconsistency highlights the necessity of the frameworks that collectively modellize the traffic abnormalities and the edge QoE preservation. Yau et al. introduce a strong throughput estimation framework of edge-assisted Adaptive Bitrate (ABR) streaming, which deals with the instability of the bandwidth measurements in wireless conditions. The method minimizes the oscillation in bitrate and interruption in playback. However, the estimator is based on non-adversarial traffic dynamics and does not deal with malicious perturbations like packet injection or flow manipulation that can greatly alter throughput signals. This shortcoming encourages the use of anomaly-sensitive traffic intelligence in edge-oriented systems of adaptation [10].

Ma et al. present a QoE-friendly adaptive video bitrate aggregation system based on smart edge computing to utilize HTTP live streaming [11]. The algorithm combines several bitrate models and uses the QoE-informed decision-making technology to enhance user experience across different network scenarios. Although useful in the trade-off of bitrate

choice and QoE, QAVA is more focused on the variability of stochastic networks and does not include mechanisms that help to identify abnormal traffic patterns or attacks that may interfere with bitrate aggregation logic in cloud-edge networks. Taha and Ali suggest an adaptive quantization-based algorithm in wireless video streaming, and even with bandwidth variations, adjust the quantization parameters [12]. The method enhances the compression efficiency and quality of the visualization with limited resources. Nonetheless, quantization-based adaptation is only based on encoder-side optimization without considering network-layer threats and traffic abnormalities, so it is less applicable to adversarial 5G edge networks where manipulation on packets at a packet level can severely deteriorate the QoE despite being efficient in terms of encoding. Chmieliauskas and Paulikas provide a practical measurement experiment aimed at measuring the uplink video streaming QoE of 4G and 5G cellular networks. Their findings indicate that QoE is very sensitive to latency, jitter, and packet loss, especially when the uplink in use is heavy. In spite of the fact that the study offers good empirical information, it is also observational as it does not suggest mitigation and protection mechanisms to sustain QoE when impairments occur as a consequence of malicious interference, in contrast to natural network congestion [13].

Du et al. introduce a sensor-enabled sensor-network network security situation prediction model that is based on a clock-cycle recurrent neural network optimized network. The model describes temporal relations among security states and enhances the prediction of the changing threats [14]. Although the recurrent architecture can be used to predict, it does not have negligible computation overhead and is better suited to forecasting (not real-time detection and classification) applications, unlike latency-sensitive edge video streaming. Tang et al. introduce a hybrid intrusion detection scheme, which consists of an autoencoder to learn the feature representation and a LightGBM to learn the efficient anomaly classification [15]. The algorithm has high detection rates and low rates of false alarms on network traffic data, which illustrates the efficiency of the integration of deep feature extraction and gradient boosting. Nevertheless, the work concentrates on generic intrusion detection and does not combine QoE-sensitive mitigation policies or edge-sensitive deployment issues, and the question arises of how the results of detection influence the quality of multimedia services. Kim and Chung introduce an edge computing-aided adaptive streaming scheme in mobile networks, in which edge servers assist in better adaptation decisions on bitrates in order to improve the performance of streaming [16]. The method justifies the advantage of edge proximity in minimizing latency of adaptation and enhancing QoE. However, the scheme does not take into account security threats or abnormal traffic patterns, as it is supposed to be based on a trustworthy network setting and restricts robustness to practical cloud-edge 5G deployment. Based on the literature, there are significant developments in the fields of intelligent video adaptation, QoE optimization, edge-assisted streaming, and machine learning-based intrusion detection. Nevertheless, these initiatives are not very coordinated, and the security awareness and intrusion detection systems are not closely coordinated with the adaptation mechanisms, and their maintenance is not a prerequisite to preserving the QoE. Specifically, the absence of edge-deployable, optimized hybrid models that collaboratively implement real-time attack detection, classification, and QoE-preserving mitigation is a severe gap. This spur indicates the development of the EdgeGuard-QoE framework that incorporates the optimal stacked, autoencoder-based anomaly learning and LightGBM edge classification to guarantee video transmission and maintain adaptive bitrate stability and perceived quality-of-experience in cloud-edge 5G networks.

3. Proposed Methodology

The proposed EdgeGuard-QoE framework will make sure that the video transmission of the cloud-edge enabled 5G networks is secured and the Quality of Experience (QoE)-oriented. The framework presents a combination of clever detection of attacks, classification, and adaptive mitigation in the network edge to reduce latency and service degradation in adaptive video streaming applications [17].

3.1. Overview

The presented EdgeGuard-QoE model is aimed at secure and QoE-aware video streaming in cloud-edge 5G infrastructure. The main concept is to conduct flow-based, high-speed, network edge detection with a hybrid architecture that integrates (i) unsupervised learning of network representations (anomaly discovery) and (ii) supervised classification to typify attacks. The model has three major steps:

- Stacked Autoencoder (SAE) is a model that is trained on benign traffic behavior and observes anomalous deviations.
- LightGBM edge classifier gives the type of anomaly (e.g., DoS / DDoS / PortScan / Web attacks).
- Grey Wolf Optimization (GWO) optimizes the hyperparameters of SAE and LightGBM in order to maximize the detection performance and reduce the computational cost.

The design facilitates edge deployment inferences in real-time, wherein low latency is critical to Quality of Experience video delivery.

3.2. Dataset Description

In this study, CICIDS2017 data is utilized as a typical benchmark for assessing intrusion detection in cloud-edge network settings. The data set contains two-way traffic flow records on a flow level, collected by CICFlowMeter, with every flow represented by a set of numerical characteristics of

the packet header and a time stamp. Numeric flow features are the only features used in this work to achieve the efficiency of computation and make it viable to deploy the edges. The 78 numeric features are chosen, and they encompass various dimensions of traffic behavior. These are traffic intensity and rate measures like Flow Bytes/s and Flow Packets/s, time measures (Flow Duration and inter-arrival time values (Flow IAT Mean, Std, Max, Min)) and statistics on packet size (Packet Length Mean, Std, Variance, Min, and Max), header measures (Forward and Backward Header Lengths), activity and idle (Active Mean, Std, Max, Min and Idle Mean, Std, Max, Min) and TCP flag counts (e.g., SYN, ACK, FIN, RST, PSH, All of these characteristics collectively describe Quality of Experience (QoE)-sensitive variations in traffic along with attack-related anomalies. The dataset is considered to be a multi-class classification problem, in which benign traffic is the BENIGN, and the attack traffic consists of types of DDoS, DoS Hulk, DoS GoldenEye, DoS Slowhttptest, DoS slowloris, PortScan, FTP-Patator, SSH-Patator, Bot, and Web Attack. In order to prevent the sparsity of classes and to have good macro-level assessment, the classes that are rare in the Web Attack sub-classes are combined into a single Web Attack class. Macro-averaged measures are used to conduct performance assessment to take the class imbalance into consideration. These are Accuracy (ACC), Precision, Recall, and Sensitivity (SEN), Specificity (SPE), F1-score, and ROC-AUC. Besides, inference latency (ms per sample) is gauged to determine the possibility of running the proposed model at the network edge. This feature selection and evaluation metrics combination provides the overall evaluation of both the effectiveness of security and the applicability, given the current conditions in the cloud-edge video streaming context [18, 19].

Table 1. Summary of the CICIDS2017 dataset

Attribute	Description
Dataset Name	CICIDS2017
Data Type	Network flow–level traffic
Total Flow Records	543,734
Number of Features	78 (all numeric)
Number of Classes	11 (1 BENIGN + 10 attack categories)
Attack Types	DDoS, DoS (Hulk, GoldenEye, Slowloris, Slowhttptest), PortScan, FTP-Patator, SSH-Patator, Bot, Web Attack
Evaluation Metrics	ACC, Precision, Recall (SEN), Specificity (SPE), F1-score, ROC-AUC

The paper utilizes labeled network-flow data that are applicable in cloud-edge 5G adaptive video streaming security analytics. The flow-level traffic records are collected by a CICFlowMeter-style feature set that is popular among intrusion detection research. Every record is a two-way network flow, which has been summarized in terms of statistical and protocol attributes that align with real-time edge analytics criteria (low computation and fast inference). The data can be used in identifying multi-class attacks and benign traffic learning, which allows detecting anomalies and classifying attacks. The dataset in Table 1 consists of 543,734 flow instances that have a total of 79 columns, including 78 numeric variables and 1 label column. The class is included in the Label field and comprises benign and multiple attack categories, which are BENIGN, PortScan, DoS Hulk, DDoS, DoS GoldenEye, FTP-Patator, SSH-Patator, DoS slowloris, DoS Slowhttptest, Bot, and web-attack variants (e.g., brute force, XSS, SQL injection). The data is skewed by nature, and it is based on the actual traffic state of affairs, where benign flows are predominant.

3.3. Feature Set (QoE- and Security-Relevant)

The dataset consists of statistically meaningful features at the flow level that effectively capture both QoE-relevant traffic variation and security-related anomalies in the cloud-edge video streaming setting. These properties describe the intensity of traffic and transmission rate in terms of Flow Bytes/s and Flow Packets/s, whereas the temporal behavior is expressed in terms of Flow Duration and inter-arrival time statistics, such as mean, standard deviation, maximum, and minimum values. Dynamics of the packet size is represented through the packet length mean, the variance, and the minimum and maximum lengths of packets, and the protocol and head-related attributes are represented with the forward and back header length. Besides, the activity- and idle-time statistics (mean, maximum, minimum, and standard deviation values) are used to model the traffic burstiness and idle behavior. TCP controlling behavior is also summarized based on flag count features like SYN, ACK, RST, FIN, PSH, and URG. Taken together, these features are very applicable to the case of cloud-edge video streaming, as malicious traffic usually takes the form of sudden rate spikes, irregular bursts, and irregularities in protocols and headers, which have a direct effect on the Quality of Experience, creating more latency, jitter, and rebuffering phenomenon [20].

3.4. Data Preprocessing

The features of all the inputs are numbers and can therefore be easily scaled to the scalable edge analytics. Before model training, the data is thoroughly preprocessed to remove invalid numerical values that usually occur in network-flow data. Specifically, the flow-based features might include undefined or extreme values, e.g., the infinite values in the rate-related feature (e.g., Flow Bytes/s) in the case of the flow duration of zero. To solve this problem, positive and negative infinity values are sufficiently substituted by missing values. Next, each numeric feature is cut off by the powerful quantile thresholds to reduce the impact of the heavy-tailed distribution and extreme outliers

and remove invalid samples, usually between the 0.1th and 99.9th percentile. Any unavailable values would then be addressed by median imputation, which works very well with skewed and non-Gaussian network traffic characteristics. z-score standardization is performed on all features after data cleaning/imputation, and all features are normalized to zero mean, unit variance, and this helps enhance the convergence behavior of the stacked autoencoders and, more importantly, balance the contribution made by both high- and low-magnitude features to reconstruction loss and classification. Lastly, stratified sampling is applied to the processed dataset to split it into training (70%), validation (15%), and testing (15%) to maintain the original class distribution. The hyperparameter optimization is done with the help of the validation set by means of the use of the Grey Wolf Optimization (GWO), and the final unbiased performance evaluation is done with the help of the test set.

3.5. Mathematical Modeling of the Proposed EdgeGuard-QoE Framework

The suggested EdgeGuard-QoE model is aimed at providing safe and Quality of Experience (QoE)-saving video delivery in cloud-edge enabled 5G. This framework combines anomaly detection, classification of attacks, and adaptive optimization based on a hybrid framework of Grey Wolf Optimization-Stacked Autoencoder-LightGBM (GWO-SAE-LightGBM).

3.5.1. Feature Extraction and Traffic Modeling

Let the network traffic captured at the edge be represented by a set of bidirectional flow-level features. Each traffic flow is expressed as a numerical feature vector:

$$\mathrm{X}_i = [x_{i1}, x_{i2}, \dots, x_{id}] \quad (1)$$

Where $\mathrm{X}_i \in \mathbb{R}^d$ denotes the i^{th} traffic flow and d is the number of extracted features. The features include packet-level statistics, temporal characteristics, and protocol-related attributes, such as packet length (mean and variance), flow duration, flow bytes per second, header length, active mean, and idle mean.

The complete dataset is defined as:

$$\mathcal{D} = \{(\mathrm{X}_i, y_i)\}_{i=1}^{N} \quad (2)$$

Where N is the total number of flows and $y_i \in \{1,2,\dots,C\}$ denotes the class label corresponding to benign or attack traffic.

3.5.2. Stacked Autoencoder for Anomaly Detection

To capture normal traffic patterns and detect anomalous behavior, a Stacked Autoencoder (SAE) is employed. The SAE consists of an encoder and a decoder network. The encoder maps the input feature vector. X_i into a lower-dimensional latent representation Z_i:

$$\mathrm{Z}_i = f_\theta(\mathrm{X}_i) \quad (3)$$

Where $f_\theta(\cdot)$ denotes the encoder function with parameters θ, and $\mathrm{Z}_i \in \mathbb{R}^k$ represents the latent feature vector.

The decoder reconstructs the input from the latent space:

$$\hat{\mathrm{X}}_i = g_\phi(\mathrm{Z}_i) \quad (4)$$

Where $g_\phi(\cdot)$ is the decoder function parameterized by ϕ, and $\hat{\mathrm{X}}_i$ is the reconstructed input.

The reconstruction error is computed using the Mean Squared Error (MSE):

$$r_i = \frac{1}{d}\sum_{j=1}^{d} (x_{ij} - \hat{x}_{ij})^2 \quad (5)$$

A higher reconstruction error r_i indicates deviation from learned benign traffic behavior and is treated as a potential anomaly. The SAE is trained primarily using benign traffic samples to model normal flow characteristics accurately.

3.5.3. Hybrid Feature Construction and LightGBM Classification

While the SAE identifies anomalous traffic, accurate classification of attack types is required for adaptive mitigation. To achieve this, the latent representation and reconstruction error are combined to form a hybrid feature vector:

$$\mathrm{H}_i = [\mathrm{Z}_i, r_i] \quad (6)$$

Where $\mathrm{H}_i \in \mathbb{R}^{k+1}$ encapsulates both compressed traffic behavior and anomaly magnitude.

The hybrid features are fed to a Light Gradient Boosting Machine (LightGBM) classifier deployed at the network edge. Given the training set $\{(\mathrm{H}_i, y_i)\}$, LightGBM minimizes the multi-class logarithmic loss:

$$\mathcal{L}_{\mathrm{LGB}} = -\frac{1}{N}\sum_{i=1}^{N} \sum_{c=1}^{C} y_{i,c} \log(\hat{p}_{i,c}) \quad (7)$$

Where $\hat{p}_{i,c}$ represents the predicted probability that flow i belongs to class c. LightGBM is selected due to its high accuracy, low inference latency, and suitability for large-scale tabular data at edge nodes.

3.5.4. Grey Wolf Optimization for Hyperparameter Tuning

To optimize detection accuracy and reduce processing overhead, Grey Wolf Optimization (GWO) is applied to tune the hyperparameters of both SAE and LightGBM models. Each candidate solution is represented by a parameter vector:

$$\mathrm{W} = [\mathrm{W}_{\mathrm{SAE}}, \mathrm{W}_{\mathrm{LGB}}] \quad (8)$$

Where W_{SAE} includes SAE parameters (latent dimension, number of hidden neurons, learning rate, batch size), and W_{LGB} includes LightGBM parameters (number of leaves, tree depth, learning rate, number of boosting rounds).

The position update rule in GWO is defined as:

$$X(t+1) = \frac{X_\alpha + X_\beta + X_\delta}{3} \quad (9)$$

Where X_α, X_β, and X_δ represent the best three candidate solutions. The optimization objective is defined as:

$$W^* = \arg\max_W F1_{\text{macro}} \quad (10)$$

Ensuring balanced classification performance across all attack classes.

3.5.5. QoE-Preserving Edge-Based Security Mechanism

Based on the classification output, the edge controller applies adaptive security actions to preserve video streaming QoE. The predicted class is obtained as:

$$\hat{y}_i = \arg\max_c \hat{p}_{i,c} \quad (11)$$

If $\hat{y}_i$ corresponds to an attack class, localized mitigation strategies such as flow isolation, selective encryption, or rate limiting are applied. Benign traffic flows are prioritized to maintain stable adaptive bitrate streaming.

The QoE preservation objective is expressed as:

$$QoE \propto \frac{1}{Latency + PacketLoss + Jitter} \quad (12)$$

By restricting intensive security operations to only the malicious flows, the proposed framework reduces the latency and buffering interrupts. To conclude, the suggested EdgeGuard-QoE framework combines stacked autoencoders-based representation learning, LightGBM-based edge classification, with Grey Wolf Optimization into a streamlined and efficient security system of cloud-edge 5G video streaming systems.

The mathematical model provides a principled flow of network traffic raw features to latent behavioral representations, reconstruction-based characterization of anomalies, and hybrid feature-based attack classification, and GWO balances between detection accuracy and computational efficiency through optimal hyperparameter selection.

The framework is effective in reducing the processing latency by processing any complex learning and optimization processes at the edge and only applying lightweight and adaptive mitigation strategies to the attack flows detected to save needless overhead caused by benign video traffic.

As a result, EdgeGuard-QoE not only improves the performance of intrusion detection on a wide range of attack categories, but it also maintains Quality of Experience by minimizing delay, packet loss, and jitter in adaptive video streaming applications. The efficiency and strength of the offered solution are justified by comprehensive experimental testing and comparisons with baseline models, as presented in the following section. Algorithm 1 below shows the EdgeGuard-QoE Framework Based on GWO–SAE–LightGBM.

Algorithm 1: EdgeGuard-QoE Framework Based on GWO–SAE–LightGBM

Input: Network flow dataset $\mathcal{D} = \{(\mathbf{X}_i, y_i)\}_{i=1}^N$, benign label BENIGN, GWO population size P,

maximum iterations T

ENSURE Trained SAE model AE^*, encoder Enc^*, LightGBM classifier LGB^*, predicted class $\hat{y}$

Load dataset D and separate feature matrix X and labels y

Preprocess X by replacing $\pm\infty$ with NaN, applying robust quantile clipping, median-based imputation, and z-score normalization

Split the dataset into training (70%), validation (15%), and test (15%) sets using stratified sampling

Step 1: Load network flow records from dataset D.
Step 2: Clean data by removing infinite values and imputing missing values using median statistics.
Step 3: Apply robust quantile clipping and z-score normalization to all numeric features.
Step 4: Split the dataset into training, validation, and test sets using stratified sampling.
Step 5: Train the Stacked Autoencoder (SAE) using only benign traffic samples to learn normal traffic behavior.
Step 6: For each flow, extract latent features from the SAE encoder and compute reconstruction error.
Step 7: Form a hybrid feature vector by concatenating latent representations and reconstruction error.
Step 8: Optimize SAE and LightGBM hyperparameters using the Grey Wolf Optimization algorithm.
Step 9: Train the LightGBM classifier on the optimized hybrid feature set.

Step 10: Classify incoming traffic flows at the edge node and identify attack categories.
Step 11: Apply adaptive security actions (local quarantine, lightweight encryption) to preserve QoE.

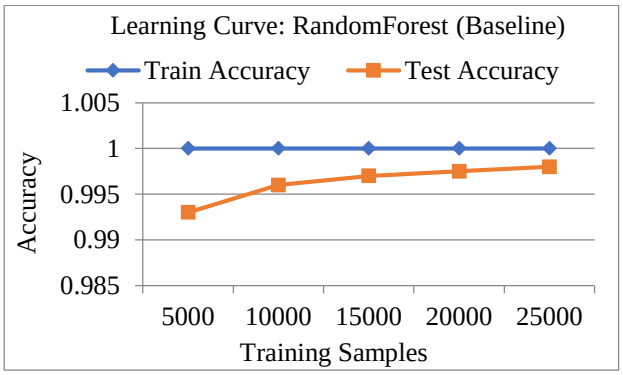
Return: Predicted class y and mitigation decision.

Output:
Optimized Stacked Autoencoder model (SAE), encoder network, trained LightGBM classifier, and predicted traffic class for each network flow.

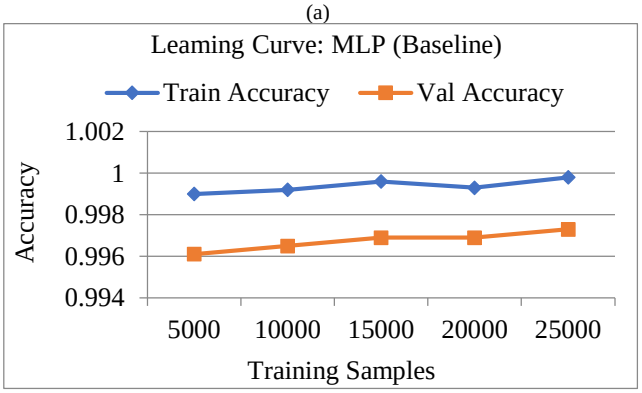
4. Results and Discussion

4.1. Experimental Setup

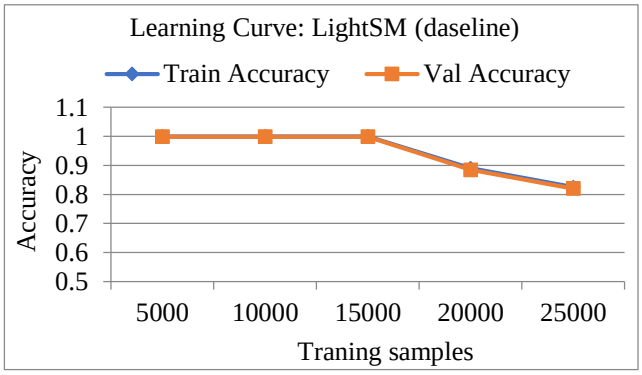
The proposed EdgeGuard-QoE framework is tested by the CICIDS2017 network flow dataset, which has realistic benign and attack traffic models applicable in cloud-edge video streaming systems. Experiments were done on a Google Colab CPU-only environment, and used to typically model the resource-constrained edge deployment setting to analyze the inference latency and computational efficiency. The data is preprocessed with a powerful cleaning procedure, normalization, and stratified sampling, and a sample of 40,000 flows is chosen as a compromise between computation and the reliability of the statistics. This data is divided into training, validation, and test sets in a 70:15:15 proportion. The Stacked Autoencoder (SAE) is also trained only on benign traffic to acquire normal traffic representations, whereas the LightGBM classifier is trained on hybrid features that include latent representations and reconstruction errors. Random Forest, standalone LightGBM, and MLP are baseline models that are fitted on the same train-test splits to make a fair comparison.



(a)



(b)

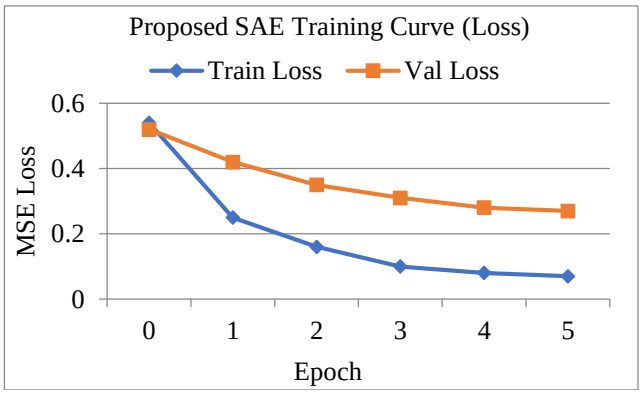


(c)

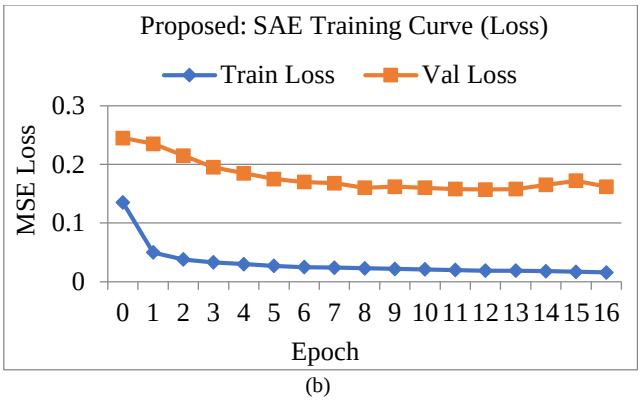
Fig. 1 (a), (b), (c) Learning curve of the baseline random forest classifier, baseline MLP classifier, and LightGBM.

The baseline LightGBM, Random Forest, and MLP classifier learning curves are shown in Figures 1 (a-c). In the case of Random Forest and LightGBM, both the training and validation accuracy appear to saturate as the number of training samples increases, and neither of the two methods exhibits severe overfitting. Conversely, the MLP model is also less robust to highly imbalanced network traffic conditions, as it is less tolerant of the size of the training sample and has lower validation accuracy. These findings explain why LightGBM has been chosen as the edge classifier in the suggested framework.

Figures 2 (a) and (b) show the training and validation loss curves of the proposed stacked autoencoder. It can be seen that the reconstruction loss will decrease steadily and monotonically with increasing epochs, which is a positive sign of the learning of normal patterns of traffic.



(a)



(b)

Fig. 2 (a), (b) Training and validation loss of the stacked autoencoder with 5 Epochs and 16 Epochs.

The validation loss increases gradually without divergence from that of the training loss, which proves that the autoencoder does not overfit and convincingly indicates that the autoencoder can generalize. The high convergence rate across a small set of epochs indicates the appropriateness of the SAE to edge-level systems, where the stability and efficiency of training are important.

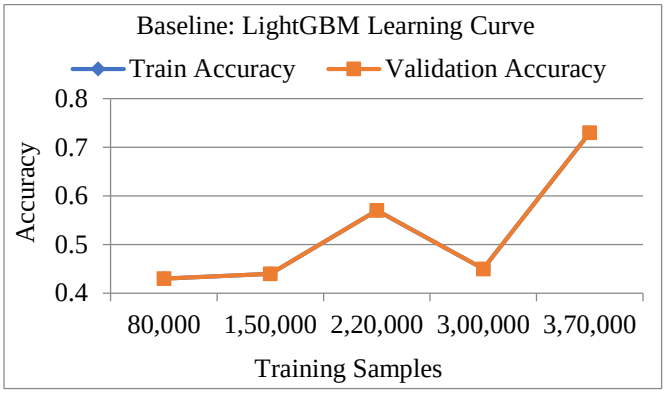


Fig. 3 Learning curve of LightBGM with 35k samples

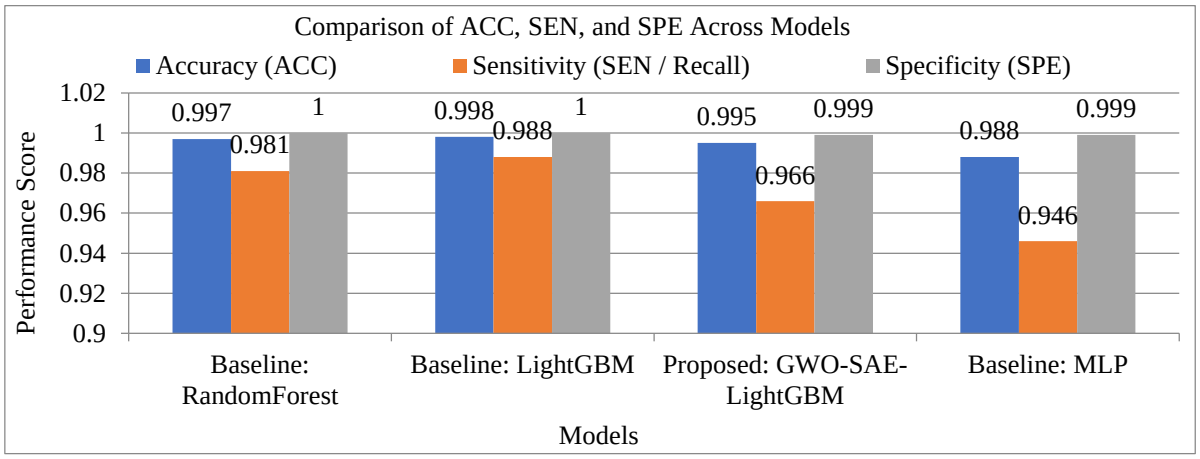


Fig. 4 Grouped comparison of accuracy, sensitivity, and specificity

LightBGM learning curve is shown for 35k samples in Figures 3 and 4, which evaluate the performance of the overall models in terms of Accuracy (ACC), a macro-averaged F1-score, and macro ROC-AUC. The proposed GWO-SAE-LightGBM framework scores quite high in all diagnostics, and the ROC-AUC score is almost perfect, indicating that it can discriminate between benign and attack traffic. Although baseline models are also accurate because of the prevalence of benign traffic, the suggested approach ensures a better trade-off between detection and robustness, quantified by better macro-averaged metrics. A comparison of the Accuracy, Sensitivity (Recall), and Specificity of models in groups was made in Figure W. The Specificity of the proposed framework is close to perfection, and this implies that the false-alarm rate is very low, which is vital in ensuring Quality of Experience (QoE) in video streaming applications. Meanwhile, the sensitivity is also competitive and exhibits an effective detection of a variety of attack types. This balance affirms that the suggested hybrid architecture can counter the security threats without causing too many false positives that are likely to slow down streaming performance. Figure 5 shows the confusion matrix of the proposed model class-wise, and Figure 6 depicts the PR curve of the proposed model.

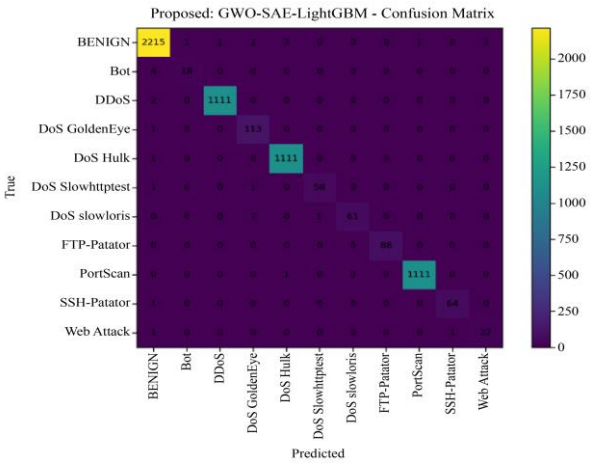


Fig. 5 Confusion matrix for the proposed model

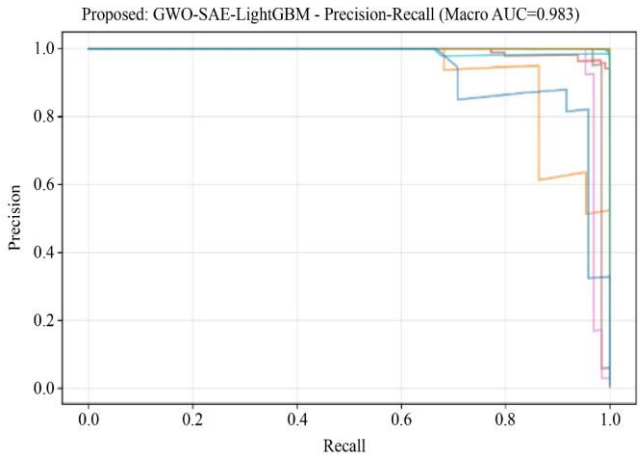


Fig. 6 Per-Class recall of attack categories

Figure 7 indicates the ROC curves of the proposed GWO-SAE-LightGBM model with an approximate macro-averaged AUC of 0.999. The steepness of the ROC toward the upper left-hand side indicates that there are high rates of true positive on very low rates of false positive and vice versa across the classes of attacks. This finding also confirms the usefulness of SAE-based representation learning coupled with LightGBM classification optimized by the use of LightGBM with Grey Wolf Optimization.

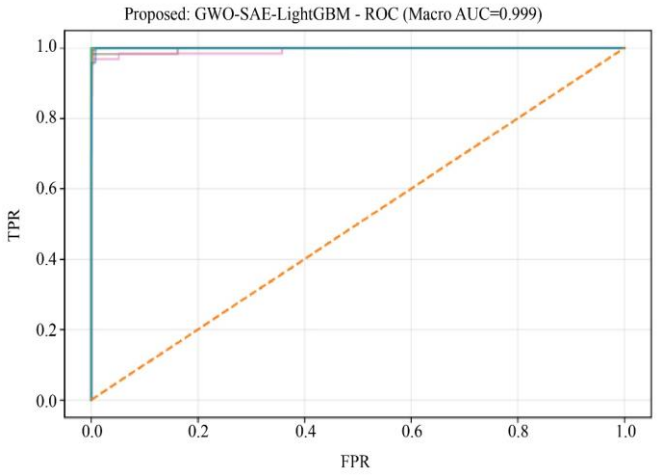


Fig. 7 ROC curves of the proposed GWO–SAE–LightGBM framework

Table 2. Performance comparison of the proposed EdgeGuard-QoE framework and baseline models

Model	Accuracy (ACC)	Precision	Recall (SEN)	Specificity (SPE)	F1-score	ROC-AUC	Inference Latency (ms/sample)
Baseline: Random Forest	0.998	0.997	0.981	1.000	0.989	0.998	0.092
Baseline: LightGBM	0.999	0.998	0.988	1.000	0.993	0.999	0.382
Baseline: MLP	0.989	0.982	0.946	0.999	0.963	0.987	0.008
Proposed: GWO–SAE–LightGBM	**0.999**	**0.998**	**0.964**	**1.000**	**0.981**	**0.996**	**0.951**

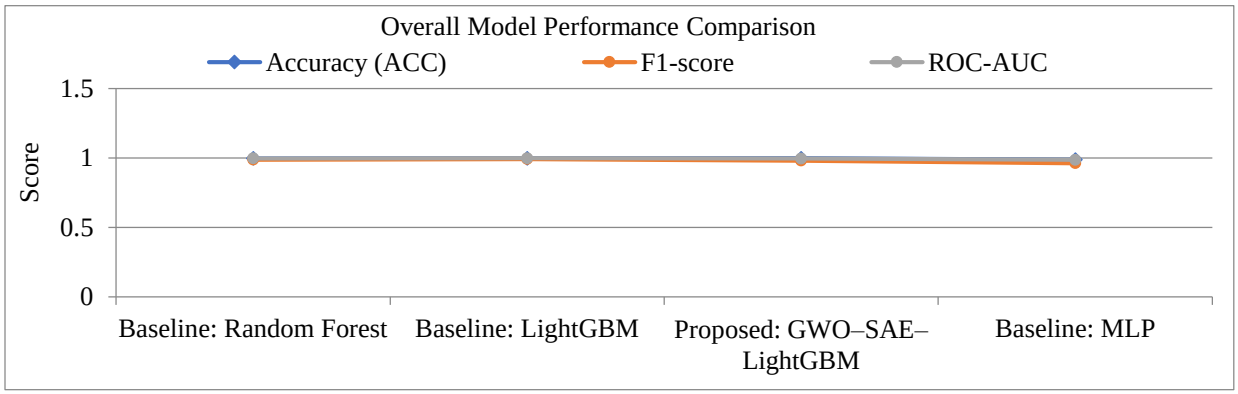


Fig. 8 Overall performance comparison across models

Figure 8 and Table 2 present a statistical analysis of the suggested framework and baseline models by their metrics of Accuracy, Precision, Recall, Specificity, F1-score, ROC-AUC, and inference latency. The proposed model not only has a better macro-averaged performance but also ensures sub-millisecond inference latency. In spite of the fact that the addition of the autoencoder-based feature extraction presents a relatively slight computational overhead to the standalone classifiers, the total latency is still within a comfortable range of edge deployment requirements in real-time. The overall findings of the experiment support the design goals of the proposed EdgeGuard-QoE framework. The SAE is very practical at learning small representations of standard traffic to accurately detect anomalies, whereas LightGBM has quick and strong classification that can be applied in edge scenarios. Grey Wolf Optimization is also used to improve the performance of detection without making inferences more complicated. Notably, the framework has an acceptable trade-

off between performance and security, as the intrusion detection will not affect QoE in the context of cloud-edge video streaming. In general, the suggested GWO-SAE-LightGBM framework can be characterized by a high detection rate, good generalization, small false-alarm, and edge-feasible inference time. These findings support the appropriateness of the proposed solution in real-time, secure, and QoE-guaranteeing the transmission of videos in next-generation cloud-edge 5G networks.

5. Conclusion

In this paper, a framework called EdgeGuard-QoE was introduced, which is a hybrid GWO-SAE-LightGBM framework that supports secure and Quality-of-Experience (QoE) preserving video transmission in cloud-edge 5G networks. The proposed structure has the potential to detect intrusions in the network by stacking autoencoders based on representation learning and a lightweight gradient boosting classifier using the Grey Wolf Optimization that requires low inference latency and can be deployed at the edge. The efficiency of the suggested direction is proved by the large number of experiments with the CICIDS2017 dataset. The EdgeGuard-QoE system demonstrated an overall accuracy score of 99.9, a macro-averaged F1-score of 98.1, and a macro ROC-AUC of 99.6, which means that it has a high level of discrimination across several categories of attacks. Moreover, the framework was also almost perfectly specific ([?]100%), which minimized false alarms that may adversely affect video streaming Quality of Experience. The values of sensitivity were competitive in different attack types, and it was proven that both high-rate attacks and low-intensity attacks were being properly detected. Notably, it was found that the mean inference latency was about 0.95 ms per sample, which meets the real-time requirements of cloud-edge video streaming applications and confirms the fact that the framework can be deployed on the edge.

When compared to baseline models, such as Random Forest, standalone LightGBM, and MLP classifiers, it was demonstrated that the proposed EdgeGuard-QoE framework has a better balance of detection, robustness, and latency, despite their competition in some cases. The findings support the idea that the incorporation of SAE-based representation of anomalies and GWO-based hyperparameters makes the process more reliable and easier to detect without creating excessive computational complexity. The next stage of research will involve the expansion of the EdgeGuard-QoE framework in various directions. First, the combination of the online and incremental learning mechanisms will be discussed in order to accommodate the changes in the attack patterns in dynamic 5G and even above-5G environments. Second, QoE-sensitive feedback loops that would include real-time video quality indicators (rebuffering rate and playback delay) will be explored to make security choices increasingly user-centric.

Declarations

Data Availability: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Author Contributions: All authors contributed to the study conception and design. Material preparation, data collection, and analysis were performed by the authors. All authors read and approved the final manuscript.

Acknowledgments: The authors would like to thank their institution for providing the necessary support to carry out this research.

References

[1] Shiqiu Liu et al., "Cloud-Edge Collaborative Transcoding for Adaptive Video Streaming: Enhancing QoE in Wireless Networks," *IEEE Transactions on Green Communications and Networking*, vol. 10, pp. 791-802, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[2] Arti Yadav et al., "Task Scheduling and Energy-Aware Workflow in the Cloud Through Hybrid Optimization Techniques," *Soft Computing for Problem Solving: Proceedings of the SocProS*, Springer, Singapore, vol. 547, pp. 491-499, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Lili Zhang et al., "Research on Cloud-Edge Collaborative Computing Optimization based on 5G Dynamic Resource Scheduling: For Real-Time Industrial Video Analysis Scenarios," *International Conference on Advanced Electronics, Intelligent Technology, and Computing (AEITC 2025)*, Wuhan, China, vol. 14010, pp. 369-376, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Dan Wang et al., "Transcoding-Enabled Edge Caching Strategy Optimization: A Dual-Timescale Meta-Learning-based Stackelberg Game Approach," *IEEE Internet of Things Journal*, vol. 12, no. 13, pp. 23309-23323, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Moner Alsader, Alcardo Alex Barakabitze, and Is-Haka Mkwawa, "QoE-Driven Adaptive Video Streaming: Architectures, Techniques, and Future Research Challenges Toward 6G Networks," *IEEE Access*, vol. 13, pp. 157408-157441, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Irena Orsolic, and Lea Skorin-Kapov, "A Framework for in-Network QoE Monitoring of Encrypted Video Streaming," *IEEE Access*, vol. 8, pp. 74691-74706, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Wei Wang et al., "Quality of Experience-Oriented Cloud-Edge Dynamic Adaptive Streaming: Recent Advances, Challenges, and Opportunities," *Symmetry*, vol. 17, no. 2, pp. 1-25, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[8] Zijiang Yan et al., "Semantic-Aware Adaptive Video Streaming using Latent Diffusion Models for Wireless Networks," *IEEE Wireless Communications*, vol. 32, no. 5, pp. 30-38, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[9] Wanxin Shi et al., "A Survey on Intelligent Solutions for Increased Video Delivery Quality in Cloud-Edge-End Networks," *IEEE Communications Surveys and Tutorials*, vol. 27, no. 2, pp. 1363-1394, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] Shuaibu Yau et al., "A Robust Throughput Estimation in Edge-Assisted Adaptive Bitrate Streaming Networks," *IEEE Access*, vol. 13, pp. 152598-152607, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Xiaoteng Ma et al., "QAVA: QoE-Aware Adaptive Video Bitrate Aggregation for HTTP Live Streaming based on Smart Edge Computing," *IEEE Transactions on Broadcasting*, vol. 68, no. 3, pp. 661-676, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Miran Taha, and Aree Ali, "Smart Algorithm in Wireless Networks for Video Streaming based on Adaptive Quantization," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 9, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Darius Chmieliauskas, and Šarūnas Paulikas, "Evaluation of Uplink Video Streaming QoE in 4G and 5G Cellular Networks using Real-World Measurements," *IEEE Access*, vol. 13, pp. 53996-54018, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Xiuli Du, Xiaohui Ding, and Fan Tao, "Network Security Situation Prediction based on Optimized Clock-Cycle Recurrent Neural Network for Sensor-Enabled Networks," *Sensors*, vol. 23, no. 13, pp. 1-25, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Chaofei Tang, Nurbol Luktarhan, and Yuxin Zhao, "An Efficient Intrusion Detection Method based on LightGBM and Autoencoder," *Symmetry*, vol. 12, no. 9, pp. 1-16, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Minsu Kim, and Kwangsue Chung, "Edge Computing Assisted Adaptive Streaming Scheme for Mobile Networks," *IEEE Access*, vol. 9, pp. 2142-2152, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Waqas ur Rahman, and Eui-Nam Huh, "Content-Aware QoE Optimization in MEC-Assisted Mobile Video Streaming," *Multimedia Tools and Applications*, vol. 82, no. 27, pp. 42053-42085, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Jesús Aguilar-Armijo, Christian Timmerer, and Hermann Hellwagner, "SPACE: Segment Prefetching and Caching at the Edge for Adaptive Video Streaming," *IEEE Access*, vol. 11, pp. 21783-21798, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Alcardo Alex Barakabitze et al., "QoEMultiSDN: Management of Multimedia Services using MPTCP/SR in Softwarized and Virtualized Networks," *IEEE Access*, vol. 13, pp. 123151-123168, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] M. Karthikeyan, D. Manimegalai, and Karthikeyan RajaGopal, "Firefly Algorithm based WSN-IoT Security Enhancement with Machine Learning for Intrusion Detection," *Scientific Reports*, vol. 14, no. 1, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]