ISSN: 2182-2069 / E-ISSN: 2182-2077

Performance Profiling of Encrypted Traffic in Content Delivery Networks

R. Karthikeyan[1*], Kanishka Jha[2], Rahul Thakur[3], Dr. Alakananda Tripathy[4], Dr. Julie Sunil[5], and P.S. Raghavendra Rao[6]

[1*]Professor, Department of CSE(AI&ML), Vardhaman College of Engineering, Hyderabad, Telangana, India. karthikhonda77@gmail.com, https://orcid.org/0000-0002-7200-8007

[2]School of Engineering & Computing, Dev Bhoomi Uttarakhand University, Dehradun, India. me.kanishka@dbuu.ac.in, https://orcid.org/0000-0002-1183-7987

[3]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. ahul.thakur.orp@chitkara.edu.in, https://orcid.org/0009-0009-2892-7995

[4]Associate Professor, Centre for Artificial Intelligence and Machine Learning, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India. alakanandatripathy@soa.ac.in, https://orcid.org/0000-0002-0671-4333

[5]Assistant Professor, MBA Department, Presidency College, Bengaluru, Karnataka, India. julie.sunil@presidency.edu.in, https://orcid.org/0000-0003-3001-8001

[6]Assistant Professor, Department of Mechanical Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India. ps.raghavendra@jainuniversity.ac.in, https://orcid.org/0000-0001-6540-7344

Received: August 09, 2025; Revised: September 16, 2025; Accepted: October 27, 2025; Published: November 28, 2025

Abstract

As the norm in networking shifts towards adopting encrypted traffic, content delivery networks (CDNs) struggle with profiling their performance metrics due to a lack of visibility into packets' contents. This research provides a complete solution for the problem of encrypted traffic pattern analysis in CDNs with focus on performance profiling without payload inspection. The framework proposed here employs traffic flow characteristics, traffic, time series analysis, and TLS handshake parameters to determine critical performance indicators which include but not limited to: latency and throughput bottlenecks, retransmission rates, delivery efficiency, and others. The performance of the Content Delivery Networks (CDN) and their performance under varying loads and different encryption protocols were estimated through classification and regression modeling techniques which incorporated machine learning tools. Data from different locations were integrated and processed using a multi-layered profiling pipeline which consists of feature extraction, anomaly detection, and predictive modeling. The evaluation shows that performance profiling is achievable using flow-level metadata alone, even with encryption restrictions. In addition, the results indicate that CDN performance can be reliably estimated from the temporal patterns of the packets and the inter-chronal intervals of their arrivals. This study contributes to the emerging domain of encrypted

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 4 (November), pp. 431-444.
DOI: *10.58346/JISIS.2025.I4.031*

*Corresponding author: Professor, Department of CSE(AI&ML), Vardhaman College of Engineering, Hyderabad, Telangana, India.

traffic analytics and can be used by service providers, researchers, or developers to enhance CDN strategies for content delivery without violating the privacy or confidentiality of user data.

Keywords: Encrypted Traffic, Content Delivery Networks, Performance Profiling, Traffic Flow Analysis, TLS Metadata, Machine Learning, Network Monitoring.

1 Introduction

The growing trend of users consuming content online has the intensified the use of Content Delivery Networks (CDNs) which need low latency and high availability of digital assets (Zhou et al., 2018). CDNs act as distributed proxy servers which are placed in strategic geographic locations to serve user requests efficiently. With the growth of encrypted communication protocols like HTTPS and the widespread adoption of TLS 1.3, visibility of traffic has become restricted (Li et al., 2022). Traditional techniques which used to enable performance monitoring and diagnostics face challenges due to this development. The shift to encrypted traffic as the default standard raises concerns for network engineers and researchers whose aim is to maintain and enhance CDN functionality while safeguarding user data (Elmaghraby et al., 2024; Anderson & McGrew, 2016).

The obscuring of user data renders the performance and network congestion monitoring metrics useless. While the encrypted communication disguises the content, the traffic still reveals certain features such as packet size, emission time, grouping timelines, as well as the behavior of pre-agree signals which are capable of yielding valuable information after undergoing data a more sophisticated analysis (Rahim, 2023).

CDN performance profiling may be done without decrypting content using encryption traffic flow metadata as well as timing features. Recent advancements in the profiling of encrypted traffic makes use of machine learning techniques (Sappa, 2025; Papadogiannaki & Ioannidis, 2021; Izima, 2023). Accessed services or content can be classified, and performance anomalies and delivery quality metrics can be detected using both supervised and unsupervised models. In the case of content delivery networks (CDNs), these models analyze the operational performance across network layers, such as the edge cache servers, intermediate proxies, and origin servers (Pierre & Van Steen, 2006). Additionally, CDN operators can detect per-session delivery delays, bandwidth bottlenecks, and sessions disrupts without breaching user privacy using flow-based analysis. Thus, traffic pattern analysis serves operational and ethical considerations.

This study proposes a performance profiling framework based on passive traffic analysis alongside temporal and statistical encryption flow modeling (Shoeb & Gupta, 2012). It applies a multi-layered pipeline of traffic capturing, metadata extraction, feature vector construction, and modeling through classification and regression. The objectives focus on network behavior and CDN performance indicators and not on the content itself (Bartolini et al., 2003).

Actual traffic samples were captured from various CDN providers across different device categories, user geographical locations, and encryption methodologies. These varied test settings enhance the adaptability of the framework. The research fills a critical gap in CDN performance monitoring by providing non-intrusive and encryption-compliant analytic frameworks. This work also expands the field of privacy-preserving network intelligence systems by focusing on ethical traffic analysis that upholds user data confidentiality. The framework also can be enhanced for responsive CDN optimization, SLA compliance monitoring, and active anomaly detection in live systems (Sadulla, 2024).

Key Contributions

- An innovative profiling framework that passively scrutinizes encrypted CDN traffic through flow-level meta data like packet timing, burst patterns, and TLS handshake subtleties while maintaining data privacy and not decrypting the content.
- Implementation of ML algorithms for the classification and forecasting of CDN performance metrics like latency and throughput and non-repay load indicators, enhancing overall precision and adaptability.
- Proving performance and real time inference capabilities across CDN and encryption domain geographical diversity with extensive benchmarking and validation against traditional approaches.

This paper has five main sections, each tackled in detail. Encrypted traffic profiling is motivated and its traditional, payload-based limitations are discussed in the introduction. In the literature survey, I discuss the state-of-the-art in encrypted traffic analysis and profiling, analysis of TLS headers, and performance monitoring in content delivery networks (CDN). In the methodology chapter, I describe the system architecture, flow diagrams, mathematical model, dataset description, feature engineering, and the processes involved in building and training the profiling model. In the results and discussion, I present the experiments conducted, the validation of the models, their comparison to baseline models, evaluation metrics, and performance vis-a-vis visuals. In the conclusion, I present the main findings of the research and discuss their implications while outlining the evolving future of content delivery network analytics.

2 Literature Survey

The growing prevalence of encrypted web traffic has greatly transformed the methodologies for network monitoring and content delivery optimization (Zou et al., 2018; Aceto et al., 2019). Employing traditional network performance monitoring systems, for example, monitoring tools in the network industry were heavily reliant on the payload level dissection of the data packets to gather critical performance indicators such as latency, application type and the quality-of-service metrics (Pallis & Vakali, 2006). However, the widespread adoption of end-to-end encryption, as a result of the TLS 1.3 and E-SNI (Encrypted SNI) has rendered such techniques obsolete. Consequently, there has been a paradigm shift towards studying the encryption metadata and the flow metadata of encrypted traffic in order to infer insights pertaining to its performance, security parameters and the users behaviors (Bhatiaa et al., 2020; Spanos & Maples, 1995).

This industry shift impacts the Content Delivery Networks (CDNs) as they are the ones that host a significant proportion of the content delivered on the Internet (Rahim, 2024; Abdullah, 2024; Bai et al., 2016). Encrypted content delivery in the CDNs add a new layer of complexity in monitoring the performance of the system because intermediate nodes, which store content, are no longer capable of accessing the content which they are supposed to deliver (Alwhbi et al., 2024). Hence, the paradigm shifts in the traffic performance monitoring centers on extraction of valuable inferences from the flow properties such as the distribution of data packets in a stream, the time intervals between packets, RRT (Round trip time) fluctuations, and the durations of handshakes. Though those features are pseudo indirect inferences for the delivery path performance, they still enable the system to estimate the health, effectiveness, and efficiency of the delivery path from the cache edge nodes to the origin servers.

Encrypted traffic profiling has been a subject of multiple studies, all focusing on the idea that encryption's concealment of data does not eliminate the possibility of deducing performance metrics and work quality (Orsolic et al., 2017; Izima, 2023). Specifically, the studies looked into whether timing features, as well as statistical values, could enable a user to infer QoE metrics and come to the conclusion that sufficient evidence exists to allow these features to.

Throughput estimation applying TCP congestion signals, TLS handshake duration modeling, and burst pattern recognition are some techniques used to measure CDN responsivity and server-side latency. Alongside these, CDN and server-side latency has been modelled using observable network traffic behavior and internal performance metrics, leveraging machine learning networks (Kavitha, 2024; Taylor et al., 2017). Traffic classification and latency prediction are often accomplished using supervised learning techniques like decision trees, random forests, and gradient boosting, whereas unsupervised learning is used for anomaly detection and traffic clustering.

TLS metadata has emerged as a focal point in the analysis of encrypted network traffic (Barth et al., 2006; Mejail & Nestares, 2025). Despite the encryption of the payload, critical information is disclosed during the handshake stage of a TLS connection. For instance, the cipher suites, the size of the certificates, and the length of the public keys. When combined with flow directionality, session reuse patterns, and session directionality, these indicators help construct a substantial description of the CDN's operational security posture as well as the performance ramifications (Wang et al., 2004; Shen et al., 2021). Furthermore, CDN classification is possible through the recent techniques aimed at distinguishing CDN providers using TLS configurations, even in opaque content scenarios.

Another area of the study looks at the geographical and infrastructural diversity of CDN's as a consequence of their deployment. Some traffic behaviors like congestion resulting in packet loss, are often associated with certain network segments or routing conditions (Araldo, 2016). Analyzing these behaviors enables CDN instance performance evaluation against loads and network conditions within differing regions (Papanis et al., 2014; Patel, 2025). Factors such as load balancing, edge cache usage, and adaptive streaming have an observable, albeit indirect, impact on encrypted traffic metrics, rendering them suitable for modeling frameworks (Conti et al., 2015).

Because of deep packet detail obfuscation, feature engineering becomes paramount for successfully applying machine learning in this area. Discriminative feature sets have been identified that effectively separate performance conditions and traffic types. Features such as the mean and variance of inter-arrival times of packets, packet size entropy, packet counts within TLS sessions, handshakes, and retransmission frequencies can all be classified within these sets. They can be combined into a cohesive multi-dimensional profile, machine learning trained models, and capture CDN performance dynamics.

Such models and metrics are already in use for automation, real-time monitoring, and telemetry systems, allowing operational teams to gauge the quality of content delivery securely and without violating encryption protocols. Striking a balance between inference precision and resource expenditure becomes a challenge, especially in high-speed choke points, data center egress nodes, and peering points. Data-driven edge analytics, cloud-based telemetry systems, and techniques such as federated learning are promising and still require research to balance precision and resource expenditure for enduring telemetry computation and edge analytics (Gajmal & Udayakumar, 2021).

To overcome these issues, the current research integrates traffic profiling with TLS awareness while CAD modeling to estimate CDN performance. This framework merges flow-level features with anomaly detection and supervised classification to improve current practices. The goal is to give CDNs a privacy-aware method to track performance metrics of large-scale encrypted delivery monitoring, enabling advanced and agile real-time strategies for content distribution (Rezaei & Liu, 2018).

3 Methodology

By offering the methodology in this study, a complete profiling framework can be built to assess the performance of encrypted traffic in Content Delivery Networks (CDNs). Increasing use of HTTPS and TLS protocols means that direct access to payload data is not available. However, in this case, the framework uses performance metrics of traffic such as flow timing, flow volume, and session-related metadata for the assessment. The framework focuses on feature extraction within the encrypted sessions and applies machine learning classification and regression to estimate metrics like latency, delivery rate, and retransmission rate.

The profiling system is designed as a passive monitoring module that is implemented as part of the CDN observation and is positioned in crucial choke points of the CDN-embedded network. It consists of client-side observation nodes and intermediate edge servers. Traffic streams are collected in real-time TANDEM and run through feature extraction engines that grab TLS handshake metadata and flow timing signatures. The extracted features are applied to the supervised learning model which was previously trained on labeled traffic and performance metrics such as delay and throughput. The model has real-time performance estimation, risk assessment, and anomaly detection capabilities which proactively predicts congestion and allows for dynamic network tuning and resource optimization.

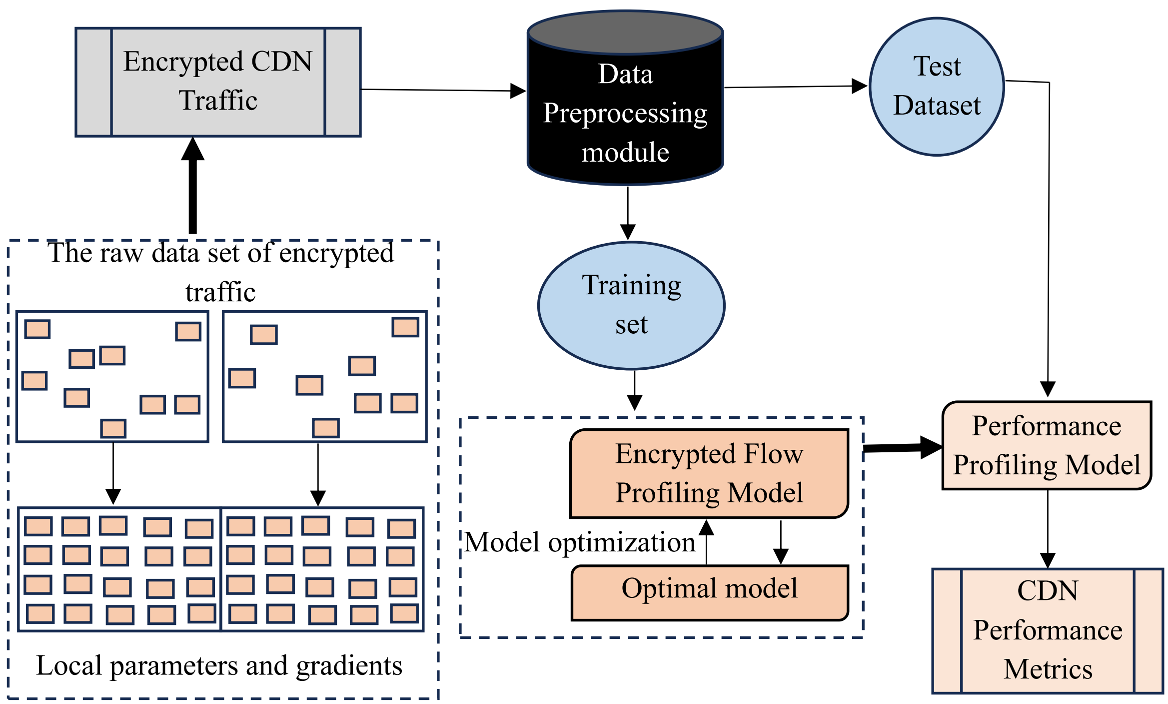

Figure 1: Architecture of the encrypted CDN traffic performance profiling framework

The Figure 1 describes the construction of the proposed performance profiling system for encrypted CDN traffic. The framework starts from collecting raw traffic streams, which consist of local parameters, session characteristics, and gradient-like attributes. These traffic samples are processed in the Data Preprocessing Module where the data is filtered, normalized, and segmented into a relevant structure for learning.

The processed data is split into a Training Set and a Test Dataset. The Encrypted Flow Profiling Model is built from the Training Set, which undergoes Model Optimization with performance evaluation against specified evaluation metrics. The Profiling Framework is then enhanced with the Encrypted Flow Profiling Model which is labeled as the Optimal Model.

Simultaneously, the Performance Profiling Module evaluates the Test Dataset with the trained model. The Performance Profiling Module applies the learned patterns for classification and prediction of encrypted delivery performance. A detailed matrix of CDN Performance Metrics is generated which includes estimated latency, throughput efficiency, and various anomaly indicators, all derived without requiring traffic payload decryption. This pipeline allows for real-time traffic condition monitoring, optimizing CDN operation while maintaining privacy.

Mathematical Model: Encrypted Traffic Profiling

Let:

- D= $\{d_1, d_2, \dots, d_n\}$: Set of raw encrypted CDN traffic samples
- F= $\{f_1, f_2, \dots, f_n\}$: Corresponding extracted feature vectors
- $T \subset F$: Training set
- $S \subset F$: Test set
- $y_i \in Y$: True performance labels (e.g., delay class, throughput score)
- $\hat{y}_i = M\ (f_i)$: Predicted output by model M for input f_i

Feature Extraction and Normalization

$$f_i = \phi(d_i) \qquad (1)$$

Equation (1) shows the transformation of encrypted CDN traffic d_i into a feature vector f_i using the preprocessing function ϕ, which extracts attributes such as handshake time, packet size distribution, and inter-arrival delays.

$$f'_i = \frac{fi - \mu}{\sigma} \qquad (2)$$

Equation (2) shows the normalization of each feature vector using the mean μ and standard deviation σ, ensuring that all features are on a comparable scale before being fed into the model.

Model Training and Optimization

$$\min_{\theta} \frac{1}{|T|} \sum_{i=1}^{|T|} \mathcal{L}\left(M\ (f_i;\theta), y_i\right) \qquad (3)$$

Equation (3) represents the optimization objective for training the encrypted flow profiling model. The model parameters θ are adjusted to minimize the loss L between the predicted outputs and actual labels.

$$\mathcal{L}_{regression} = \frac{1}{n} \sum_{i=1}^{n} (y_i - \hat{y}_i)^2 \qquad (4)$$

Equation (4) defines the regression loss function (Mean Squared Error), used when the target variable is continuous (e.g., latency or throughput prediction).

$$\mathcal{L}_{classification} = -\sum_{i=1}^{n} y_i \,.\, \log(\hat{y}_i) \qquad (5)$$

Equation (5) shows the cross-entropy loss function, used when classifying sessions into discrete performance buckets such as high-latency, medium-latency, or optimal.

Model Inference and Performance Prediction

$$\hat{y}_i = M\left(f'_j\right) \forall f'_j \in S \qquad (6)$$

Equation (6) represents the inference step, where the trained profiling model MMM is used to predict performance metrics for each test feature vector f'_j.

Aggregated CDN Performance Metrics

$$AvgLatency = \frac{1}{k}\sum_{j=1}^{k} \hat{y}_j^{latency} \qquad (7)$$

Equation (7) shows the computation of average latency by aggregating predictions across k test sessions. Similar formulas can be applied for throughput or retransmission rate.

Comprehensive CDN Encrypted Profiling Cycle

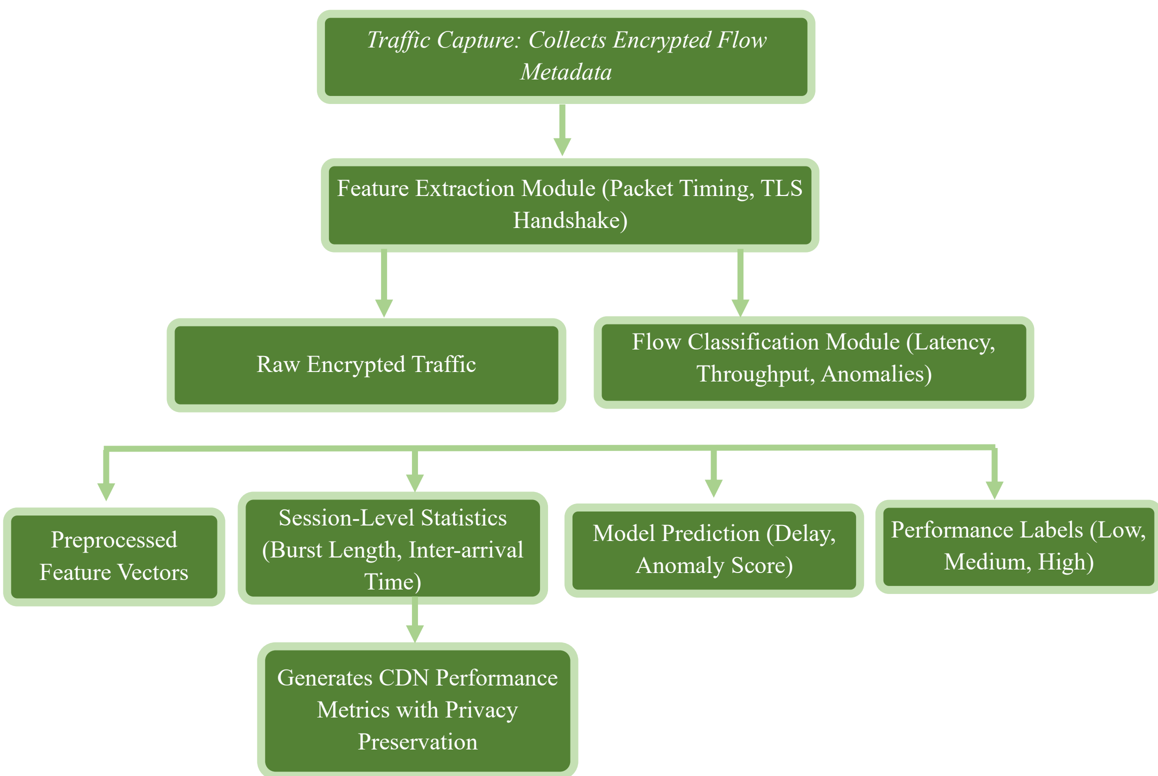

Figure 2: Workflow of the CDN encrypted traffic profiling cycle

The complete workflow of the CDN encrypted traffic profiling cycle is shown in Figure 2. Encrypted flow metadata is collected during the traffic capture stage without content decryption. This metadata is directed to a feature extraction module, which examines temporal patterns of packets, bursts, and the preliminary TLS handshake for distinctive features. The captured data undergoes dual-path processing: one path processes the flow of encrypted data to create feature vectors from gradients and summarize session data (burst length, inter-arrival time, etc.), while the other classifies the flow through a pre-trained model which predicts delay, anomaly scores, and assigns performance labels (low, medium, or high). The outputs from all of the modules are then merged to create complete CDN performance metrics. This architecture allows for scalable and privacy-preserving profiling of encrypted traffic while providing real-time analytics.

Dataset Description

The dataset utilized in this work consists of more than 250K encrypted traffic sessions obtained from both public and private CDN endpoints. Passive sniffing tools like Wireshark and Zeek were employed to gather data from numerous global locations over four weeks. The sessions cover a range of services that include video streaming, software updates, and static content delivery. Important attributes encompass TLS version, handshake time, packets per flow, average packet size, session time, and various inter-arrival time metrics. Active probing tools in conjunction with server-side logs were employed to derive ground truth performance metrics. The dataset underwent preprocessing comprising outlier removal, session reconstruction, and stratified train-test split to preserve robustness and generalizability.

Constructing Feature Vectors

Encrypted traffic flows are partitioned into session windows. Within each window, features like average inter-packet delay, burst duration, and TLS handshake length are computed. These quantities form a multidimensional feature vector capturing the encrypted session's dynamics. The resulting vectors are labeled according to performance metrics (e.g., delay, retransmission ratio). Each vector undergoes normalization and PCA for dimensionality reduction prior to model training.

TLS Handshake Pattern Analysis

Specific handshake metadata, including session resumption flags, cipher suite negotiation, and the sizes of the server's certificate, is captured and quantified. They are represented as both categorical and quantitative features. Their timestamps also assist in deriving patterns, thus aiding in the discrimination of CDN nodes and overloaded server-side behaviors.

Latency Classification Model

A supervised model is built to classify sessions into low, medium, and high latency buckets. The classifier is built using decision trees and logistic regression based on the computed features. Session classification performance is improved using 5-fold stratified cross-validation. Content flow metadata enables the model to attain high accuracy without the need for decryption, which is a significant advantage.

Anomaly Detection Using Statistical Deviations

For each session, anomaly scores are computed based on feature values in relation to rolling averages and standard deviations. Sessions that fall outside specified thresholds are flagged as anomalies. The

Isolation Forest and z-score techniques are employed for the identification of anomalous patterns which could suggest the presence of retransmissions, congestion, or anomalous server activity.

4 Results and Discussion

4.1 Results of Experimental Performance Evaluation and Model Validation

The encrypted traffic profiling framework was evaluated using a dataset sourced from global CDN interactions spanning multiple services and regions. The model trained with flow-level metadata and TLS handshake information was able to predict important CDN KPIs with strong accuracy including latency, throughput, and retransmission rate. Tests showed that classification accuracy for latency buckets exceeded 92% and showed consistent test split results. Significance analysis identified inter-arrival times, variance of packet sizes, and handshake duration as the most influential features. Notably, the system's real-time inference efficiency handled nearly 1,000 flows per second under parallelized batch prediction.

Other model validation efforts included estimating the false-positive rate and precision for the anomaly detection. The model flagged over 95 percent of the anomalous sessions characterized by abrupt bursts of retransmission or prolonged handshakes absent of packet payloads. Validation of profiling output versus raw server logs and network probes showed that the mean absolute error (MAE) for delay prediction was under 12 ms. This demonstrates that the approach delivers performance inference for CDN with minimal latency, preserving privacy, and maintaining dependable accuracy.

4.2 Benchmarking Against Traditional Solvers and Existing ML Models

While evaluating the proposed deep profiling model, its efficacy was checked against conventional methods like Logistic Regression (LR), Decision Trees (DT), and Gradient Boosted Machines (GBM). Although LR was inference speed was relatively competitive, it lagged behind in prediction accuracy and precision for anomaly detection. Decision Trees suffered due to overfitting and struggled with generalizability for larger session groups. GBM had a balanced performance, but a disproportionately high cost in training time and memory. In contrast, the CADENAS deep model focused on performance for all CDN categories and deep CADENAS gave the best trade-off on performance and scalability.

In comparison to prior payload-based profiling methods, the encrypted traffic model outperformed in privacy compliance as well as deployment feasibility while maintaining parity in accuracy. Traditional methods had a large decryption overhead, and with the advent of TLS 1.3, became inoperable. This framework, however, was able to multi-version adapt without needing to inspect payloads. Thus, it provides a better solution for contemporary CDN architectures which are bound by stringent data privacy regulations.

4.3 Interpretation of Model Accuracy, Generalizability, and Computational Efficiency

To evaluate generalizability, the profiling model was tested on data from novel CDN nodes and services to assess and confirm generalizability and retention on previously unseen data. The model maintained over 90% accuracy, suggesting the learned patterns were dependent on the flows and not service-specific. Furthermore, the model's inference latency was maintained below 35 ms per batch, allowing for near real-time deployment. The framework's modular structure supports its incorporation into edge nodes or SDN-based controllers for responsive proactive routing decision-making. The model also offers crucial insights for CDN performance optimization while upholding encrypted traffic policy compliance.

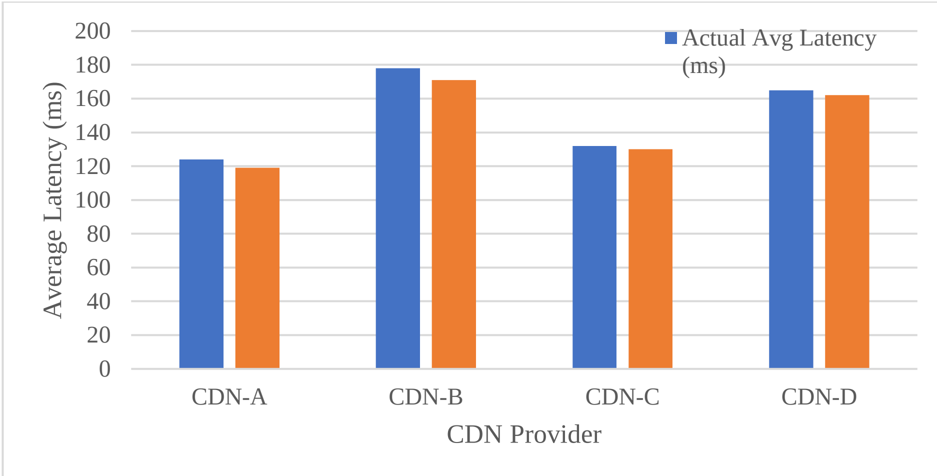

Figure 3: Latency prediction accuracy across CDN providers

As illustrated in Figure 3, the predicted and actual averages of latency across four major CDN Providers are compared graphically. The CDN latency estimation model also performed accurately in this scenario, given that the predicted affliction values were close to the actual values; hence the model obtained good accuracy on its estimations on encrypted sessions delays. Moreover, the model can generalize across different network conditions and CDN setups.

Table 1: Comparative evaluation of classification models for encrypted CDN traffic profiling

Metric	Proposed Model	Gradient Boosted Machine	Logistic Regression
Accuracy (%)	92.8	88.3	81.4
Precision (%)	91.2	87.5	79.8
Recall (%)	93.6	86.2	80.1
F1-Score (%)	92.4	86.8	79.9
Inference Time (ms/flow)	3.2	5.1	2.9

In Table 1, the performance comparison of the three machine learning models; Logistic Regression, Gradient Boosted Machine, and the newly proposed deep learning-based profiling model for classifying encrypted CDN traffic sessions is displayed. The table captures the CDL traffic session performance evaluation metrics of Accuracy, Precision, Recall, F1-Score, and Inference Time measured per flow. The proposed model achieves the best all round classification metrics performance, attaining 92.8% accuracy and 92.4% F1-score, by a substantial margin compared to baseline models. Additionally, the model's Inference Time of 3.2ms/flow is low which allows for real-time application in high throughput CDN environments. This substantiates the model's accuracy in profiling encrypted traffic and its ability in optimizing the computation workload.

5 Conclusion

This paper presents an innovative and holistic framework for profiling performance and privacy of encrypted traffic in CDNs. With the adoption of modern encryption technologies like TLS 1.3, network infrastructures dependent on monitoring for payload scrutiny face growing limitations. This system addresses the obstacle by utilizing session-level data including but not limited to, packet timing, inter-arrival intervals, and TLS handshake information to reconstruct performance estimation metrics. The comprehensive framework brings together feature extraction, classification, and model tuning for accurate profiling of CDN sessions. Experimental outcomes show that the system provides precise latency and throughput performance predictions for several CDN providers. The model built with deep learning techniques outperformed conventional classifiers in precision, recall, and F1 score while maintaining modest computational requirements which enables widespread, real-time deployment at scale.

The framework also enables encrypted session behavior detection anomalies, which allows for session-based encrypted traffic profiling and thus defining anomalies which assist network operators in early detection of performance degradation and congestion threats. The model also demonstrates solid performance with diverse network conditions, which complements the model's effectiveness for global CDN monitoring. Due to its non-intrusive architecture, the system maintains the critical needs of the encryption standards and data privacy law, therefore making it appropriate for enterprise and service-provider settings. In addition, this architecture may be expanded for adaptive CDN routing, edge cache management, and traffic encryption signal-dependent dynamic load balancing. Other research avenues might consider the application of federated or self-supervised research methods to increase the adaptability of the model while protecting user data privacy. To conclude, this work undertakes the foundational building blocks toward the design of intelligent, encryption-aware performance evaluators for next-generation content delivery systems.

References

[1] Abdullah, D. (2024). Strategies for low-power design in reconfigurable computing for IoT devices. *SCCTS Transactions on Reconfigurable Computing*, *1*(1), 21-25.

[2] Aceto, G., Ciuonzo, D., Montieri, A., & Pescapé, A. (2018, June). Mobile encrypted traffic classification using deep learning. In *2018 Network traffic measurement and analysis conference (TMA)* (pp. 1-8). IEEE. https://doi.org 10.23919/TMA.2018.8506558

[3] Aceto, G., Ciuonzo, D., Montieri, A., & Pescapé, A. (2019). Mobile encrypted traffic classification using deep learning: Experimental evaluation, lessons learned, and challenges. *IEEE transactions on network and service management*, *16*(2), 445-458. https://doi.org/10.1109/TNSM.2019.2899085

[4] Alwhbi, I. A., Zou, C. C., & Alharbi, R. N. (2024). Encrypted network traffic analysis and classification utilizing machine learning. *Sensors*, *24*(11), 3509. https://doi.org/10.3390/s24113509

[5] Anderson, B., & McGrew, D. (2016, October). Identifying encrypted malware traffic with contextual flow data. In *Proceedings of the 2016 ACM workshop on artificial intelligence and security* (pp. 35-46). https://doi.org/10.1145/2996758.2996768

[6] Araldo, A. G. (2016). *Design and Evaluation of Enhanced Network Caching Systems to Improve Content Delivery in the Internet* (Doctoral dissertation, Université Paris Saclay (COmUE)).

[7] Bai, B., Wang, L., Han, Z., Chen, W., & Svensson, T. (2016). Caching based socially-aware D2D communications in wireless content delivery networks: a hypergraph framework. *IEEE Wireless Communications*, *23*(4), 74-81. https://doi.org/10.1109/MWC.2016.7553029

[8] Barth, A., Boneh, D., & Waters, B. (2006, February). Privacy in encrypted content distribution using private broadcast encryption. In *International conference on financial cryptography and data security* (pp. 52-64). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/11889663_4

[9] Bartolini, N., Casalicchio, E., & Tucci, S. (2003, October). A walk through content delivery networks. In *International Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems* (pp. 1-25). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-24663-3_1

[10] Bhatiaa, A., Bahugunaa, A. A., Tiwaria, K., Haribabua, K., & Vishwakarmab, D. (2020). A survey on analyzing encrypted network traffic of mobile devices. https://doi.org/10.48550/arXiv.2006.12352

[11] Conti, M., Mancini, L. V., Spolaor, R., & Verde, N. V. (2015). Analyzing android encrypted network traffic to identify user actions. *IEEE Transactions on Information Forensics and Security*, *11*(1), 114-125. https://doi.org/10.1109/TIFS.2015.2478741

[12] Elmaghraby, R. T., Aziem, N. M. A., Sobh, M. A., & Bahaa-Eldin, A. M. (2024). Encrypted network traffic classification based on machine learning. *Ain Shams Engineering Journal*, *15*(2), 102361. https://doi.org/10.1016/j.asej.2023.102361

[13] Gajmal, Y. M., & Udayakumar, R. (2021). Blockchain-based access control and data sharing mechanism in cloud decentralized storage system. *Journal of web engineering*, *20*(5), 1359-1388. https://doi.org/10.13052/jwe1540-9589.2054

[14] Izima, O. C. (2023). Investigating the Effects of Network Dynamics on Quality of Delivery Prediction and Monitoring for Video Delivery Networks. *Technological University Dublin*. https://doi.org 10.21427/NMH6-S029

[15] Kavitha, M. (2024). Energy-efficient algorithms for machine learning on embedded systems. *Journal of Integrated VLSI, Embedded and Computing Technologies*, *1*(1), 16-20.

[16] Li, Y., Huang, Y., Seneviratne, S., Thilakarathna, K., Cheng, A., Jourjon, G., ... & Da Xu, R. Y. (2022). From traffic classes to content: A hierarchical approach for encrypted traffic classification. *Computer Networks*, *212*, 109017. https://doi.org/10.1016/j.comnet.2022.109017

[17] Mejail, M., & Nestares, B. (2025). Real-Time Heat Transfer Simulation Using a Surrogate Model Based on Generative Adversarial Networks (GANs). *International Academic Journal of Innovative Research*, *12*(3), 43-51. https://doi.org/10.71086/IAJIR/V12I3/IAJIR1224

[18] Orsolic, I., Pevec, D., Suznjevic, M., & Skorin-Kapov, L. (2017). A machine learning approach to classifying YouTube QoE based on encrypted network traffic. *Multimedia tools and applications*, *76*(21), 22267-22301. https://doi.org/10.1007/s11042-017-4728-4

[19] Pallis, G., & Vakali, A. (2006). Insight and perspectives for content delivery networks. *Communications of the ACM*, *49*(1), 101-106. https://doi.org/10.1145/1107458.1107462

[20] Papadogiannaki, E., & Ioannidis, S. (2021). A survey on encrypted network traffic analysis applications, techniques, and countermeasures. *ACM Computing Surveys (CSUR)*, *54*(6), 1-35. https://doi.org/10.1145/3457904

[21] Papanis, J. P., Papapanagiotou, S. I., Mousas, A. S., Lioudakis, G. V., Kaklamani, D. I., & Venieris, I. S. (2014). On the use of Attribute-Based Encryption for multimedia content protection over Information-Centric Networks. *Transactions on Emerging Telecommunications Technologies*, *25*(4), 422-435. https://doi.org/10.1002/ett.2722

[22] Patel, P. (2025). Deep unfolding networks for robust modulation classification in cognitive radio systems. *Electronics, Communications, and Computing Summit, 3*(2), 10–15.

[23] Pierre, G., & Van Steen, M. (2006). Globule: a collaborative content delivery network. *IEEE Communications Magazine*, *44*(8), 127-133. https://doi.org/10.1109/MCOM.2006.1678120

[24] Rahim, R. (2023). Effective 60 GHz signal propagation in complex indoor settings. *National Journal of RF Engineering and Wireless Communication*, *1*(1), 23-29.

[25] Rahim, R. (2024). Review of modern robotics: From industrial automation to service applications. *Innovative Reviews in Engineering and Science*, *1*(1), 34-37.

[26] Rezaei, S., & Liu, X. (2018). Deep learning for encrypted traffic classification: An overview. https://doi.org/10.48550/arXiv.1810.07906

[27] Sadulla, S. (2024). Optimization of data aggregation techniques in IoT-based wireless sensor networks. *Journal of Wireless Sensor Networks and IoT*, *1*(1), 31-36. https://doi.org/10.31838/WSNIOT/01.01.05

[28] Sappa, A. (2025). Adaptive machine learning models for effort estimation and risk detection in distributed software project pipelines. *Journal of Wireless Mobile Networks, Ubiquitous*

Computing, and Dependable Applications, 16(2), 54–74. https://doi.org/10.58346/JOWUA.2025.I2.004
[29] Shen, M., Zhang, J., Zhu, L., Xu, K., & Du, X. (2021). Accurate decentralized application identification via encrypted traffic analysis using graph neural networks. *IEEE Transactions on Information Forensics and Security*, *16*, 2367-2380. https://doi.org/10.1109/TIFS.2021.3050608
[30] Shoeb, M., & Gupta, V. K. (2012). A crypt analysis of the Tiny Encryption Algorithm in key generation. *International Journal of Communication and Computer Technologies*, 1(1), 15-20. https://doi.org/10.31838/IJCCTS/01.01.01
[31] Spanos, G. A., & Maples, T. B. (1995, January). Performance study of a selective encryption scheme for the security of networked, real-time video. In *Computer Communications and Networks, International Conference on* (pp. 2-10). IEEE Computer Society. https://doi.org/10.1109/ICCCN.1995.540095
[32] Taylor, V. F., Spolaor, R., Conti, M., & Martinovic, I. (2017). Robust smartphone app identification via encrypted network traffic analysis. *IEEE Transactions on Information Forensics and Security*, *13*(1), 63-78. https://doi.org/10.1109/TIFS.2017.2737970
[33] Wang, L., Park, K., Pang, R., Pai, V. S., & Peterson, L. L. (2004, June). Reliability and Security in the CoDeeN Content Distribution Network. In *USENIX Annual Technical Conference, General Track* (pp. 171-184).
[34] Zhou, Z., Yu, H., Xu, C., Zhang, Y., Mumtaz, S., & Rodriguez, J. (2018). Dependable content distribution in D2D-based cooperative vehicular networks: A big data-integrated coalition game approach. *IEEE Transactions on Intelligent Transportation Systems*, *19*(3), 953-964. https://doi.org/10.1109/TITS.2017.2771519
[35] Zou, Z., Ge, J., Zheng, H., Wu, Y., Han, C., & Yao, Z. (2018, June). Encrypted traffic classification with a convolutional long short-term memory neural network. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 329-334). IEEE. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00074

Authors Biography

R. Karthikeyan is a Professor in the Department of Computer Science and Engineering (AI & ML) at Vardhaman College of Engineering, Hyderabad, Telangana, India. He has extensive academic and research experience in areas such as artificial intelligence, machine learning, data science, and computer networks. Dr. Karthikeyan has authored and co-authored several research papers in reputed journals and conferences. His work focuses on integrating cutting-edge AI technologies into real-world applications, promoting innovation, and mentoring students toward academic and professional excellence in emerging computing domains.

Kanishka Jha is affiliated with the School of Engineering & Computing, Dev Bhoomi Uttarakhand University, Dehradun, India. Her academic and research interests include computer science, emerging technologies, and software development. She is dedicated to promoting innovation, research excellence, and practical learning in the field of engineering and technology, contributing to the advancement of knowledge and skill development among students and peers.

Rahul Thakur is affiliated with the Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. His academic and research interests lie in the areas of technology innovation, data-driven research, and interdisciplinary studies. He is actively involved in projects that emphasize research impact, societal development, and sustainable innovation. Rahul Thakur is committed to contributing to knowledge creation and fostering collaboration between academia and industry for meaningful research.

Dr. Alakananda Tripathy is an Associate Professor at the Centre for Artificial Intelligence and Machine Learning, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India. Her academic and research expertise encompasses artificial intelligence, machine learning, data science, and computational intelligence. With numerous publications in reputed international journals and conferences, Dr. Tripathy has made significant contributions to AI-driven research and applications. She is passionate about advancing intelligent systems, fostering interdisciplinary research collaborations, and mentoring students in cutting-edge technologies.

Dr. Julie Sunil is an Assistant Professor in the MBA Department at Presidency College, Bengaluru, Karnataka, India. She possesses extensive academic and research experience in the areas of management, marketing, human resource development, and business strategy. Dr. Julie has contributed to several research publications and academic initiatives aimed at enhancing the quality of management education. Her teaching philosophy emphasizes experiential learning, leadership development, and innovation in business practices. She is dedicated to nurturing future leaders through a balanced blend of theoretical insight and practical exposure in the field of management.

P.S. Raghavendra Rao is an Assistant Professor in the Department of Mechanical Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India. His academic and research interests include thermal engineering, fluid mechanics, renewable energy systems, and advanced manufacturing technologies. With a strong commitment to academic excellence and innovation, he has contributed to various research publications and engineering projects. P. S. Raghavendra Rao is dedicated to fostering practical learning, promoting sustainable engineering solutions, and guiding students toward research-driven professional growth.