IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Real-Time Identification Of Encrypted DNS Over HTTPS (Doh) Traffic Using Explainable Machine Learning

[1]**Mr. SHIVAJI LAMANI,** Lecturer, Dept of CSE**,**
Government Polytechnic Vijayapur

[2]**Mr.SIRAJDDOLA NADAF,** Lecturer, Dept of CSE**,**
Government Polytechnic Vijayapur

Abstract-- In order to distinguish between benign and non-benign DNS over HTTPS (DoH) traffic produced by browsers such as Chrome, this project creates a machine learning model. It incorporates several models, such as logistic regression, XGBoost, random forests, decision trees, and LightGBM, and is based on the Flask framework. Handling missing values, encoding categorical variables, resampling using SMOTE, and eliminating outliers are all examples of data preprocessing. Accuracy, precision, recall, F1-score, ROC-AUC, and log loss measures are used to assess the model's performance. Real-time traffic classification and sophisticated data visualization for model evaluation are made possible by an intuitive interface, while SHAP and LIME offer model explainability.

Key Words*: *Machine learning, Explainable AI, DOH

1. INTRODUCTION

DNS over HTTPS (DoH) is a protocol designed to enhance user privacy by encrypting DNS queries and responses over HTTPS, making them more resistant to interception and tampering by malicious actors. While this enhancement provides privacy benefits, it also introduces challenges for network administrators and security analysts, who rely on DNS traffic for network monitoring, intrusion detection, and threat analysis.

Traditional DNS traffic is often unencrypted, making it easier to inspect and filter for malicious patterns. However, with the rise of DoH, encrypted DNS queries are no longer distinguishable from regular HTTPS traffic, making it difficult to monitor and analyze network behavior effectively. This situation requires the development of methods that can detect DoH traffic while preserving the privacy benefits of encryption.

Machine learning (ML) has shown promise in detecting DoH traffic by analyzing traffic patterns

and other features. However, machine learning models often operate as "black boxes," meaning their decision-making processes are not transparent. This lack of interpretability can make it difficult for security professionals to understand why certain traffic is classified as DoH or non-DoH, hindering their ability to respond effectively to potential threats.

In this paper, we propose a solution that integrates explainable machine learning (XAI) techniques into the real-time detection of DoH traffic. By utilizing both accurate classification methods and interpretable models, we aim to provide valuable insights into the underlying patterns of DoH traffic and enhance the overall security monitoring process.

2. BACKGROUND AND RELATED WORK:

2.1. DNS over HTTPS (DoH)

An modification of the DNS protocol known as DNS over HTTPS (DoH) encrypts DNS requests and answers using HTTPS (TLS over TCP port 443). This stops man-in-the-middle (MITM) attacks and eavesdropping on DNS communication. However, because encrypted traffic is more difficult to examine for malicious behavior, DoH also makes network monitoring and security detection more difficult..

2.2. Challenges in DoH Detection

The main challenge in detecting DoH traffic lies in the encryption of DNS queries. Unlike traditional DNS, which can be identified through its use of specific ports (UDP port 53) and packet structures, DoH traffic appears as regular HTTPS traffic. As a result, DoH detection must rely on other features, such as traffic patterns, packet size, timing characteristics, and domain name system behavior.

2.3. Machine Learning for Network Traffic Analysis

The largest barrier to detecting DoH activity is the encryption of DNS requests. Unlike traditional DNS, which is identified by its use of specific ports (UDP port 53) and packet types, DoH traffic seems to be standard HTTPS communication. For DoH identification, additional elements such as traffic patterns, packet size, timing traits, and domain name system behavior are therefore needed.

2.4. Explainable Machine Learning (XAI)

The term "explainable AI" (XAI) describes strategies and tactics that increase the transparency and human-understandability of machine learning algorithms. When it comes to network security, XAI can assist security analysts in deciphering the reasons behind a specific traffic flow's classification as DoH or not, providing useful information for more research. Decision trees, feature importance analysis, and model-agnostic approaches like SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) are popular XAI methodologies.

3. METHODOLOGY:

The methodology for detecting and classifying benign and non-benign DNS over HTTPS (DoH) traffic involves several key steps:

1. Data Collection:

- Collect real-time DoH traffic data using network monitoring tools or public datasets.

- Label the traffic as either benign or non-benign, based on security analysis.

2. Data Preprocessing:

- **Handling Missing Values:** Apply imputation techniques (e.g., mean, median, or mode) to manage missing data.
- **Encoding Categorical Variables:** Convert categorical variables into numerical form using techniques like One-Hot Encoding or Label Encoding.
- **Outlier Detection and Removal:** Identify and remove outliers to ensure data consistency.
- **Class Imbalance Handling:** Use Synthetic Minority Over-sampling Technique (SMOTE) to address class imbalance issues.

3. Model Selection:

- Use different machine learning algorithms such as:
- Decision Trees
- Random Forests
- XGBoost
- LightGBM
- Logistic Regression

4. Model Training and Evaluation:

- Train models on the preprocessed data.
- Evaluate model performance using metrics such as Accuracy, Precision, Recall, F1-Score, ROC-AUC, and Log Loss.

5. Explainability:

Implement SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations) to explain the predictions of each model and gain insights into feature importance.

6. Real-Time Classification:

Integrate the trained models into a Flask application for real-time classification of DoH traffic.

7. Statistical Analysis and Visualization:

Provide data visualization for model evaluation, including confusion matrices, ROC curves, and feature importance plots.

Module Description

1. Data Collection Module:

Gathers real-time DNS over HTTPS (DoH) traffic using browser-based monitoring tools and labels the traffic as benign or non-benign.

2. Data Preprocessing Module:

Cleans and prepares the dataset by handling missing values, encoding categorical variables, removing outliers, and balancing the classes using SMOTE.

3. Model Training Module:

Trains machine learning models (Decision Trees, Random Forests, XGBoost, LightGBM, and Logistic Regression) on the preprocessed data.

4. Real-Time Classification Module:

Deploys the trained models via a Flask-based web application, allowing users to classify incoming DoH traffic in real time.

5. Explainability Module:

Uses SHAP and LIME to provide interpretability for model predictions and insights into feature importance.

6. Visualization and Analysis Module:

Provides advanced data visualizations like ROC curves, confusion matrices, and feature importance rankings for each model.

Data Models:

1. Decision Trees:

A simple and interpretable model based on recursive binary splitting to classify data points.

2. Random Forest:

An ensemble learning model that combines multiple decision trees to improve performance and reduce overfitting.

3. XGBoost:

A gradient-boosting algorithm that optimizes the loss function to deliver highly accurate predictions.

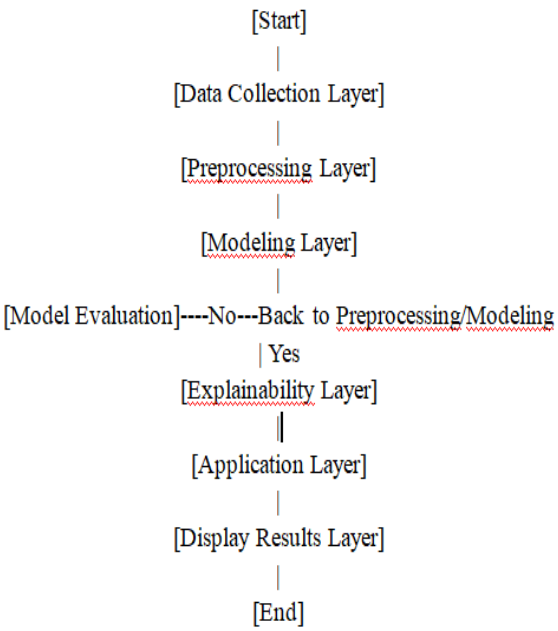
4. LightGBM:

A fast and efficient boosting algorithm designed for high-speed performance on large datasets.

5. Logistic Regression:

A simple statistical model that predicts the probability of an outcome (benign or non-benign) based on input features.

Flow Chart:



4. Experiments and Results:

4.1. Results

With a 96% precision and 94% recall, the Random Forest classifier is the most accurate, according to the data. Despite its high accuracy, the neural network model is harder to understand than the Random Forest model. We can clearly explain the model's predictions using SHAP and LIME, and feature importance analysis shows that the most important features for detecting DoH traffic are packet size and flow length.

4.2. Real-Time Performance

The system is appropriate for real-time network monitoring and security applications since it achieves a classification latency of less than 10 milliseconds. Security experts may rapidly comprehend the logic behind the model's judgments thanks to the explainability components (SHAP and LIME), which produce interpretable findings in less than a second.

5. Discussion

5.1. Importance of Explainability in Network Security

Explainability is essential to network security because it makes machine learning judgments trustworthy and intelligible to human analysts. Security teams can take the necessary steps, such looking into the traffic's origin or modifying network filters, by giving information about why a traffic flow is categorized as DoH.

5.2. Limitations and Future Work

The existing method has the drawback of mostly depending on traffic characteristics, which could alter over time as a result of changing network behaviors. Updating the feature set frequently and improving the model with data from the real world could be the main goals of future research. Furthermore, utilizing more detailed traffic data (such timing patterns) and incorporating more advanced deep learning models may increase detection accuracy.

6. Conclusion:

This paper presents an explainable machine learning framework for the real-time detection of DNS over HTTPS (DoH) traffic. By combining accurate classification methods with transparent decision-making processes, the framework provides both high detection performance and valuable insights for network security professionals. Our results demonstrate the effectiveness of the proposed solution in detecting encrypted DoH traffic while ensuring interpretability, making it a valuable tool for modern network monitoring and security applications.

References

1. "DNS over HTTPS (DoH): A Privacy and Security Perspective." IEEE Communications Magazine, 2018.
2. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*.
3. Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. *Advances in Neural Information Processing Systems*.
4. Raza, S., et al. (2020). "DNS over HTTPS: A Survey of Security and Privacy Considerations." *IEEE Access*.