Journal of Artificial Intelligence and Metaheuristic (JAIM)

♦ ISSN: 2833-5597 Vol: 07, No. 02, 2024 ♦ PP. 43–47

Article DOI: https://doi.org/10.54216/JAIM.070207



FULL LENGTH ARTICLE

Securing DNS over HTTPS: A Machine Learning Study on Traffic Classification Using DoHBrw-2020

Al-Seyday T. Qenawy[1,*] **Hussein Alkattan**[2] **Amany Khaled**[3]

[1] Intelligent Systems and Machine Learning Lab, Shenzhen 518000, China

[2] Department of System Programming, South Ural State University, 454080 Chelyabinsk, Russia

[3] Department of Clinical Pharmacy and Pharmacy Practice, Faculty of Pharmacy, Mansoura University, Mansoura, Egypt

Emails: S.Qenawy@asia.com · alkattan.hussein92@gmail.com · amany24khaled@gmail.com

Received: July 15, 2023 Revised: September 29, 2023 Accepted: March 10, 2024 ⋆ Corresponding author

ABSTRACT

This study investigates machine-learning approaches for classifying secure DNS traffic and identifying threats associated with DNS over HTTPS (DoH). Using the DoHBrw-2020 dataset, we compare Decision Tree, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Naive Bayes, a multilayer perceptron (MLP), Gradient Boosting, and SVM with an RBF kernel. Models are evaluated using accuracy, sensitivity, specificity, positive predictive value, negative predictive value, and F-score. The Decision Tree achieves the highest accuracy (99.65%) and strong results across the evaluation criteria. These findings demonstrate the potential of machine learning to improve DNS traffic security and support the development of real-time DoH threat detection. The results also inform the design of safer DNS solutions for contemporary information-security environments.

Keywords: DNS over HTTPS ▪ Machine Learning ▪ Traffic Classification ▪ DoHBrw-2020 ▪ Cybersecurity

1. INTRODUCTION

The internet has become a central communication medium, making the security and privacy of its communications increasingly important. Essential internet traffic includes Domain Name System (DNS) traffic, which translates human-readable domain names into IP addresses recognized by computers. DNS over HTTPS (DoH) improves privacy by encrypting DNS queries, making users' browsing activity harder to monitor. However, this integration also creates new challenges for traffic classification and security monitoring. An important task in analyzing DNS test traffic, particularly DoH and related protocols such as DNS over HTTPS carried over HTTP/3 by browsers, is distinguishing traffic classes in order to assess system security risks [1, 2, 3].

Traffic classification sorts data according to network-traffic characteristics. In DNS traffic analysis, classification algorithms can help distinguish regular traffic from traffic that may indicate security problems or malicious activity. Analysis of DoHBrw traffic is challenging because DNS traffic is encrypted with HTTPS and carried over HTTP/3 by browsers, introducing new challenges for traffic-analysis methods [3, 4, 5].

This paper examines classification approaches for DNS test traffic that incorporates DoHBrw. It compares machine-learning models using traffic characteristics such as packet sizes, timing patterns, and signatures typical of DoH and DoHBrw. The aims are to develop and assess classification models, distinguish DNS traffic types, detect potential threats in DNS queries, and evaluate the contribution of DoH to DNS security [6, 2, 7].

Accurate categorization of encrypted DNS traffic can help security programs identify anomalies such as DNS tunneling and denial-of-service attacks. Understanding DoHBrw traffic

© 2024 The Author(s). Published by ASPG. This article is licensed under CC BY 4.0.

characteristics can therefore inform the tools and protocols used to manage and secure DNS traffic. Information from classification models may also support traffic monitoring and DoH protocol implementations [4, 8, 9].

Classification of DNS test traffic involving DoHBrw is con-sequently relevant to the analysis and protection of contem-porary DNS communications. This study aims to improve understanding of DNS traffic characteristics and support ef-fective monitoring and protection, contributing to the devel-opment of DNS security in response to modern technologies and threats.

2. RELATED WORKS

DNS traffic classification, particularly for DNS over HTTPS (DoH) with browser-based rewriting (DoHBrw), is an ac-tive topic in network security and privacy. Classification approaches have been applied to analyze network traffic, se-cure DNS, and detect threats.

Decision trees and random forests are commonly used to classify DNS traffic patterns and detect anomalies. Decision trees partition traffic according to features such as packet size, timing, and destination IP address. Random forests combine multiple trees to model complex DNS traffic patterns [10, 3].

Support Vector Machines (SVMs) have been used in DoH-tunneling and encrypted-traffic classification, where they can operate in high-dimensional feature spaces and model nonlin-ear relationships [11, 3].

Neural networks and convolutional neural networks can ex-tract complex structures and relationships from raw traffic data, including encrypted DNS queries and traffic correla-tions. Deep-learning approaches have been applied to detect malicious DoH traffic and DNS tunnels [12, 3]. Machine-learning intrusion-detection methods have also been used to identify malicious DNS traffic [7].

Intrusion detection systems (IDSs) use classification algo-rithms to monitor network traffic for possible intrusions. Machine-learning-based IDSs can extend detection beyond fixed attack signatures by learning from traffic patterns [13, 7].

Feature selection and engineering can improve classification performance. Features such as query length, encryption flags, and timing information can make raw traffic data more useful to a classifier. Feature fusion and traffic-feature selection have also been studied for DoH and encrypted traffic [11, 14]. Research on encrypted DNS also emphasizes balancing traffic analysis with users' confidentiality and privacy [14].

Machine-learning and ensemble approaches have been ex-plored to improve the accuracy and reliability of DNS traffic analysis [7, 3]. Prior work also describes the use of classifica-tion techniques to identify security threats in DoH and other encrypted traffic [7].

3. DATASET DESCRIPTION

3.1 Overview of the DoHBrw-2020 Dataset

The DoHBrw-2020 dataset contains real network traffic collected to investigate and benchmark the DoH protocol. It was compiled by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick with assistance from the Canadian Internet Registration Authority (CIRA) [9].

DoHMeter, a tool designed for aggregated DoH traffic analysis, was used to create the dataset. It identifies and categorizes network traffic in real time, separating normal and abnormal activity over both traditional DNS and DoH. The dataset is intended to support the development and evaluation of techniques for monitoring attacks concealed by DoH traffic.

The dataset is divided into multiple CSV files containing network-flow records. These records include timestamps, source and destination IP addresses, protocol and packet-size information, indicators of DNS or DoH traffic, and labels for benign or malicious traffic. The flow records provide data for training and testing machine-learning algorithms for secure DNS traffic classification.

3.2 Data Preprocessing

Several preprocessing steps were used to prepare the DoHBrw-2020 dataset for model training:

- **Data cleaning:** Missing values and data gaps were checked. Incomplete or erroneous records were corrected or removed, and features that did not contribute to classification, such as constant-valued columns or identifiers, were excluded.
- **Normalization:** Features with different scales, such as packet sizes and time intervals, were normalized, commonly to the range 0–1, to prevent any single feature from dominating the model.
- **Feature selection:** Correlation analysis and feature-importance ranking were used to identify features associated with the traffic-classification label. This step reduced the feature set and the likelihood of overfitting.
- **Dataset splitting:** The preprocessed data were divided into training and test sets so that model performance could be evaluated on unseen data. Common splits include 80/20 and 70/30.

Figure 1 presents the dataset's feature-correlation matrix. The heatmap makes the direction and strength of pairwise linear relationships visible, helping to identify feature interactions relevant to modeling and feature engineering.

Figure 2 shows the ten most important features in the dataset. Feature-importance information can help guide feature selection and model development.

4. METHODOLOGY

4.1 Machine-Learning Models

This study uses the DoHBrw-2020 dataset and several machine-learning methods to classify DoH traffic and detect its presence in the analyzed data. The models were selected to cover different approaches to identifying malicious traffic in encrypted communications.

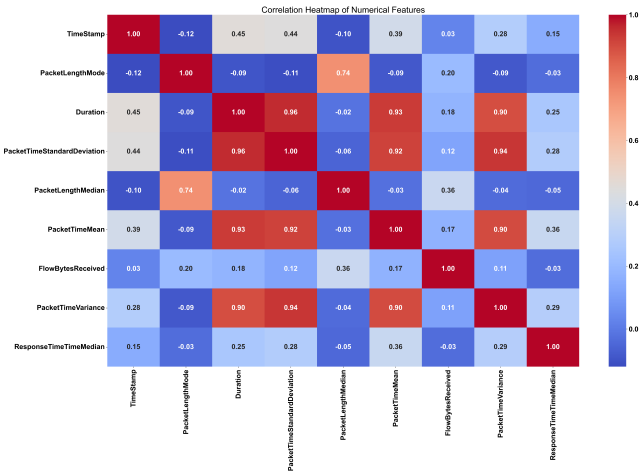


Figure 1. Correlation matrix heatmap for the dataset.

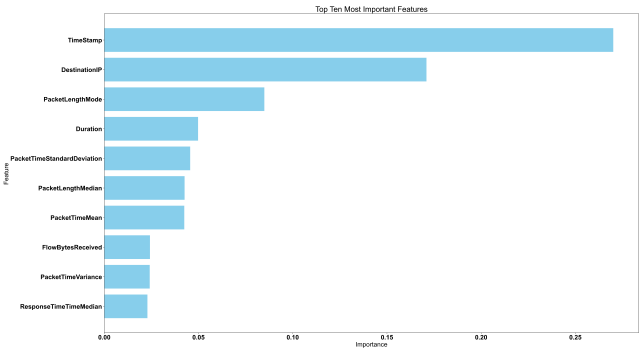


Figure 2. Ten most important features in the dataset.

- **Decision Tree:** A tree-based classifier that successively partitions the dataset according to feature values. It can handle numerical and categorical data and is relatively easy to interpret.
- **Support Vector Machine (SVM):** A classifier that seeks a separating hyperplane between classes. A linear SVM was used, which can be effective when classes are separable in the feature space and is suited to settings with many features and relatively few samples.
- **K-Nearest Neighbors (KNN):** A non-parametric classifier that assigns a class based on the majority class among the k nearest training samples. It can model nonlinear decision boundaries.
- **Naive Bayes:** A classifier based on Bayes' theorem that assumes feature independence. Despite this simplifying assumption, it can be efficient on large datasets with many features.
- **Neural Network (MLP):** A multilayer perceptron with input, hidden, and output layers that can learn complex, nonlinear relationships.
- **Gradient Boosting:** An ensemble method that trains weak models sequentially, with each model attempting to correct errors made by its predecessors.
- **SVM with RBF kernel:** An SVM variant that uses a radial basis function kernel to map data into a higher-dimensional space for classification.

These models were selected to provide diverse approaches to encrypted-traffic classification and to compare their effectiveness at detecting malicious traffic.

4.2 Evaluation Metrics

Model performance was evaluated using accuracy, sensitivity (true positive rate, TPR), specificity (true negative rate, TNR), positive predictive value (PPV), negative predictive value (NPV), and F-score. Here, TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}, \tag{1}$$

$$\text{Sensitivity} = \frac{TP}{TP+FN}, \tag{2}$$

$$\text{Specificity} = \frac{TN}{TN+FP}, \tag{3}$$

$$\text{PPV} = \frac{TP}{TP+FP}, \tag{4}$$

$$\text{NPV} = \frac{TN}{TN+FN}, \tag{5}$$

$$\text{F-score} = \frac{2\,\text{PPV}\,\text{Sensitivity}}{\text{PPV}+\text{Sensitivity}}. \tag{6}$$

Sensitivity measures the proportion of malicious-traffic instances correctly identified, while specificity measures the proportion of benign instances correctly identified. PPV and NPV describe the reliability of positive and negative predictions, respectively. The F-score is the harmonic mean of precision (PPV) and recall (sensitivity), making it useful when class imbalance is present. Together, these metrics compare model accuracy while accounting for threat detection and false alarms.

5. RESULTS

The models were evaluated on DoHBrw-2020 to compare their ability to detect malicious traffic in encrypted DNS flows. Table 1 summarizes their performance across the evaluation metrics.

The Decision Tree achieves the highest accuracy, sensitivity, specificity, and F-score in Table 1. Its tree structure can represent feature relationships useful for classifying encrypted DNS traffic. The high TPR values for Decision Tree and Gradient Boosting indicate that both identify malicious traffic effectively. The Decision Tree's specificity also corresponds to fewer benign instances being incorrectly flagged. The linear and RBF SVM models show competitive performance, though below that of the Decision Tree in this comparison.

Figure 3 presents the accuracy values plotted for the machine-learning models. The figure provides a visual comparison of the models' correct-prediction rates.

Figure 4 compares model sensitivity, or the ability to identify positive (malicious-traffic) cases. This measure is important when missing a threat has serious consequences.

Overall, the results indicate that Decision Tree and Gradient Boosting are among the most effective models for classifying secure DNS traffic in the DoH setting. These findings can inform further research and the development of frameworks for detecting improper DNS activity.

Table 1. Performance of machine-learning models based on evaluation metrics.

Model	Accuracy	Sensitivity (TPR)	Specificity (TNR)	PPV	NPV	F-score
Decision Tree	0.9965	0.99598	0.99702	0.99698	0.99603	0.99648
Support Vector Machine	0.995	0.99497	0.99503	0.99497	0.99503	0.99497
K-Nearest Neighbors	0.9925	0.99396	0.99105	0.99097	0.99402	0.99247
Naive Bayes	0.9815	0.98994	0.97316	0.97329	0.98989	0.98155
Neural Network (MLP)	0.9815	0.98994	0.97316	0.97329	0.98989	0.98155
Gradient Boosting	0.971	0.99195	0.95030	0.95174	0.99170	0.97143
SVM (RBF kernel)	0.947	0.94165	0.95229	0.95122	0.94291	0.94641

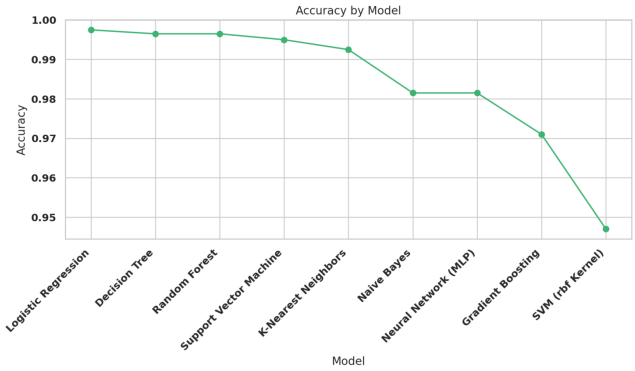


Figure 3. Accuracy by machine-learning model.

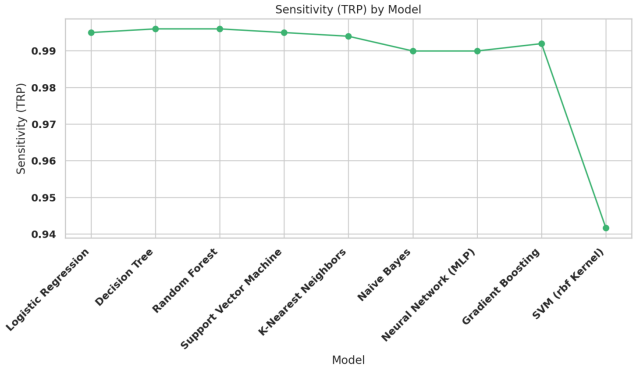


Figure 4. Sensitivity (TPR) by machine-learning model.

6. CONCLUSION

This study compared machine-learning models for analyzing DoH traffic and distinguishing legitimate from malicious activity using the DoHBrw-2020 dataset. The evaluated models were Decision Tree, linear SVM, SVM with an RBF kernel, KNN, Naive Bayes, MLP, and Gradient Boosting. The Decision Tree achieved the highest accuracy (99.65%) and strong sensitivity, specificity, and F-score, supporting its use in secure DNS traffic classification. Gradient Boosting also performed well in sensitivity and may be useful when detecting positive cases is the primary concern.

The findings demonstrate the potential of machine learning to improve the detection of threats concealed within encrypted traffic. Because cyber threats and network traffic continue to evolve, further work is needed to develop these models and improve comprehensive, dependable DNS traffic analysis as part of modern security strategies.

REFERENCES

[1] M. Lyu, H. H. Gharakheili, and V. Sivaraman, "A survey on DNS encryption: Current development, malware misuse, and inference techniques," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1–28, 2022.

[2] K. Jeřábek, K. Hynek, T. Čejka, and O. Ryšavý, "Collection of datasets with DNS over HTTPS traffic," *Data in Brief*, vol. 42, p. 108310, 2022.

[3] T. A. Nguyen and M. Park, "DoH tunneling detection system for enterprise network using deep learning technique," *Applied Sciences*, vol. 12, no. 5, p. 2416, 2022.

[4] M. Zhan, Y. Li, G. Yu, B. Li, and W. Wang, "Detecting DNS over HTTPS based data exfiltration," *Computer Networks*, vol. 209, p. 108919, 2022.

[5] S. Ding, D. Zhang, J. Ge, X. Yuan, and X. Du, "Encrypt dns traffic: Automated feature learning method for detecting dns tunnels," in *2021 IEEE International Conference on Parallel and Distributed Processing with Applications, Big Data and Cloud Computing, Sustainable Computing and Communications, Social Computing and Networking*, pp. 352–359, 2021.

[6] K. Hynek, D. Vekshin, J. Luxemburk, T. Cejka, and A. Wasicek, "Summary of dns over https abuse," *IEEE Access*, vol. 10, pp. 54668–54680, 2022.

[7] T. Zebin, S. Rezvy, and Y. Luo, "An explainable AI-based intrusion detection system for dns over https (DoH) attacks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2339–2349, 2022.

[8] R. Mitsuhashi, A. Satoh, Y. Jin, K. Iida, T. Shinagawa, and Y. Takai, "Identifying malicious dns tunnel tools from doh traffic using hierarchical machine learning classification," in *Information Security* (J. K. Liu, S. Katsikas, W. Meng, W. Susilo, and R. Intan, eds.), pp. 238–256, Springer International Publishing, 2021.

[9] M. MontazeriShatoori, L. Davidson, G. Kaur, and A. H. Lashkari, "Detection of doh tunnels using time-series classification of encrypted traffic," in *2020 IEEE International Conference on Dependable, Autonomic and Secure Computing; International Conference on Pervasive Intelligence and Computing; International Conference on Cloud and Big Data Computing; International Conference on Cyber Science and Technology Congress*, pp. 63–70, 2020.

[10] X. Li, Y. Song, and Y. Li, "DNS tunnel detection scheme based on machine learning in campus network," in *2022 4th International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI)*, pp. 253–257, 2022.

[11] S. Roy, T. Shapira, and Y. Shavitt, "Fast and lean encrypted internet traffic classification," *Computer Communications*, vol. 186, pp. 166–173, 2022.

[12] G. D'Angelo, A. Castiglione, and F. Palmieri, "DNS tunnels detection via DNS-images," *Information Processing & Management*, vol. 59, no. 3, p. 102930, 2022.

[13] S. K. Singh and P. K. Roy, "Detecting malicious dns over https traffic using machine learning," in *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, pp. 1–6, 2020.

[14] Y. Wang, C. Shen, D. Hou, X. Xiong, and Y. Li, "FF-MR: A doh-encrypted dns covert channel detection method based on feature fusion," *Applied Sciences*, vol. 12, no. 24, p. 12644, 2022.