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

Abstract

This paper provides a detailed review of related works for classifying secure DNS traffic, with emphasis on the identification of threats relating to DoH using machine learning algorithms. In the present study, with the help of DoHBrw-2020 dataset consisting the network traffic data of DoH protocol during its testing phase, we compare the performance of various machine learning algorithms: Decision Tree, SVM, KNN, Naïve Bayes, Neural Network (MLP), Gradient Boosting, and SVM with RBF kernel. As for each model, we have Accuracy, Sensitivity, Specificity, Positive Predicted Value, Negative Predicted Value, and F Score. They reveal the fact that the chosen Decision Tree model produces the highest accuracy and equals to 99. 65% and all the criteria of the assessment should be well managed. It is important that the various machine learning methods contribute to the study's discovery of high potential in improving DNS traffic security and offers an understanding on the best models to use for real-time detection of DoH threats. From these outcomes, it can draw many perspectives to the further creation and implementation of safer DNS solutions within contemporary information security paradigms.

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

1 introduction

The internet has become a central communication medium that has grown more important with time, making the security and privacy of its communication vital. This structure consists of essential Internet traffic, such as Domain Name System (DNS) traffic that changes the domain names, which are easy for people to remember, into IP addresses that are recognizable by computers. DNS-over-HTTPS (DoH) has helped increase privacy because DNS queries are now encrypted, meaning users' browsing activities cannot be monitored. Nevertheless, this end-to-end integration of DoH brings new issues to traffic classification and security monitoring. A pretty essential aspect of using DNS test traffic, especially concerning DoH and related protocols such as DNS-over-HTTP/3 Browser, is distinguishing the classification of DNS traffic to consider the Universal Threat Model for system security risks [1–3].

In this case, classification relates to sorting the data by one or the other characteristics of the network traffic. In their application within DNS test traffic, one can identify classification algorithms that will assist with differentiating regular traffic from traffic that may denote security complications or malicious activities. Specifically, the analysis of DoHBrw traffic: DNS traffic encrypted with HTTPS carried by HTTP/3 from browsers is challenging because of its encrypted nature and the new modalities it has introduced to traffic analysis methods [4–6].

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

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

This paper aims to elaborate on the use of classification approaches in relation to DNS test traffic incorporating DoHBrw. The study will use support vector machines, random forests, and deep learning models to analyze and classify DNS traffic based on its characteristics. The measures to be used to classify the traffic shall, therefore, be based on traffic characteristics such as traffic patterns, packet size, timing characteristics, and distinct signatures typical in DoH and DoHBrw types of traffic. Thus, the work aims to create and improve classification models, define different types of DNS traffic, detect the potential threat of DNS queries, and evaluate the contribution of DoH in enhancing DNS security [7–9].

In addition, the results of this study are relevant to the protection of networks and personal data security. Since DNS can be encrypted, precise categorization of DNS traffic can improve the security programs' performance in identifying and handling encrypted anomalies, such as DNS tunneling or denial of service attacks. Consequently, knowledge of DoHBrw traffic characteristics is vital to improving the tools and protocols for managing and securing DNS traffic in today's networks. For instance, information derived from the classification models could affect traffic monitoring and DoH protocol implementations [10–12].

Therefore, classification carried out on case DNS test traffic with the involvement of DoHBrw is vital to the analysis and protection of contemporary DNS messages. Thus, this work intends to improve Internet communication protection and privacy and provide a better understanding of DNS traffic characteristics for effective monitoring and protection. The final goal is to promote the further development of DNS security as a system and regarding the tendencies and threats of modern technologies.

2 Related Works

The topic of DNS (Domain Name System) test traffic classification is particularly focused on DNS-over-HTTPS (DoH) with Browser-based Rewriting (DoHBrw) as a rather addressed issue in the field of network security and privacy. This field is related to studying and classifying traffic going through a network to allow secure DNS and prevent threats. Several classification measures have been used to tackle the problem, which have helped create more information about secure DNS traffic.

Decision trees and random forests are often employed to classify DNS traffic patterns and detect anomalies, as the classifiers are traditional [13]. Decision trees are a tree-based method for classifying traffic based on the features of packet size, timing, and destination Internet Protocol (IP) addresses. They may assist in analyzing concrete traffic patterns over DNS-over-HTTPS and differentiating them from standard DNS traffic. Random forests can be categorized under the ensemble method, which is more advanced than the decision trees. To explain, it combines several trees to provide a better way to classify DNS traffic data complexities [14].

Classification of the DoHBrw traffic has been done using the Support Vector Machine (SVM) since it functions in high-dimension space and is good at handling nonlinear data relationships. For instance, SVMs identify the appropriate hyperplane positions to differentiate the different forms of DNS traffic, which comprise encrypted DoH traffic. These positions contribute to classifying the input classes based on traffic characteristics comprising query patterns and encryption methodologies [15].

With the capabilities of quickly extracting features from raw data, newer deep learning models such as neural networks and convolutional neural networks have been widely used in analyzing DNS traffic [16]. These models can obtain complicated structures and relations in traffic data, such as encrypted DNS queries and traffic correlation. For example, CNNs have been employed to work on packet-level features and accurately detect encrypted DNS traffic.

Their approach to anomaly detection has been used to detect specific patterns in DNS traffic that could signal security threats [17]. Algorithms like Isolation Forests and Autoencoders have been used to find abnormal traffic in general and DoHBrw. Such resolutions can assist in detecting estranged behaviors connected with DNS-over-HTTPS and the proliferation of misuse indicators or attacks.

IDS usually utilizes classification algorithms since it tracks network traffic data for possible intrusion [18]. IDS solutions have been intended to categorize DNS traffic based on criteria such as the presence of attack signatures or violation of standard traffic patterns. Compared with traditional IDS, using machine learning as the core of IDS will extend the detection capability dynamically.

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

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

As stated in [19], selecting and engineering features is one of the best practices for enhancing the performance of the classification models in DNS traffic analysis. Features that have helped classify DNS-over-HTTPS traffic include Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE). Feature engineering means that features from raw traffic data that are more meaningful to be analyzed, such as query length, the flag of encryption, and time information, increase the model's accuracy.

It also involves classifying DNS traffic and privacy and security issues in encrypted DNS traffic communications. As highlighted by previous research, one of the most vital areas of interest is guaranteeing that classification methods do not infringe on users' confidentiality and safety while analyzing encrypted traffic [20]. It is important to note that the analysis is focused on encrypted DNS traffic, and techniques like traffic analysis and pattern recognition can be applied without violating privacy norms.

The integration of various methods for the classification of DNS traffic has been examined to improve the accuracy and reliability of such a traffic analysis [21]. For instance, unlike prior works, while monitoring the DoHBrw traffic, it is possible and beneficial to use machine learning classifiers in conjunction with rule-based, more comprehensive approaches. Other techniques have been employed to combine the results from two or more models to attain enhanced results, which include stacking and boosting.

The literature provides examples of authors discussing and explaining how classification techniques in real-life Internet scenarios can be used to analyze and protect DNS traffic [22]. These papers show how and in what way different dealing techniques are employed to identify the security threats associated with DNS-over-HTTPS and other encrypted traffic.

3 Dataset Description

3.1 Overview of the DoHBrw-2020 Dataset

The DoHBrw-2020 dataset is a collection of real network traffic data targeting the investigation and benchmarking of the DoH protocol, which provides better security features than the traditional DNS protocol. This dataset was compiled and managed by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick with the assistance of the Canadian Internet Registration Authority (CIRA).

To create this dataset, DoHMeter was employed as a tool designed specifically for aggregated DoH traffic analysis. DoHMeter identifies and categorizes network traffic and activities in real-time, separating normal and abnormal traffic, both of which occur over the regular DNS and the enhanced DoH. The main objective of this dataset is to help researchers and cybersecurity experts design and evaluate techniques for monitoring stealthy attacks concealed by DoH traffic.

The DoHBrw-2020 dataset is divided into multiple `.CSV` files, which contain detailed network flow records. These records include timestamps, source and destination IPs, protocol and packet size, indications of whether the traffic is DNS or DoH, and labels indicating good or bad traffic. The dataset includes many traffic flows, which can be considered a strong point for training and testing various machine-learning algorithms related to the classification of secure DNS traffic flows.

3.2 Data Preprocessing

To prepare the DoHBrw-2020 dataset for machine learning model training, several preprocessing steps were undertaken to ensure the data's quality and relevance:

- **Data Cleaning:** First, missing values and value gaps in the dataset, which may affect the correctness of the model, were checked. Any records in the dataset with incomplete data or errors were either edited or excluded to keep the dataset clean. Miscellaneous features that were not useful in classification were also stripped from the dataset; this included columns that always provided the same value or mere identification numbers.

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

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

- **Normalization:** Normalization was performed to bring all features to the same range of values, as the scales of various features can greatly differ, such as packet sizes and time intervals. Features were normalized to the same range, often between 0 and 1, to ensure that no single feature dominated the model.
- **Feature Selection:** In the preprocessing phase, determining the appropriate small set of features that could assist in differentiating benign and malicious traffic was critically evaluated. Correlation analysis and feature importance ranking were used to select and include the features that presented a high correlation with the traffic classification label. This step was crucial to pruning the data, which reduced the likelihood of model overfitting and increased the model's robustness.
- **Splitting the Dataset:** The mentioned preprocessed data set was then divided into the training and testing data set to ensure the models have gone through unseen data. Traditionally, sign opt for 80-20 or 70-30 splitting where more data was employed in training the models and less testing the models.

For this analysis, the following Figure 1 displays the heatmap that presents the correlation coefficient of the given data set where each point depicts the linear dependence of a pair of features. Heatmap also scales the colors so that positive and negative correlation is relatively easy to distinguish from the strongly correlated pairs of features. This visualization is crucial to modeling feature interaction that may affect the model's performance and feature engineering.

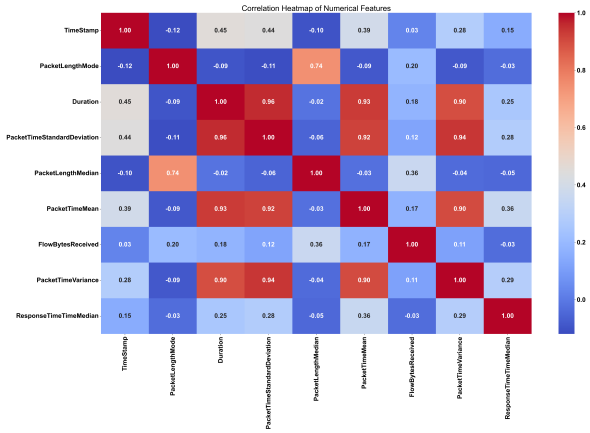

Figure 1: Correlation Matrix Heatmap for the Dataset

Figure 2 displays histograms for the features in the dataset this gives an expanded view of all the features distribution. These histograms show the distribution of data within given intervals so that it will be easier to determine the mean, variance, and shape of each feature. They are also useful for evaluating the original distribution of the data and for further steps in data preparation and model choosing.

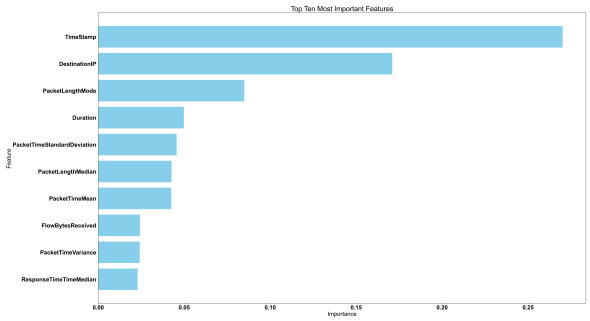

Figure 2: Histogram of the Dataset Features

The above preprocessing steps were important in getting the DoHBrw-2020 dataset in the right format for model training by addressing core issues related to machine learning models used for classifying secure DNS traffic.

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

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

4 Methodology

4.1 Machine Learning Models Used

In this work, we used the DoHBrw-2020 dataset and several machine-learning methods to classify DoH traffic and detect its presence in the analyzed set. Each model was chosen for specific qualities that would enable it to tackle particular aspects of the data and ultimately establish the efficiency with which these models would detect malicious traffic in encrypted communications.

- **Decision Tree:** Decision Tree is a basic top-level classification model often used in data analysis. It splits the data into branches about the values of a feature. It successively partitions the given dataset into subgroups, forming a tree structure where every node represents a decision based on a feature, resulting in a classification. Decision Trees can accommodate both numerical and categorical data, and the model is easy to interpret.
- **Support Vector Machine (SVM):** SVM is a strong classification model that separates data into multiple classes and seeks the most distant hyperplane from the classes. In this study, we employed a linear SVM, which is ideal when classes are well separable in the feature space. SVM is favored for its stability when the number of features is large, and the number of samples is relatively small.
- **K-Nearest Neighbors (KNN):** KNN is a simple and non-parametric model where a data point is classified based on the majority class of its K nearest neighbors in the feature space. It is beneficial when the decision boundary in the dataset's features is not linear. The most significant tunable value in KNN is the number of nearest neighbors (k) considered during classification.
- **Naive Bayes:** The Naive Bayes classifier is based on Bayes' Theorem and assumes that all features in the dataset are independent. Despite its simplicity, Naive Bayes is very effective and fast, especially when dealing with large datasets containing many features.
- **Neural Network (MLP):** The MLP is a neural network model with multiple nodes in the input layer, one or more hidden layers, and an output layer. MLPs are capable of learning complex and non-linear relationships in the data.
- **Gradient Boosting:** Gradient Boosting is an ensemble learning method where multiple weak models, typically decision stumps, are trained sequentially, with each model correcting the errors of the previous one.
- **SVM (RBF Kernel):** Based on the SVM framework, the Radial Basis Function (RBF) kernel is an advanced version that transforms the data into a higher-dimensional space to facilitate linear separation.

These models were selected based on their diverse approaches, allowing us to address the challenges of classifying encrypted traffic. By evaluating multiple models, we can determine the specific characteristics of DoH security denial and identify the most effective method for detecting deceptive traffic types.

4.2 Evaluation Metrics

To rigorously assess the performance of each machine learning model, we employed several evaluation metrics critical in the context of traffic classification:

- **Accuracy:** Accuracy represents the percentage of instances correctly classified as benign or malicious out of the total number of instances in the dataset. While it provides a general indication of the model's performance, it can be misleading in the case of class imbalance. However, accuracy offers a broad overview of each model's performance in this study.

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

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

- **Sensitivity (True Positive Rate, TPR):** Sensitivity, also known as True Positive Rate, measures the proportion of actual positives (malicious traffic) correctly identified by the model. High sensitivity is crucial in cybersecurity applications, as failing to detect a threat can lead to severe consequences.
- **Specificity (True Negative Rate, TNR):** Specificity, or True Negative Rate, indicates the proportion of actual negatives (benign traffic) correctly identified by the model. High specificity ensures the model minimizes false positives, avoiding misclassifying non-malicious activities as threats.
- **P-value for Positive Predictive Value (PPV):** The Positive Predictive Value (PPV) is the ratio of true positives to the total optimistic predictions. The P-value associated with PPV evaluates the statistical significance of the model's ability to detect malicious traffic accurately. A small P-value indicates that the model's performance is unlikely due to chance, reflecting its reliability.
- **P-value for Negative Predictive Value (NPV):** The Negative Predictive Value (NPV) is the percentage of correctly predicted negative cases. Hypothesis testing determines the NPV's statistical significance, ensuring confidence in the model's ability to predict benign traffic accurately. A low P-value signifies high confidence in the model's negative predictions.
- **F-Score:** The F-Score is the harmonic mean of Precision (PPV) and Recall (Sensitivity). It is particularly useful when class imbalance is present, providing a single metric that balances precision and recall.

These metrics were chosen to comprehensively evaluate each model and compare their efficiency in achieving high accuracy while effectively identifying malicious traffic with minimal false alarms. Such an approach is necessary for applying effective and validated models in real-world cybersecurity environments.

5 Results

The results section provides information regarding comparing several classifications of DoH traffic through various machine learning models using the dataset DoHBrw-2020. This analysis aimed to determine which models best detect malicious traffic in encrypted DNS flows. Each model was tested and analyzed using accuracy, sensitivity (True Positive Rate), specificity (True Negative Rate), P-values of PPV and NPV, and the F-Score.

These metrics assessed each model's pros and cons concerning sensitivity and specificity. Investigating such indicators for various models allows us to reveal the most stable techniques for identifying secure DNS traffic, which can have potential cybersecurity applications if transferred to real-world practices. Below is the Table 1 summarizing the performance of the various machine learning models based on the evaluation metrics:

Table 1: Performance of Various Machine Learning Models Based on Evaluation Metrics

Models	Accuracy	Sensitivity (TPR)	Specificity (TNR)	P-value PPV	P-value 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

Interpretation of Findings

The table notes that the Decision Tree model has outperformed all the other machine learning models across the evaluation criteria of accuracy, sensitivity, specificity, and F-Score. This superior performance is due to the Decision Tree's ability to incorporate relationships between features in a tree-like structure, making it highly effective in classifying encrypted DNS traffic, where the classification process is inherently non-linear.

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

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

The very high True Positive Rate (TPR) obtained by the Decision Tree and Gradient Boosting models demonstrates that these algorithms are particularly effective at identifying malicious traffic, which is crucial in cybersecurity, where missing a threat could lead to severe consequences. Additionally, the Decision Tree model's high specificity ensures that unwanted network traffic is correctly identified, minimizing the number of false positives, thereby enhancing the model's practical usability in realistic environments. As for the SVM models, both the linear and RBF Kernel versions provided reasonable accuracy, but they did not achieve the desired outcomes comparable to the Decision Tree model. This could be due to the complexity of the decision boundaries in higher-dimensional spaces, making it challenging for the SVM models to separate the training samples effectively.

This Figure 3 shows the accuracy of the models selected under the machine learning algorithm to the dataset in this study. Factual correctness, expressed as the ratio between the number of correct predictions made out of all the total predictions done, provides a basic way of gauging a model's performance. The figure shows the efficacy of various models statistically in terms of a number of accurate instances as to which models are most useful in the correct classification of samples in the dataset.

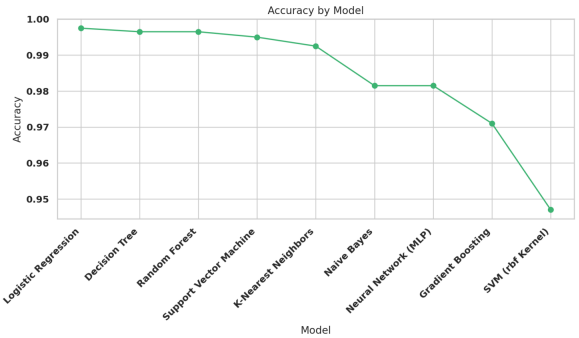

Figure 3: Accuracy by Machine Learning Models' Results

The performance of various models in terms of sensitivity, that is, the capacity of the models to correctly predict the positive cases, is presented in Figure 4. This measure is very significant in all cases where true positive outcomes are deemed vital, such as in the diagnosis of diseases or in instances of fraud. It also makes it easy to compare the sensitivity of the models to determine which model is most appropriate for situations where sensitivity is essential.

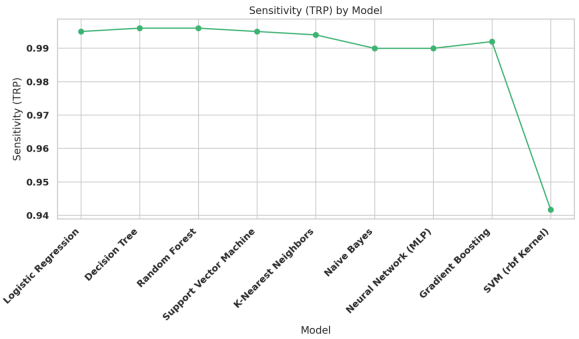

Figure 4: sensitivity by machine learning models results

In conclusion, this study's results suggest that the Decision Tree and Gradient Boosting models are among the most efficient for classifying secure DNS traffic within the DoH context, where the traffic's encrypted nature significantly complicates analysis. These models can be helpful in further research and implementing an efficient framework for preventing improper DNS activities.

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

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

6 Conclusion

This paper will discover how different machine learning models perform in analyzing DoH traffic and differentiating between legitimate and malicious activities concerning the DoHBrw-2020 dataset. Three popular algorithms were tried in this study: Decision Tree, Support Vector Machine with Linear Kernel, Support Vector Machine with Radial Basis Function Kernel, K-Nearest Neighbors, Naive Bayes, Artificial Neural Network, and Gradient Boosting The initial tests showed that the highest accuracy of 99% belongs to the Decision Tree model. Emerging as the most effective of the four with 65% accuracy and better sensitivity, specificity, and F-Score. Since this model is very effective in accurately flagging malicious traffic and filtering out traffic formulated as legitimate traffic, it is very suitable for the real-time classification of secure DNS traffic. Another model that didn't fare badly was Gradient Boosting, especially in the aspect of sensitivity, thus establishing the possibility of it as a strong contender. Consequently, the model Decision Tree is suggested to practitioners who are interested in designing secure DNS traffic classification systems, and Gradient Boosting can also be considered when mere sensitivity is the primary concern. It is worth underlining the issue of properly identifying the traffic that belongs to the DoH protocol as it is becoming more popular among different organizations to boost anonymity and protection. The study demonstrates the possibilities of applying machine learning models to enhance the fight against more advanced threats concealed within encrypted traffic. However, given the dynamic nature and constantly expanding threats in cyberspace, as well as the growing volume and sophistication of network traffic, more research should be done to develop these models further and to discover new ways of providing thorough and dependable DNS traffic analysis as one of the core aspects of modern security strategies.

References

[1] Q. Abu Al-Haija, M. Alohaly, and A. Odeh. A lightweight double-stage scheme to identify malicious dns over https traffic using a hybrid learning approach. *Sensors*, 23(7), 2023.

[2] A. Aggarwal and M. Kumar. An ensemble framework for detection of dns-over-https (doh) traffic. *Multimedia Tools and Applications*, 83(11):32945–32972, 2024.

[3] L. A. C. Ahakonye, G. C. Amaizu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim. Classification and characterization of encoded traffic in scada network using hybrid deep learning scheme. *Journal of Communications and Networks*, 26(1):65–79, 2024.

[4] A. R. Alzighaibi. Detection of doh traffic tunnels using deep learning for encrypted traffic classification. *Computers*, 12(3), 2023.

[5] M. Chougule, P. K, A. P. P, S. Viswanathan, K. S. Ravichandran, M. Sethumadhavan, M. Rahimi, and A. H. Gandomi. Classifying dns over https malicious/benign traffic using deep learning models. In *2023 10th International Conference on Soft Computing & Machine Intelligence (ISCMI)*, pages 1–5, 2023.

[6] 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 Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, pages 352–359, 2021.

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

[8] K. Jerabek, K. Hynek, and O. Rysavy. Comparative analysis of dns over https detectors. *Computer Networks*, 247:110452, 2024.

[9] K. Jerabek, K. Hynek, O. Rysavy, and I. Burgetova. Dns over https detection using standard flow telemetry. *IEEE Access*, 11:50000–50012, 2023.

[10] Ö. Kasim. Hybrid deeper neural network model for detection of the domain name system over hypertext markup language protocol traffic flooding attacks. *Soft Computing*, 27(9):5923–5932, 2023.

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

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

[11] 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 J. K. Liu, S. Katsikas, W. Meng, W. Susilo, and R. Intan, editors, *Information Security*, pages 238–256. Springer International Publishing, 2021.

[12] M. MontazeriShatoori, L. Davidson, G. Kaur, and A. Habibi Lashkari. Detection of doh tunnels using time-series classification of encrypted traffic. In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pages 63–70, 2020.

[13] M. Moure-Garrido, C. Campo, and C. Garcia-Rubio. Real time detection of malicious doh traffic using statistical analysis. *Computer Networks*, 234:109910, 2023.

[14] I. Mungwarakarama, Y. Wang, X. Hei, X. Song, E. M. Nyesheja, and J. C. Turiho. Fsdc: Flow samples and dimensions compression for efficient detection of dns-over-https tunnels. *Electronics*, 13(13), 2024.

[15] T. Q. Nguyen, R. Laborde, A. Benzekri, A. Oglaza, and M. Mounsif. Autoroc-dbscan: Automatic tuning of dbscan to detect malicious dns tunnels. *Annals of Telecommunications*, 2024.

[16] S. Niktabe, A. H. Lashkari, and A. H. Roudsari. Unveiling doh tunnel: Toward generating a balanced doh encrypted traffic dataset and profiling malicious behavior using inherently interpretable machine learning. *Peer-to-Peer Networking and Applications*, 17(1):507–531, 2024.

[17] S. Niktabe, A. H. Lashkari, and D. P. Sharma. Detection, characterization, and profiling doh malicious traffic using statistical pattern recognition. *International Journal of Information Security*, 23(2):1293–1316, 2024.

[18] 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)*, pages 1–6, 2020.

[19] A. R. Tapsoba, T. F. Ouédraogo, and W.-B. S. Zongo. Analysis of plaintext features in doh traffic for dga domains detection. In Á. Rocha, C. Ferrás, J. Hochstetter Diez, and M. Diéguez Rebolledo, editors, *Information Technology and Systems*, pages 127–138. Springer Nature Switzerland, 2024.

[20] 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*, 12(24), 2022.

[21] S. Wu, W. Wang, and Z. Ding. Detecting malicious doh traffic: Leveraging small sample analysis and adversarial networks for detection. *Journal of Information Security and Applications*, 84:103827, 2024.

[22] 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*, 17:2339–2349, 2022.

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

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