ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

Improving Tor Hidden Service Classification with a Hybrid LSTM and BiGRU Deep Learning Model

1.J.Lakshmi,2.Potti.Tanuja,3.Somu. karthik,4.kavuri.jayasree,5.oguri.shesha manindra

6.haridasula. venkatesh

#1- Associate professor, department of CSE, Tirumala institute of technology and sciences,AP

#2#3#4#5#6 department of CSE, Tirumala institute of technology and sciences,AP

Abstract: The Tor network provides strong anonymity through onion routing, but its hidden services are often exploited for illegal activities, posing significant challenges to network security and monitoring. Traditional website fingerprinting methods rely mainly on packet-level features, which fail to capture semantic and contextual information, resulting in limited accuracy. To address this issue, this paper proposes a novel fingerprinting framework that integrates BERT for extracting rich semantic features from Tor webpage content and LSTM for modeling temporal patterns across multiple pages. Furthermore, an enhanced architecture incorporating a BiGRU layer is introduced to enable bidirectional feature learning and improve classification robustness. The proposed system effectively analyzes both textual and sequential characteristics of Tor services, leading to more accurate identification of normal and malicious activities. Experimental results demonstrate that the model achieves an accuracy of 97.86%, outperforming conventional CNN-based deep fingerprinting methods in terms of precision, recall, and F1-score, thereby providing a reliable and scalable solution for secure Tor traffic analysis.

Index terms - *Tor Network, Hidden Services, Website Fingerprinting, BERT, LSTM, BiGRU, Deep Learning, Time-Series Analysis, Network Security, Traffic Classification, Semantic Feature Extraction, Dark Web Analysis*

1. INTRODUCTION

The Tor network has become one of the most widely used privacy-preserving systems, enabling anonymous communication through onion routing and multi-layered encryption. While it plays a vital role in protecting user identity and ensuring freedom of expression, it is also increasingly exploited for malicious activities such as illegal trading, cybercrime, and malware distribution. This dual nature of Tor creates a critical need for effective identification and classification of hidden services to enhance network security and monitoring.

Traditional website fingerprinting techniques primarily rely on traffic-based features such as packet size, direction, and timing patterns. Although these methods provide a certain level of detection capability, they fail to capture the semantic and contextual information present in web content. As a result, their performance is limited when dealing with dynamic, multi-page Tor services and evolving traffic patterns. Recent deep learning approaches, such as Convolutional Neural Networks (CNN), have improved feature extraction by learning hierarchical representations; however, they remain computationally intensive and still lack the ability to fully utilize textual and sequential information.

To overcome these limitations, this paper proposes a novel semantic-temporal fingerprinting framework that combines Natural Language Processing (NLP) and deep learning techniques. The proposed method utilizes BERT to extract rich semantic features from Tor hidden service webpages, including both homepages and sub-pages. These features are then structured into sequential windows and processed using Long Short-Term Memory (LSTM) networks to capture temporal dependencies and content evolution over time.

As an extension to the existing approach, a Bidirectional Gated Recurrent Unit (BiGRU) layer is integrated after the LSTM model to enhance bidirectional feature learning. This extension allows the system to analyze sequential data in both forward and backward directions, improving feature representation and classification accuracy. Additionally, the proposed system is implemented with a Flask-based web interface, enabling real-time prediction and user interaction, thereby demonstrating practical applicability in real-world scenarios.

Experimental results show that the integration of BERT, LSTM, and BiGRU significantly improves classification performance compared to traditional CNN-based fingerprinting methods. The proposed model achieves higher accuracy, precision, recall, and F1-score, making it a robust and efficient solution for detecting and analyzing Tor hidden services.

2. LITERATURE SURVEY

2.1 SRP: A Microscopic Look at the Composition Mechanism of Website Fingerprinting:

Tor protects users' privacy more than other anonymous communication methods. Tor is immune to deep packet inspection, however the website fingerprinting (WF) attack can de-anonymize it. WF attacks using deep learning outperform those using manually specified features and classical machine learning. Simulating traffic-website mapping interactions using a deep learning model is data-intensive, which may not be realistic. In this research, we investigate website fingerprinting composition and use bionic traffic traces to alleviate data scarcity. To deconstruct traffic traces and build SRP-based cumulative features, we introduce the send-and-receive pair (SRP). Rearranged SRPs are used to rebuild and produce bionic traces (BionicT). Our bionic traces boost the performance of the cutting-edge deep-learning-based Var-CNN. In the five-shot situation, accuracy increases by 50%, outperforming HDA. Our technique defeated TF in 15/20-shot situations with over 95% accuracy in closed-world settings and over 90% accuracy in open-world circumstances. Expensive experiments indicate that our strategy improves the deep learning model's idea

drift resistance. The SRP is useful for analyzing and characterizing internet traffic trails.

2.2 FedFingerprinting: A Federated Learning Approach to Website Fingerprinting Attacks in Tor Networks:

Using Tor traffic, website fingerprinting attacks (WF) can identify anonymous individuals browsing unlawful websites in Tor networks. These attacks leverage packet length, number of packets, and time to identify users who access restricted content. Machine learning or deep learning approaches have been frequently employed for WF to produce an appropriate model to shatter illicit users' privacy because to AI advances. However, state-of-the-art WF methods assumed that all Tor node data is gathered and trained centrally to build the model: However, Tor nodes may not wish to disclose crucial training data. Collecting and training data centralizedly requires substantial CPU and network bottleneck at the centralized server. This research offers FedFingerprinting, a unique architecture for WF on the Tor network utilizing federated learning (FL), allowing Tor nodes to cooperatively create the global model without disclosing their local data sets. To reduce the cost of local training of selected Tor nodes in FL, the value of various handcrafting features utilized for WF is first evaluated by analyzing feature correctness under the ensemble of tree machine learning algorithms. Instead of raw data, the model is trained utilizing FL methods on the selected top-ranked features to balance accuracy and training time. Additionally, effective Tor node selection for the FL process is created based on each Tor node's local model correctness. In closed-world scenarios with real-world Tor data sets, we experimentally evaluate FedFingerprinting with raw data and feature selection to various benchmarks in training time and accuracy. FedFingerprinting with Tor node selection performs better in convergence speed.

2.3 A Multi-Granularity Features Representation and Dimensionality Reduction Network for Website Fingerprinting:

Website fingerprinting (WF) is essential to cybercrime investigation and forensics since it identifies target websites viewed anonymously. This discipline has recently focused on deep learning-based WF research. These approaches are accurate but lose performance with time. The progression of network protocol versions and the development of obfuscation methods cause idea drift and deterioration. This research introduces LRCT, a multi-granularity features representation and dimensionality reduction network for Website Fingerprinting, to overcome concept drift. The local feature extraction block (LRC Block) of the LRCT network extracts fine-grained local features from 2000-dimensional original sequences and reduces the dimensionality to 125, leveraging the temporal learning advantages of Local Recurrent Networks (Local RNN) and the spatial learning strengths of Convolutional Neural Networks (CNN). From low-dimensional input, the network utilizes a Transformer Encoder to capture stronger global properties. Experimental results show that LRCT outperforms state-of-the-art WF techniques with 99.34% accuracy in a closed-world situation. The LRCT network halves the parameter count and cuts the average training time per epoch to 20% of the benchmark WF-Transformer approach. Even with idea drift, LRCT is 89.9% accurate. LRCT improves accuracy and recall in open-world circumstances.

2.4 Neural-FacTOR: Neural Representation Learning for Website Fingerprinting Attack over TOR Anonymity:

The Onion Router (TOR) network is a popular open-source anonymous communication technology, but its misuse makes it challenging to keep an eye on the spread of online crimes, such as gaining access to illegal websites. The majority of current methods for de-anonymizing TOR networks mostly rely on manually extracted characteristics, which is time-consuming and performs poorly. This research suggests a neural representation learning method based on a classification algorithm to identify website fingerprints in order to address the drawbacks. Based on convolutional neural networks (CNNs) with dilation and causal convolution, we developed a novel website fingerprinting attack model that can enhance CNN's perception field and capture the sequential nature of input data. Experiments on three widely used public datasets demonstrate that the suggested model is reliable and efficient for classifying website fingerprints, increasing accuracy by 12.21% when compared to the most advanced techniques.

2.5 Realistic Website Fingerprinting By Augmenting Network Traces:

Tor users' (and other anonymity systems') anonymity is seen to be seriously threatened by website fingerprinting (WF). While cutting-edge WF approaches have claimed great attack accuracy, such as by utilizing Deep Neural Networks (DNN), a number of recent studies have questioned the viability of such WF assaults in the real world because of the assumptions made in its design and assessment. In this work, we contend that such impracticality issues are primarily caused by the attacker's incapacity to gather training data under comprehensive network conditions. For example, a WF classifier may be deployed on connections with different network conditions but trained only on high-bandwidth samples collected on particular high-bandwidth network links. We demonstrate how enhancing network traces can improve WF classifier performance under unseen network settings. In particular, we provide NetAugment, an augmentation method specifically designed for Tor trace requirements. We use self-supervised and semi-supervised learning methods to implement NetAugment. Our comprehensive open-world and close-world experiments show that our WF attacks outperform the state-of-the-art under realistic evaluation settings. This is because they use augmented network traces for training, which enables them to learn the characteristics of target traffic in unobserved settings (e.g., unknown bandwidth, Tor circuits, etc.). For example, our self-supervised WF assault (called NetCLR) achieves up to 80% accuracy with a 5-shot learning in a closed-world scenario when the evaluation traces are gathered in a setting that the WF adversary is not aware of. This is contrasted with the cutting-edge Triplet Fingerprinting, which has an accuracy of 64.4% [34]. We think that our work's encouraging outcomes will promote the application of network trace augmentation in various kinds of network traffic analysis.

3. METHODOLOGY

i) Proposed Work:

The proposed work introduces an enhanced website fingerprinting framework for Tor hidden service

classification by integrating semantic feature extraction with sequential deep learning models. Initially, textual data is collected from Tor hidden service homepages and their corresponding sub-pages through web crawling. This textual content is processed using the BERT model to generate high-dimensional semantic feature vectors, capturing contextual and linguistic information that is typically ignored in traditional traffic-based approaches. These extracted features are then organized into sequential windows to represent temporal changes in webpage content across multiple pages. A Long Short-Term Memory (LSTM) network is employed to learn time-dependent patterns from these sequences, enabling the model to understand how content evolves over time. This sequential modeling significantly improves the system's ability to distinguish between normal and malicious Tor services.

As an extension to the base model, a Bidirectional Gated Recurrent Unit (BiGRU) layer is incorporated after the LSTM to enhance feature learning. The BiGRU processes the sequence data in both forward and backward directions, allowing the model to capture deeper contextual dependencies and refine feature representation. This hybrid BERT–LSTM–BiGRU architecture improves classification performance, robustness, and generalization capability. Finally, the trained model is deployed using a Flask-based web interface, enabling real-time prediction of Tor service types by allowing users to upload test data. The system demonstrates superior performance compared to conventional CNN-based fingerprinting methods, achieving higher accuracy and efficiency in detecting hidden service activities.

ii) System Architecture:

The proposed system architecture is designed to effectively classify Tor hidden services by integrating semantic and temporal feature analysis. Initially, Tor traffic or webpage content is collected from hidden service URLs, including both homepages and sub-pages. This data undergoes preprocessing, where it is cleaned, normalized, and organized into structured sequential windows. These windows represent the temporal evolution of webpage content. The processed data is then passed through the BERT model, which generates high-dimensional embeddings capturing rich semantic and contextual information from the textual content, overcoming the limitations of traditional packet-based features.

The extracted BERT embeddings are fed into a temporal feature learning module consisting of LSTM and an extended BiGRU layer. The LSTM captures sequential dependencies and learns time-based patterns in the data, while the BiGRU enhances feature learning by processing sequences in both forward and backward directions. The learned features are further transformed into compact representations and passed through fully connected layers with activation functions for final classification. The system outputs the predicted category of Tor hidden services (normal or malicious), and the integration with a Flask-based interface enables real-time prediction and user interaction, making the system practical and efficient for network security applications.

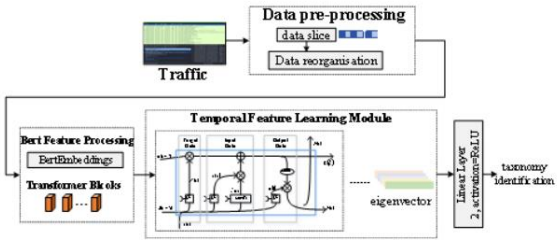

Fig.1. Proposed Architecture

iii) MODULES:

1. Data Collection Module

- Collects Tor hidden service URLs and extracts textual data from homepages and sub-pages.
- Uses datasets like AWF or crawled Tor URLs to build input data for analysis.

2. Data Preprocessing Module

- Cleans, normalizes, and organizes extracted text data into structured format.
- Converts data into sequential windows to capture temporal changes in webpages.

3. BERT Feature Extraction Module

- Applies BERT model to convert text into high-dimensional embeddings.
- Captures semantic and contextual information from webpage content.

4. Temporal Learning Module (LSTM)

- Learns sequential patterns from windowed feature data.
- Captures temporal dependencies and changes across multiple pages.

5. Extension Module (BiGRU)

- Enhances feature learning using bidirectional sequence processing.
- Improves classification accuracy by capturing forward and backward dependencies.

6. Classification Module

- Uses fully connected layers with activation functions to classify data.
- Predicts whether Tor service is **Normal or Malicious**.

7. Prediction & Interface Module

- Deploys model using Flask web interface for real-time predictions.
- Allows users to upload data and view classification results interactively.

iv) ALGORITHMS:

1. CNN-based Deep Fingerprinting Algorithm

The CNN-based Deep Fingerprinting algorithm is a feature-learning approach designed to automatically extract hierarchical patterns from traffic or content data. It applies multiple convolutional layers to capture both local and global variations present in structured feature sequences. This algorithm is primarily used to identify Tor hidden service behavior by analyzing numerical representations derived from webpage content or network traffic.

The main purpose of this method is to eliminate manual feature engineering by enabling automatic multi-level feature extraction. CNN learns spatial dependencies within feature vectors, allowing it to distinguish between normal and malicious services effectively. It serves as a strong baseline model by providing reliable classification based on structural variations in the encoded input data.

2. BERT + LSTM Fingerprinting Algorithm (Proposed)

The proposed BERT with LSTM fingerprinting algorithm integrates semantic feature extraction with temporal sequence modeling to generate robust hidden service signatures. BERT is used to convert textual data from Tor webpages into high-dimensional embeddings that capture contextual and linguistic meaning. These embeddings are then organized into sequences and processed by the LSTM model.

The purpose of this algorithm is to improve classification accuracy by combining deep semantic understanding with long-term dependency learning. LSTM captures temporal changes in webpage content across multiple pages, enabling the model to detect behavioral patterns over time. This approach provides richer and more meaningful feature representations, leading to more accurate identification of malicious Tor services.

3. BERT + LSTM + BiGRU Algorithm (Extension)

The extended algorithm enhances the proposed model by incorporating a BiGRU layer along with BERT and LSTM to improve sequential learning. While LSTM captures forward temporal dependencies, BiGRU processes the sequence in both forward and backward directions, enabling the model to learn deeper contextual relationships within the data.

The purpose of this extension is to strengthen feature representation, reduce noise, and improve prediction robustness. By combining semantic embeddings with bidirectional temporal learning, the model achieves better discrimination between normal and malicious hidden services. This results in higher accuracy, improved generalization, and more reliable performance under dynamic and complex Tor environments.

4. EXPERIMENTAL RESULTS

The performance of the proposed Tor hidden service fingerprinting framework is evaluated using a dataset of crawled Tor URLs, where textual content from homepages and sub-pages is extracted and processed. The dataset is divided into training and testing sets in an 80:20 ratio to ensure reliable evaluation. Multiple models, including the existing CNN-based Deep Fingerprinting, the proposed BERT with LSTM model, and the extended BERT + LSTM + BiGRU model, are trained and compared. The evaluation is carried out using standard performance metrics such as accuracy, precision, recall, F1-score, confusion matrix, and ROC curves.

Experimental results demonstrate that the CNN-based Deep Fingerprinting model achieves an accuracy of 95%, serving as a baseline. The proposed BERT + LSTM model significantly improves performance by achieving 97.50% accuracy, due to its ability to capture semantic and temporal features. Furthermore, the extended BERT + LSTM + BiGRU model achieves the highest accuracy of 97.86%, benefiting from bidirectional sequence learning. The confusion matrix shows minimal misclassification, while ROC curves indicate strong predictive capability. Training accuracy increases steadily with epochs, and loss decreases consistently, confirming model stability. These results validate that the proposed and extended models outperform traditional approaches and provide an effective solution for accurate and reliable Tor hidden service classification.

Accuracy: A test's accuracy is determined by its capacity to distinguish between healthy and ill cases.

To gauge the accuracy of the test, find the percentage of examined instances that had true positives and true negatives. According to the computations:

Accuracy = TP + TN /(TP + TN + FP + FN)

$$Accuracy = \frac{(TN + TP)}{T}$$

Precision: Precision is the number of affirmative cases or the classification's accuracy rate. The following formula is applied to assess accuracy:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\Pr e\,cision = \frac{TP}{(TP + FP)}$$

Recall: A model's ability to recognise every instance of a pertinent machine learning class is measured by its recall. The ratio of accurately predicted positive observations to the total number of positives indicates how well a model can identify class instances.

$$Recall = \frac{TP}{(FN + TP)}$$

mAP: Mean Average Precision is one ranking quality metric (MAP). It considers the number of relevant recommendations and their position on the list. MAP at K is calculated as the arithmetic mean of the Average Precision (AP) at K for each user or query.

$$\boldsymbol{mAP = \frac{1}{n}\sum_{k=1}^{k=n} AP_k}$$

$$\boldsymbol{AP_k = \text{ the AP of class } k}$$

$$\boldsymbol{n = \text{ the number of classes}}$$

F1-Score: An accurate machine learning model is indicated by a high F1 score. combining precision and recall to increase model correctness. The accuracy statistic quantifies the frequency with which a model correctly predicts a dataset.

$$F1 = 2 \cdot \frac{(Recall \cdot \Pr e\,cision)}{(Recall + \Pr e\,cision)}$$

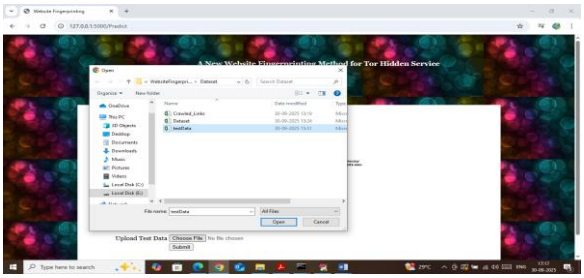

Fig.1: Test Data Upload Interface

This figure illustrates the Flask-based web interface where users can upload test data files containing Tor webpage content. The system allows easy selection and submission of input data for prediction, enabling real-time interaction with the trained model.

Fig.2: Prediction Output Interface

This figure shows the prediction results generated by the system after processing the uploaded data. The left column displays the extracted webpage text, while the right column shows the predicted Tor service type as either **Normal Tor Page** or **Attack Tor Page**, demonstrating the effectiveness of the classification model.

Algorithm Name	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)
Existing CNN Based Deep Fingerprint	95.374	95.207	95.31	95.257
Proposed LSTM with BERT Fingerprint	97.509	97.393	97.502	97.446
Extension LSTM with BERT + BiGRU	97.865	97.926	97.692	97.803

Table 1: Performance Comparison of Algorithms

The table compares the performance of CNN, BERT+LSTM, and the extended BERT+LSTM+BiGRU models. The extension model achieves the highest accuracy and overall performance, proving the effectiveness of bidirectional temporal learning.

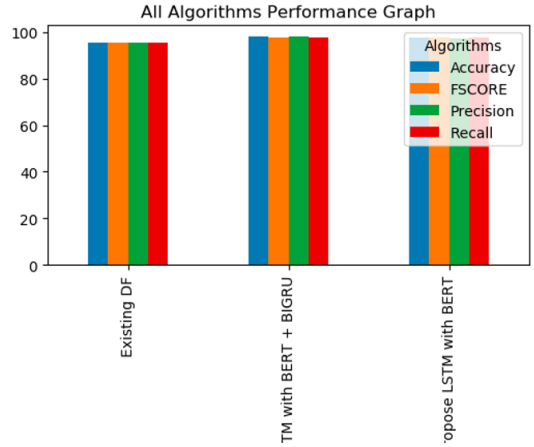

Fig.3: All Algorithms Performance Graph

The graph shows that the BERT + LSTM + BiGRU model achieves the best performance among all algorithms.

5. CONCLUSION

In this paper, an enhanced website fingerprinting framework for Tor hidden service classification is proposed by integrating semantic and temporal analysis techniques. The combination of BERT for feature extraction and LSTM for sequential modeling significantly improves the ability to capture contextual and time-dependent patterns in webpage content. The proposed approach overcomes the limitations of traditional traffic-based methods by utilizing rich textual information from Tor services.

Furthermore, the extension of the model using a BiGRU layer enhances bidirectional learning, leading to improved feature representation and higher classification accuracy. Experimental results demonstrate that the proposed system achieves superior performance compared to CNN-based deep fingerprinting methods, with an accuracy of 97.86%. Overall, the system provides an effective, robust, and scalable solution for identifying and monitoring Tor hidden services, contributing to improved network security and reliable detection of malicious activities.

6. FUTURE SCOPE

The proposed Tor hidden service fingerprinting system can be further enhanced by integrating advanced deep learning models such as Transformer-based architectures and attention mechanisms to improve semantic understanding and feature selection. These improvements can help the model focus on more relevant patterns within webpage content, thereby increasing classification accuracy and interpretability. Additionally, optimizing the model for real-time and large-scale deployment will enable faster processing of Tor traffic, making it suitable for practical cybersecurity applications.

In future work, the system can be extended to detect a broader range of darknet activities, including fraud detection, malware identification, and illegal content monitoring. Moreover, lightweight and edge-based implementations can be explored to reduce computational complexity and support deployment in resource-constrained environments. Integrating the model with advanced cybersecurity frameworks can

further enable automated threat detection and response, transforming the system into a comprehensive and intelligent network security solution.

REFERENCES

[1] Chen, Y., Wang, Y., & Yang, L. (2022). SRP: A microscopic look at the composition mechanism of website fingerprinting. *Applied Sciences*, *12*(15), 7937.

[2] Bang, J., Jeong, J., & Lee, J. (2023). Fedfingerprinting: A federated learning approach to website fingerprinting attacks in tor networks. *IEEE Access*, *11*, 78431-78444.

[3] Ding, Y., & Hu, B. (2024). A Multi-Granularity Features Representation and Dimensionality Reduction Network for Website Fingerprinting. *IEEE Access*.

[4] Sun, H., Huang, Y., Han, L., Long, X., Liu, H., & Zhou, C. (2022, December). Neural-FacTOR: Neural Representation Learning for Website Fingerprinting Attack over TOR Anonymity. In *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 435-440). IEEE.

[5] Bahramali, A., Bozorgi, A., & Houmansadr, A. (2023, November). Realistic website fingerprinting by augmenting network traces. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1035-1049).

[6] Y. Wang, R. Chen, X. Huang, and B. Wang, "Secure anonymous communication on corrupted machines with reverse firewalls," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 6, pp. 3837–3854, 2022.

[7] Q. Tan, X. Wang, W. Shi, J. Tang, and Z. Tian, "An anonymity vulnerability in Tor," *IEEE/ACM Transactions on Networking*, vol. 30, no. 6, pp. 2574–2587, 2022.

[8] I. Karunanayake, J. Jiang, N. Ahmed, and S. K. Jha, "Exploring uncharted waters of website fingerprinting," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1840–1854, 2024.

[9] S. E. Oh, N. Mathews, M. S. Rahman, M. Wright, and N. Hopper, "GANDaLF: GAN for data-limited fingerprinting," *Proceedings on Privacy Enhancing Technologies*, vol. 2021, no. 2, pp. 305–322, 2021.

[10] F. Qian, Y. Tu, C. Hou, and B. Cao, "TLN-LSTM: An automatic modulation recognition classifier for extremely long sequences," *International Journal of Web Information Systems*, vol. 20, no. 3, pp. 248–267, 2024.

[11] N. Gao et al., "Generative adversarial networks for spatio-temporal data: A survey," *ACM Transactions on Intelligent Systems and Technology*, vol. 13, no. 2, pp. 1–25, 2022.

[12] Guo, C., Chen, G., Jin, D., & Lin, Z. (2025). An Enhanced Website Fingerprinting Attacks Based on Attention Mechanism and Spatial-Temporal

Features. *International Journal of Pattern Recognition and Artificial Intelligence*, *39*(06), 2559005.

[13] Zhou, Q., Wang, L., Zhu, H., Lu, T., & Song, H. (2024). Joint alignment networks for few-shot website fingerprinting attack. *The Computer Journal*, *67*(6), 2331-2345.

[14] Hong, X., Ma, X., Li, S., Cai, Y., & Liu, B. (2024). SSBM: A spatially separated boxes-based multi-tab website fingerprinting model. *Journal of Network and Computer Applications*, *232*, 104023.

[15] Sinha, M., & Dave, M. (2025, October). Enhanced Website Fingerprinting Attack Model: A CNN-Based Approach with. In *Proceedings of International Conference on Computational Intelligence and Data Engineering: ICCIDE 2024* (p. 323). Springer Nature.

[16] Liu, L., Wei, Z., Chen, S., Su, J., & Yuan, Y. (2024, October). KP-WF: Cross-Domain Few-Shot Website Fingerprinting. In *International Conference on Digital Forensics and Cyber Crime* (pp. 227-245). Cham: Springer Nature Switzerland.

[17] Xu, Y., Wang, L., Li, J., Song, K., & Yuan, Y. (2023, October). Zoomer: A website fingerprinting attack against tor hidden services. In *International Conference on Information and Communications Security* (pp. 370-382). Singapore: Springer Nature Singapore.

[18] Zou, H., Wei, Z., Su, J., Chen, S., & Qin, Z. (2024). Relation-CNN: Enhancing website fingerprinting attack with relation features and NFS-CNN. *Expert Systems with Applications*, *247*, 123236.

[19] Yuan, Y., Zou, W., & Cheng, G. (2025). MW3F: Improved multi-tab website fingerprinting attacks with Transformer-based feature fusion. *Journal of Network and Computer Applications*, *236*, 104125.

[20] Xu, Y., Li, J., Hou, Y., Wang, L., Song, K., & Cheng, G. (2024, June). NuanceTracker: A Website Fingerprinting Attack against Tor Hidden Services through Burst patterns. In *2024 IEEE Symposium on Computers and Communications (ISCC)* (pp. 1-7). IEEE.

[21] Liang, D., Sun, J., Zhang, Y., & Yan, J. (2022, December). Lightweight Neural Network-based Web Fingerprinting Model. In *2022 International Conference on Networking and Network Applications (NaNA)* (pp. 29-34). IEEE.

[22] Dani, J., & Wang, B. (2021, August). Hiddentext: Cross-trace website fingerprinting over encrypted traffic. In *2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI)* (pp. 274-281). IEEE.

[23] Ling, Z., Xiao, G., Wu, W., Gu, X., Yang, M., & Fu, X. (2022, May). Towards an efficient defense against deep learning based website fingerprinting. In *IEEE INFOCOM 2022-IEEE Conference on Computer Communications* (pp. 310-319). IEEE.

[24] Zou, H., Su, J., Wei, Z., Chen, S., Yang, C., & Chen, M. (2025). Toward an Effective Few-shot Website Fingerprinting

Attack with Quadruplet Networks and Deep Local Fingerprinting Features. *IEEE Transactions on Dependable and Secure Computing*.

[25] Gong, J., Cai, W., Liang, S., Guan, Z., Wang, T., & Chang, E. C. (2025). WFCAT: Augmenting Website Fingerprinting with Channel-wise Attention on Timing Features. *IEEE Transactions on Dependable and Secure Computing*.

[26] Lyu, G., Kong, J., Chen, Y., & Wang, F. (2024, December). CTWF: Website Fingerprinting Attack based on Compact Convolutional Transformer. In *2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 57-67). IEEE.

[27] Wang, M., Chen, M., Li, Z., Wang, X., Shi, J., & Fang, B. (2023, November). Deanonymize tor hidden services using remote website fingerprinting. In *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 998-1005). IEEE.

[28] Sun, Y., Luo, X., Wang, H., & Ma, Z. (2022). A method for identifying tor users visiting websites based on frequency domain fingerprinting of network traffic. *Security and Communication Networks*, *2022*(1), 3306098.

[29] Shen, M., Gao, Z., Zhu, L., & Xu, K. (2021, June). Efficient fine-grained website fingerprinting via encrypted traffic analysis with deep learning. In *2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS)* (pp. 1-10). IEEE.

[30] Zhou, Q., Wang, L., Zhu, H., & Lu, T. (2023). Few-shot website fingerprinting attack with cluster adaptation. *Computer Networks*, *229*, 109780.