Vulnerability of Virtual Private Networks to Web Fingerprinting Attack

Khaleque Md Aashiq Kamal, Sultan Almuhammadi
College of Computer Sciences and Engineering,
King Fahd University of Petroleum and Minerals,
Dhahran, Saudi Arabia
Emails: aashiqkamal@gmail.com, sultan@almuhammadi.com

Abstract

Virtual private networks (VPN) are used to maintain secrecy of internet usage. They provide end-to-end encrypted traffic to hide the content and destination details from potential eavesdroppers. Recent studies show that 72% of VPN users apply it to access blocked content or hide identity from government. Concerned government departments and other organizations need to analyze the encrypted traffic of VPN to observe whether people are using blocked content or not. Typical traffic analysis fails in this case as traffic is encrypted and the destination IP address is hidden. However, traffic metadata and some packet attributes, like packet size and time, could be considered as fingerprint of any specific web service. In this paper, we analyze five commonly used VPN services, namely: Psiphone, Softether, HotspotShield, OpenVPN, and AviraPhantom. Our goal is to identify which VPN service is vulnerable to Cai et al. fingerprinting attack, and what types of web services are most appropriate to detect using this attack. The results show that Open VPN is more vulnerable to this attack compared to the other VPNs in this study. The efficiency of the web traffic classification through VPN is also estimated for four different web services with Cai et al. Useful recommendations are provided as a result of this study.

Keywords

VPN, Web Fingerprinting, Classifier, Machine Learning, Privacy.

I. Introduction

Privacy in the internet is a challenge for both users and service providers. Every step of internet activities can be tracked by the eavesdropper. An internet user location might be disclosed easily. If a user accesses his own residence server remotely, an eavesdropper can easily snip the traffic between server of that residence and user. Therefore, presently accessing private resources securely is observed as most crucial need. Even though maintaining privacy is not an easy task, Virtual Private Networks (VPNs) are one of the most effective ways to achieve privacy in the internet [1]. The main objectives of the VPNs are to evade the sniffing attack and to maintain the data integrity in the untrusted network of the internet [2].

In VPN communication, all the traffic is end-to-end encrypted between the VPN client user and the VPN server. The IP of the destination web address is kept hidden to the hops in the VPN tunnel. In this case, any eavesdropper will fail to find out which web page is being actually accessed by the VPN user as the IP is hidden. As a result, sometimes people might misuse the VPN service. For example, companies may not allow their employees to use social media, video streaming site, playing online games, etc. during office hours and sometimes schools block some website for their students for containing adult content [3]. This censorship can be easily avoided by using VPN services.

According to the renowned market research company Global Web Index [4], around 410 million people all over the world use anonymous software, like: VPN, Tor browser, Proxy Servers, etc. to hide their identity. Among them, 166 million people use VPNs. Figure 1 shows the region-wise VPN users in the world. It shows that users in Asia pacific and Latin America region use VPN more than other regions in the world. They have 50% of the total VPN users. Middle East come next with 18% of VPN users. While Europe and North America have 16% each. The frequency of the VPN usage varies from daily to once a month as shown in Figure 2. One fourth of the VPN users need it every day. While 7% of them use it once a month.

Moreover, the statistics in [4] show that most of the VPNs usage is not limited to security purposes. In fact, 72% of the VPNs users need it to access blocked websites, access blocked content at work, or hide identity from government. Therefore, it very important to analyze VPN traffic to find out which web service is accessed by any given user.

This paper presents a comparative analysis of five different VPN services based on the website fingerprinting attack given by Cai et al. [5], to find out which VPN service is more vulnerable to this a attack. Moreover, it estimates the efficiency of the web traffic classification through Psiphon VPN for four different web services, namely: video call communication, video streaming, online gaming site, and peer-to-peer file sharing.

The remaining of this paper is as follows: Section II give a general background on VPN. While Section III discussed related work of the website fingerprinting attack in the literature. Section IV explains the main goals of this study. Section V highlights

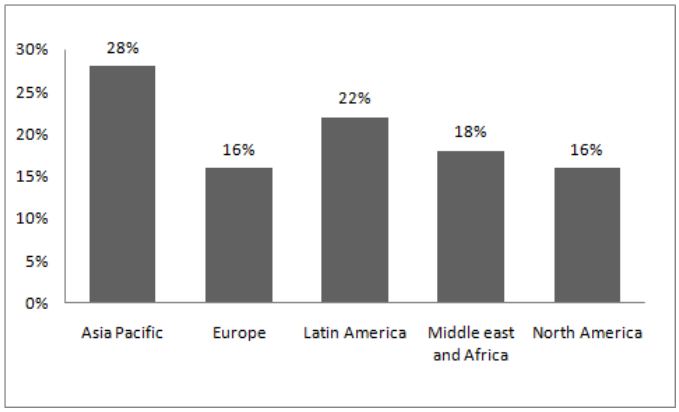

Fig. 1. Frequency of VPN users in different region

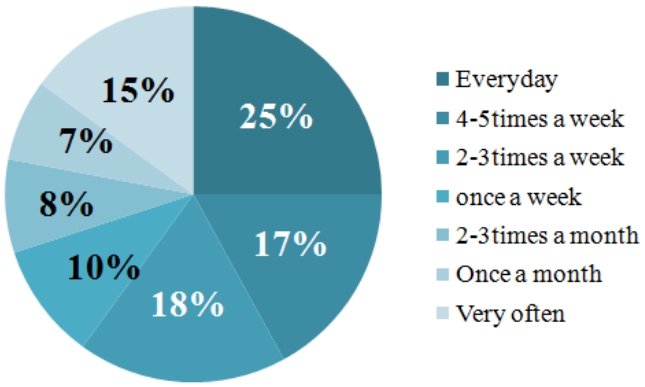

Fig. 2. Frequency of uses of VPNs

the main phases of our methodology. The data collection process and the fingerprinting techniques are discussed in Sections VI and VII, respectively. The results are presented in Section VIII, and further discussed in Section IX. Finally, the conclusion comes in Section X with useful recommendations based on our results.

II. Background

VPNs transfer sensitive information through public networks while minimizing the risk of information exposure. The goal is achieved by encrypting traffic payload at the source before sending it through public network while decrypting at the destination. An usual VPN tunnel communication is shown in Figure 3. VPNs permit user of internet to transmit and receive data over open networks transversely, as if they were connected to a private network. This also helps avoiding blockade and overcoming geo-restrictions.

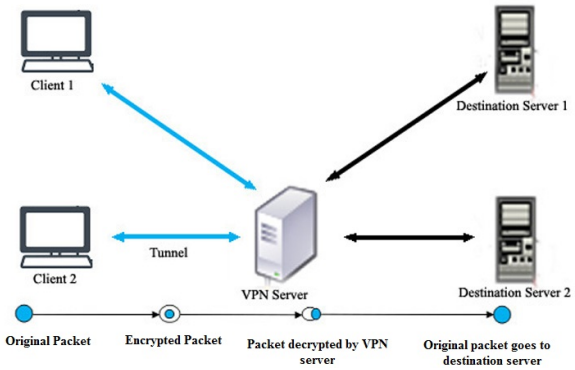

Fig. 3. Encryption configuration through a VPN tunnel

A. Security Protocols in VPN

There are many variations of VPN in terms of the tunneling protocol used to create a secure tunnel. Two of the most popular protocols in use are the Internet Protocol Security (IPsec), and the Secure Socket Layer/Transport Layer Security (SSL/TLS).

- **IPSec**: IPsec is standard network protocol suite that is used to provide a security at the network layer of the Internet model. It contains three protocols: Authentication Header (AH) Protocol, Encapsulating Security Payload (ESP) Protocol, and Internet Key Exchange (IKE) Protocol. IPsec operates in one of two different modes: transport mode, which is typically used for host-to-host communication, and tunnel mode, which is used when one or both ends of a security association are a security gateway [6].
- **SSL/TLS**: SSL/TLS is one of the most widely used security protocols at the transport layer of the Internet model. It is a general-purpose service implemented as a set of protocols that rely on TCP/SCTP. It provides five services which are fragmentation, compression, authentication, confidentiality, and framing. It can be implemented either as a part of the underlying protocol suite or embedded in specific packages. It accomplishes its tasks by four protocols (Record, Alert, Change Cipher Spec and Handshake protocols) in two layers [6].

Since IPsec works at the network layer and SSL/TLS works at the transport layer, they are both capable of protecting the traffic payload, but in different ways. SSL/TLS does not need any extra header to hide the metadata, but IPSec makes a new header to protect the metadata.

IPSec protects metadata of the payload, by making a new header. On the other hand, SSL/TLS does not protect the metadata, and therefore, it does not need any extra header to hide the metadata. Typical structures of an IPsec packet and an SSL/TLS packet are shown in Figure 4 and Figure 5.

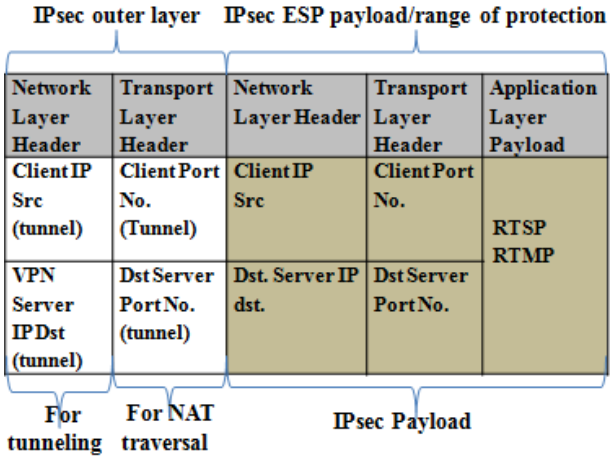

Fig. 4. IPSec VPN tunnel

B. VPN Services

There are many different VPN services. We choose five of them in this work. Table I shows a technical summary of the VPN services used in this work. For each VPN service, it shows the communication and security protocols. It also indicates whether or not the VPN service changes the IP address (IP Change) or the port number (Port No. Change).

TABLE I. TECHNICAL SUMMARY OF VPNS

Name	Protocol	Change of IP	Changes of Port No. (during session)	Changes of Port No. (new session)	Secuirty Protocol
Softether	UDP	Yes	No	Yes	IPSec/SSL
Open VPN	UDP	Yes	No	Yes	Own Protocol based on SSL
Avira	TCP	Yes	No	Yes	Own Protocol based on SSL
Psiphon	TCP	Yes	Yes	Yes	IPSec/SSL
Hotspot Shield	TCP	Yes	No	Yes	SSL
Tunnel Bear	TCP	Yes	No	Yes	SSL
Betternet	UDP	Yes	No	Yes	SSL

C. Fingerprinting Approach

Traffic analysis or fingerprinting is technological process that allows capturing the traffic activities even though its content is concealed or encrypted. For the web applications or services, it is attained by observing specific patterns inside the traffic packets. Those features can direct to the web services accessed by the users. These features or patterns are size of network packet, and direction of the packet.

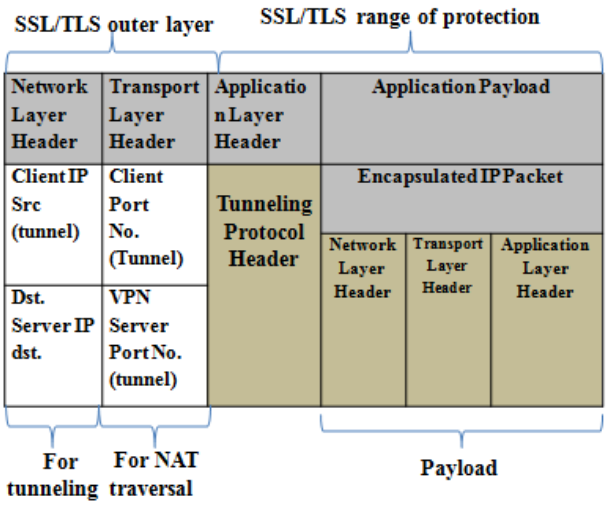

Fig. 5. SSL/TLS VPN tunnel

To build a fingerprinting approach, a number of sub-processes needs to be achieved. Figure 6 shows the complete scenario of the fingerprinting approach. First, inward/outward traffic of internet should be observed by using a network analyzer or snipping tool, like *Wireshark*. Then, a number of traces of web access is recorded. Next, selected packet features are collected to signify the fingerprint for particular web services. Those features are classified through a specific Machine Learning algorithm. After the training stage, a testing stage is executed and the accuracy of the classifier algorithm is observed and further fine tuned accordingly.

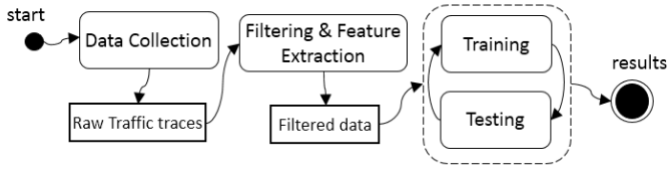

Fig. 6. Fingerprinting Procedure Model

III. Related Work

There is a good number of works on encrypted and non-encrypted traffic analysis. This section highlights the related work in both types of traffic analysis, with more focus on the analysis of encrypted traffic, more particularly on Tor and VPN traffic analysis.

A. Web traffic Classification

Li and Moore [7] used a supervised method named C4.5 to categorize the internet traffic. They classified browsing, peer to peer application, e-mail, FTP and services with good accuracy rate of 99%, but it was not on encrypted traffic. Moor and Zaev [8] also classified non-encrypted internet traffic based on port number, inter arrival time, flow length etc. They used Naive Bayes classifier to distinguish among peer to peer, email, web browsing, and multimedia and achieved an accuracy level of 95%.

MCgregor et al. [9] proposed a method to distinguish different traffic pattern including: SMTP, HTTP, DNS, FTP, etc. They clustered different traffic flows based on their pattern by employing Expectation Maximization algorithm. Zander et al. [10] also proposed a method to cluster different traffic flow includes: Telnet, FTP, HTTP, SMTP etc. They used AutoClass (which is based on Bayesian algorithm) for clustering the traffic.

Another method based on clustering approach was developed by Bernaille et al. [11], in which K-means algorithm was used to cluster the traffic flow. The k-means uses distance vector scheme to cluster the given data. Their method was only capable to classify TCP based traffic. Their study includes: HTTP, POP3, SMTP, SSH , HTTPS, etc. K-means algorithm was also used in Erman et al. [12] to distinguish peer to peer traffic from normal web traffic including FTP. They assumed that traffic flow can be distinguished using payload and information of header. Another approach was studied by Junior et al. [13] to identify P2P traffic from other application type traffic.

Perenyi and Molnar [14] and Freire et al. [15] independently proposed methods to identify Skype traffic flows from normal web traffic. However, Freire et al. achieved a relatively better success rate with 5% false positive.

According to the literature, we found that some researchers focused on only one application type, while others focused on number of applications. HTTP, SMTP, P2P, web traffic protocols are the main focus in most of these studies. Moreover, encrypted traffic classification mostly related to either SSL or SSH. However, analysis or classification of encrypted traffic faces more challenges and difficulties than others.

Wright et al. [16] proposed a model to identify traffic flow in encrypted communication using Hidden Markov Models (HMM). They considered as features: packet sizes, direction and timing information and set the main focus on HTTPS communication. They identified 20% applications in their work.

Alshammari and Zincir-Heywood [17] worked on SSH traffic and used machine learning algorithms, like RIPPER and AdaBoost, to classify the SSH traffic without knowing the payload (IP address and port numbers). They succeed to classify applications such as DNS, FTP and telnet with high accuracy of 99%. They extended their work in [18], to identify traffic of Skype as a P2P VoIP. They successfully distinguished between SSH traffic from non SSH and Skype from non-Skype. They used five types of machine learning algorithms, namely: SVM, Naive Bayes, RIPPER, AdaBoost and C4.5 to deploy thier work. Among these algorithms, C4.5 has given the best result of 97% accuracy.

Leroux et al. [19] also developed a fingerprinting attack based on machine learning techniques. This attack targeted traffic through IPsec and Tor tunnel. They distinguished between four types of traffic: web browising, voip, video streamming and P2P. But, they only considered single application from every type of traffic. Naive Bayes, logistic regression and random forest were used as classifier algorithm. They considered the timing and size of the packets as features to train the classifier.

B. Web fingerprinting through encrypted communication

In [20], the author presented an analysis based on weakness in web proxy named SafeWeb. This weakness exposes to eavesdroppers the website being browsed by the user. To analyze the test dataset, they depended on the port no. of client, size of traffic and the direction. Their program can decide how to distinguish two fingerprints of different websites.

On the other hand, Sun et al. [21] identified web traffic in a SSL communication from a large sample. Their traffic signature was based on website's requested object number and size of objects. Using this signature, they got accuracy of identification is 75%.

Liberatore and Levine [22] showed how unique packet lengths are a powerful WF feature. They made two attacks using the Jaccard coefficient and the Naive Bayes classifier. Each packet sequence was mapped to its set of unique packet length, and Jaccard coefficient attack was used to measure it. It discarded packet ordering and packet frequency. After that, the Jaccard coefficient has been used to measure the distance of the sequences of two packets. The classifier of Naive Bayes also used packet lengths and their frequencies of occurrence, but the packet ordering and timing are discarded. The Naive Bayes assumption is that the probabilities of occurrence of different packet lengths are independent of each other.

Later, Herrmann et al. [23] presented a fingerprinting approach in different encrypted traffic that uses text mining techniques. They used Multinomial Naive-Bayes as a machine learning classifier. Single hop and multi hop systems have been used in their approach. They considered OpenSSH, OpenVPN, CiscoVPN, Stunnel as single hop and Tor as multihop systems. Their work can correctly classify 97% of unique website from encrypted communication.

Zhou et al. [24] developed a website fingerprinting attack based on Profile Hidden Markov Model (PHMM). They conducted experiments of both closed world and open world scenario by collecting web dataset via SSH. They used packet size and direction as feature. They achieved more than 95% accuracy rate in every case.

C. Web fingerprinting through Tor communication

In 2012, Cai et al. [5] also used SVM to classify web fingerprinting attack on Tor communication. For post processing data, they used Damerau-Levenshtein edit distance algorithm for calculating distance between packet sizes of two different traffic traces of web browsing, which is described in more detail in Section VIII. They achieved an accuracy of 87%.

In 2013, Tao Wang and Ian Goldberg [25] improved the attack for tor by modifying the distance based algorithm of Cai et al. In the closed-world experiments, their accuracy is 91%, as compared to 87% from the best previous classifier on the same data.

Jahani and Jalili [26] introduced a technique based on the Fast Fourier Transform (FFT) to estimate similarity distance between two different instances from traffic flows.

Tobias Pulls and Rasmus Dahlberg [27] introduced a robust technique based on the Website Oracle (WO). It gives a website fingerprinting attacker the ability to find out whether a particular website was among the websites visited by Tor users during the victim's trace. Their work showed that combining of website oracle and website fingerprinting significantly decreases false positive (FP) for about half of the visited websites. They also used packet size and direction as feature to train the classifier. They achieved 95% in tor network.

D. Web fingerprinting through VPN

Shi and Biswas [3] worked on traffic analysis to detect web traffic in encrypted tunnel named Juniper VPN. Their target was to detect video streaming from encrypted tunnel. They designed a signature based on the packet size and timing of each packet. Finally, they achieved good results for BayesNet Classifier with lower false positive rate. In their related work [28], packet size distribution has been used as a feature vector to analyze the traffic. J4.8 tree classifier has been used in this work to recognize the video stream from other web traffic. They achieved 90% accuracy in JuniperVPN, which is the same accuracy achieved by Herrman et al. in [23].

Shi and Biswas also used traffic analysis to detect encrypted video traffic [29] where packet arrival interval (PAI) was used as a classification feature to detect video streaming traffic from encrypted OpenVPN tunnel. They also used J4.8, SVM and 1-NN as classifier in this work. The 1-NN classifier gave the best results with 94% accuracy. Table II summarizes the details of these web fingerprinting techniques through VPN.

TABLE II. SUMMARY OF THE WEB FINGERPRINTING THROUGH VPN

Study	Techniques	Feature	Domain	Result
Herrman et al. [23]	Multinomial Naïve Bayes	Packet size and direction	Open VPN and Cisco VPN	90%
Shi et al. [3]	Bayes net Classifier	Packet Sizes, timing info	Video traffic in Juniper VPN	80%
Shi et al. [28]	Decision Tree Classifier	Packet Size distribution	Video traffic in Juniper VPN	90%
Shi et al. [29]	k-NN	Packet arrival information	Video traffic in Open VPN	94%

Feghhi et al. [30] introduced a traffic analysis attack on VPN traffic. They used timing information of packet as feature for analyzing the encrypted traffic. Their success rate is 90%. This attack is suitable for wired and wireless network.

According to our literature review no work has been conducted on different VPN services to find out which web services were accessed by the user. In this work, different top most visited dynamic web pages, social networking sites, video streaming sites, online games and video communications will be considered as web services. Moreover, no work has been found related to traffic classification with diverse and mixed traffic data set through VPN.

IV. OBJECTIVE

The main goals of this paper are as follows:

- ***Website fingerprinting of different VPNs:*** There are several VPN services today, and the most commonly used are listed in Table I with brief descriptions. The listed VPN services have been installed and configured for our experiment. Different VPN services uses different security protocols to encapsulate their network traffic before sending it to the public network. We performed a comparative analysis of these different VPN services based on website fingerprinting attacks. The comparative analysis gives a clear idea about the vulnerability of these VPNs to web fingerprint attack. The goal here is to assess how vulnerable the different VPNs are to this type of attack.
- ***Website traffic Classification through VPN:*** For the second goal, we use one VPN service to access different web services. Then we record the encrypted traffic, and analyze it using fingerprint to retrieve high level information, namely the web service has been accessed through VPN. The goal here is to identify which web service is accessed given only the recorded encrypted traffic.

V. METHODOLOGY

The proposed experiment builds an environment for different VPN services and uses the real world web through these VPNs to study the web traffic applying website fingerprinting attack on these VPNs, in order to find out the identity of the accessed website. This work will be carried out in several phases as follows:

- ***Installing and Configuring VPN Services:*** This phase starts after selecting five most commonly used VPN services. Selected VPN tools will be installed and configured to real world uses for different web services.
- ***Analyzing VPN Services:*** In this phase, installed VPN services are analyzed according to their distinctiveness. More specifically, the protocol (TCP or UDP) which is being used by any specific VPN tools is studied.
- ***Data Collection of Different Web Services Traffic:*** This phase involves collecting data of different types of web traffic through five VPN services. Top twenty most visited websites according to Alexa [31] have been used as a data source for website fingerprinting attack. In order to do the, traffic classification, we collected data for mostly used video call, video streaming sites, online game sites, P2P sites etc. Every access for all applications have been repeated for forty times. Then the individual incoming and outgoing web traffic for each access has been captured at the client side by using *tshark* tool.
- ***Data Setup:*** After collecting the required data, we need to process them to make appropriate format for the Cai et al. [5] fingerprinting techniques. The details are given in Section VI.
- ***Website fingerprinting attack:*** We apply Cai et al. [5] fingerprinting techniques on collected data of five different VPNs.

TABLE III. EXPERIMENTAL SETUP

Operating System	Windows (64 bit)
CPU	CPU 2020M 2.40GHz
Physical Memory	2048 MB
Browser	Google Chrome Version 57.0.2987.133
Network protocol analyzer.	*tshark* 2.2.1

- ***Web traffic Classification:*** We investigate the recorded data in offline mode to identify which specific web service is accessed by a given user based on the captured traffic data.

VI. DATA COLLECTION AND SETUP

In this experiment, we used a fresh windows based computer. Table III shows the details of the computer and installed software. We have chosen Google Chrome as it is more secure than other browsers for fingerprinting attacks [32]. Then we installed and configured five most commonly used VPN client in the client machine. As discussed in Section 2.

A. Data collection for website fingerprinting through VPN

In order to apply the fingerprinting attack on the five different VPN services, twenty most popular websites have been chosen according to Alexa [31]. The list of these websites with their type is given in Table IV. An encrypted VPN communication has been initiated from VPN client to the VPN server. Website traffic traces are collected by visiting every website forty times. The visited traffic has been logged using network protocol analyzer *tshark*.

To automate the browsing and traffic capture process we used a windows batch program. The script follows the following steps: (1) It opens the Chrome browser and enables the *tshark*, (2) it reads the file containing website names and requests the browser to open it, (3) it waits for thirty seconds to load the website, (4) it captures and stores the individual traffic, and (5) it waits ten seconds to ensure a delay between two visits of websites. The whole process is repeated forty times for twenty websites, one for each of the five VPNs. In order to avoid the noise in the traffic the browser cache has been completely cleared after every iteration. The data collection process is done during morning, evening and night to simulate the real network traffic scenario. We ended up having $20 \times 40 \times 5 = 4000$ *pcap* files of web traffic at the end of the capture process.

TABLE IV. LIST OF TOP 20 WEBSITE

Website Name	**Type of website**
www.google.com	search engine
www.youtube.com	video sharing
www.facebook.com	social network
www.baidu.com	search engine
www.wikipedia.com	encyclopedia
www.yahoo.com	portal media
www.amazon.com	e commerce
www.qq.com	portal media
www.live.com	software services
www.taobao.com	e commerce
www.vk.com	social network
www.twitter.com	social network
www.instagram.com	social network
www.hao123.com	web directories
www.sohu.com	portal
www.sina.com.cn	portal
www.reddit.com	entertainment
www.linkedin.com	social network
www.tmall.com	e commerce
www.weibo.com	social network

B. Data collection for web traffic classification through VPN

For applying the fingerprinting attack on different web services, we selected four common web services: video call communication, video streaming website, online gaming sites, and peer to peer file sharing. From every services, we selected three different service provider. The list are given in Table V. An encrypted VPN communication has been initiated from VPN client to the VPN server. To collect the video call communication data, 40 times video call has been initiated using three different service provider mentioned in Table V. The same process is repeated for other services for only one VPN to collect data.

C. Data Setup for Cai Classifier

We have used Cai et al. [5] classifier to evaluate the vulnerability of the different VPNs to website fingerprinting attack. After collecting both types of data (for website fingerprinting and web traffic classification), we process them to make appropriate format for the Cai et al. fingerprinting techniques. We used $tsahrk$ command to filter out all the packet sizes from stored *pcap*

TABLE V. LIST OF DIFFERENT SERVICES

Services Types	Name of the service provider
Video Call communication	Facebook,Hangout,Skype
Video Streaming	Youtube, Metacafe, Vimeo
Online gaming	Dota2, Solitaire, Patterns
Peer2Peer file sharing	Thepiratebay, Extratorrent, Torrentz2

files of each and every iteration of web browsing and web services. The packet sequences of every website visit are stored in a different text files of the form *X_N.txt*, where X is the number of website, and N is the trace number of that website. For example , the file 5_1.txt contains filtered-out packet sequences with corresponding packet sizes of the fifth website's (wikipedia) in the first attempt web trace.

To automate the process, we used a batch script which reads all forty captured *pcap* files of one individual website from a folder, then filter out the packet sizes and sequences from that file and save it on text files. The process is repeated for 20 websites for each VPN. Then the data process is also repeated on captured data of traffic classification through VPN.

VII. FINGERPRINTING TECHNIQUES

In this experiment, we used Cai et al. [5] approach to assess the accuracy of website fingerprinting attack on five VPNs. Moreover, we used it for classifying different web services through VPN. Cai et al. developed an efficient website fingerprinting attack based on SVM. This approach takes specific types of input data files, named: X_N.txt where X is the website and N is the trial number. All combinations of X and N, where $1 \leq X \leq$ WebsiteNum, $1 \leq N \leq$ TrialNum, must exist in the folder, or the process cannot continue. The user can set website number and trial number. Other combinations are ignored. Each such file represents a traffic instance and it is a list of integers separated by newline.

Once the data file is read, it calculates the Damerau-Levenshtein edit distance [33], which is a string metric for measuring the difference between two sequences. It is the minimum number of single character edits (insertions, deletions, substitutions, transpositions) required to change one word into the other. The bigger the return value is, the less similar the two text are, because different words take more edits than similar words.

In Cai et al. work, the costs of insertion, deletion and substitution are the same, but they assign a lower cost to transpositions than others. After post-processing the input data, the training and testing are done based on SVM classifier. Finally it gives an output result with percentage accuracy.

VIII. RESULTS AND ANALYSIS

In this section, we show the results of our experiment and analyze them. Further discussion is given in Section IX.

A. Website fingerprinting through VPN

Popular VPNs differ in several aspects, in particular, they use different protocol and different packet sizes for same websites. The types of the protocol and packet sizes contain influences on the encrypted communication traffic. In order to compare the resistance of popular VPNs to website fingerprinting attacks, the visit of web traces have been collected using different VPNs and the traces of traffic are converted to the setup essential for the Cai's technique as mentioned in Section VII.

We evaluated the accuracy of website fingerprinting attack using the data of most popular five VPNs as shown in Table VI. The accuracy results of the experiment are illustrated in histogram shown in Figure 7. Avira Phantom has the best resistance to the attack with almost only 32% of website visit traffic recognized appropriately. The next best VPN in resisting this attack is Psiphon, with the accuracy of about 42%. Next come Softether VPN, with accuracy of around 50%. Finally, Hotspot Shield and OpenVPN have the highest levels of accuracy of 65% and 72% respectively, which implies that they are very vulnerable to Cai's technique. It states that almost three-fourth of the web site visits through OpenVPN can be detected successfully by this fingerprinting attack

TABLE VI. WEBSITE FINGERPRINTING USING CAI CLASSIFIER

Name of the VPNs	Classification Accuracy (%)
Psiphon	41.125%
Softether	49.75%
Hotspot Shield	65.00%
OpenVPN	72.00%
Avira Phantom	31.50%

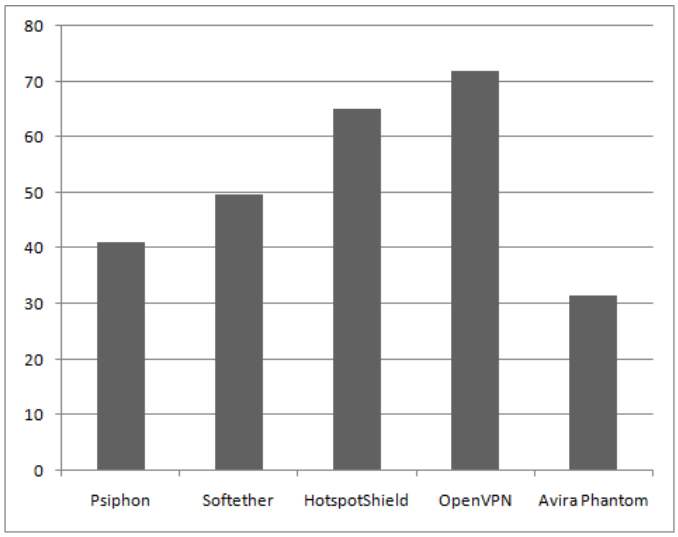

Fig. 7. Accuracy of the website fingerprinting attack on the five VPNs using Cai et al.

TABLE VII. EFFICIENCY OF THE WEB TRAFFIC CLASSIFICATION ESTIMATED WITH CAI ET AL.

Results	Classification Accuracy (%)
	68.75%
	81.25%
	84.375%
	84.375%
	87.50%
Average	81.25%

B. Web traffic classification through VPN

In order to classify between different web services, uses of different web service mentioned in Table V are collected using Psiphon VPN, and the traces of traffic are converted to the setup essential for the Cai's technique as mentioned in Section VIII. Different video Call communication, video Streaming, online gaming and Peer2Peer file sharing have been used through Psiphon VPN to collect data. We assess the accuracy of web services classification attack using the Psiphon VPN's data.

Table VII depicts the accuracy findings of the experiment on our diverse collected data. The average accuracy of traffic classification through VPN is around **82%**. It implies that 82% of different web services have been correctly classified. This traffic classification method has a great impact in the field of censorship. If any organization wants to block video streaming sites for their employees, this classification technique can be used to distinguish real web traffic and apply censorship on the contents. Although the user depends on VPN communications, our technique can successfully intercept and correctly detect with the high accuracy rate (over 80%).

IX. DISCUSSION

The purpose of this section is to discuss how different factors may effect the accuracy rate of our experiments.

A. Challenges of Data Storage

When the analysis is done in offline mode, maintaining the data storage of different websites is a real challenge. To maintain the huge signatures of each visited websites is both time and space consuming. On the other hand, discovering which web services are targeted is a complex assessment as it is not known to the internet service provider which service is suspicious.

B. Web Browsers Variety

Web browsers are numerous nowadays with various editions. Every browser can have special strategy about transmission of packets, which can take part in defense of consumer's privacy. Particularly, traces created by using a web service can have a different mark or signature, depending on the browser which was employed. This matter deserves a study on how security mechanisms are engaged by browsers activity. This study can facilitate in fingerprinting the browsers in the early period of investigation, and subsequently, investigate web services based on the resulting browser. During our investigation, we have observed that most fingerprinting techniques have been estimated under data collected from the Firefox web browser. Based on [32], the accuracy of fingerprinting techniques might be change if evaluated under data collected from different web browsers, given that browsers might contribute in preserving user's privacy. In our work, we used Google chrome which is the most secure [32]. The less secure browser may increase the vulnerability rates.

C. Diversity of Data Collection Ways

The majority of web fingerprinting techniques are performed on recorded traffic, in offline mode, in several phases. First, huge amount of data is collected. Then, data is filtered out and assessed in offline mode. In contrast, different fingerprinting techniques assess the traffic in online mode. Definitely, a fingerprinting approach will not generate the similar results if performed in these different traditions. In our work, we analyzed in offline mode. The traffic analysis in online mode may affect the results since the online mode is an unpredictable open world.

X. Conclusion

The web fingerprinting attack is an effective analysis attack on encrypted traffic. It is based on monitoring the manners of traffic for the purpose of finding out valuable patterns in the packets flow. Although Web fingerprinting attack is regarded as a harmful action, it can sometimes be beneficial and be used in beneficial ways, e.g., when government agencies and organizations may require to carry out a Web fingerprinting attack for homeland security reasons and cyber-crimes prevention.

This paper investigates the vulnerability of five different VPN services through website fingerprinting attack using Cai et al. approach. It shows that Open VPN is vulnerable with 72% accuracy rate. This means that if someone browses any websites through Open VPN, 72% websites can be traced successfully by the fingerprinting attack. Although the VPN communication is totally encrypted, it leaves traceable metadata that can be further analyzed to carry out the attack. The Open VPN has the highest vulnerability as compared to other studied VPNs. On the other hand, Avira phantom VPN is the least vulnerable with accuracy rate of 32%.

Moreover, we estimated efficiency of the web traffic classification through VPN for four different web services, namely: video streaming, online games, video call communications and peer to peer application with Cai et al. classifier. The result shows an accuracy level of almost 82%.

According to these results, we recommend avoiding the use of VPN whenever the service type is critical, since VPN is vulnerable to fingerprinting attack. However, other usages of VPN, like hiding identity of users and content of media are still protected. Moreover, government agencies need to develop more sophisticated attacks to retrieve high level information other than the types of the web services.

Acknowledgment

The authors would like to thank King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, for supporting this research.

References

[1] A. Thomas and G. Kelley, "Cost-effective vpn-based remote network connectivity over the internet," *Department of Computer Science, University of Massachusetts*, vol. 100, 2002.

[2] R. Venkateswaran, "Virtual private networks," *IEEE potentials*, vol. 20, no. 1, pp. 11–15, 2001.

[3] Y. Shi and S. Biswas, "Detecting tunneled video streams using traffic analysis," in *7th International Conference on Communication Systems and Networks (COMSNETS)*. IEEE, 2015, pp. 1–8.

[4] "Globalwebindex," www.globalwebindex.net.

[5] X. Cai, X. C. Zhang, B. Joshi, and R. Johnson, "Touching from a distance: Website fingerprinting attacks and defenses," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 605–616.

[6] R. Stanton, "Securing vpns: Comparing ssl and ipsec," *Computer Fraud & Security*, vol. 2005, no. 9, pp. 17–19, 2005.

[7] W. Li and A. W. Moore, "A machine learning approach for efficient traffic classification," in *15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*. IEEE, 2007, pp. 310–317.

[8] A. W. Moore and D. Zuev, "Internet traffic classification using bayesian analysis techniques," in *ACM SIGMETRICS Performance Evaluation Review*, vol. 33, no. 1. ACM, 2005, pp. 50–60.

[9] A. McGregor, M. Hall, P. Lorier, and J. Brunskill, "Flow clustering using machine learning techniques," in *International Workshop on Passive and Active Network Measurement*. Springer, 2004, pp. 205–214.

[10] S. Zander, T. Nguyen, and G. Armitage, "Automated traffic classification and application identification using machine learning," in *Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on*. IEEE, 2005, pp. 250–257.

[11] L. Bernaille, R. Teixeira, I. Akodkenou, A. Soule, and K. Salamatian, "Traffic classification on the fly," *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 2, pp. 23–26, 2006.

[12] J. Erman, A. Mahanti, M. Arlitt, and C. Williamson, "Identifying and discriminating between web and peer-to-peer traffic in the network core," in *Proceedings of the 16th international conference on World Wide Web*. ACM, 2007, pp. 883–892.

[13] G. P. S. Junior, J. E. B. Maia, R. Holanda, and J. N. de Sousa, "P2p traffic identification using cluster analysis," in *Global Information Infrastructure Symposium, 2007. GIIS 2007. First International*. IEEE, 2007, pp. 128–133.

[14] M. Perényi, A. Gefferth, T. D. Dang, and S. Molnár, "Skype traffic identification," in *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*. IEEE, 2007, pp. 399–404.

[15] E. P. Freire, A. Ziviani, and R. M. Salles, "Detecting skype flows in web traffic," in *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE*. IEEE, 2008, pp. 89–96.

[16] C. V. Wright, F. Monrose, and G. M. Masson, "On inferring application protocol behaviors in encrypted network traffic," *Journal of Machine Learning Research*, vol. 7, no. Dec, pp. 2745–2769, 2006.

[17] R. Alshammari and A. N. Zincir-Heywood, "A flow based approach for ssh traffic detection," in *IEEE International Conference on Systems, Man and Cybernetics*. IEEE, 2007, pp. 296–301.

[18] ——, "Machine learning based encrypted traffic classification: Identifying ssh and skype." *CISDA*, vol. 9, pp. 289–296, 2009.

[19] S. Leroux, S. Bohez, P.-J. Maenhaut, N. Meheus, P. Simoens, and B. Dhoedt, "Fingerprinting encrypted network traffic types using machine learning," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018, pp. 1–5.

[20] A. Hintz, "Fingerprinting websites using traffic analysis," in *International Workshop on Privacy Enhancing Technologies*. Springer, 2002, pp. 171–178.

[21] Q. Sun, D. R. Simon, Y.-M. Wang, W. Russell, V. N. Padmanabhan, and L. Qiu, "Statistical identification of encrypted web browsing traffic," in *IEEE Symposium on Security and Privacy.* IEEE, 2002, pp. 19–30.

[22] M. Liberatore and B. N. Levine, "Inferring the source of encrypted http connections," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 255–263.

[23] D. Herrmann, R. Wendolsky, and H. Federrath, "Website fingerprinting: attacking popular privacy enhancing technologies with the multinomial naïve-bayes classifier," in *ACM workshop on Cloud computing security.* ACM, 2009, pp. 31–42.

[24] Z. Zhuo, Y. Zhang, Z.-L. Zhang, X. Zhang, and J. Zhang, "Website fingerprinting attack on anonymity networks based on profile hidden markov model," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1081–1095, 2017.

[25] T. Wang and I. Goldberg, "Improved website fingerprinting on tor," in *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*. ACM, 2013, pp. 201–212.

[26] H. Jahani and S. Jalili, "A novel passive website fingerprinting attack on tor using fast fourier transform," *Computer Communications*, vol. 96, pp. 43–51, 2016.

[27] T. Pulls and R. Dahlberg, "Website fingerprinting with website oracles," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 1, pp. 235–255, 2020.

[28] Y. Shi and S. Biswas, "Characterization of traffic analysis based video stream source identification," in *IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)*. IEEE, 2015, pp. 1–6.

[29] ——, "Protocol-independent identification of encrypted video traffic sources using traffic analysis," in *IEEE International Conference on Communications (ICC).* IEEE, 2016, pp. 1–6.

[30] S. Feghhi and D. J. Leith, "A web traffic analysis attack using only timing information," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1747–1759, 2016.

[31] "Top visited website," http://www.alexa.com/topsites.

[32] S. Zhioua and M. Langar, "Traffic analysis of web browsers." in *FMS@ Petri Nets*. Citeseer, 2014, pp. 20–33.

[33] V. I. Levenshtein, "Binary codes capable of correcting deletions, insertions, and reversals," in *Soviet physics doklady*, vol. 10, no. 8, 1966, pp. 707–710.