IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 January 2022, accepted 25 February 2022, date of publication 22 March 2022, date of current version 31 March 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3161547

The Anonymity of the Dark Web: A Survey

JAVERIAH SALEEM, RAFIQUL ISLAM, (Senior Member, IEEE),
AND MUHAMMAD ASHAD KABIR, (Member, IEEE)
School of Computing, Mathematics and Engineering, Charles Sturt University, Albury, NSW 2640, Australia
Cyber Security Cooperative Research Centre, Bathurst, NSW 2795, Australia

Corresponding author: Javeriah Saleem (javeriahsaleem1@gmail.com)

This work was supported in part by the Cyber Security Cooperative Research Centre (CSCRC) through the Australian Government's Cooperative Research Centre's Program.

ABSTRACT The dark web is a section of the Internet that is not accessible to search engines and requires an anonymizing browser called Tor. Its hidden network and anonymity pave the way for illegal activities and help cybercriminals to execute well-planned, coordinated, and malicious cyberattacks. Cyber security experts agree that online criminal activities are increasing exponentially, and they are also becoming more rampant and intensified. These illegal cyber activities include various destructive crimes that may target a single person or a whole nation, for example, data breaches, ransomware attacks, black markets, mafias, and terrorist attacks. So, maintaining data privacy and secrecy is the new dilemma of the era. This paper has extensively reviewed various attacks and attack patterns commonly applied in the dark web. We have also classified these attacks in our unique trilogies classification system. Furthermore, a detailed overview of existing threat detection techniques and their limitations is discussed for anonymity providing services like Tor, I2P, and Freenet. Finally, the paper has identified significant weaknesses that make the dark web vulnerable to different attacks.

INDEX TERMS Attack taxonomy, crimes, dark web, Freenet, I2P, threat intelligence, Tor.

I. INTRODUCTION

As the 21st century is a digital era, more and more information is online. People can share information and connect with any part of the world with just a click. The web visible to an ordinary user seems like a vast knowledge resource, but it is just the surface web. In reality, there is a lot more to the Internet. The websites we access make up approximately 4% of the whole web [1]. The other 96% of the web is hidden and invisible. This invisible, deeply hidden, non-indexed web is generally named the deep web. However, the dark web, a subset of the deep web, is mainly used for illegal purposes [2]. We can better understand the magnitude of this problem by examining statistics. According to the literature, 57% of activities on the dark web are illegal, including data breaches, illegitimate drugs, pornography, human trafficking, and more [1]. A study conducted by the University of Surrey found the total revenue generated from cybercrimes in 2018 was approximately $1.5 trillion [3], and cybercrimes will become more frequent and aggressive over time.

For a long time, the Dark Web has existed beneath the surface of the internet. The US Department of Defense's started to develop the internet in the 1960s, driving to network their computer systems, but it wasn't until the 1990s that it became a household term. Most people were unaware of the Dark Web until 2013, when the Silk Road's operator, Ross William Ulbricht (alias D. P. Roberts), was imprisoned. The Silk Road was an underground marketplace for illegal goods and services operated on the Tor network [4].

The dark web, alternatively referred to as darknets or hidden services, is a subset of the deep web that is not indexed by search engines due to the specialized software required to access it. It has both public and private aspects, which means that anyone or only those with credentials can access it if the appropriate software is installed. The absence of accountability on the dark web is the primary distinction between it and the surface or deep web. Because users' actions are unidentifiable to the network or anyone watching them, they are essentially anonymous. Furthermore, the dark web allows for the hosting of online services (hidden services) that remain anonymous, even to the users, in terms of their true IP address and thus location. The dark and deep webs are distinguished

The associate editor coordinating the review of this manuscript and approving it for publication was Amin Zehtabian.

because unique technology-enabled protocols and anonymity distinguish the former.

In contrast, the latter is more reliant on authentication and thus lacks public access. Because both the deep and surface webs contain unauthenticated areas that are easily scanned by search engines, anonymity is not a feature either. The dark web has become an institutionalized intimate relationship between people by giving anonymity. Which also leads cybercriminals to do illegal activities on the dark web.

Dark web websites are mostly encrypted, which helps maintain the confidentiality of user identities and makes activities untraceable. Anonymity tools are based on overlay networks to help users communicate worldwide without revealing their identity or location [5]. Researchers have used overlay techniques in various fields such as anonymous emails, anonymous voting, communication censorship, private information retrieval, taxonomy, traffic analysis, etc. Many companies and developers provide anonymity services; some are commercial companies like anonymizer.com or gotrusted.com, whereas others are open-source developers like Tor, FreeNet, Subgraph O.S., and the invisible Internet project I2P [6]. Websites in the dark web are referred to as onion sites or hidden services that are only accessible through browsers like Tor, Riffle, I2P, and Whoinx, etc. Tor is the most robust unidentified communication tool among them. It has a broad user base as it allows users to dodge hostile government surveillance activities by providing secrecy [7].

I2P is popular as it is a distributed control system, which makes it more anonymous. Our goal is to see the different aspects of the three most popular dark web systems: Tor, I2P, and Freenet. Although there are surveys available on anonymous networks [8]–[10], [1], [11]–[13], [6], [14], there is no comprehensive survey of the complex deanonymizing attacks on the dark web and threat intelligence techniques – that is the focus of this study.

This survey aims to assess the current state, usage, and growth of the dark web. We have described the dark web's anonymity, its weak points, and how various cyberattacks can breach this anonymity. We have also surveyed threat intelligence techniques, their efficiency, and limitations in attack detection and generation of adequate response. More specifically, investigation of the following questions is under focus in this project: i) How and what level of anonymity is provided by Tor, I2P, and Freenet? ii) What significance does the dark web have in cybercriminal activities and operations? iii) What are the known threat intelligence techniques to detect cybercriminal activities, and how should we categorize these techniques? iv) What is a possible attack pattern to deanonymize Tor, I2P, and Freenet? This paper is important as a compact package covering all the different areas of the dark web and provides insightful information about it. Prior to this, no such comprehensive paper covering all the basic areas of understanding the dark web existed. This deficient hole in the existing literature served as the motivation to write this paper. This research is the baseline for developing a prototype to detect cyberthreats and generate an adequate response.

The main contributions of this paper are as follows:

- We have conducted an extensive analysis of the dark web threat intelligence literature.
- We presented a comparative study of the existing anonymity tools with their pros and cons.
- We have proposed a novel and detailed threat taxonomy for the Tor network.
- A discussion on existing counterattacks is also included.
- We have also outlined future research directions.

A. BACKGROUND

Under this segment, we focus on providing background information on the attack's taxonomy in the dark web. Table 1 presents a summary of related work focusing on the relevance and significance of the research. For example, Salo [15] proposed a survey and categorized 14 Tor attacks into five categories: 1. probabilistic models based on mathematical modelling that provide information about the network, 2. onion router selection attacks that attempt to compromise the victim's entry and exit nodes, 3. Autonomous System (AS) and global level attacks by a passive global adversary, 4. traffic and time analysis attacks and 5. protocol vulnerabilities address weaknesses in the Tor protocol. On the other hand, Salo's work ignores website fingerprinting attacks against Tor.

Nepal *et al.* [14] presented Tor hidden services deanonymization scheme by categorizing attacks on HS as cell manipulating, padding, and count-based method. Nepal *et al.* describe the basic functioning of these assaults and compare the attack strategies in terms of the simulated environment, the time necessary for de-anonymization, the true positive rate, and the number of compromised nodes needed to launch the attack effectively. The same year Erdin *et al.* [6] presented a survey of attacks on I2P and Tor by categorizing almost 18 attacks into application-level and network-level attacks. Application attacks can be controlled as they mainly occur due to the carelessness and unawareness of the users. In contrast, network-level attacks arise either because of the network constraint or the up-gradation tradeoff. The author categorizes network attacks into intersection, flow multiplication, fingerprinting, timing, and congestion attacks. In contrast, Yang *et al.* [16] introduced single hop and multiple hop communication models and deanonymizing techniques in two dimensions: firstly, active/ passive, secondly, single-end and end-to-end attacks. They also suggested counter-measurement techniques deployed on three layers, network, protocol, and application.

Alsabah and Goldberg [13] provided a survey on the Tor network's performance and security aspects in different areas, including Tor architecture, traffic management, route selection, scalability, circuit construction, and Tor attacks. Alsabah explains 22 Tor attacks into active, passive categories, which are further subdivided into different classifications.

They also explain the threats and challenges facing in Tor. The same year, Evers *et al.* [10] presented a thirteen-year

TABLE 1. Significance of related survey articles (legend: √ means covered; × means not covered).

	Focus								**Idea**
			Attacks						
Researcher	**Crimes in the Dark Web**	**Threat Intelligence Techniques**	**Number of Attacks**	**Categorization of Attack**	**Anonymous Network Discussed**	**Counter Attacks**	**Attack Detection**	**Measurements**	
S. Saleh et al. [8]	×	×	23	Not mentioned	Tor	×	×	√	Deals with the survey, classification, quantification, and comparative analysis of research work on Tor
S. Kaur et al. [9]	√	×	11	Not mentioned	Tor, FreeNet, Whonix, I2P. TAILS, Sub graph O.S.	×	×	×	Overview of the attacks, exploits browsers, and crimes of the dark web
B. Evers et al. [10]	×	×	84	Seven groups and two types of active, passive attacks	Tor	×	√	√	Discussed and categorize Tor attacks They discussed Tor's ethical vulnerabilities
E. Cambiaso et al. [12]	×	×	17	Client-server network	Tor	×	×	×	Tor attack categorization
J. Salo et al. [11]	×	×	18	Five categories: Probabilistic model, entry and exit, onion router selection attack, AS and global level attack, traffic, and time-based attacks, Protocol vulnerabilities	Tor	×	×	×	Introduce and sort the attacks into five categories
I. Karunanayake et al. [17]	×	×	50	Categorized Tor attacks into entry/ exit, sever, side-channel and hybrid with active-passive classification	Tor	×	×	√	Provides survey on Tor attacks and countermeasures

TABLE 1. *(Continued.)* Significance of related survey articles (legend: √ means covered; × means not covered).

Alsabah et al. [13]	×	×	22	Classify active attacks as side-channel attacks, path selection attacks, and end-end confirmation attacks. Whereas passive attacks as fingerprinting and AS level adversary attacks	Tor	×	×	√	Survey on performance and security of Tor
E. Erdin et al. [6]	×	×	18	Categorize all attacks as application-level and network-level attacks	Tor, I2P	×	×	×	Provides a survey of attacks on Tor and I2P
S. Nepal et al. [14]	×	×	3	Categorize H.S. attacks as cell manipulating, padding, and count-based method	Tor	×	×	×	Survey on Tor hidden services deanonymizing schemes
M. Yang et al. [16]	×	×	6	Classified as active/passive single end and end-end attacks	Tor	×	×	√	Provided single-hop and multi-hop anonymous communication models.
M. Mohd et al. [18]	×	×		Analysed the literature based on attack type and attack target	Tor	×	×	×	Analysis of paradigm of attack studies on Tor
O. Catakoglu et al. [5]	×	×	6	Classified attacks in scattered, automated, and manual attacks	Tor	×	×	×	Real-time attacks detection through honeypot
S. Nazah et al. [1]	√	√	×	×	×	×	×	×	Presented crimes of the dark web
G. Cascavilla et al. [19]	×	√	×	×	×	×	×	×	Presented a taxonomy of threat intelligence techniques for surface web and dark web
Our Survey	√	√	34	Active/passive attacks targeted on client-server and the Tor network	Tor, I2P, Freenet	√	√	√	Discusses the attacks on Tor, I2P, and Freenet and threat intelligence techniques in the dark web

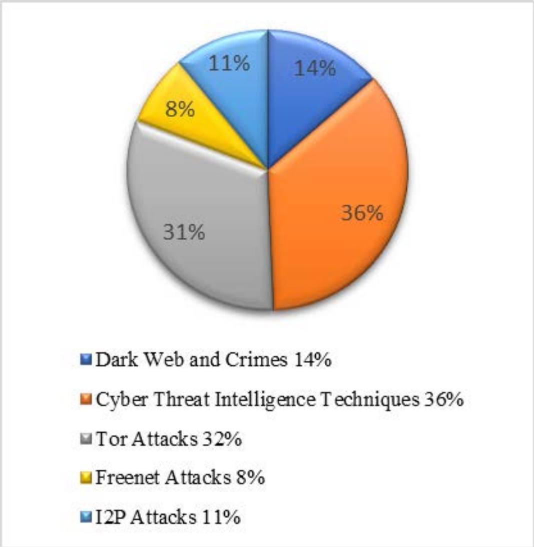

FIGURE 1. **Classification of literature surveyed.**

attack survey that classifies 84 attacks into correlation, DoS, Congestion, Timing, Supportive, Fingerprinting, and HS revealing attacks. They also reported some countermeasures in their survey.

Saleh *et al.* [8] presented a literature survey that deals with classification, quantification, and comparative analysis of research work on Tor. They classified the literature into three broad categories: deanonymization, path selection, analysis, and performance improvement. Saleh discussed 23 attacks but could not provide any attack categorization and missed some popular attacks like raptor and Sybil attacks.

Cambiaso *et al.* [12] analyzed the Tor attacks and categorized them as per the target of the attacker client, server, network, and generic attacks. Attacks on servers target the hidden services attacks, while attacks on the network are considered attacks targeting the route or the bridge discovery attacks. Whereas in the generic category, all the attacks targeting more than one target are included. Cambiaso discussed 18 attacks in the Tor network. We referenced work in combination with the active, passive nature of the Tor attack. We developed a unique trilogy of attack taxonomy that explained and categorized all the attacks occurring in different anonymity browsers.

Recently there is some more work presented to discuss Tor attack taxonomy. Karunanayake *et al.* [17] introduced 50 Tor deanonymization attacks in 2020 into four categories. Those are entry-exit onion router attacks, server attacks, hybrid and supportive attacks, and the attack's active-passive nature.

Sulaiman [11] presented different types of unpopular Tor attacks. Sun *et al.* [20] discussed the raptor attacks which the autonomous system can launch to deanonymize the user. Barbera *et al.* [21] discussed the methodology, accessing the resources, and effect of cell flood attacks on the Tor network. Casenove and Miraglia [22] analyzed the botnet's infrastructure and how the botmasters use them in the Tor network. Kaur and Randhawa [9] also mentioned 11 Tor attacks in their work but was unable to provide any attack categorization in the network. Basyoni *et al.* [23] examined traffic analysis attacks from the perspective of threat models and the practicality of these attacks in real-time. They discussed three traffic attack models, which are 1) global adversary model, 2) capturing entry flow, and 3) compromising Tor's relays.

Whereas I2P protects against several attacks such as Brute force attacks, Timing attacks, Tagging attacks, Predecessor attacks, Harvesting attacks, Cryptographic attacks, Development attacks, and implementation attacks [24]. To deanonymize the I2P network, some researchers presented a few attacks [25]–[28], which will be explained in the later sections. Tian *et al.* [29], [30] and Baumeister *et al.* [31], [32] have significant contributions in presenting the attacks and counterattack techniques in the Freenet.

We have analyzed and reviewed their work and have tried to simplify and unify various attacks and attack patterns. A single attack was categorized differently by different researchers. We came up with our unique classification system to mitigate this problem, unifying various classification models already existing and explained by multiple researchers. It's an attempt to make things easy and straightforward. With this classification, one can understand whether the attack is client, server, network-level, active or passive, single-end or end-to-end. Understanding these features also aids in comprehending attack operations and workings.

B. LITERATURE REVIEW SCOPE

This article aims to review and present a comprehensive analysis of the anonymity of the dark web, featuring its key areas. We have briefly described the anonymity of the dark web tools, crimes in the dark web, threat intelligence techniques to detect crimes and lastly, attacks on the dark web with their counterattack techniques.

Identifying and organizing the most pertinent literature on the subject is a significant initial challenge for the literature review. Our primary goal was to collect the literature and collectively give an overview of threats, their implementation, and the pattern of attacks followed by cybercriminals, which could help identify the baseline for researchers to design a prototype to mitigate such threats. The approach to this was to search with keywords in central databases, go back and forth, i.e., to review citations and review material citing those critical articles.

To gather the literature for our analysis, various databases and journals are used to collect academic indexed literature, namely IEEE Xplore, ACM digital library, Scopus, Springer, Science Direct, and Google Scholar. The broad keywords initially used in the searches were "dark web" or "darknet," as these terms referred to the investigation's central concept. The most popular dark web browser was added in the search, and thus the keywords "Tor," "I2P," and "Freenet." The search was restricted to articles published between 2011 and 2021. The themes of interest were then specifically searched for alongside the main keywords ("dark web, Tor, I2P, Freenet") by adding keywords such as "markets," "cybercrime," "Tor

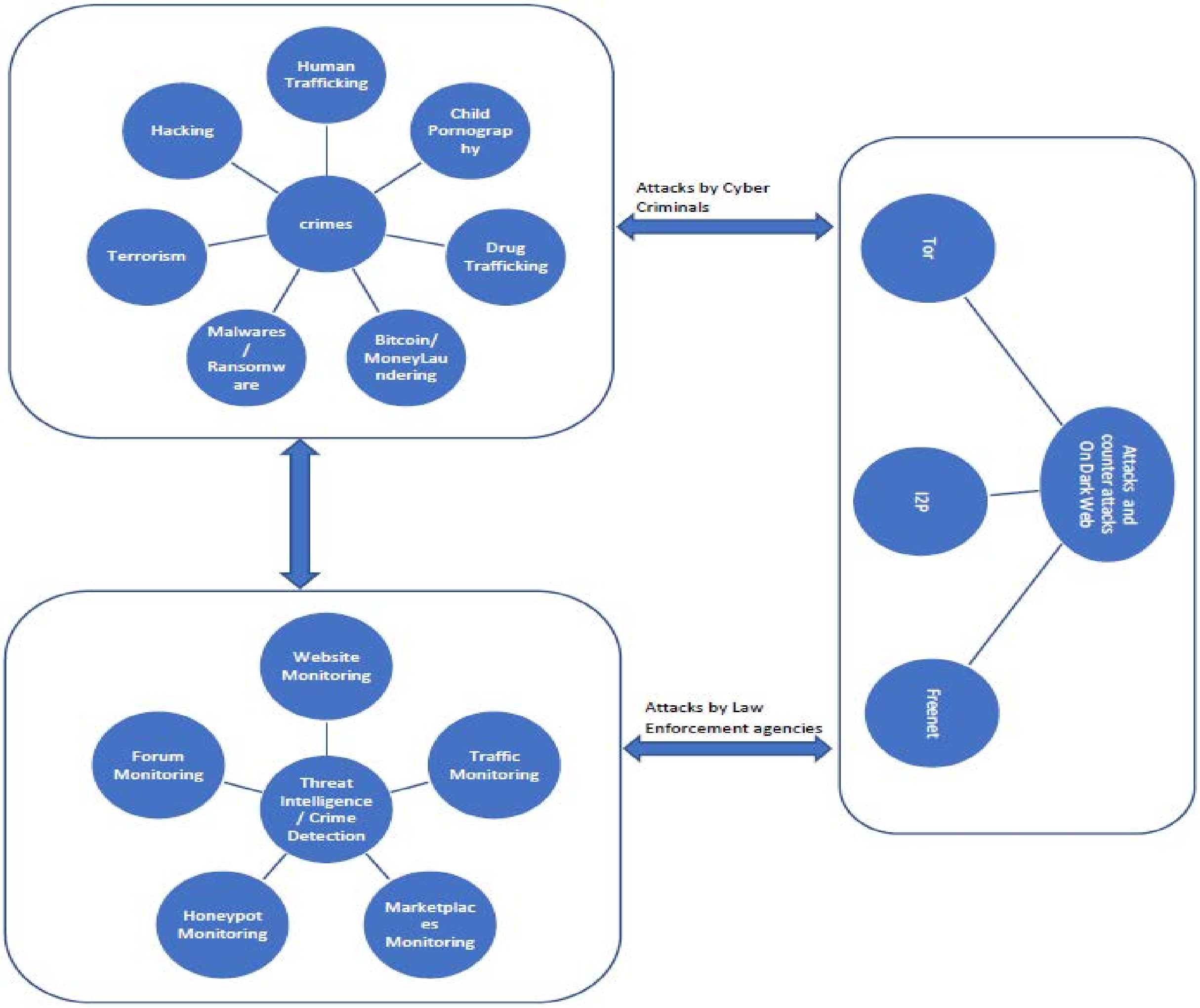

FIGURE 2. Research architectural framework.

hidden services,'' ''threat intelligence techniques,'' ''attack pattern,'' ''threat landscape,'' ''anonymity OR deanonymization'' one at a time. These different keywords were added to allow for a more in-depth discussion of each aspect of the topic. This keyword search had yielded a list of 150 journal articles and conference papers.

The lists have identified the documents published in leading journals through the journal ranking by CORE 2020. Papers were then filtered manually for greater relevance by selecting only those focused on the topics and peripherally relevant. The final list was composed of 79 articles categorized in 5 different areas mentioned in Figure 1. In our review process, almost 50% of our literature review focuses on attacks, 36% on threat intelligence techniques, and 14% on the dark web's anonymity and crimes taking place in the dark web. However, there is a lack of literature on mitigating techniques against those attacks.

Figure 2 presents the entire architectural perspective of the literature surveyed. It should be noted that in this framework, many elements are not restricted to what is depicted in the Figure 2. We have broadly classified this reviewed literature under three main categories which are elaborated in Figure 2. The first category discusses the anonymity of the dark web and crimes occurring because of this anonymity. We have mainly focused on the anonymity of Tor, I2P and Freenet in the dark web. The second category examines the detection approaches for crimes, and the third category discusses the attacks on the dark web. These attacks are made mainly by the two groups of people; one group by law enforcement (LE) agencies to deanonymize the criminals and the second group by the criminals to do malicious activities like hacking, ransomware and information leakage etc. Human and drug trafficking, child pornography, Terrorism, bitcoin and money laundering are also included.

C. ORGANIZATION OF THE PAPER

The paper is organized as follows; Section II presents the literature review on the dark web, including its architecture, crimes, and a comparison of different anonymity

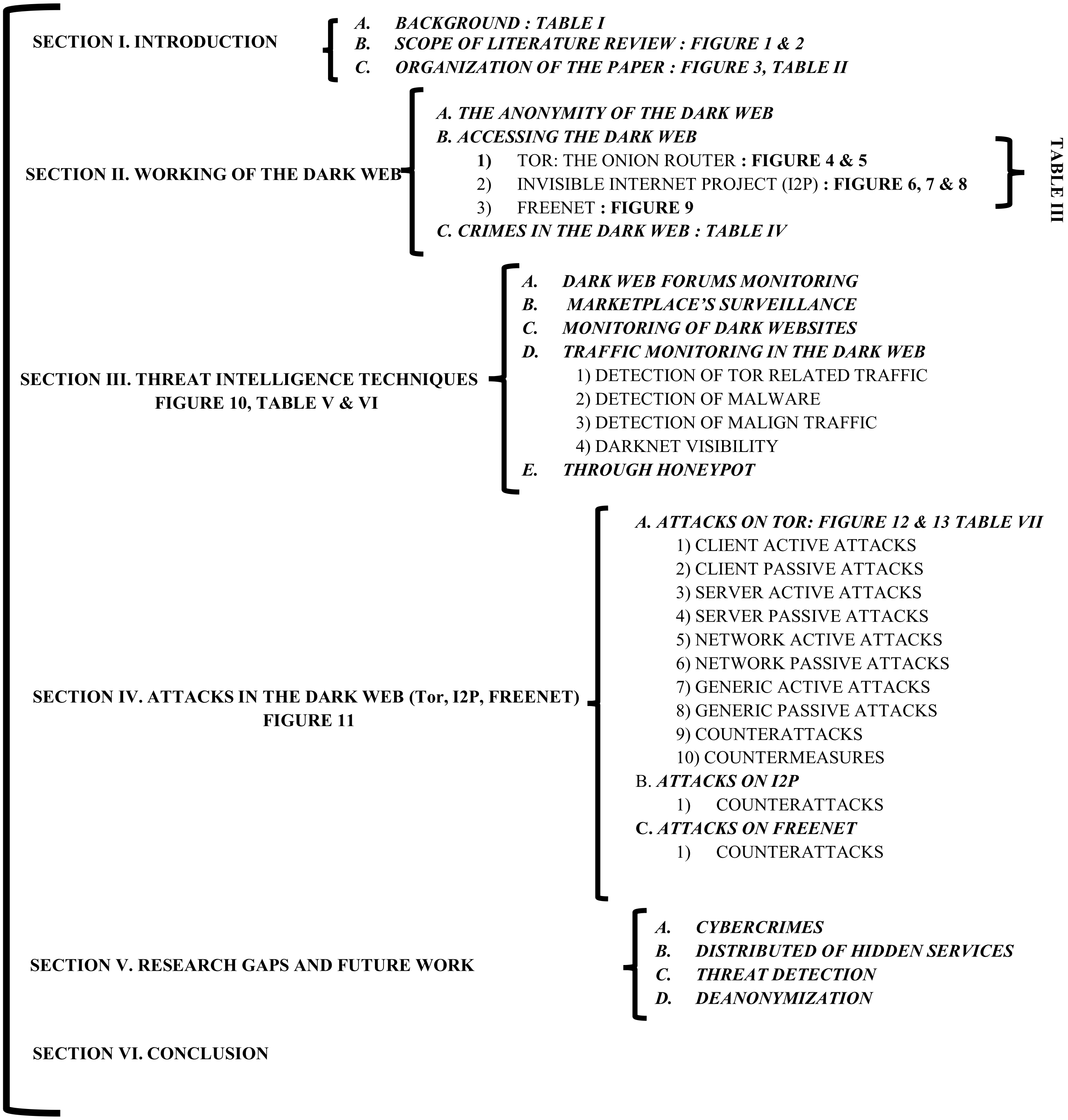
SECTION I. INTRODUCTION
A. BACKGROUND : TABLE I
B. SCOPE OF LITERATURE REVIEW : FIGURE 1 & 2
C. ORGANIZATION OF THE PAPER : FIGURE 3, TABLE II
SECTION II. WORKING OF THE DARK WEB
A. THE ANONYMITY OF THE DARK WEB
B. ACCESSING THE DARK WEB
1) TOR: THE ONION ROUTER : FIGURE 4 & 5
2) INVISIBLE INTERNET PROJECT (I2P) : FIGURE 6, 7 & 8
3) FREENET : FIGURE 9
TABLE III
C. CRIMES IN THE DARK WEB : TABLE IV
SECTION III. THREAT INTELLIGENCE TECHNIQUES
FIGURE 10, TABLE V & VI
A. DARK WEB FORUMS MONITORING
B. MARKETPLACE'S SURVEILLANCE
C. MONITORING OF DARK WEBSITES
D. TRAFFIC MONITORING IN THE DARK WEB
1) DETECTION OF TOR RELATED TRAFFIC
2) DETECTION OF MALWARE
3) DETECTION OF MALIGN TRAFFIC
4) DARKNET VISIBILITY
E. THROUGH HONEYPOT
SECTION IV. ATTACKS IN THE DARK WEB (Tor, I2P, FREENET)
FIGURE 11
A. ATTACKS ON TOR: FIGURE 12 & 13 TABLE VII
1) CLIENT ACTIVE ATTACKS
2) CLIENT PASSIVE ATTACKS
3) SERVER ACTIVE ATTACKS
4) SERVER PASSIVE ATTACKS
5) NETWORK ACTIVE ATTACKS
6) NETWORK PASSIVE ATTACKS
7) GENERIC ACTIVE ATTACKS
8) GENERIC PASSIVE ATTACKS
9) COUNTERATTACKS
10) COUNTERMEASURES
B. ATTACKS ON I2P
1) COUNTERATTACKS
C. ATTACKS ON FREENET
1) COUNTERATTACKS
SECTION V. RESEARCH GAPS AND FUTURE WORK
A. CYBERCRIMES
B. DISTRIBUTED OF HIDDEN SERVICES
C. THREAT DETECTION
D. DEANONYMIZATION
SECTION VI. CONCLUSION

FIGURE 3. Outline of this paper.

networks. Section III presents current threat intelligence techniques, their successes in attack detection, and their strengths. Section IV highlights the categorization of cyber-attacks in different networks, including our unique 'trilogies classification' in the Tor network. Counter-attacks and counter-measures to prevent the networks from these attacks are also described. Section V refers to the research gaps and future work to make the dark web a safer network for regular users and retain it from criminals. Finally, Section VI presents the conclusion of the whole research. Figure 3 depicts the complete outline of the paper, including the literature reviewed and its presentation in the form of figures and tables [33].

II. WORKING ON THE DARK WEB

Many people think that all the Internet is accessible through Google or any other search engine. In reality, a large Internet section is not indexed and cannot be accessed with standard browsers. The world wide web has three layers, which are:

TABLE 2. List of acronyms.

AS	Autonomous System
ASD	Average Shortest Distance
BP-HMM	Beta Process Hidden Markov Model
BGP	Border Gateway Protocol
C&C	Command-And-Control
CHK	Content-Hash Keys
CSCRC	Cyber Security Cooperative Research Centre
D2WEB	Deep Dark Web
DHT	Distributed Hash Table
DGA	Domain Generation Algorithms
DNS	Domain Name System
DS	Directory Server
GOZ	Gameover Zeus
GUID	Globally Unique Identifier
HDFs	Hadoop-Based Frameworks
HMM	Hidden Markov Model
HS	Hidden Services
HSDs	Hidden Service Directories
I2P	Invisible Internet Protocol
IP	Internet Protocol
ISPs	Internet Service Providers
IP	Introductory Point
LE	Law Enforcement
LDA	Latent Dirichlet Allocation
ML	Machine Learning
NetDB	Network Database
OP	Onion Proxy
OR	Onion Router
P2P	Peer To Peer
RPO	Rendezvous Point
SSK	Signed-Subspace Keys
SNA	Social Network Analysis
SVM	Support Vector Machines
TLS	Transport Layer Security
TCP	Transport Control Protocol
UDP	User Datagram Protocol
Tor	The Onion Router
VM	Virtual Machine
VoIP	Voice Over I.P
VPN	Virtual Private Network
ZBOT	Zeus Botnet

A. SURFACE WEB

An everyday Internet user believes that the Internet and the web are the same. But in reality, the web is a sub-section of the Internet to access information over the Internet. The web that conventional search engines can access like Google is the "Surface Web" [16] or "Clear Web" [17].

B. DEEP WEB

As reviewed by the literature, the deep web is the web layer that is not indexed. So, the data and information on these websites are not accessible by standard search engines. Information on the deep web is usually static, and different pages are linked together to fulfil the requirement. Research reveals the total volume of the deep web is uncertain. The deep web is estimated to be 4000–5000 times more than the surface web and is continuously expanding [16]. The interesting point is that the deep web has content from private, corporate, government, and some educational as well.

C. DARK WEB

If someone can dive deeper into the deep web, the next layer is the dark web, where data is intentionally hidden. Only purpose-oriented groups, through special techniques, can gain access. The content is given access only where desired (this could be HTML pages or any assets or files); the primary reason is anonymity. There are two essential distinctions from the deep/regular web -

- First: Non-indexed search engines of the dark web.
- Second: Dark web information/content is not accessible using a standard web browser [6].

It is not clear to what extent the dark web occupies the deep web [16]. Still, it is evident that some illegal activities routinely occur within the dark web, such as child pornography, phishing, scams, fraud, hacking, human trafficking, etc. Exact figures are not known yet [8].

1) THE ANONYMITY OF THE DARK WEB

Below is an overview of different techniques commonly used to achieve anonymity and confidentiality in the dark web.

Proxy: This is a service for filtering and bypassing. It is a gateway between the user and the Internet. It separates the end-user from the website by working as an intermediary server.

Virtual Private Network: This is a private network used to build a secretive "tunnel" from a device to the Internet. Encryption techniques are used to hide the user's vital data. It can be paid for through a personal VPN provider, Paid Nord, or Phantom VPN so, Internet users cannot be tracked [8].

Domain Name System Based bypassing: Regular browsers are programmed to use indexed websites through a DNS index (which converts the domain name to I.P. addresses). DNS makes it convenient to access Internet resources. Dark websites bypass DNS-based indexing, so the dark web and the regular web cannot cross-pollinate.

Onion Routing: Provides anonymous connections by encryption during transmission; messages are encrypted in layers, like some onion layers; thus, it hides the identity of the client and server. It is a crucial feature in the dark web [8].

2) ACCESSING THE DARK WEB

An essential component of the dark web is browsers. Websites are hosted in an overlay network technology in the dark web, which is not accessible without special-purpose browsers like Tor (The Onion Router) or I2P (Invisible Internet Project), Freenet, Riffle, and subgraph O.S., etc. Tor is the most widely used browser as it is easy and ready to use with a fully configured Firefox browser. Its most important aspect is the hidden or onion service that keeps users anonymous. The client cannot identify the service provider and the service provider cannot determine its client.

a: TOR: THE ONION ROUTER

The Onion Router (Tor) was initially released as a project; by the U.S. Naval Research Laboratory in 2002. They created it as a tool for anonymous online communication. Although many professional privacy and anti-censorship tools are freely available on the Internet, Tor is the most robust and widely used unidentified communication web. Its unique feature avoids relaying access to encrypted data using the onion layer protocol [18]. It also provides its users with low latency by not changing packet timings or sizes. However, as a result, it poses a threat to anonymity if someone can observe the traffic both ways.

There are possibly two ways for someone to sneak into Tor traffic: compromising relays or manipulating the primary network and Internet Service Providers (ISPs), which are large Autonomous Systems (ASes).

The architecture of Tor contains the *onion proxy (O.P.), onion router (OR),* and *directory server (D.S.)* as its three components [1]. The O.P. takes the latest relay/router information from directory servers. Users can select specific routers by using O.P. [19].

Tor works based on an overlay network, and each relay has to maintain a Transport Layer Security (TLS) connection. Tor establishes a random pathway using *Circuit* by selecting OR's entry. D.S. contains information on all available ORs [7].

1) *Guard & Middle Relay*: This relay must be fast and stable. The middle relay cannot act as a guard or exit relay.
2) *Exit Relay*: Selected on the criteria of weighted random selection. The last relay of a Tor Circuit guides traffic to the destination.
3) *Bridge*: If Tor relays are blocked by attack or a government, Bridge exists with D.S. using an underground group of three relays. Onion relays only have their immediate predecessor and successor node in an established connection.

TOR PROTOCOL

To maintain anonymous communication between the client and server, Tor follows the following protocol, shown in Figure 2.

- The client will send an HTTP request to D.S. for information about ORs.
- O.P. will select three ORs (guard, middle, and exit relays) using the Tor selection algorithm.
- O.P. will send "create cell request" to the guard node, which replies with the key1 hash.
- Then an extended cell request is sent by O.P. to the entry relay, which already has the address, encryption key2. This request then goes to the middle-relay, and the middle relay responds with "create cell and hash of the negotiated key," and the process continues till the exit relay replies with "created cell and hash of the key3."
- O.P. gets access to three encryption keys, which encrypt the message three times and wrap it under three layers.

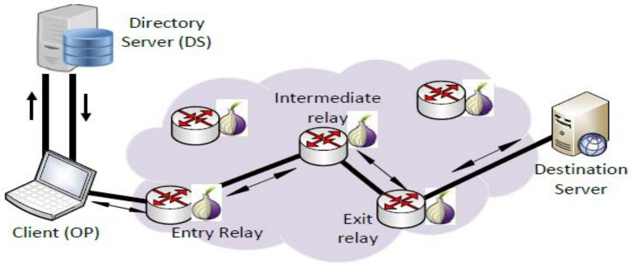

FIGURE 4. Tor architecture [7].

First, O.P. constructs a packet containing source and destination I.P. addresses of exit, and the Destination Server encrypts the packet with key3. It includes the middle and exit relay's source and destination addresses.
- Next, encryption is with key2 and the source-destination address of the entry and middle relay.
- Finally, the packet is encrypted with key1 and the source-destination address of O.P. and the entry relay.
- The encrypted message is sent to the entry relay, where the message is decrypted using key1 and forwarded to the middle relay.
- The middle relay then decrypts the packet with key2 and forwards it to the exit node.
- The exit node decrypts the packet with key3 and a "get a request for YouTube," passed to the destination servers.
- The destination servers complete the requests; the whole process is in the reverse direction of O.P. with encryption layer by key1, key2, and key3 that reaches the client [8].

In this scenario, relays seem in one hop as a circuit; hence no one can trace communication between the source and destination. Since only one exit point is sending the information to the destination, the Target Server cannot have an idea of the source, only the exit point.

HIDDEN SERVICE PROTOCOL

Hidden services inbound connections help provide anonymity in Tor. It connects itself to the client circuit, and hidden service is made accessible via an onion address. H.S. is a remote server for these services, which hosts them inside Tor. The Directory Server (D.S.) has all the details of relays as mentioned above; the client elects the Rendezvous Point (RPO) and uses it for data transmission to a remote server, whereas the Introductory Point (I.P.) is the Tor relays chosen by the H.S. to connect with the clients.

- A set of relays in the H.S. works as its I.P. (A Figure 5).
- This protocol generates the hidden service descriptor with a public key and its I.P., inserted by using an address like *ABC. Onion* into Distributed Hash Table (DHT) (B in Figure 5).
- A *.onion* address contacts the H.S. with clients (C in Figure 5).
- The descriptor is executed in Tor using these Hidden Service Directories (HSDs). The client gets the *.onion* address using a descriptor to create a new virtual circuit

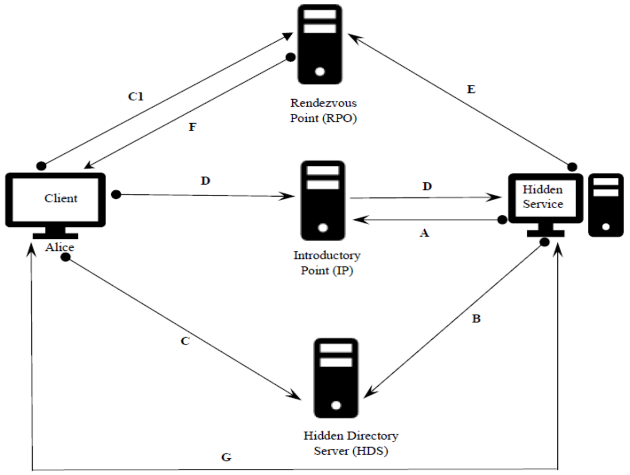

FIGURE 5. Tor hidden service architecture [37].

to some random relay, making it a rendezvous point (C1 in Figure 5).

- The client uses I.P. to inform the hidden service about the RPO (D in Figure 5).
- Finally, the H.S. produces a virtual circuit for the RPO and communication stats (E in Figure 5).

Hidden service may get exposed in standard Tor design if someone pedals any edge of the circuit by traffic confirmation and pattern observations. This way, the attacker confirms two parties are still communicating. Thus, guard nodes help to mitigate that risk in Tor. In a circuit, special relays select entry guards at random. Unfortunately, even with entry guards, weaknesses still exist. A completely secure system is not suitable. Although Tor is not foolproof yet, anonymity is good enough [38].

b: INVISIBLE INTERNET PROJECT (I2P)

I2P is a low latency, anonymous, message-oriented relay network centred and based on P2P networks. These peers can be nodes, relays, or routers. The I2P provides anonymity in file sharing, emails, and web hosting and sharing. Its architecture depends on garlic routing protocol tunnels, address books, and network databases.

- *Garlic routing*: When multiple messages are encapsulated into an encrypted data packet called "garlic." The message inside that packet is called a "clove."
- *Tunnels* are of two types used by an I2P client to communicate: "inbound" and "outbound." The first one is to receive messages while the other is to send messages. Each of them has two hops, a gateway, and an endpoint. Figure 6 illustrates a single request, and its response requires four tunnels between two parties. According to the required anonymity, these tunnels can be configured with up to seven hops. In contrast, one new tunnel is formed within 10 minutes [39].
- *The address book* channels the identity of the application provider and its domain name. A unique identifier of 512-byte base 64 encoded is generated for every user, which is called the destination on joining this system.
- *The Network Database* or NetDB, stores the router info and leaseset. Routerinfo is a structure that keeps critical information regarding an I2P router required for communication between the nodes. It also holds the public key and address of the I2P routers. In comparison, Leaseset contains lease information, gateway information of the destination, gateway information of the inbound tunnel, address, and tunnel I.D., including tunnel expiration time [40].

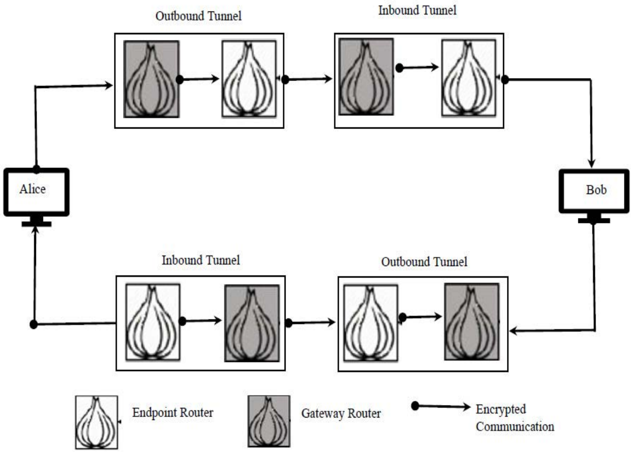

FIGURE 6. I2P architecture [25].

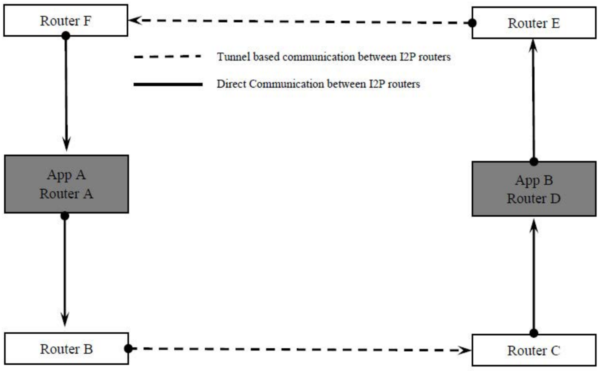
Router F
Router E
Tunnel based communication between I2P routers
Direct Communication between I2P routers
App A
Router A
App B
Router D
Router B
Router C

FIGURE 7. I2P Protocol [28].

I2P PROTOCOL

Figure 7 illustrates a communication between applications App A and App B through the I2P protocol. To establish an anonymous I2P communication, the I2P will follow the protocol as:

- According to Figure 7, A routes to the inbound tunnel with router F, the gateway to receive data, and router B is the endpoint to the outbound tunnel.
- App B uses router C as an inbound tunnel with an outbound tunnel to router E as the endpoint.
- In the leaseset (destination, encryption keys, a signing key, data receiver gateways list), App A comprises F, and

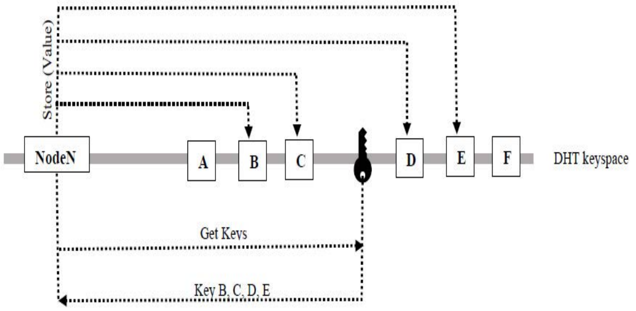

FIGURE 8. KAD based key sorting [28].

the I2P router is a gateway. In contrast, for App B, the leaseset uses the I2P router C as the gateway.

- The NetDB is a distributed table based on Kademlia containing *floodfill* nodes. Floodfill peers are I2P routers with high bandwidth. Figure 8 explains this procedure, where node N stores data and a key value. In the first step replica set, nodes close to the key-value are retrieved. In Figure 8, nodes B, C, D, and E are replica sets. A store message is sent to these nodes in the second and last step. The NetDB also works parallel to this manner, where metadata, leasesets, or router info are stored [28].

c: FREENET

Freenet is a system that distributes data publicly. The aim is to provide privacy, particularly for whistle-blowers and activists. Hence, the identity of content providers and subscribers is kept hidden to shield them from any persecution. Due to anonymity, terrorists may also use it to attack, gain authority, and dodge law enforcement agencies.

Freenet is an anonymous peer-to-peer network, which offers anonymity for data publishers and retrievers. A user allocates some part of their hard disk in this system and shares it as a distributed storage system. While the privileges like insertion, retrieval, and deletion are at the discretion of the Freenet system itself, that allocated location of the shared file is determined by a unique routing key associated with it. Thus, each peer in the Freenet has information about their adjacent neighbours. Moreover, rewriting the source of messages at each peer and hop-by-hop forwarding of user messages incorporates Freenet's anonymity.

There are two operational modes in the Freenet *Darknet*, where only trusted people can connect, and *Opennet,* where anyone can get connected [41].

Privacy is maintained using a mix-net scheme by Chaum for mysterious communication. Messages fold away by P2P chains, while it encrypts links unless the message reaches the recipient. The endpoints could be anywhere among the networks. Even nodes are continually exchanging indecipherable messages. Through this structure, information producers and consumers are protected.

Participants provide storage space in the network to add a new file and an insert message sent by the user in the network, containing the file with its assigned location-independent globally unique identifier (GUID). A file migrates from node to node to replicate during its life. The file is retrieved by request using the GUID key. This request is forwarded to the originator by the file's current storage node.

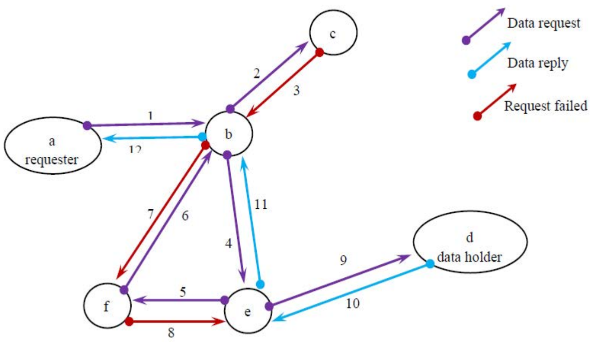

FIGURE 9. File requesting protocol in Freenet [42].

GUID Keys: These keys are calculated using the SHA-1 hash algorithm. Two types of keys are used; content-hash keys for primary data storage and signed-subspace keys envisioned for higher-level human use. These two are considered parallel to nodes and filenames in a conventional file system.

Content-Hash Keys: A CHK is a low-level data-storage key and is generated by the hashing of the stored file. This way, every file gains a unique identifier that is also verifiable. A CHK reference is specific and points to the concerned files only. It ensures merging the exact copies of a file as everyone has the same key in the network.

Signed-Subspace Keys. An SSK is used for the personal namespace, which is readable to all, but only its owner has the privilege to write. Indirect files pointing to CHKs are stored using these keys. These files are combined with readability, authentication of SSKs, and fast verification of CHKs. Referential integrity can also be updated with these keys.

FREENET PROTOCOL

In Freenet, nodes maintain the routing table and the GUID keys. The message is bounced back if a node is already in the chain and sends the request again [27]. If any node runs out of candidates, a failure report is sent back to the predecessor node in the chain and then tries its alternative. The file requesting algorithm follows the steps shown in Figure 9.

- A user will initiate a request at node A, which will look for the file in its data. An identifying tag 'A' will be returned; otherwise, A forwards the request to B and C.
- If Node C fails to connect any node in its neighbourhood other than B, it replies with a message to B with ''request failed.'' Then B will try to reach Node E, which forwards the request to F.
- When F forwards the request to B, it perceives a loop and bounces back the message. If it cannot contact any other nodes, node F backpedals to E, which forwards the request to D as its second choice.
- D will check its stored content and locates the file.

TABLE 3. Summary of browsers.

Browser	Routing Protocol	Features	Anonymity Services	Disadvantages
Tor	Onion Routing	• Overlay Network • Free to access • Easy to install • Designed in C • Internet activity is not traceable through Tor • Provide anonymity to clients and servers • Tor supports all the Internet content • 3 Hop tunnels • Bi-directional tunnel • Bandwidth based peer selection	• HTTP • HTTPS • TCP • Remote DNS • Hides I.P.	• It does not protect against Traffic monitoring attacks • Not suitable for torrents, • Low Latency • It does not protect against Sybil attacks. • Can face high congestion leading to high latency due to circuit switching
I2P	Garlic Routing	• Easy to set up • Designed in Java • It provides an internal chat facility • Timing and man-in-middle attacks are difficult in I2P • Anonymous for torrents • File sharing is speedy • Best work with Linux • Distributed control system • Randomized number of Hops • Uni-directional tunnel • Performance-based peer selection	• HTTP • HTTPS • UDP/TCP • Remote DNS • Hides I.P.	• Not useful for windows and O.S. systems. • I2P does not guarantee anonymity for the surface web. • Documentation in different languages is not available in I2P • Memory usage is in efficient
FreeNet	Decentralized distributed data system	• It is peer-to-peer • Provide anonymity to the user requesting data and data carrier • Data can be transmitted over a large number of hosts • The number of hosts depends on data downloading speed • Global distributed storage sharing system • Highly resilient to attacks	• HTTP • HTTPS • UDP • Hides I.P.	• Storage size is not fixed. • It does not protect again routing table insertion attacks.

- D will follow the paths E, B to A nodes in the chain. The file is passed back, and D generates a new entry in its routing table, linking the data holder with the requested key. This way, E, B, and A will also cache the file.

The dark web is based on anonymity and confidentiality entirely. Table 3 summarizes all three browsers mentioned above [9], [8], [43], [44].

3) CRIMES IN THE DARK WEB

The explosive growth in anonymity-providing tools has resulted in a massive increase in cybercrimes and made the dark web a nesting ground for criminal activities. A large number of the dark web traffic is involved in illegal activities. Most Tor users are simply looking for privacy and maybe using Tor for legitimate reasons. The problem is the 1.5% of Tor users who access the Dark Web. It is impossible to create a tool that allows users to remain anonymous while monitoring their activity to ensure they do not visit illegal websites. Tor's creators would like to believe that the browser primarily carries traffic from journalists bravely writing stories from countries without free speech laws, but this is not the case. The majority of traffic to hidden Dark Web sites via various browsers is for viewing and distributing images of child abuse and purchasing illegal drugs. Dr Gareth Owen and Nick Savage of the University of Portsmouth conducted a six-month study on Tor usage and hidden services. They concluded that more than 80% of Tor traffic requests to hidden sites observed in the study were directed towards known child abuse sites [45]. However, they admitted that this data might not be completely accurate because government agencies frequently use computers that will automatically access websites containing child abuse images as part of their investigation. It is almost impossible to determine or figure out the ratio of percentages of police activity and traffic generated by a criminal within cyberspace. Even if police activity accounted for half of the observed child abuse traffic, much user traffic remains on the Dark Web targeting child abuse sites. Child abuse images are not limited to the Dark Web. There is a lot more going on the dark web.

a: HUMAN TRAFFICKING AND SEX TRAFFICKING

Human trafficking is also known as slavery, which has long been a human rights challenge affecting millions of people worldwide. International labour organizations reported as 40.3 million in modern slavery [46]. Trafficking is plausible in every job sector or industry; for example, in the sex trade, human trafficking is found as prostitution and pornography; similarly, it also occurs in restaurants, bars, street gangs, the drug trades, etc. Since the last decade, the issues of human trafficking have become more complex as it is now done digitally and in the dark. Globalization and technology facilitate its spread, as there are ways to connect to multiple customers to exploit the victims. Human trafficking has many categories such as sex, and labour traffic, organ, and baby trafficking, etc. For organ collection, individuals are taken to the location of the organ recipients for removal of organs on-site, known as transplantation tourism in the dark world. It is estimated by the Global Financial Integrity 2017, annual profits by illegal means of organ trade lie between $840 million to $1.7 billion. Babies' adoption is another booming industry that involves human trafficking. Baby harvesting in ''baby factories'' causes young women to be captive for industrial vaginas to produce babies for selling purposes [47].

Darknet is meant to protect anonymity, but these protocols assist human traffickers and protect users from law enforcement agencies. Several studies and documents prove that Darknet assists criminal activities with the availability of substandard protocols, anonymous I.P. allocations, peer-to-peer content sharing platforms, and untraceable payment transactions. It is easy to pay for illicit services on the Darknet with cryptocurrencies like Bitcoin. These criminogenic features of the Darknet are providing an advantage to criminals.

b: CHILD PORNOGRAPHY

The dark web is widely used for child pornography by paedophiles and criminals. Most users accessing the hidden sites related to child pornography are on Tor. Freedom hosting allocated almost 550 servers in Europe to give a space hosting child pornography. Its video feature applications are also used for live child abuse to gain profit [1]. Another feature, Voice over I.P. (VoIP), is used for webcam child prostitution. It is an alarming online danger due to child sexual abuse where the victim's images are sold.

Hundreds of people worldwide were arrested in 2018 after knocking out one of the largest child pornography sites called ''welcome to video,'' based in South Korea. An estimated 144,000 individuals alone in Britain could access pornography using the dark web in 2018 [1].

c: TERRORISM AND ARMS TRAFFICKING

The dark web is an enabler for selling and buying illegal weapons. Although the volume of arms trafficking is small compared to the other crimes on the dark web, its impact on the world's security is much greater. Europe, Denmark, and Germany are the leading countries in dark web arms sales with the highest share of the dark web market [1].

Terrorism and terrorist organizations on the dark web are massive threats to the world's security. Al-Qaeda and ISIS have used the dark web for their negative motives to spread hate and terrorism in the world. They also used the dark web to recruit, radicalize and distribute information among their members, raise funds, weapon buy, and coordinate terrorist activities worldwide.

d: DRUG TRAFFICKING

There are many websites over the dark web for selling and purchasing illegal drugs. There are two types of drug markets on the dark web: one is the narcotics market, selling contraband tobacco, cannabis, psychedelics, cocaine, and so on, and the other one includes general shops selling drugs chemicals. The dark web allows for selling drugs in exchange for cryptocurrencies. The silk road was one of the famous markets for illegal drugs that sold drugs worth over a billion dollars. It was shut down in 2013. But still, several illicit drug markets are running over the dark web, such as Mr Nice Guy, Dream Market, Wall Street Market, and Valhalla, etc. [9]. ''Grams'' with a logo styled like Google, is the most popular search engine for illegal drugs on the dark web [35].

e: INFORMATION LEAKAGE

There are two types of crimes in terms of information leakage; one is hacking, and the other is the sale of stolen data. The dark web is a haven for hackers to leak sensitive and confidential content. It is conjoint for like-minded people to form an organization from hackers to online gaming. In doxing, one's identification is broadcast, and hackers use it to ''unmask'' a rival. But the doxing or exposing private details are not restricted to hackers. Hackers can target companies, celebrities, and public figures. In every case, the purpose is fame, money, etc. The best example is Wikileaks, which also has a Deep Web presence and also offers a page to submit new leaks anonymously [34].

Another growing feature of the dark web is the trade of stolen accounts; its presence is also found openly on the surface web. Accounts ranging from credit cards, banking, online auction sites, and gaming are among the most common items being sold on these websites. On the surface web, prices vary with location, but prices for PayPal accounts are pretty mature. These accounts are sold as high-quality accounts, verified statements with a known balance, or bulk amounts of unverified reports. Only in 2017, about 1.4 billion personal records were sold on the dark web [8].

f: MALWARE/RANSOMWARE

The deep web and malware are perfectly matched in many ways, specifically in the case of command-and-control (C&C) hosting infrastructure. It is the best feature of Tor or I2P to hide the location of servers using strong cryptography. Here traditional investigation tools such as examining a server's I.P. address, checking registration details, etc., do not work for forensic researchers. Several cybercriminals also use Tor for C&C. Many dominant malware families use Tor for some setups by adding the legitimate Tor client within their setup files. Trend Micro wrote about this for the first time in 2013 when a spike in Tor traffic was due to MEVADE malware by switching to Tor-hidden services for C&C. As a first example, VAWTRAK malware is a banking Trojan that was spread via phishing emails [35]. Each sample communicates with a list of C&C servers whose I.P. addresses are retrieved by downloading an encrypted icon file (i.e., favicon.ico) from hard-coded Tor-hosted sites [5]. This technique hides the location of a criminal server, but users who access it are vulnerable. This seems no issue as their systems are already infected by malware. Crypto Locker is another malware family that uses the deep web. Crypto Locker is based on a ransomware variant, and it encrypts victims' documents and then redirects them to a site. So, if someone wants access to these files, they have to pay first. It is developed smartly as it automatically adjusts payment methods and local languages. It shows why cybercriminals are attracted to the deep web as it has made it easy for them to have their infrastructures more robust to possible takedowns [8]. With an increasing number of ransomware attacks, many ransomware detection engines have been developed tools to identify the infected file. However, even if the infected file is detected and removed, there is no way to recover the data of the infected file [48].

g: BITCOIN AND MONEY LAUNDRY

Bitcoin is a cryptocurrency designed with anonymity. Nowadays, it is common and widely accepted even for illegal purchasing. Although Bitcoin transactions are considered anonymous, users have to attach their identity with crypto-wallets. As per blockchain architecture, Bitcoin transactions are fully public, which investigators can examine. So, tracking money is possible even though it is not easy. Many services have been added to improve anonymity in the system; the aim is to make it more challenging to trace cryptocurrency. This is generally achieved by ''mixing'' bitcoin essentially through a spidery network of microtransactions transferring before returning to the owner [1], [49]. In this process, the owner gets the money with fewer chances of it getting traced back, and only a fraction is deducted as a fee. Laundry services help to increase the anonymity of money moving through the bitcoin system. Numerous anonymous services are added to the deep web; for example, PayPal, ACH, and Western Union are available [8].

III. THREAT INTELLIGENCE TECHNIQUES

There is an established cybercrime community on the dark web. It is also expected for law enforcement and security products and service providers to observe the activities to keep pace with the rapidly growing threat landscape. Usually, antivirus and other security companies have protected their users from malware based on signatures derived from past attacks. However, there is a shift towards a more proactive approach to security. A part of threat intelligence is collecting and processing data, which can help manage security.

This section discussed the architectural analysis of the literature reviewed to detect threats. We can categorize threat intelligence techniques mainly in five categories focusing on the main target to monitor and detect threats. These five classifications are forums, marketplaces, websites, traffic monitoring, and honeypots, which can be used everywhere. Table 5 presents a detailed elaboration of these classifications as per the monitoring target. We employed a generally used process to summarise the detecting architecture. Figure 10 depicts the architectural framework analysis process[1].

- Data Gathering: This component describes the data sources, the data collection size, and the data set's availability for the models. Researchers and businesses use several types of data while collecting information. Many studies have used data that has already been scraped from Internet databases; others have used onion sites as their data set, while others have used Tor traffics.
- Data Pre-Processing: This is a critical phase in the data processing process. The major components of this process include important feature selection, filtering, extraction, and duplication or noise reduction. This stage is usually followed by their appropriate needs to feed the model in most research.
- Data Processing: This is the essential stage of any model because it involves the implementation of algorithms such as machine learning (ML), data classifications such as clustering or labelling, testing the algorithms' performance with training and testing data, and applying the techniques to their respective fields.
- Results: The final outcome aimed to develop the framework is the results, which vary depending on the deployed model. It could be in the form of alerts, reports, graphs, mail notifications, or maltego.

The outcome of the models can be used by security agencies or law enforcement, which is the ultimate purpose of all frameworks. It should be noted that the procedures and examples described in Figure 10 and the description are not exhaustive. Table 5 presents some strategies from our peer-reviewed papers that use various models and tools to detect threats in the categories mentioned above.

A. DARK WEB FORUMS MONITORING

The detection of forums discussing criminal and illegal activities on the dark web can improve current security measures significantly. In this section, we have tried to present various security strategies devised by different cyber security scientists and researchers to support the integrity of the Tor network.

Marin systematically reports a key-hacker proof of identity issue based on status to legalize the results. Their revision mainly reveals three altered methods – content, social network, and seniority-based analysis performed to detect key hackers on the dark web. An optimization metaheuristic is used to train and test the model. A comparison of performance is made with machine learning algorithms. By leveraging the users' reputation scores provided by the three forums analyzed to systematically cross-validate the results through those sites, models trained in one hacker forum are generalized to make predictions. As a result, Genetic Algorithms have the best performance in 87.5% of cases [54].

TABLE 4. Category of dark web crimes.

Broad Role	Crimes Subcategories	Reported Cases
Human trafficking	a. Labour trade b. Sex trade c. Organ trade or transplantation tourism d. Baby trade	• According to the International Labor Organization (ILO), nearly 40.3 million people were subjected to modern slavery in 2016, with 24.9 million subjected to forced labour and 15.4 million subjected to forced marriage. 2017 [46]. • It is estimated that the internet facilitates 75% of sex trafficking of minors in the United States, compared to approximately 38% prior to 2004 [51]. • According to a 2017 report, the majority of human trafficking survivors were recruited for sex trafficking and labour trafficking [9]. • Annual profits from illegal organ trade range from $840 million to $1.7 billion globally in 2017 [47]. • Baby harvesting takes place in "baby factories," where young women are imprisoned and used as industrial vaginas to produce babies for sale [52]
Child pornography	a. Child abuse	• "Welcome to Video," one of the largest child pornography sites based in South Korea. Back in 2018, an estimated 144,000 people in the United Kingdom could access pornography via the Dark Web [1] • Lolita City, a dark website with around 15,000 members, contained over 100 GB of photos and videos of child pornography when it was taken down [9]. • Freedom hosted 550 servers in Europe used for illegal child pornography [53].
Drug trafficking	a. Narcotics trafficking b. Illegal medicine trafficking	• Silk Road was one of the first Dark Web marketplaces, selling narcotics for over a billion dollars and shipping them via DHL or drop shipping [1]. • Mr Nice Guy, Dream Market, Wall Street Market, Valhalla, and Grams with a logo styled like Google are the most popular search engines for illegal drugs on the dark web [9].
Information leakage	a. Hacking b. Stolen data for sale	• Hackers can target celebrities, companies, and public figures. In every case, the purpose is fame, money, etc. The best example is Wikileaks. [50] • A hacker gang once exposed the credit card information and logins of around 32 million Ashley Madison clients in a 9.7 GB data dump on the black web. • Over 1.4 billion personal records were released in plain text on the dark web in 2017 [9].
Malware	a. Ransomware Attacks	• In the so-called "dark web," the Cryptolocker Ransomware, also known as the CTB Locker, creates a Bitcoin wallet for each victim, using digital bitcoins as payment [48].
Terrorism	a. Recruit and radicalize b. fundraising c. arm trafficking d. spread propaganda e. communication	• ISIS has used the Dark Web to broadcast news and propaganda. In November 2015, attacks in Paris ostensibly shielded the identity of the group members and its content from hackers [1] • "Fund the Islamic Struggle Without Leaving a Trace" is a dark website that encourages people to donate to Jihad by sending money to a specific Bitcoin address [50].
Bitcoin	a. Money laundering	• The US government case against Ross Ulbricht contains 9.9 million bitcoins in transactions, which is $214 million when adjusted for currency rates, according to 30 months of Silk Road data from February 2011 to July 2013 [49].

Deliu designed an automatic hybrid cyberthreat intelligence model of ML called Support Vector Machine (SVM) to identify hacker forums' posts and then cluster the posts using latent Dirichlet allocation (LDA). A copy of leaked data is taken from a popular hacker forum Nulled.IO for an experiment. The forum's data went through some pre-processing; for example, words that appeared less than three times in the corpus were excluded. Over a million posts were selected from hackers' forums to train the SVM, while remaining (security-relevant) posts were analyzed. The trained SVM filtered out the irrelevant posts from these one million posts. SVM identified about 90% of the posts that were found security threats [55].

L'Huillier [37] addressed the community key member extraction problem by combining text mining and proposed social network analysis techniques. First, LDA was applied to build two topic-based social networks, one social network oriented towards the thread creator point-of-view and the other towards the repliers of the overall forum. Subsequently, topic-based key members are evaluated using different Social Network Analysis measures, a network benchmark built with plain documents. A study is done by using VCol; LDA (latent Dirichlet allocation) and ASD (average shortest distance) used on the Ansar1 forum, where data was collected for 14 months from December 2008 to January 2010 after that SNA (Social Network Analysis) applied on the two different topologies for forums used as creator oriented and the last reply oriented, which gives the information of key members of VCol based on the 14 months of data [56].

Yang *et al.* [57] developed a post association analysis to visualize a dark web forum system and graphically display the relationship between various forum messages and posters. This platform is designed to handle a large amount of forum information. The structure of the system consists of:

1) Data acquisition module: mainly crawl name, content, theme, time using python+ onion scans crawler and save data in SQL server database

- according to poster messages, it queries from the forum message database
- visualize the forum information into diagrams

2) Designing and implementing forum information query

- Query conditions: a multi-condition combination query performed by the user using the Boolean logic retrieval method rendering the required search field
- The content list displays the message which satisfies the query condition and will be displayed in the "content list" of the main interface

3) Visualization and implementation of the design content. Kadoguchi *et al.* [58] has created a dataset using sixgill's web crawler tool. After collection, the data is manually categorized into two datasets as critical and non-critical datasets. Doc2vec is used for natural language processing and feature extraction. The feature values and context are taken into consideration. They perform word tokenization, cleaning, word normalization, stemming, and stop-word processing as preprocessing steps. Then the ML is performed on the doc2vec output. It consists of two phases:

- Learning phase: a model is generated by learned and acquired features of doc2vec.
- Evaluation phase: functioning is assessed by evaluating the model.

After learning data, anonymous data will be introduced to the model, and then comes the identification of the forums having the most critical posts.

A methodology to monitor and categorize the criminal activities on D2WEB is proposed by Tavabi *et al.* [59]. For this purpose, a new model is introduced in which a web crawler first collects data, and then a new technique, LDA, is used to learn the topics discussed on the forum. This paper also discusses the hidden Markov Model (HMM) through Beta Process to generate dynamic processes into time series.

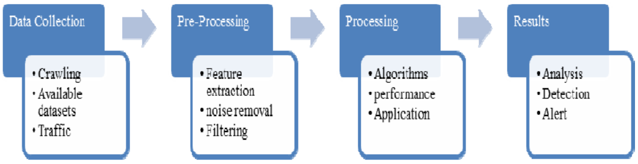

FIGURE 10. Threat detection architectural framework [1].

Beta Process (BP-HMM) identifies latent states collected by different time series during the experimental work. After that, clustering is performed on BP-HMM data; four different clusters having different cybercriminal activity discussion forums are identified as below:

- Cluster1 discussing cyber hacking,
- Cluster 2 discusses criminal activities regarding the marketplace,
- Cluster 3 completed forums related to hacking PlayStation.
- Cluster 4 consists of the white-hat hacker.

Schafer *et al.* [60] discussed the architecture of the Blackwidow for the early detection of cyberthreats. They took seven forums; three related to the dark web and four associated with the deep web, having three different languages; English, French and Russian. They analyzed the data in five steps:

1) Planning and requirements: Identifying forums and gaining access to the forum through a Blackwidow's account.
2) Collection: Raw data collection and anonymous access to forums.
3) Processing: It includes parsing raw HTML data, translation of content in foreign languages, and information extraction from the data.
4) Analysis: Includes inferring user relationships, identifying topics, and identifying cyber security trends.
5) Dissemination: Kibana dashboards deliver a real-time outlook of the processed data stored in the Elastic search database.

Alnabulsi and Islam [61] proposed a methodology to evaluate relationships between dark web forums. In the process, an M.S. Excel file is used for the data from three dark web forums; and for data mining, the VSM is used to find out the number of posts for particular subjects. Finally, they classify the data in terms of eight illicit activities through Weka 3.9 and draw the VSM diagram to determine the similarities and relationships between forums.

A framework of attack prediction in the real-time point t is designed by Sarkar [62]. In the process, they applied a combination of social network analysis and a supervised learning model on 53 forums of the dark web over 12 months; by using the features from the dark web forums as an input to the model to predict an attack at time index t, which is equal to 1-day. During the analysis, they came across two cyberattacks.

B. MARKETPLACE'S SURVEILLANCE

The deep web, darknet, and marketplaces have attracted broad attention worldwide, including blackhat users and law enforcement agencies [63]. Quantitative, statistical analysis is provided by analyzing hidden web markets and surveillance operation programs inside the dark web. Some research on dark web marketplaces surveillance is outlined below.

Dong designed a framework to detect cyberthreats through text mining techniques in dark web marketplaces. The framework encompasses data collection, warnings, passing through an item classifier, a data processing unit, and term verification. A scrappy framework is used to sneak into web pages that analyze relevant information at the data collecting stage. A customized parse is designed to fold important information from the marketplace like hacking, security, and cyberthreats related categories called *items*. Porter Stemmer is used for stemming and reducing the dimensions of the text matrix. MLP is used as the model of the classifier. In the hacking category, items are classified, and then text mining techniques are applied. Using AlienVault OTX, the source of existing threats is verified and checked to see if it is a new or existing one. After verification, an error is generated [64].

Cherqi *et al.* [65] performed an experimental study about illegal trade, which is evolving in marketplaces and creating threat ideas that can be harmful to a person or organization or whole industry. The study involved the e-commerce networks of the dark web; these networks include Silk-road 2, Agora, Alphabay, and Nucleus. The present evaluation is about activities on these sites during 2013–2015. The focus is on hacking and cyber criminality, malicious ads and services. A cost assessment of all products reveals that colossal crimes are occurring. It is not easy to scale such organized and well-anchored crimes, which are constantly booming. Well-organized cells that monopolize the market are also highlighted. Actually, 98% of the market is controlled by only 20% of sellers. Additionally, customer feedback is a matter of reputation – users are satisfied if outcomes match their desire [65].

Nunes *et al.* [66] designed a system that influences threat intelligence and makes a decision based on at-risk systems; simultaneously, and it also provides arguments about the decision made. Based on deliberations, it explores the at-risk component and multiple competing hypotheses according to platforms, vendors, and products. The resultant method is a fusion that chains DeLP with machine learning classifiers. This hybrid system is between classical knowledge representation and reasoning techniques along with machine learning classifiers. The authors collected discussions from nearly 300 dark web forums and marketplaces to evaluate the system provided by a threat intelligence company. The design accuracy was enhanced by 15% to 57%, preserving recollection over baseline approaches.

C. MONITORING OF DARK WEBSITES

An experiment was set up by Alkhatib and Basheer [67] in 2019 using a python library, Scrapy1, known as Darky. This library brings the content of the dark market and analyzes it to arrange the number of products in each category. Crawling is a method restricted to one website in revision. In comparison, Ferry *et al.* [68] used a regular dark web scan by monitoring policy. The authors maintained a list of sites from the dark web and categorized them successively. They got.onion sites by the native Linux tool, Alyze. An API website is used for semantic examination, and frequent keyword counts. Websites are classified into six categories subject to purpose.

A Hadoop-based framework was designed in 2019 to identify the individualities of dark network criminals' networks using HDFS as a database and web crawler storage system to collect Tor data [69]. The author has discussed dark web threats via Hadoop-based intelligence analysis framework by:

- data collection (through web crawlers),
- data pre-processing (to remove duplication, noise, and segmentation through fudanNLP),
- data analysis (text categorization and clustering).

Another important aspect of threat intelligence is personal attribute extraction. For this purpose, Wang *et al.* [70] suggested a method to obtain personal attributes by implementing three steps, i.e., block filtration, attribute candidate generation and attribute candidate verification. Block filtration is a newly proposed technique based on the quantization method and generates the candidate attributes, which the binary classifier later verifies. After extracting and analyzing attributes information from the darknet, the data of the top K organizations, countries, email domains, and people on the darknet is a significant achievement to identify the leading criminals of the dark web.

D. TRAFFIC MONITORING IN THE DARK WEB

Darknet traffic contains traces of several attacks like Botnets, Spoofing, DDoS attacks, probes, and scanning attacks. Monitoring traffic activity in the dark web can detect many malware activities and attacks.

1) DETECTION OF TOR RELATED TRAFFIC

To identify if a host is generating Tor-related traffic or not, Cuzzocrea *et al.* [71] describe a procedure using a machine learning technique and a basic rule of analyzing whether the traffic flows are TCP or UDP. In the process, the authors took 22 G.B. of real-world data through Wireshark and the tcpdump tool. The ISCXFlowmeter application generates the packet flow and calculates all the statistical time-related features. A machine learning algorithm demonstrates the effectiveness of the proposed technique, and evaluation is done using a classifier built with 23 elements of traffic flow. These 23 features are divided into six groups. This deployed method can recognize activities based on seven tools (email, p2p, VoIP, FTP, streaming, chat, and browsing). The proposed algorithm can achieve precision ranging between 0.982 and 0.998.

2) DETECTION OF MALWARE

Han *et al.* [73] proposed a new method to continue their previous work, based on the real-time detection of malware activities using online processing of the Glasso engine by analyzing dark web traffic. All the data is gathered by setting up sensors on the dark web to collect traffic information. In the Glasso engine, several packets received from sensors as variables apply a graphical Gaussian model, which achieves the dependency of variables. The input of the online Glasso engine is the PCAP file capture from the dark web traffic for T seconds; in contrast, the engine's output is the alert information containing a timestamp, targeted destination TCP port, source I.P. address, and the number of addresses. The output generated by the Glasso has been analyzed, and 128/1634 TCP ports classified into three different categories:

1) Cyberattacks (network scan that attempted intrusions and attacks on multiple hosts);
2) Survey scans (network scan that attempted research on TCP ports using multiple hosts of organizations);
3) Sporadically focused traffic (a phenomenon in which packets suddenly concentrate from various source hosts to one dark web destination).

Their proposed engine detects malware activities in real-time with an accuracy of 91.2%.

3) DETECTION OF MALIGN TRAFFIC

A threat detection method by monitoring dark web traffic using a machine learning classifier is proposed by Kumar *et al.* [74]. The suggested system consists of traffic generation and collection, feature extraction, dataset processing, and classifier designing. For darknet traffic collection, they used the software SURFnet, which is the highest quality network for research work. They gathered the traffic data by monitoring the traffic through the darknet sensor. At the same time, regular traffic was collected by using various applications like Facebook, Twitter, and YouTube, etc. After extracting 76 features from the generated traffic data, Microsoft Azure ML was used for pre-processing and to train the machine learning model. The proposed framework can detect malign and benign traffic with a precision value of up to 99%.

4) DARKNET VISIBILITY

Soro *et al.* [75] deployed three different darknets composed of IPv4 addresses in Brazil, the Netherlands, and Italy to identify darknet visibility facts. Network traffic was captured through probes storing complete packet information in a Hadoop-based cluster at each location. The analysis was done on the data gathered in one month, and the results show that a few source I.P. addresses generate significant scan traffic. The traffic source significantly varies according to the I.P. range, and the size of the darknet impacts its visibility.

E. THROUGH HONEYPOT

A honeypot is a cyber security tactic intended to deceive cybercriminals. It works as a trap that detects and deflects a potential malware, which is isolated and monitored for information or a resource. Depending on the expected outcome, the types vary from production honeypots and research honeypots. The main goal of these honeypots is the diversion of the attacker from a running system. All the traffic generated by a honeypot is suspicious as nothing is provided by this resource. So, the data collected by a honeypot is fascinating as it has moderate logs. It helps identify what type of attacks a company or natural system may experience, acts as a lodge to distract adversaries from systems, and detects attacks. Honeypots can be classified as:

Low Interaction – has a partial range of communication with the external system. It simply simulates the services of a real system. The major determination of this type is to detect delimited linking efforts.

Medium Interaction is a semi-virtual honeypot. It provides better-quality model services compared to low interaction honeypots, but attacker response is also given.

High Interaction is the most advanced type of honeypot. This has a higher level of collaboration with the invasive model. The efficiency is in realistic approaches to the attackers and folds more information related to envisioned attacks.

Zeid *et al.* [36] executed two honeypots with three automated secure virtual machines on the dark web. Deployment was made more secure by these virtual machines. The first one is a research honeypot that comprises a chatroom web server – it collects chats from the dark web. The other virtual machine is a helpless web-based honeypot whose aim is cyber services. The last one is an ELK log server where all logs from the dark web, chatroom, and the cyber tool web-based honeypot are stored. On each machine, hidden services of Tor were installed, configured along with the dark net domain. The chatroom honeypot logged about 700 malicious requests. These requests involved child pornography and hacking techniques. The second one is the production honeypot which provides hacking services and is maintained on a vulnerable virtual machine. This was arranged to gather attacks and record requests to facilities and tenacity. As a result, the honeypot was targeted with a script attack for four days, and 600 hacking requests were logged for the two weeks it was maintained in the dark web.

Catakoglu *et al.* [5] applied a high interaction honeypot, consisting of three types of web-based and system-based honeypots. These honeypots are associated with Tor to host hidden services. They are individually installed on every virtual machine (V.M.); thus, it can degenerate honeypots to a clean state if they are conceded. V.M. works as a patch to prevent any escalation; in a way, if a hacker compromises any of them, they could not obtain all the files. Besides, the authors set a firewall that restrains the attackers from Denial-of-Service attacks. Three different honeypot templates were deployed to bait attackers:

TABLE 5. Process of threat intelligence techniques.

Author Reference	Data Collection	Data Preprocessing	Data Processing	Results
E. Marin et al. [54]	Available dataset	Feature extraction using social network analysis	Used four supervised learning algorithms: • Genetic Algorithms (GA.) • multiple Linear Regression approach (LR.) • Random • Forests (RF.) • SVM filtering	GA techniques have an accuracy of 87.5% to detect hackers.
Deliu et al. [55]	Available known hacker forum	Applied probabilistic data filtering	• SVM filtering • LDA modelling	Extracted Top 10 security-related words from hacker's forums
M. Kadoguchi et al. [72]	Sixgill (web crawler tool)	Doc2vec for language processing and feature extraction.	MLP, a multi-layer perceptron technique, is used by machine learning.	Classification receives only critical posts from the forums and generates the ranking of the forum based on the number of critical posts with the accuracy of 79.4%.
M. Schäfer et al. [60]	node.js headless Chrome browser puppeteer is used as a crawler.	Parsing raw HTML data. Automated machine translation to translate the languages.	Extractor in Scala is used.	Blackwidow automatically found relationships between threads and forums.
Y. YANG, et al. [57]	Python+onionscaon used as a data crawler	Filtering through Boolean logic retrieval model	KMP algorithm	Network diagram and histogram visualization of threats.
M. Wang et al [70]	Web crawling through python+onionscan	FudanNLP for pre-processing	Mahout's naive Bayesian for text classification Kanopy+Kmean algorithm for text clustering	SNA provides characteristics of special participants with the accuracy of 58%.
Tavabi et al. [59]	Web crawling	preprocessed the data by using NLTK, SpaCy, and sci-kit-learn tools.	Latent Dirichlet allocation and Hiden Markov model techniques for data modeling	Clusters were representing different malicious activities discussing in forums.
F.dong et al. [64]	Webpage crawling and parsing through Scray	PorterStemmer used for feature extraction	AlenVaultOTX for threat intelligence	Warning generation mentioning new or existing threats with the accuracy of 81% using SVM.
O. Cherqi et al. [65]	Scraped already available data of four marketplaces	Applied parser for feature extraction and TF-IDF supervised learning approach	Logistic regression Naive Bayes, SVM Random forest	Provided the general economical analysis. 97% true positive for hacking related trades and 93% true positive for not hacking related trades with the precision of 93.3%.
E.Nunes et al. [66]	Web crawling	parsing	A-CLKT is used, which is an Adversarial Cross-Lingual Knowledge Transfer	Detect threats across languages with recall rate of 92% of marketplace products and 80% of the hacking related discussion with the accuracy of 87%.
A. Cuzzocrea et al. [71]	Wireshark and tcpdump tool are used to get real-world data	ICSXFlowmeter is used to generate the packet flow	Machine learning classification	Identify and categorize the traffic based on the services used by the clients with the precision equals to 99.8%.
Han et al. [73]	Real-time data through the sensors received in the PCAP file	Graphical Gaussian model to achieve the dependency of the input data.	Glasso Engine	Provide alerts against malware detection with the accuracy of 91.2%.

TABLE 5. ***(Continued.)*** **Process of threat intelligence techniques.**

S. Kumar et al. [74]	Used SURFnet for real-time traffic collection.	76 features extracted	Microsoft Azure machine learning	The framework can detect malign and benign traffic with the precision of 99%
R. Islam, et al. [61]	Available data	Vector space model is used	Weka 3.9	Classify the data in eight illicit activity groups, VSM diagram to show the similarities.

a. A website concealed as a private drug marketplace that trades to a close group of summoned followers.
b. A blog webpage that promotes modified Internet results for hosting in the Tor network.
c. A convention private setting that only allows privileged persons to log in.

The honeypots' values show that assaults from the Surface Web effectively undermined the principal clone. Out of 115 assault-related solicitations, 105 (91%) of them were fruitful assaults. For the second clone, by and large, 1,255 (65.0%) of the assault-related solicitations beginning through Tor2web succeeded. Despite what might be expected, just 154 (7.2%) of the ones getting through the Tor network succeeded. While the third clone never got a solitary assault from Tor2web. The authors clarified the idea of threats found from the honeypots. Table 6 summarizes the threat intelligence techniques discussed in this paper.

IV. ATTACKS ON THE DARK WEB

As discussed before, numerous cyberattacks are launching inside the dark web. Anonymous feature of the dark web is a primary cause that gives the assurance to the attacker. In this section, different attacks on different browsers, Tor being the most popular browser, are discussed and their categorization in detail. Figure 11 gives a detailed overview of the attacks on the dark web discussed in this section.

A. ATTACKS ON TOR

Although anonymity has practical applications worldwide and is the ultimate need of the online world, like everywhere else, it also is invaded by the cyber world's black sheep, performing all kinds of malicious and nasty activities. Every year Tor is subjected to multiple attacks, leading to data breaches and leakage of sensitive information. Verifier tools like CIPAV (multiple computer and Internet protocol addresses) act like malware. These tools can collect information despite the operator's use of anonymizing technology. Law enforcement agencies can use such tools to find cybercriminals and launch various attacks on secured anonymous networks, causing significant harm. Understanding such deanonymizing attacks is paramount to users of these technologies as they must understand the limits of the technology they rely on. Even though there are surveys of anonymous communication networks, there is no comprehensive survey of attack mechanisms on anonymity. This study aims to provide an overview of the potential attacks on anonymity networks and examine the risks and protection mechanisms for users of these networks.

Non-indexed data and overlay techniques provide anonymity to the dark web, especially Tor. According to existing methods, we categorize the deanonymization techniques into two groups:

Active/Passive attacks: the adversary can actively manipulate the traffic or passively observe the network.

The second group is based on the target of the attacker:

- Client: Attacks on the client aimed to create damage to the Tor client.
- Server: Attacks on servers target the Hidden Service. Adversary client and guard node are used to deanonymize the H.S., H.S. is enforced to choose a compromised guard node as their entry nodes, and this attack reveals the H.S. IP address.
- Network: Multiple nodes of the Tor network can be affected. In some cases, the effect could be propagated to the whole network just to compromise a single node.
- Generic: Attacks are those in which attackers can target more than one entity.

1) CLIENT ACTIVE ATTACKS

a: TRAFFIC ATTACK

These attacks vigorously insert a malicious program into unencrypted circulation at the server-side. This malicious program helps to reveal the actual I.P. address of the customer after dodging the actual client and linking its construction with a malicious server, thus compromising the client's anonymity. That's how an attacker can control an unencrypted link between the proxy and remote server. For example, an adversary can randomly add or modify non-encrypted movement data in the Tor network. Thus, anonymity is breached by gaining control of a non-encrypted link and injecting various software instances into that link, including Flash, JavaScript, ActiveX Controls, and Java. Once these codes are accomplished in any browser, it can sidestep indigenous substitute sets in the browser and unswervingly form a link to the exact distant host. From there, the I.P. address of the actual client can be obtained [10].

b: CELLFLOOD ATTACK

Barbara presented a practical and easy-to-perform cellflood attack [21]. This attack hampers Tor relays by flooding the circuit setup requests. This over flooding targets a relay to

TABLE 6. Summary of threat intelligence techniques in the dark web.

MONITORING TARGET	AUTHOR	IDEA	FINDING
Forum	E. Marin et al. [54]	Proof of identity of hackers from the dark web forum based on the standing to validate the results	Results shows the identification of one third of Top hackers among the 92 users of a forum.
	Deliu et al. [55]	A method is presented to automatically get content about threats by observing the hackers' forums	The system discovered leaked credentials, malicious proxies and malware
	M. Kadoguchi et al. [72]	Using ML and doc2vec Extraction of forums that have intelligence information and identify traits	MLP model success rate in classification is 79.4%
	M. Schäfer et al. [60]	Using Blackwidow, a survey is conducted on seven different services across three other languages	Managed to get the five years security and fraud related data from the dark web.
	L'Huillier et al. [56]	The idea is to resolves topic-based key members issue	Thirty-six topics are discovered from 29,057 posts.
	Y. YANG, et al. [57]	Developed a visual dark web forum post association analysis system to display the relationship graphically	Forum requests are presented in histograms and diagrams
	Tavabi et al. [59]	The author disclosed a non-parametric HMM model that learns the forum's collective topic dynamics based on the results obtained from LDA	Grow with different groups having illicit activities
	M. Ebrahimi et al. [76]	Designed a framework to detect cyberthreats in non-English forums using A- CLKT (a machine-learning algorithm to detect threats in the Russian and French language)	A-CLKT approach has a 74% accuracy rate in detecting cyberthreats from non-English forums
	R. Islam, et al. [61]	Affect analysis is performed. Detect the illicit subjects in the dark web forum	Results demonstrate high similarity and low topic shifting between all forums
Marketplaces	F.dong et al. [64]	Agenda to detect the cyberthreat through text mining tools	Discovered two threats, goznym 2.0 and alienspy rat 5.0.
	O. Cherqi et al. [65]	Enlighten illegal trade on dark web marketplaces through analysis of data	98% of the market is controlled by only 20% sellers.
	E.Nunes et al. [66]	Design a system that influences threat intelligence and makes a decision based on at-risk systems	The system shows precision of 57%
Websites	M. Wang et al [70]	Person attribute extraction process using three steps block filtration, attribute candidate generation, and attribute candidate verification	Paper reflects the data of topmost organizations, countries, email domains, and people on the darknet
	Al Nabki et al. [2]	The idea is to categorize the illegal activities of Tor HS by using two text representation methods and three classifiers	Combinations of these methods and classifiers give an accuracy rate from 93.7% to 96.6%
	Y. Yang et al. [69]	Hadoop-based model to detect threats on the dark web	He explained how to analyze the Hadoop-based data to detect threats
	B. Alkhatib et al. [67]	Proposed a dark website-based data crawling method	Results show the percentage of products in each category
	Z. Li et al. [77]	The study was conducted on the hosts of 4 million URLs to identify the relation between hosts of the malicious websites	All hosts are interconnected and do not allow traffic from legitimate sites
	N. Ferry et al. [68]	Monitoring methodology implemented dark website for frequently scanning purposes	Data from 4 samples of 100 websites are analyzed and categorized into six fields (drugs, money, crime, virus, adult, and market)
Traffic	A. Cuzzocrea et al. [71]	Describes a classifier to use for traffic-related attacks	Discover Tor or non-Tor related traffic
	Han et al. [73]	Presented the real-time Glasso engine to detect malware	Engine detects three types of activities: attacks, survey scan, and sporadically focused traffic
	S. Kumar et al. [74]	The idea is to monitor the dark web traffic using an ML classifier	The model can detect malign traffic with an accuracy of 99%
	Soro et al. [75]	Deploys three different darknets on three other locations to check the visibility of the dark web	Discovers that the size of the dark net impacts its visibility
Honeypots	R. zeid et al. [36]	Deploys two research honeypots on a chatroom web server and a vulnerable web-based server	The first honeypot received 700 malicious requests, whereas the second honeypot received 600 requests
	O. Catakogly et al. [5]	Deploys a honeypot in the dark web to detect attacks on websites, forums, and drug marketplace	Attackers uploaded 287 files on the honeypot

9

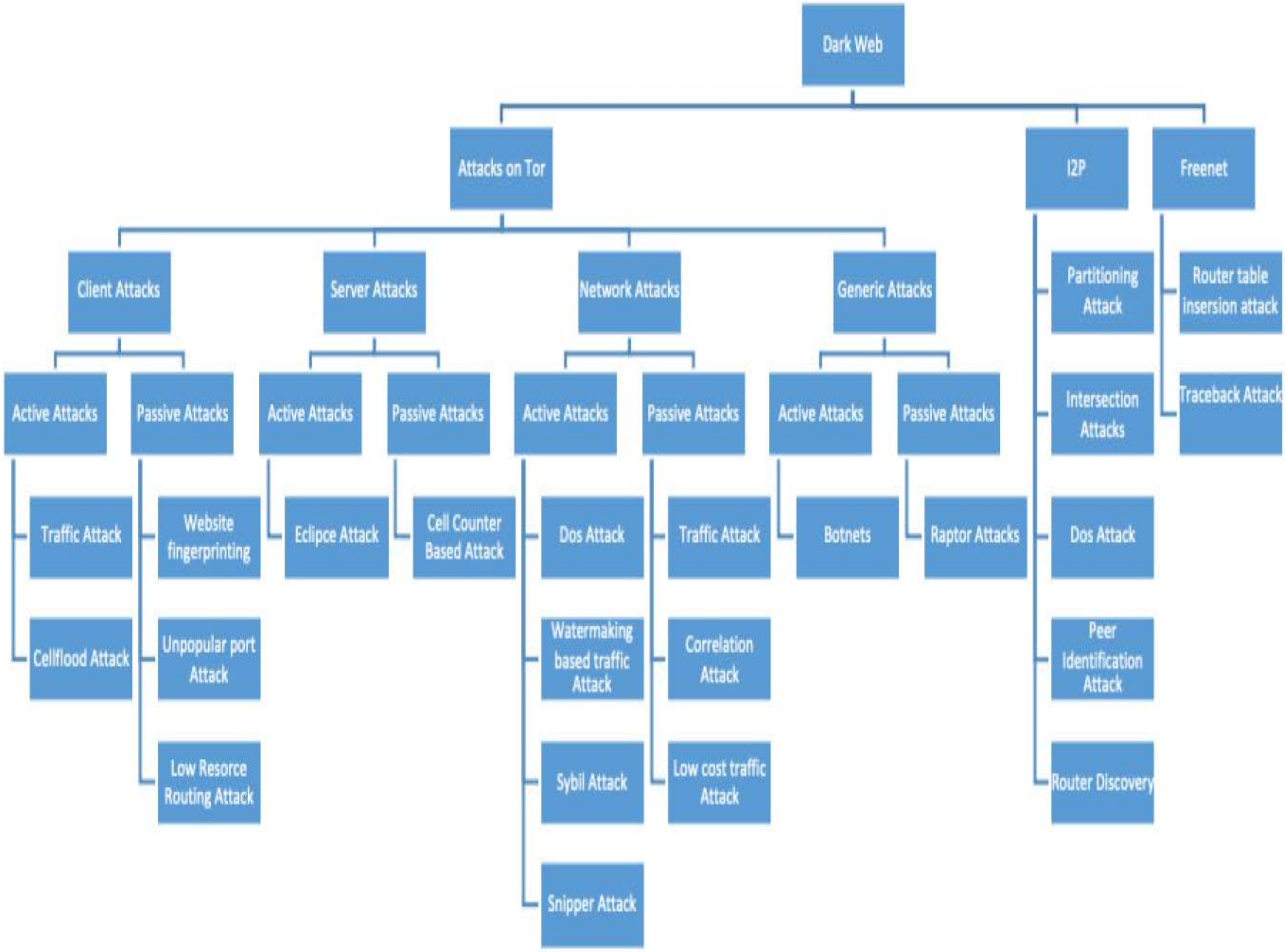

FIGURE 11. Attack taxonomy of the dark web

use its bandwidth, decreasing the processing capacity. The invader exploits the point that handling commands take more time than creating them. For example, the generate command is practised through a user to encompass a track.

2) CLIENT PASSIVE ATTACKS

a: WEBSITE FINGERPRINTING ATTACK

For this attack, one needs to monitor circulation among clients and secret substitution to identify retrieved websites by comparing a prospective traffic pattern with pre-collected web page fingerprints. This consists of two phases in an attack, offline training and online classification.

In the offline training phase, several websites of interest are selected. They are browsed one by one to collect the traffic. Afterwards, an adversary needs to pre-process the data to remove all unnecessary data so that useful analysis of the required information can be done. Additionally, only appropriate features are extracted from the pre-processed traffic, including packet length distribution, traffic volume, total time, traffic direction, packet length order, up/downstream bytes, bytes in traffic bursts, etc. Frequently used classifiers are Bayes classifiers, multinomial naive-Bayes classifiers, (SVMs) decision trees, etc.

In the second phase, recording actual traffic and launching threats to classify the target's opened web links are done. Then a monitoring tool assembles the dupe's traffic between the client and mysterious proxy [78]. After obtaining this traffic, the adversary processes traffic to measure the features and performs the attack using the classification rule.

b: UNPOPULAR PORT ATTACKS

In this case, the attacker injects as many malicious Tor nodes as possible and waits for the victim to pick from these nodes to construct a circuit. This was more feasible when the Tor network consisted of less than 500 relays. But currently, the Tor network contains more than 7000 relays. This has made it quite an ineffective technique. Sulaiman and Zhioua [79] proposed an attack inspired by this idea. The authors suggested using unpopular ports 25 and 119 instead of popular ports 80 and 53. Since a fraction of Tor nodes allows unpopular ports, the malicious nodes will outnumber the valid ones, which increases the probability of the circuit being compromised by Tor clients. The critical condition for such an attack is a Tor client that uses an unpopular port through the Tor network. Once a malicious unpopular port is used, the attacker gets control of the webserver and victim's client to open the Tor page by injecting a program request page using unpopular ports. The chances are significant that the client will choose one of the challenger's injected malicious nodes. The attacker gains control of a conceded web server and then injects many malicious entries and exit routers that use an unpopular port. When a client joins a compromised web server anonymously using the Tor network through the port, e.g., 80, 53, etc., a hidden stored script is injected into the server. The Tor client machine executes these injected scripts, which direct the opening of a new connection through the Tor network to a remote server using the unpopular port. The attack becomes successful when the Tor client picks two compromised Tor routers for circuit entry and exit [79].

c: LOW RESOURCE ROUTING ATTACKS

In this attack, the selection of entry guards is based on specific variables, plus bandwidth and uptime. In other words, onion routers having better variables than average could become entry guards [20]. They can be compromised with high bandwidth and uptime. The next stage in the attack is to exploit the victim's circuit creation. The attack exposes a circuit even before any payload data is sent from the user. It identifies the path by recognizing patterns in Tor's circuit structure algorithm. An attack in a simulated environment with 66 onion routers having six malicious onion routers compromised over 46% of paths. A similar attack concentrating on entry guards by flooding false router advertisement data can increase the threshold for choosing entry guards, thus reducing correct entry guards being selected. Theoretically, it is possible to displace all valid entry guards with malicious ones.

d: FINGERPRINTING ATTACKS

Fingerprinting attacks are unique because they can be launched as active or passive. For a single-end passive fingerprinting attack, the adversary needs to monitor users' devices traffic to compromise security and privacy. Thus, traffic patterns referred to as fingerprints and content of traffic can be accessed via such attacks. To expose the I.P. address of the clients, this attack can be converted into an active one; thus, actively altering data at the application layer or users' accessed websites [11].

3) SERVER ACTIVE ATTACKS

a: ECLIPSE ATTACKS

Such attacks allow attackers an extremely low-cost block to random Tor hidden services. Researchers have deployed a valuable prototype of the Eclipse attack to evaluate its severity on the live Tor network. They formalize the Eclipse attack process as a balls-into-bins problem for numerical estimates of Tor hidden services' security [80]. The approach states security metrics that calculate exactly how many I.P. addresses need to be in control of the adversary for making Eclipse attacks and how likely it is to control the responsible HSDirs during a random period. With only six I.P. addresses, experimental results show that a random hidden service can be eclipsed with a 100% success probability.

- Experimental results show that acquiring a unique ideal mark requires 21 seconds in the most pessimistic scenario (five same beginning characters); all things considered, it requires just 0.32 seconds in commonplace cases.
- An Eclipse assault would need around 25833916 events to produce the wanted fingerprints in the most pessimistic scenario. However, it will take about 30282 activities in a typical case. Later in 2019, the author improved the effectiveness of the attack and reduced the expense to just three IPs to overshadow a discretionary HS with 100% achievement likelihood [81].

4) SERVER PASSIVE ATTACKS

a: CELL COUNTER BASED ATTACK

This attack allows the invader to insert a signal at a cell counter of an entry or exit relay to influence the time of sending relay. On the other end of the circuit, the relay recognises the rooted signal to confirm that a client communicates with a server. Traffic is transferred through cells, stored temporarily in a queue, then sent to an output buffer before entering the network. A signal can be deployed in the traffic by gaining control of a cell count of the output buffer, as shown in Figure 12. The time selection is essential while sending each 'symbol,' as short waiting will cause cells combined with other relays to wait for a long time to look suspicious and increase the latency, which may cause the user to create a new circuit [10].

Awkwardly, due to the jamming, cell patterns might also be injected at the middle Tor or delay in the network. Thus, the number of cells per symbol should be such that combined cells can still be recognized as symbols at receiving relay. A progressed recuperation component was created to recon, but these mutilate signals analyze some sort of combination [12]. This assault is difficult to recognize since the sign can be concise and can have various properties, making it hard to recognize from typical traffic. The circumstance between two images can be constrained by a pseudo-commotion code known to the aggressors.

5) NETWORK ACTIVE ATTACKS

a: DOS ATTACKS

Packet spinning offers attacks using looping circuits and malicious onion routers by compromising anonymity. Looping aims to block other onion routers from being selected. There are two conventions; circular circuits cannot be visible, and a legitimate onion router will spend time executing cryptographic calculations. In other words, a malicious onion proxy creates denial-of-service attacks, creating loops

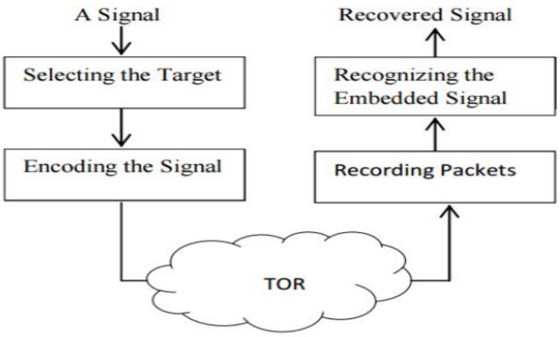

FIGURE 12. Workflow of cell counter based attack [10].

in circuits. If a looping attack is successful, there are more chances of malicious onion routers being chosen in circuits because the other legitimate onion routers are busy. It can also help in executing more attacks [11].

b: WATERMARKING BASED TRAFFIC ATTACK

In this threat, the adversary implants a signal/watermark in the target's traffic. Then watermarked communication traffic is monitored to establish a relationship between the sender and receiver [11]. Since the rival can misuse different constructions of independent layers to install watermarking into network traffic, it presents these assaults by three different layers – the convention-layer, network layer, and application layer. In the case of a network layer, the foe may misuse the traffic rate, parcel postpones span, and bundle size to create a watermark into the targeted traffic. As an example, a foe can influence traffic from a sender and shape its traffic rate design. Thus, an undetectable direct grouping spread range (DSSS) sign can be inserted in the rush hour gridlock. At that point, these established signs alongside the traffic imparted through an unknown correspondence network arrive at the collector.

c: SYBIL ATTACK

In June 2010, Tor relays suddenly increased in minimal time due to the Sybil attack. It seems that someone created several hundred Tor relays on PlanetLab machines. This may seem harmless, but it can be used to attack the Tor network – this is called a Sybil attack.

Figure 13 illustrates datasets that contribute to the assailant, agreement, and worker descriptors; malevolent transfers and the exit map [10]. In a Sybil attack, an enemy oversees virtual personalities to acquire an unnecessarily massive impact on the organization. The effectiveness of assaults on Tor relies upon the agreement haul of the assailant, which is the measure of traffic an adversary can see. At the point when an agreement weight rises, it is not difficult to create other Tor assaults. Instances of these attacks that are not difficult to take with a Sybil attack are fingerprinting and connection attacks. Apart from making other attacks easier, the Sybil attack puts the Tor network and, by extension, its user's anonymity at risk. However, the pinnacle viability relies upon the dependability of the Tor transfers. Questionable transfers are a hazard to client encounters and weaken the secrecy given by Tor. Specific clients will avoid using the framework when experiencing issues brought about by suspicious transfers. Fewer clients imply a decline in the general secrecy of the organization. The leftover clients will keep using the organization with lower obscurity, introducing better freedoms for perception. This issue can be misused by adding vindictive transfers and deliberately influencing the unwavering quality of mysterious correspondences to build the chances of an enemy trading off client namelessness [11].

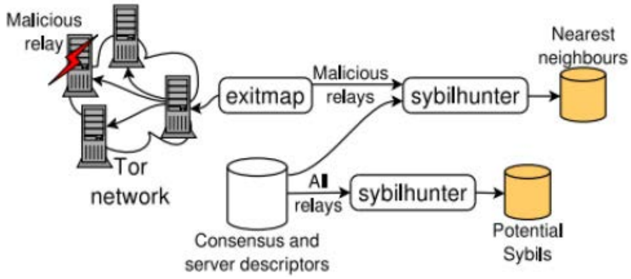

FIGURE 13. Setup of sybil attack [10].

The real safeguard against Sybil attacks is a test; these attacks will most likely consistently be conceivable in nameless networks without a focal position. There are a few heuristics to apply to recognize a Sybil attack. Transfers that are important for a Sybil attack regularly join and leave the organization immediately. They have normal boundaries and may change their character's unique mark to control a Tor circulated hash table.

Ge and He [82] proposed a counter Sybil attack method centred on Integer Linear Program that detects malicious users from performing enumeration attacks on resources. A bipartite graph is established between users and unavailable resources, which finds the minimum set covered by this method. This method is effective if the quantity of inaccessible means in the system does not cross 50%. When the number of unavailable resources in the system approaches 50%, it can leverage repeated rounds of resource distribution to identify the suspicious harmful user and use that information to build the bipartite graph. Now a method of integer-linear-program is used to sense mischievous customers in the classification. Future work can aim to improve the precision of this method when unobtainable resources outstrip 50%. Experimental results reveal that the accuracy of the proposed technique in this paper is more than 80% when these unavailable resources in a model are less than 50%.

d: SNIPER ATTACK

In a Tor circuit, traffic analysis is established by an active watermarking technique that discloses the communication partners. The results show that if a snipper attacks the Tor network, effectiveness is near 100% with low latencies and is challenging to detect. The test uses a specific onion proxy with the circuit, a malicious entry onion router, and an exit onion router. Usually, both ends of the circuit are controlled in a sniper attack, but it can also be executed even if the attacker controls a single onion switch. The man-in-the-middle assault is made between the passage switch and the client in this situation. The essential idea of such an assault is to install a mysterious sign in the cell counter in the rush hour gridlock. Another malevolent hub is perceived to affirm conveying parties [14]. The mysterious sign can be a succession of pieces. The sign infusion can be executed on one or the other passage or leave an onion switch. This works by controlling the number of lined hand-off cells on every one of the onion switches. For example, the attacker may show three hand-off cells for ‘1’ and one true cell for ‘0’.

6) NETWORK PASSIVE ATTACKS

a: TRAFFIC ATTACKS

The entity of the endways passive attack is to observe traffic without any active intervention and assess the commonality between the sender’s outbound and the receiver’s inbound traffic. This technique can exploit packet counter, traffic pattern correlation, and timing correlation. An example is that the adversary counts packets leaving and entering at both ends; after that, the distance function can be applied in terms of traffic features to compute the distance between these two links. The limited chance of detection is a primary advantage in end-to-end attacks because the traffic is monitored. Nevertheless, the true positive rate is low, while the false positive rate is high. Consequently, an attacker can only get traffic pattern similarities between senders and receivers in a significant amount of time. Besides, end-to-end active attacks have been proposed to improve the true positive rate and reduce the false positive rate by manipulating traffic to generate the desired signal [78].

b: CORRELATION ATTACKS

Correlation attacks are designed to detect communication relationships between clients and servers. They are end-to-end attacks that can either be active or passive. For these attacks, the adversary monitors entry and exit nodes at both ends [11].

c: LOW-COST TRAFFIC ANALYSIS OF TOR

Low cost refers to a small level adversary who only has a small view of the network, unlike global adversaries who can see all the network links. These small adversaries can also perform timing and traffic analysis attacks. Even a single addition on a Tor node can cause a huge load on the network. Furthermore, the traffic burden on a single Tor node can be compared to overall network traffic. A modified type of this attack comprises a malicious server that sends data to the victim in a pattern. Traffic analysis is executed by observing this pattern and creating a connection over the candidate onion routers. Thus, unrelated communication streams can be traced back to the initiator.

Tor cannot protect against a global passive adversary. In a global adversary, the attacker can observe all links in the network. The threat model in Tor assumes that only a fraction of the network is under the observation of the adversary. Further, the attacker can compromise some onion routers with their onion routers and generate, modify, delay or delete traffic. Tor’s threat model cannot focus on traffic confirmation attacks. In a traffic confirmation attack, an adversary can confirm the communication between two parties over Tor by observing the timing patterns and volume of the traffic. Instead, Tor’s focus is to prevent traffic analysis attacks, where an attacker tries to determine at which points in the network a traffic pattern-based attack should execute. In other words, a low-latency anonymous system aims to prevent attackers from knowing where to attack [11].

7) GENERIC ACTIVE ATTACKS

a: BOTNETS

An overlay network of compromised machines (malware is introduced in machines thus compromised) called bots conjointly make a botnet controlled by the attacker. Bots can be compromised in many ways, such as 0-day exploits, including the famous drive-by download method [22]. When users visit the page, they may unknowingly download malware. Once the user’s system becomes infected, the botmaster can command botnets to do illegal, malicious activities like DDoS, spam campaigns, credential theft, cyberespionage, bitcoin mining, etc.

The architecture of botnets, protocols followed, and type of malicious activities performed help to distinguish different botnets. The botnet structure is relatively simple, where every bot having IRC-based communication is connected to a central server called C&C controlled by the botmaster. This centralized structure is easy to monitor and easier to attack. The whole system will be shut down by taking down the server. Thus, botmasters have been untiringly trying to improve the architecture of their botnets by various techniques like the fast-flux technique, domain generation algorithms (DGA), replacement of previous single C&C with multiple C&C servers, and recently shifting to the P2P network. The P2P architecture replaces the central C&C with an entirely distributed network of bots. Bots exchange information between each other, transmitting commands and overlaying management information using custom protocols. They also use standard protocols, such as HTTP, DNS, and others, to be as stealthy as possible for operations like downloading new malware versions. Of course, this also makes the botnet more difficult to manage and monitor. The P2P structure makes the botnets more resilient but less vulnerable [11]. The P2P botnet can be identified using *crawling,* which can delineate most of the bots in a botnet. Once detected, a sinkhole can destroy these bots that install crafted information in every bot connecting them to a centralized network. The defender or inexistent injected node can be controlled, making all the bots point to a black hole.

8) GENERIC PASSIVE ATTACKS

a: RAPTOR ATTACKS

Together three different attacks take advantage of the Border Gateway Protocol (BGP) and formulate Raptor attacks [10].

First, attackers at the AS level penetrate Internet routing to observe at least one direction of user traffic. As there is no encryption of TCP headers of packets, these packet numbers can be related at both ends. After this, malicious AS can interject these packets. Asymmetric traffic analysis makes traffic analysis easy as only one direction of traffic at both ends of the circuit is needed to correlate the client and the server.

Second, AS-level adversaries may use Internet routing to lie on the BGP paths for increased users' overtime. Malicious AS nodes can be inserted in between client and entry node with every change in the BGP path. Then, these malicious nodes can analyze traffic to confirm the relationship between client and server. With time, as more malicious nodes get introduced, the chances of correlation also increase.

Third, strategic adversaries use BGP hijacks to find users of specific Tor guard nodes and analyze the traffic of these nodes.

9) COUNTERATTACKS

a: COUNTER RAPTOR

Sun *et al.* [83] have presented a study on tor network immunity against attacks on BGP prefix, which showed that high tor bandwidth ASes could be less resilient and more vulnerable to threats than ASes with low bandwidth. He has also introduced a selection algorithm for tor guard relay that selects relays based on their resilience and helps proactively protect against prefix hijack attacks. Moreover, for the safety of Tor, against active BGP routing attacks, he has given the idea to use proactive and reactive countermeasures. In his live monitoring system, a mechanism generates alerts for a subscriber against any potential hijack attacks using multiple new detection mechanisms in real-time. During the evaluation of the monitoring system, they found a negligible false rate of an actual hijack attack and the ability to detect simulated attacks after real-world attacks.

b: CENTRALIZED ZEUS BOTNET (ZBOT)

This famous malware has infected various hosts leading to the breach of personal information. It propagated by sending spam, phishing attacks, and stealing a massive volume of data. Encryption of all traffic and files make ZBot challenging to detect by forensic analysis. An example is GameOver Zeus (GOZ) that utilized P2P technology where it was possible to steal bank credentials using the decentralized infrastructure. These decentralized infrastructures comprised many hosts coupled with web servers aimed at executing the C&C server. GOZ also could be propagated through DDoS phishing attacks to harvest users' credentials [84].

c: COUNTER SYBIL

Ge and He [82] proposed a counter Sybil attack method centred on Integer Linear Program that detects malicious users from performing enumeration attacks on resources. A bipartite graph is established between users and unavailable resources, which finds the minimum set covered by this method. The effectiveness of this method is possible if the quantity of inaccessible means in the system does not cross 50%. When the number of unavailable resources in the system approaches 50%, it can leverage repeated rounds of resource distribution to identify the suspicious harmful user and use that information to build the bipartite graph. Now method of integer-linear-program is used to sense mischievous customers in the classification. Future work can be aimed to improve the precision of this method when unobtainable resources outstrip 50%. Experimental results reveal that the accuracy of the proposed technique in this paper is more than 80% when these unavailable resources in a model are less than 50% [82].

d: COUNTER ECLIPSE ATTACK

To mitigate eclipse attacks, Tan *et al.* [80] suggested the following three schemes to make the Tor network more secure.

- Randomized ID mapping scheme: The mapping of HS descriptor-ids to HSDirs fingerprints determines which HSDirs are responsible for storing the descriptors, and it can also be identified how these fingerprints change over time. We propose a randomized ID mapping approach to solve this problem, making Eclipse assaults in large-scale DHTs computationally infeasible.
- HSDir density tracking detection scheme: Statistical study of the Tor's consensus can be used to calculate the HSDir density. After completing this analysis, we can determine whether or not a suspect HS is accessible by repeatedly connecting to it. We can identify Eclipse attacks on Tor HSs automatically this way.
- Run own responsible HSDir scheme: can be used to protect against Eclipse attacks is for an HS's operators to use onion routers as responsible HSDirs. To reduce the cost of Eclipse attacks, operators should generate HSDirs fingerprints that are as close as feasible to the HS descriptor-ids, making it more difficult for an opponent to monopolize the responsible HSDirs.

10) COUNTERMEASURES

To reduce the de-anonymizing attacks some countermeasures have been established to retaliate or boost immunity against these attacks.

1) Packet padding: This method is generally used to pad the packet size to eliminate the length of packet features from descriptions like packet order and packet size. Using this technique, the size of every packet can easily be padded into the exact size, such as the maximum transmission unit (MTU). Similarly, numerous techniques have also been analyzed in various studies to pad

the packet size efficiently and effectively [22]. In order to obfuscate the traffic time, possible delays can also be deliberately added between every packet to improve the traffic time.

2) Dummy traffic techniques: This method can be practised to insert the dummy packets into users' original traffic to obfuscate the traffic volume.
3) Traffic morphing: This method can be applied to traffic to make it seem different from its actual pattern. For example, to thwart a website fingerprinting attack, the web server can first select a target page and then mimic the packet size distribution.

Broadly the countermeasures can be arranged for the following reasons:

a: NETWORK LAYER

Usually, defence techniques are general at the network layer. They could be applied in different systems to communicate anonymously, while a high transmission overhead can be experienced. So, the network traffic characteristics may be used to deanonymize the communication between users. A defensive tool to thwart attacks at the network layer involves removing traffic features associated with users, including packet size distribution, packet order, traffic volume, and traffic time [16].

b: PROTOCOL LAYER

Protocol-level padding and dummy techniques at the protocol layer can hide traffic features that are associated with users. The secure shell (SSH), TLS, and IPsec apply these protocol-level padding techniques to align plaintext with block cipher boundaries, obscuring some part of the packet size. Additionally, a random amount of padding can be added with protocol-level dummy techniques to improve security. The functionality of padding cells for circuit-level padding reduces the efficiency of the circuit – this is why Tor does not use it. If protocol-level padding and dummy techniques are not designed carefully to reduce the overhead incurred, they can become a reason for an MTU end-to-end active attack [16].

c: APPLICATION LAYER

A comprehensive solution lies in hybrid techniques to avoid threats that can be deployed at the various layers. The application layer's HTTP features and background traffic can be exploited to remove traffic features from user flows. For instance, incoming and outgoing packet sizes can be tuned by using HTTP pipelining and ranges. Likewise, changing HTTP request orders at the client-side will differ the traffic pattern [16]. When a user is browsing a web page, a decoy web page can be silently loaded in the background to apply background traffic techniques at the application layer. In actuality, this defence technique is suitable for specific applications (e.g., HTTP), so it cannot be widely adopted for diverse applications.

B. ATTACKS ON I2P

To address Tor's centralized design limitations, researchers have proposed an alternative of I2P, which is a distributed system. It is by far the most complicated and promising anonymous P2P system for many reasons. As I2P stores all the metadata in the DHT, also known as NetDB, it provides scalability to the network. The I2P protects against a number of attacks, such as Brute force attacks, Timing attacks, Tagging attacks, Predecessor attacks, Harvesting attacks, Cryptographic attacks, Development attacks, and implementation attacks and traffic flow attacks. The traffic can be monitored locally, but the attacker cannot deanonymize the network traffic flow. Also, it does not have an exact threat model, but some attacks can compromise its anonymity. This paper will discuss all the attacks proposed by researchers to deanonymize I2P. Just as for Tor, malicious peers can be part of the I2P network, collect data and perform requests [25]. However, the attacker could not control more than 20% of the peers due to the decentralised configuration. Below are some details of the possible attacks that could run on I2P.

1) PARTITIONING ATTACKS

I2P maintains a distributed system by using Kademlia and keeping nodes in contact using NetDB. Kademlia is vulnerable to partitioning attacks that can disconnect targets in the system and reveal all parties involved in a communication stream. A partitioning attack targets end-users in the design and only connects to a smaller set of malicious nodes. Once the connection is made, malicious nodes can simulate the functionality of the anonymous system to the target node. Users can still create different tunnels and choose various hops, but all sender and receiver identities are compromised as malicious nodes are connected to the system. Sometimes adversaries are strong enough to block certain destinations, including other legitimate nodes, intentionally. They may disconnect the target from the rest of the nodes in the system and then introduce other malicious nodes and a set of NetDB options and routes. One can fully exploit sender and receiver identities in the system and data by coupling such partitioning attacks to others like Sybil and timing attacks, especially if one of the malicious nodes is used as an exit node to the Internet [26].

2) INTERSECTION ATTACKS

These attacks involve monitoring a specific target and finding out how many nodes are constantly connected to the system. Tunnel rotation variation in target reachability helps the attacker narrow down the target by eliminating nodes not involved in communication with the target. Thus, once nodes involved in the target are narrowed down, they are monitored for a message being traversed from source to destination. These attacks can also be coupled with other attacks to increase their effectiveness [26].

TABLE 7. Tor attack pattern (legend: √ determines the attack type, nodes and level; × means respective type nodes and level is not included in this attack).

Study		Attack type		Attack Nodes		Attack Level	
Attack Target	Attacks	Active	Passive	Single End	End to End	Application Level	Network Level
	Torben attacks	×	√	×	√	×	×
	Plug-in based attacks	×	√	×	×	√	×
	Tor guard selection induced	×	√	×	√	×	×
	Raptor routing attacks	×	√	×	√	×	×
	Unpopular port exploitation	×	√	×	√	√	×
	Low resource routing attacks	×	√	×	√	×	√
	Java applets	×	√	×	√	√	×
	Active documents	×	√	×	×	√	×
	URI methods	×	√	×	×	√	×
	Code injection	×	√	√	×	√	×
	BitTorrent	×	√	×	×	√	×
	Clickjacking	×	√	×	×	√	×
	Predecessor attack	×	√	×	×	×	√
Server	Snipper attack	×	√	×	√	×	×
	Tor cell manipulating	√	×	×	×	×	√
	Caronte attack	×	√	×	×	√	×
	Off path MitM	√	×	×	√	×	√
	Correlation attacks	×	√	×	√	√	×
Network	Bridge discovery	×	√	×	√	×	√
	Denial of service	√	×	√	×	×	√
	Cell counting based attack	√	×	√	×	×	√
	Flow multiplication attacks	×	×	×	√	×	√
	Cellflood attacks	√	×	√	×	×	√
	Traffic analysis attacks	√	×	×	√	×	×
	Timing attacks	√	×	×	√	×	√
	DNS	√	×	×	√	√	×
	Fingerprinting attacks	×	√	√	×	×	√
	Congestion attacks	√	×	×	√	×	√

3) DOS ATTACKS

Cristopher Kack proposed a Dos attack against I2P, in this attack, malicious I2P nodes keep cyclically opening many service connections to consume the resources of the target node [85]. As an initial response, the ratio of system resources available on I2P was increased, including total bandwidth, permitted tunnel limit and memory size in the I2P router. However, this helps the I2P router to accommodate even larger Dos attacks. When a P2P connection is established in the I2P, that means a router is constantly receiving TCP/UDP packets from a similarly large number of I.P. addresses. If the I2P nodes stop running altogether and the I2P node has been monitored, the change in performance and network availability can be related to a Dos attack.

4) PEER IDENTIFICATION ATTACK

Egger *et al.* [26] proposed a combination of attacks with a motive of peer identification using a particular service. To achieve this goal, the authors proposed implementing the following three attacks on the network:

Floodfill Takeover Attack: For this attack, 20 controlled nodes are used as a part of the network that acts as floodfill peers and takes control of the flood fill database. These nodes are configured as manual floodfill nodes to ensure their participation in the database. Once floodfill takeover is achieved, we can launch a sybil attack or link store and verification connection done by the peers; thus, deanonymizing these peers. Also, legitimate floodfill nodes can be decreased by a DoS attack against legitimate floodfill participants creating job lag and using available resources.

Sybil Attack: It gives the attacker control over a limited part of the keyspace. At least eight nodes near the target key are required to do this. In addition, introducing new nodes into the system requires a set-up time of up to an hour, during which the node gets known by a more significant number of peers and is actively used for lookup. Also, the storage location of keys changes every day at midnight. Thus, the second attack node-set can occur at the exact location before midnight, so they are already integrated once the keyspace shifts.

Eclipse Attack: This attack allows the attacker to make any database record unavailable to network participants. The attacker needs to have control over at least eight nodes closest to the keyspace in the NetDB. Once control over the keyspace is established, the attacker can lock access to items in the region by sending a reply claiming not to know the resource. If the obstructed resource contains the information, the attacker can stop anyone from availing the service information.

Herman and Grothoff [25] proposed another attack to identify peers likely to be chosen by the Eepsite host assuming the Eepsite is available to the I2P network during the attack. Three types of I2P peers are used to make this attack possible:

1) Monitor peer to report information about the tunnel to the attacker.
2) Attack peer to perform a DoS attack.
3) Visitor peer to act like a visitor and query the NetDB for the leaseset and HTTP request to Eepsite.

The leaseset is used to determine which peers should be attacked. Using the I2P peer selection algorithm causing normal high peers in the victim's fast tier to reject tunnel requests increases the chances of the adversary's monitoring tier being chosen. Once the monitoring peer gets chosen, it provides the information about the received packet count and time interval of packets. And the tunnel is reported to the adversary as detected.

5) ROUTER DISCOVERY

I2P is based on Kad and many voluntarily running routers, so discovering the router can lead to many collusion attacks. P. Egger *et al.* [26] introduced four methods of router discovery.

1) Introducing a normal router in the network to continuously send and accept the request to establish a tunnel attacker can save the router information exchanged during the communication.
2) Another passive way is by introducing a FloodFill router to the network; to better integrate into the network, the I2P floodfill router asks the neighbouring Floodfill peer for information about the other routers. Although storage spaces change every midnight, which can also lead to the change of floodfill peers, part of the routers remain the same, and the attacker's router can communicate with new floodfill peers every night.
3) By crawling the reseed URLs, router information can be extracted. When an I2P client does not find enough routers in the NetDB, it starts receding to get routers from several recede URLs hardcoded in the I2P sources. The number of routers can be counted from the available recede URLs.
4) By exploiting the NetDB, when an I2P router does not have enough routers available, it generates a database lookup message DLM to the nearest FloodFill peers to get new routers. The floodfill peers' lookup for the router is contained in the DLM locally, and once it finds it, it will respond to the query with the router information.

a: COUNTERATTACKS

COUNTER SYBIL

Alachkar and Gaastra [86] provides a blockchain Sybil attack analysis in the I2P network. A distributed and decentralized ledger system is known as a blockchain. As the name implies, it is a 'chain' of blocks. A block is a collection of data that has been aggregated. A hash of the previous block will be included in the newly produced block, allowing blocks to create a chain from the first to the newly formed block. It is a way for nodes to achieve consensus on recognizing a Floodfill router and determining how long that entity has been a Floodfill router using blockchain. Furthermore, the adoption of blockchain can result in proactive as well as reactive reactions to attackers.

C. ATTACKS ON FREENET

As we have already discussed in section III, the Freenet operates as an opennet and darknet. In the following section, we focus on the attacks on the openness mode of the FreeNet, which anyone can join. We examine two attacks with their countermeasures to understand the anonymity status of the Freenet better.

1) ROUTING TABLE INSERTION (RTI) ATTACK

There are three basic steps to perform an RTI attack in the Freenet – gathering network topology and peer relationships, predicting routing paths, and inserting attack nodes into the target nodes routing table. Freenet code allows a node to select its location so the RTI attack on the network can occur from any location. When a new node joins the network, a message is sent to the other nodes in the network via a controlled message broadcast, and multiple nodes may accept it as a neighbour depending on the node bandwidth. Once the node has responded to a preconfigured number of requests (by default 10), it can replace the least recently used peers. An attacker uses the insertion node to insert keys into the intersection node and the query node to request the keys inserted in the intersection node and then insert the RTI attack into the targeted node. By controlling the insertion and query node, the attacker can predict the route to find the intersection and target node [31].

2) TRACEBACK ATTACK ON FREENET

There are two essential factors in launching the traceback attack. The first is to connect an attack node to a suspect node in the Freenet. When a message broadcast arrives at the node not having enough neighbours, it is automatically accepted, or the requesting node can replace an existing neighbour. The second step is to query neighbours if they have seen a message with a particular UID. Each node maintains a specific set of UIDs that have not been processed yet. In order to determine if the neighbour has seen a content request message with a UID value, the attacker can send a request message with some UID value. A number of monitoring nodes can also be deployed in the network to identify content request messages. When an interested content request message is accepted, some information will be sent back to the attacking node, including the content request message and neighbouring nodes, to determine which of them has seen the respective UID [29].

a: COUNTERATTACKS

COUNTER RTI

RTI attacks can be prevented by a simple randomized routing method which reduces the attacker's ability to predict the routing paths. There are multiple ways to add randomness into the routing algorithm, e.g., GNUnet's R5N, which split the route into two phases based on the message's life counter, easily bypassed by the attacker. But a more generic case is by adding randomness at each node with a given probability [32].

b: COUNTER TRACEBACK

The UID associated with the content request message plays an essential role in conducting a Freenet traceback attack. To counter this attack, [30] provided a methodology that can dynamically change the UID value, which is called the dynID scheme. DynID is designed to reduce the chances of forming routing loops, and hence there are scarce chances of traceback attack.

V. RESEARCH GAPS AND FUTURE WORK

After reviewing the literature, many research gaps have been identified to continue the investigation in this area. These are outlined below:

A. CYBERCRIMES

Criminal's Reliance on the dark web for purchasing exploits from markets, communicating with other like-minded people on forums, hosting botnet servers, and hiring skilled criminals or their expertise to achieve their illegal targets. The confidentiality of the dark web enables consumers to do this and allows cybercriminals to handle out their business [4].

a. How and with what ratio the dark web crimes and growth in the crypto market are correlated?
b. How critical is the dark web to the success of coordinated strikes?

B. DISTRIBUTED HIDDEN SERVICES

The Tor Network uses the anonymity feature to keep Tor's site and address privately located but still is available by stakeholders to hidden services on the Dark Web, like the '.onion' website. Because their hosting provider and geographic location are secrets, law authorities will find it difficult to take them down. However, as evidenced by the recent closures of darknet markets Hansa, Silk Road, and AlphaBay, they are not immune to regulation. In this way, market operators and interested traders explore ways to remove the bottleneck associated with a centralized web platform on the marketplace. In such circumstances:

a. What is the trend towards more decentralized existing web infrastructure, mainly hidden services?
b. What and how do technological factors affect Dark Web scalability and observability?
c. What plan of action can law enforcement agencies use to exercise Dark Web control? Is it worth it focusing on users, servers, or the protocol, e.g., Tor itself?

C. THREAT DETECTION

Current law enforcement is to deanonymize hidden services, marketing agents, website managers, and everyone else involved in facilitating a rather centralized (but anonymous) infrastructure to carry out illegal activities on the dark web. As technology progresses, these elements may become increasingly difficult to monitor, identify and dismantle, especially as their present form ceases to exist.

a. What are the real-time threat detection techniques to prevent crimes?
b. What patterns can be discerned from the dark web's current hidden services?
c. How can we incorporate artificial intelligence as an automatic reply tool to the forums and marketplaces to monitor and detect a threat?

D. DE-ANONYMIZATION

To ensure the safety of the dark web, it is imperative to either lessen the inherent vulnerabilities of these platforms to make them more resilient to cyber threats and attacks. Or we should design a system that can detect cyber threats, attacks, and criminals and generate an adequate response to prevent any future intervention of such activities. For example, let's consider that web-browser is like a castle to which the general public can't gain access whenever and however they like. There are particular browsers or gates, or pathways by which one can enter into the castle of the dark web. To make this castle safer, it has to improve its infrastructure so that there are no tunnels, underground entrance areas, regulated entry, and exit points and needs a secure safety protocol system. Guards, checkpoints, safety dogs that bark at any intruders but also an automatic phone call to police, updated records of an intruder to be cautious next time constitutes an adequate response. We have pointed out some of them in this paper concerning the inherent vulnerabilities of these platforms.

a. To what extent attacks on Tor can be crucial or successful to the anonymity of its users.
b. What is the effectiveness of denial of service attacks in Tor, I2P, Freenet, etc.?
c. How efficient is the traceback attack on the I2P network?

d. Investigate the comparison of traffic attacks on the anonymity-providing tools.

VI. CONCLUSION

This review paper discussed different browsers of the dark web, including their structure, workings, strengths, and vulnerabilities. We have briefly described different attacks and attack patterns in line with the browsers' vulnerabilities. Our paper also entails mitigation techniques devised by researchers to counteract, control, detect and prevent damage by these attacks. A comparison of different cyber intelligence techniques on the parameters of theoretical and practical implications has also been presented. We have tried to explain different threat models in-depth; their workings and dynamics of attacks; also, their efficiency and limitations have been discussed in the context of our suggested threat taxonomy model. Besides pointing out how various adversaries operate to breach immunity and leak sensitive data, some attack detection techniques and countermeasures to firewall some attacks have also been presented. Finally, we have categorized our paper in sections for easy understanding, as described in the introduction. Table 1 depicts and compares our work with others. We have explained 34 attacks and categorized each of them in our trilogies classification system, explaining whether an attack is a client, server, or network level attack, whether it is a single end or end-to-end, and active or passive. We have presented threat intelligence techniques currently operating, how successful these attack detection techniques are, how many attacks have been detected, how they are lacking, and exactly which features need improvement. We have summarized these threat intelligence techniques in Table 5 and 6. This is a summary paper with our analysis and simplification of various attacks and attack detection techniques. It is written to provide an easy understanding of existing works in this field, loopholes, deficits, and areas of potential improvement.

However, there still needs to be work done to aid future study, for example, uncovering crime and the relative crime ratio of reported and real-time crimes in the dark web and how the growth in the dark web and crypto market are related.

Researchers also need to focus on real-time threat detection and the prevention of threats on a large scale of data by incorporating artificial intelligence techniques. The existing techniques only focus on a small amount of data and a particular monitoring target. We need to design a prototype that can simultaneously monitor forums, marketplaces, websites, and traffic to get an insight into cybercriminals, and this task needs the support of law enforcement agencies, researchers, and whitehat hackers to make the dark web anonymous and less vulnerable for everyone.

Further research is required to find out the effectiveness of Denial of Service attacks on Tor, I2P, and Freenet and how the traceback attack can be performed on other peers to peer systems with a comparison of traffic attacks different anonymity tools.

REFERENCES

[1] S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, "Evolution of dark web threat analysis and detection: A systematic approach," *IEEE Access*, vol. 8, pp. 171796–171819, 2020, doi: 10.1109/access.2020.3024198.

[2] M. W. A. Nabki, E. Fidalgo, E. Alegre, and I. de Paz, "Classifying illegal activities on Tor network based on web textual contents," in *Proc. 15th Conf. Eur. Chapter Assoc. Comput. Linguistics*, vol. 1, 2017, pp. 35–43, doi: 10.18653/v1/e17-1004.

[3] P. B. Patel, H. P. Thakor, and S. Iyer, "A comparative study on cyber crime mitigation models," in *Proc. 6th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2019, pp. 466–470.

[4] A. Gupta, S. B. Maynard, and A. Ahmad, "The dark web phenomenon: A review and research agenda," 2018, *arXiv:2104.07138*.

[5] O. Catakoglu, M. Balduzzi, and D. Balzarotti, "Attacks landscape in the dark side of the web," in *Proc. Symp. Appl. Comput.*, Apr. 2017, pp. 1739–1746, doi: 10.1145/3019612.3019796.

[6] E. Erdin, C. Zachor, and M. H. Gunes, "How to find hidden users: A survey of attacks on anonymity networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2296–2316, 4th Quart., 2015, doi: 10.1109/COMST.2015.2453434.

[7] M. Parkar and A. Chembur, "Introduction to deep web," *Int. Res. J. Eng. Technol.*, vol. 4, no. 6, pp. 229–234, 2017, doi: 10.1111/dial.12424.

[8] S. Saleh, J. Qadir, and M. U. Ilyas, "Shedding light on the dark corners of the internet: A survey of Tor research," *J. Netw. Comput. Appl.*, vol. 114, pp. 1–28, Jul. 2018, doi: 10.1016/j.jnca.2018.04.002.

[9] S. Kaur and S. Randhawa, "Dark web: A web of crimes," *Wireless Pers. Commun.*, vol. 112, no. 4, pp. 2131–2158, Jun. 2020, doi: 10.1007/s11277-020-07143-2.

[10] B. Evers *et al.*, "Thirteen years of Tor attacks," 2016. [Online]. Available: https://github.com/Attacks-on-Tor/Attacks-on-Tor

[11] M. A. Sulaiman and S. Zhioua, "Attacking Tor through unpopular ports," in *Proc. IEEE 33rd Int. Conf. Distrib. Comput. Syst. Workshops*, Jul. 2013, pp. 60–66, doi: 10.1109/ICDCSW.2013.29.

[12] E. Cambiaso, I. Vaccari, L. Patti, and M. Aiello, "Darknet security: A categorization of attacks to the Tor network," in *Proc. Italian Conf. Cybersecur.*, vol. 2315, 2019, pp. 1–12.

[13] M. Alsabah and I. Goldberg, "Performance and security improvements for Tor: A survey," *ACM Comput. Surv.*, vol. 49, no. 2, pp. 1–36, Nov. 2016, doi: 10.1145/2946802.

[14] S. Nepal, S. Dahal, and S. Shin, "Deanonymizing schemes of hidden services in Tor network: A survey," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2015, pp. 468–473, doi: 10.1109/ICOIN.2015.7057949.

[15] J. Salo. (2010). *Recent Attacks on Tor*. [Online]. Available: http://www.cse.hut.fi/en/publications/B/11/papers/salo.pdf

[16] M. Yang, J. Luo, Z. Ling, X. Fu, and W. Yu, "De-anonymizing and countermeasures in anonymous communication networks," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 60–66, Apr. 2015, doi: 10.1109/MCOM.2015.7081076.

[17] I. Karunanayake, N. Ahmed, R. Malaney, R. Islam, and S. Jha, "Anonymity with Tor: A survey on Tor attacks," 2020, *arXiv:2009.13018*.

[18] M. A. I. M. Aminuddin, Z. F. Zaaba, A. Samsudin, N. B. A. Juma'at, and S. Sukardi, "Analysis of the paradigm on Tor attack studies," in *Proc. 8th Int. Conf. Inf. Technol. Multimedia (ICIMU)*, Aug. 2020, pp. 126–131, doi: 10.1109/ICIMU49871.2020.9243607.

[19] G. Cascavilla, D. A. Tamburri, and W.-J. Van Den Heuvel, "Cybercrime threat intelligence: A systematic multi-vocal literature review," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102258, doi: 10.1016/j.cose.2021.102258.

[20] Y. Sun, A. Edmundson, L. Vanbever, O. Li, J. Rexford, M. Chiang, and P. Mittal, "Raptor: Routing attacks on privacy in Tor," in *Proc. 24th USENIX Secur. Symp.*, 2015, pp. 271–286.

[21] M. V. Barbera, V. P. Kemerlis, V. Pappas, and A. D. Keromytis, "CellFlood: Attacking tor onion routers on the cheap," in *Computer Security—ESORICS* (Lecture Notes in Computer Science), vol. 8134. Berlin, Germany: Springer, 2013, pp. 664–681, doi: 10.1007/978-3-642-40203-6_37.

[22] M. Casenove and A. Miraglia, "Botnet over Tor: The illusion of hiding," in *Proc. 6th Int. Conf. Cyber Conflict (CyCon)*, Jun. 2014, pp. 273–282, doi: 10.1109/CYCON.2014.6916408.

[23] L. Basyoni, N. Fetais, A. Erbad, A. Mohamed, and M. Guizani, "Traffic analysis attacks on Tor: A survey," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 183–188, doi: 10.1109/ICIoT48696.2020.9089497.

[24] B. Zantout and R. Haraty, "I2P data communication system," in *Proc. ICN*, 2011, pp. 401–409. [Online]. Available: http://www.thinkmind.org/index.php?view=article&articleid=icn_2011_19_10_10010.

[25] M. Herrmann and C. Grothoff, "Privacy-implications of performance-based peer selection by onion-routers: A real-world case study using I2P," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, in Lecture Notes in Computer Science, vol. 6794, Jan. 2011, pp. 155–174.

[26] C. Egger, J. Schlumberger, C. Kruegel, and G. Vigna, "Practical attacks against the I2P network," in *Proc. 16th Int. Symp. Res. Attacks, Intrusions Defenses (RAID)*, in Lecture Notes in Computer Science: Including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 8145, 2013, pp. 432–451, doi: 10.1007/978-3-642-41284-4_22.

[27] J. P. Timpanaro *et al.*, "Monitoring the I2P network To cite this version?: Monitoring the I2P network," 2011. [Online]. Available: https://hal.inria.fr/hal-00653136

[28] J. P. Timpanaro, T. Cholez, I. Chrisment, and O. Fester, "Evaluation of the anonymous I2P network's design choices against performance and security," in *Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, Feb. 2015, pp. 46–55, doi: 10.5220/0005226600460055.

[29] G. Tian, Z. Duan, T. Baumeister, and Y. Dong, "A traceback attack on Freenet," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 3, pp. 294–307, Jun. 2017, doi: 10.1109/TDSC.2015.2453983.

[30] G. Tian, Z. Duan, T. Baumeister, and Y. Dong, "Thwarting traceback attack on Freenet," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 741–746, doi: 10.1109/GLOCOM.2013.6831161.

[31] T. Baumeister, Y. Dong, Z. Duan, and G. Tian, "A routing table insertion (RTI) attack on Freenet," in *Proc. Int. Conf. Cyber Secur.*, Dec. 2012, pp. 8–15, doi: 10.1109/CyberSecurity.2012.8.

[32] T. Baumeister, Y. Dong, G. Tian, and Z. Duan, "Using randomized routing to counter routing table insertion attack on Freenet," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 754–759, doi: 10.1109/GLOCOM.2013.6831163.

[33] K. Shaukat, S. Luo, S. Chen, and D. Liu, "Cyber threat detection using machine learning techniques: A performance evaluation perspective," in *Proc. Int. Conf. Cyber Warfare Secur. (ICCWS)*, Oct. 2020, pp. 1–6, doi: 10.1109/ICCWS48432.2020.9292388.

[34] K. Finklea. (2017). *Dark Web Kristin Finklea Specialist in Domestic Security*. Dark Web. [Online]. Available: https://fas.org/sgp/crs/misc/R44101.pdf

[35] V. Ciancaglini and M. Balduzzi, "Cybercrmine in the deep web," 2015, pp. 1–31. [Online]. Available: https://www.blackhat.com/docs/eu-15/materials/eu-15-Balduzzi-Cybercrmine-In-The-Deep-Web-wp.pdf

[36] R. B. Zeid, J. Moubarak, and C. Bassil, "Investigating the darknet," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 727–732, doi: 10.1109/IWCMC48107.2020.9148422.

[37] K. Loesing and G. Wirtz, "Virtual private services," HotPETs, Tech. Rep., Jul. 2008, pp. 1–13.

[38] F. Platzer, M. Schäfer, and M. Steinebach, "Critical traffic analysis on the Tor network," in *Proc. 15th Int. Conf. Availability, Rel. Secur.*, Aug. 2020, pp. 1–10, doi: 10.1145/3407023.3409180.

[39] L. Ye, X. Yu, J. Zhao, D. Zhan, X. Du, and M. Guizani, "Deciding your own anonymity: User-oriented node selection in I2P," *IEEE Access*, vol. 6, pp. 71350–71359, 2018, doi: 10.1109/ACCESS.2018.2881719.

[40] N. P. Hoang, P. Kintis, M. Antonakakis, and M. Polychronakis, "An empirical study of the I2P anonymity network and its censorship resistance," 2018, *arXiv:1809.09086*.

[41] S. Roos, F. Platzer, J.-M. Heller, and T. Strufe, "Inferring obfuscated values in Freenet," in *Proc. Int. Conf. Workshops Networked Syst. (NetSys)*, Mar. 2015, pp. 1–8, doi: 10.1109/NetSys.2015.7089062.

[42] I. Clarke, S. G. Miller, T. W. Hong, O. Sandberg, and B. Wiley, "Protecting free expression online with Freenet," *IEEE Internet Comput.*, vol. 6, no. 1, pp. 40–49, Jan./Feb. 2002, doi: 10.1109/4236.978368.

[43] B. Conrad and F. Shirazi, "A Survey on Tor and I2P," in *Proc. 9th Int. Conf. Internet Monit. Protection*, 2014, pp. 22–28.

[44] A. Ali, M. Khan, M. Saddique, U. Pirzada, M. Zohaib, I. Ahmad, and N. Debnath, "Tor vs I2P: A comparative study," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Mar. 2016, pp. 1748–1751, doi: 10.1109/ICIT.2016.7475027.

[45] G. Owen and N. Savage, "The Tor dark net," Global Commissiion Internet Governance Paper Ser., 2015, no. 20, p. 9. [Online]. Available: https://www.cigionline.org/publications/tor-dark-net/

[46] *Global Estimates of Modern Slavery: Forced Labour and Forced Marriage*, Int. Labor Org., Geneva, Switzerland, 2017.

[47] J. Reid and B. Fox, "Human trafficking and the darknet: Technology, innovation, and evolving criminal justice strategies," in *Science Informed Policing* (Advanced Sciences and Technologies for Security Applications). Jun. 2020, pp. 77–96, doi: 10.1007/978-3-030-41287-6_5.

[48] R. Upadhyaya and A. Jain, "Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground Web and bitcoin wallet," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, Apr. 2016, pp. 143–148, doi: 10.1109/CCAA.2016.7813706.

[49] B. Sandor and D. J. Feher, "Examining the relationship between the bitcoin and cybercrime," in *Proc. IEEE 13th Int. Symp. Appl. Comput. Intell. Inform. (SACI)*, May 2019, pp. 121–126, doi: 10.1109/SACI46893.2019.9111568.

[50] G. Weimann, "Terrorist migration to the dark web," *Perspect. Terrorism*, vol. 10, no. 3, pp. 40–44, 2016.

[51] V. Bouché, *A Report on the Use of Technology to Recruit, Groom, and Sell Domestic Minor Sex Trafficking Victoms*. Los Angeles, CA, USA: Thorn, Jan. 2015.

[52] J. C. Nwaka and A. Odoemene, "'Baby factories: Exploitation of women in southern Nigeria," *Dignity, J. Sexual Exploitation Violence*, vol. 4, no. 2, pp. 1–2, Mar. 2019, doi: 10.23860/dignity.2019.04.02.02.

[53] T. Gillespie, "Governance of and by platforms," in *The SAGE Handbook of Social Media*, J. Burgess, A. Marwick, and T. Poell, Eds. London, U.K.: Sage, Forthcoming 2017. [Online]. Available: http://culturedigitally.org/wp-content/uploads/2016/06/GillespieGovernance-ofby-Platforms-PREPRINT.pdf

[54] E. Marin, J. Shakarian, and P. Shakarian, "Mining key-hackers on darkweb forums," in *Proc. 1st Int. Conf. Data Intell. Secur. (ICDIS)*, Apr. 2018, pp. 73–80, doi: 10.1109/ICDIS.2018.00018.

[55] I. Deliu, C. Leichter, and K. Franke, "Collecting cyber threat intelligence from hacker forums via a two-stage, hybrid process using support vector machines and latent Dirichlet allocation," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 5008–5013, doi: 10.1109/BigData.2018.8622469.

[56] G. L'Huillier, H. Alvarez, S. A. Ríos, and F. Aguilera, "Topic-based social network analysis for virtual communities of interests in the dark web," *ACM SIGKDD Explor. Newslett.*, vol. 12, no. 2, pp. 66–73, 2011, doi: 10.1145/1964897.1964917.

[57] Y. Yang, L. Yang, M. Yang, H. Yu, G. Zhu, Z. Chen, and L. Chen, "Dark web forum correlation analysis research," in *Proc. IEEE 8th Joint Int. Inf. Technol. Artif. Intell. Conf. (ITAIC)*, May 2019, pp. 1216–1220, doi: 10.1109/ITAIC.2019.8785760.

[58] H. Kobayashi, M. Kadoguchi, S. Hayashi, A. Otsuka, and M. Hashimoto, "An expert system for classifying harmful content on the dark web," in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Nov. 2020, pp. 1–6, doi: 10.1109/ISI49825.2020.9280536.

[59] N. Tavabi, N. Bartley, A. Abeliuk, S. Soni, E. Ferrara, and K. Lerman, "Characterizing activity on the deep and dark web," 2019, *arXiv:1903.00156*.

[60] M. Schafer, M. Fuchs, M. Strohmeier, M. Engel, M. Liechti, and V. Lenders, "BlackWidow: Monitoring the dark web for cyber security information," in *Proc. 11th Int. Conf. Cyber Conflict (CyCon)*, May 2019, pp. 1–21, doi: 10.23919/CYCON.2019.8756845.

[61] H. Alnabulsi and R. Islam, "Identification of illegal forum activities inside the dark net," in *Proc. Int. Conf. Mach. Learn. Data Eng. (iCMLDE)*, Dec. 2018, pp. 30–34, doi: 10.1109/iCMLDE.2018.00015.

[62] S. Sarkar, "The cyber defense review," in *Proc. Annu. Int. Conf. Cyber Conflict, (CyCon)*, vol. 126, no. 1, 2019, pp. 1–7.

[63] K. Godawatte, M. Raza, M. Murtaza, and A. Saeed, "Dark web along with the dark web marketing and surveillance," in *Proc. 20th Int. Conf. Parallel Distrib. Comput., Appl. Technol. (PDCAT)*, Dec. 2019, pp. 483–485, doi: 10.1109/PDCAT46702.2019.00095.

[64] F. Dong, S. Yuan, H. Ou, and L. Liu, "New cyber threat discovery from darknet marketplaces," in *Proc. IEEE Conf. Big Data Anal. (ICBDA)*, Nov. 2018, pp. 62–67, doi: 10.1109/ICBDAA.2018.8629658.

[65] O. Cherqi, G. Mezzour, M. Ghogho, and M. E. Koutbi, "Analysis of hacking related trade in the Darkweb," in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Nov. 2018, pp. 79–84, doi: 10.1109/ISI.2018.8587311.

[66] E. Nunes, P. Shakarian, and G. I. Simari, "At-risk system identification via analysis of discussions on the darkweb," in *Proc. APWG Symp. Electron. Crime Res. (eCrime)*, May 2018, pp. 1–12, doi: 10.1109/ECRIME.2018.8376211.

[67] B. AlKhatib and R. Basheer, "Crawling the dark web: A conceptual perspective, challenges and implementation," *J. Digit. Inf. Manage.*, vol. 17, no. 2, p. 51, Apr. 2019, doi: 10.6025/jdim/2019/17/2/51-60.

[68] N. Ferry, T. Hackenheimer, F. Herrmann, and A. Tourette, ''Methodology of dark web monitoring,'' in *Proc. 11th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Jun. 2019, pp. 1–7, doi: 10.1109/ECAI46879.2019.9042072.

[69] Y. Yang, H. Yu, L. Yang, M. Yang, L. Chen, G. Zhu, and L. Wen, ''Hadoop-based dark web threat intelligence analysis framework,'' in *Proc. IEEE 3rd Adv. Inf. Manage., Communicates, Electron. Autom. Control Conf. (IMCEC)*, Oct. 2019, pp. 1088–1091, doi: 10.1109/IMCEC46724.2019.8984106.

[70] M. Wang, X. Wang, J. Shi, Q. Tan, Y. Gao, M. Chen, and X. Jiang, ''Who are in the Darknet? Measurement and analysis of Darknet person attributes,'' in *Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2018, pp. 948–955, doi: 10.1109/DSC.2018.00151.

[71] A. Cuzzocrea, F. Martinelli, F. Mercaldo, and G. Vercelli, ''Tor traffic analysis and detection via machine learning techniques,'' in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 4474–4480, doi: 10.1109/BigData.2017.8258487.

[72] M. Kadoguchi, S. Hayashi, M. Hashimoto, and A. Otsuka, ''Exploring the dark web for cyber threat intelligence using machine leaning,'' in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Jul. 2019, pp. 200–202, doi: 10.1109/ISI.2019.8823360.

[73] C. Han, J. Shimamura, T. Takahashi, D. Inoue, M. Kawakita, J. Takeuchi, and K. Nakao, ''Real-time detection of malware activities by analyzing darknet traffic using graphical lasso,'' in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2019, pp. 144–151, doi: 10.1109/TrustCom/BigDataSE.2019.00028.

[74] S. Kumar, H. Vranken, J. V. Dijk, and T. Hamalainen, ''Deep in the dark: A novel threat detection system using darknet traffic,'' in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 4273–4279, doi: 10.1109/BigData47090.2019.9006374.

[75] F. Soro, I. Drago, M. Trevisan, M. Mellia, J. Ceron, and J. J. Santanna, ''Are darknets all the same? On darknet visibility for security monitoring,'' in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN)*, Jul. 2019, pp. 1–6, doi: 10.1109/LANMAN.2019.8847113.

[76] M. Ebrahimi, S. Samtani, Y. Chai, and H. Chen, ''Detecting cyber threats in non-English hacker forums: An adversarial cross-lingual knowledge transfer approach,'' in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2020, pp. 20–26, doi: 10.1109/SPW50608.2020.00021.

[77] Z. Li, S. Alrwais, Y. Xie, F. Yu, and X. Wang, ''Finding the linchpins of the dark web: A study on topologically dedicated hosts on malicious web infrastructures,'' in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 112–126, doi: 10.1109/SP.2013.18.

[78] P. Mayank and A. K. Singh, ''Tor traffic identification,'' in *Proc. 7th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Nov. 2017, pp. 85–91, doi: 10.1109/CSNT.2017.8418516.

[79] M. A. Sulaiman and S. Zhioua, ''Attacking Tor through unpopular ports,'' in *Proc. IEEE 33rd Int. Conf. Distrib. Comput. Syst. Workshops*, Jul. 2013, pp. 33–38, doi: 10.1109/ICDCSW.2013.29.

[80] Q. Tan, Y. Gao, J. Shi, X. Wang, and B. Fang, ''A closer look at eclipse attacks against Tor hidden services,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6, doi: 10.1109/ICC.2017.7996832.

[81] Q. Tan, G. Yue, J. Shi, X. Wang, B. Fang, and Z. Tian, ''Toward a comprehensive insight into the eclipse attacks of Tor hidden services,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1584–1593, Apr. 2019, doi: 10.1109/JIOT.2018.2846624.

[82] K. Ge and Y. He, ''Detection of Sybil attack on Tor resource distribution,'' in *Proc. IEEE Int. Conf. Power, Intell. Comput. Syst. (ICPICS)*, Jul. 2020, pp. 328–332, doi: 10.1109/ICPICS50287.2020.9202013.

[83] Y. Sun, A. Edmundson, N. Feamster, M. Chiang, and P. Mittal, ''Counter-RAPTOR: Safeguarding Tor against active routing attacks,'' in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 977–992, doi: 10.1109/SP.2017.34.

[84] V. R. Kebande, L. Mlotshwa, and N. M. Karie, ''Botnet's obfuscated C&C infrastructure take-down approaches based on monitoring centralized Zeus bot variant's propagation model,'' in *Proc. IST-Afr. Week Conf. (IST-Afr.)*, May 2019, pp. 1–10, doi: 10.23919/ISTAFRICA.2019.8764837.

[85] M. Wilson and B. Bazli, ''Forensic analysis of I2P activities,'' in *Proc. 22nd Int. Conf. Autom. Comput. (ICAC)*, Sep. 2016, pp. 529–534, doi: 10.1109/IConAC.2016.7604974.

[86] K. Alachkar and D. Gaastra. (2018). *Blockchain-Based Sybil Attack Mitigation: A Case Study of the I2P Network*. [Online]. Available: https://www.os3.nl/_media/2017-2018/courses/rp2/p97_report.pdf

JAVERIAH SALEEM received the B.Sc. degree in electrical engineering specialization in computer from the Taxila, University of Engineering and Technology, Pakistan. She is currently pursuing the Bachelor of Honours degree in computing with the School of Computing and Mathematics, Charles Sturt University, Australia, under the supervision of Dr. Rafiqul Islam. Her main research interests include cybersecurity, dark web, machine learning, and data analysis.

RAFIQUL ISLAM (Senior Member, IEEE) is currently an Associate Professor with the School of Computing, Mathematics and Engineering, Charles Sturt University, Australia. He has a strong research background in cybersecurity, with a specific focus on malware analysis and classification, authentication, security in the cloud, privacy in social media, and the Internet of Things (IoT). He is leading the Cybersecurity Research Team and has developed a strong background in leadership, sustainability, and collaborative research in the area. He has a strong publication record with more than 180 published peer-reviewed research papers.

Dr. Islam is recognized as being at the national forefront of his research field cybersecurity. His contribution is recognized nationally and internationally by achieving various rewards, such as a professional excellence reward, a research excellence award, and a leadership award.

MUHAMMAD ASHAD KABIR (Member, IEEE) received the Ph.D. degree in computer science from the Swinburne University of Technology, Melbourne, Australia.

He is currently the Deputy Leader of the Data Mining Research Group and a Senior Lecturer with the School of Computing Mathematics and Engineering, Charles Sturt University, Australia. He has published over 75 peer-reviewed articles. His research interests include data mining, data analytics and visualization, blockchain and security, smart mobile applications, health informatics, human–computer interactions, adaptive, and context-aware software.