Journal of Network and Information Security
12 (1) 2024, 39-46
http://www.publishingindia.com/jnis

The Dark Web: An Analysis of its Structure, Activities and Implications

Sushma Malik[1*], Anamika Rana[2] and Madhu Chauhan[3]
[1]Associate Professor, Institute of Innovation in Technology and Management, Janakpuri, New Delhi, India. Email: sushmamalikiitm@gmail.com
[2]Associate Professor, Maharaja Surajmal Institute, Janakpuri, New Delhi, India. Email: anamica.rana@gmail.com
[3]Associate Professor, Institute of Innovation in Technology and Management, Janakpuri, New Delhi, India.
[*]Corresponding Author

Abstract: The internet has indeed become an integral part of daily life for people worldwide, offering a wealth of information and communication opportunities. However, alongside the conventional and easily accessible content on the internet, there exists a hidden portion known as the dark web. The dark web refers to websites and content that are intentionally concealed and can only be accessed through specific software or configurations. This research paper provides an in-depth analysis of the dark web, a hidden part of the internet known for its anonymity and association with illicit activities. The paper examines the structure of the dark web, the range of activities that occur within it, and the implications it poses for society, law enforcement, and cybersecurity. By exploring both the positive and negative aspects, this paper aims to provide a comprehensive understanding of the dark web and its impact on the digital landscape.

Keywords: Dark web, Internet, Security, TOR, Web, World Wide Web (WWW).

I. Introduction

The Internet has, over time, completely transformed the computer and communications industries. Without regard to a person's physical location, the Internet, which has global broadcasting capabilities, is employed as a method for information transmission as well as a medium for collaboration and engagement [1]. The rapid growth of the Internet has had an impact on the lives of billions of people. The network has severely pierced every little aspect of our lives. In addition to giving people the chance to travel the world from their desks, the internet has developed into a potent artificial intelligence resource [2]. The World Wide Web can be accessed via a link known as the Internet. The "dark web" refers to internet content that is encrypted and inaccessible to conventional search engines. The dark web can only be accessed with a select few browsers, such as TOR Browser. Using the dark web instead of regular websites provides far greater privacy and anonymity. The dark web is a part of the internet that is intentionally hidden and inaccessible through standard web browsers and search engines. It forms a small fraction of the overall internet and is characterized by its anonymity and encrypted communication channels [3] [4].

Structure of Internet

The World Wide Web (web) and the Internet are sometimes confused, but they are not the same thing. The Internet is a global network of interconnected computer networks that allows for the transfer of data and communication between devices. It encompasses a wide range of technologies and services beyond just the web. The World Wide Web

(web), on the other hand, is a network of connected hypertext pages that can be accessed via the Internet and web browsers. It is a subset of the Internet and represents the collection of websites, web pages, and other resources that are publicly accessible and interconnected through hyperlinks. While the web is a significant part of the Internet, it is important to understand that the Internet itself includes various other services and protocols such as email, file transfer (FTP), peer-to-peer networks, instant messaging, and more. These services operate independently of the web and contribute to the broader functionality of the Internet as a whole. So, when people refer to "the Internet," they may be referring to the entire network infrastructure, whereas the "World Wide Web" specifically pertains to the collection of websites and web pages accessible through web browsers [5] [6] [7] [8].

The World Wide Web is a network of connected HTML pages that may be accessed online. It has three layers as shown in Fig. 1:

- *Surface Web:* The surface web refers to the portion of the World Wide Web that is easily accessible and indexed by search engines. It includes websites and web pages that are publicly available and can be accessed through standard web browsers like Google Chrome, Firefox, or Safari. Examples of surface web content include news sites, social media platforms, online shopping websites, and most of the content you come across during regular internet browsing [5].
- *Deep Web:* The deep web, also known as the invisible web or hidden web, refers to the portion of the Internet that is not indexed by search engines. This includes content that is not directly accessible through traditional search engine queries. The deep web consists of pages that are behind paywalls, password-protected sites, private databases, academic resources, medical records, online banking systems, and other similar content. It is estimated that the deep web is significantly larger than the surface web in terms of content [5].
- *Dark Web:* The dark web is a small, hidden portion of the Internet that requires special software, such as the Tor network, to access. It is intentionally concealed and provides anonymity to its users. The dark web is known for hosting various illegal activities, such as illicit marketplaces, hacking forums, illegal pornography, and other forms of criminal activity. It is important to note that while the dark web itself is not illegal, engaging in illegal activities within it is against the law [5].

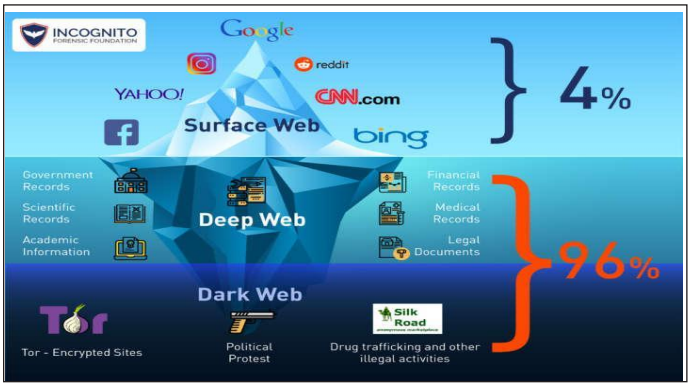

Fig. 1: Layers of World Wide Web [8]

II. Some Key Aspects of the Dark Web

The term "dark web" refers to a part of the internet that is intentionally hidden and inaccessible to conventional search engines. It is often associated with illicit activities, anonymity, and a lack of regulation. Here are some aspects and characteristics commonly associated with the dark web:

- *Anonymity and Privacy:* The dark web provides a level of anonymity to its users by utilizing software like Tor (The Onion Router) or other similar anonymizing networks. These networks encrypt and route internet traffic through a series of relays, making it difficult to trace the source or destination of the communication [9].
- *Hidden Websites and Content:* On the dark web, websites and content are deliberately concealed and are not indexed by traditional search engines. Instead, users rely on special software, configurations, or specific URLs to access these hidden sites, often using .onion domains [9].
- *Darknet Marketplaces:* One prominent feature of the dark web is the presence of darknet marketplaces. These online platforms allow

users to buy and sell various goods and services, including drugs, weapons, counterfeit currencies, hacking tools, stolen data, and more. Transactions in these marketplaces are often conducted using cryptocurrencies for increased anonymity [10].

- *Illicit Activities:* The dark web has gained notoriety for facilitating illegal activities. Criminal operations such as drug trafficking, weapons trading, cybercrime, identity theft, and hacking services are prevalent. However, it is important to note that not all activities on the dark web are illicit, and there are legitimate use cases as well [4].
- *Communication and Whistleblowing:* The dark web also provides a platform for anonymous communication and whistleblowing. Individuals can engage in private and encrypted conversations, exchange information, and share sensitive documents without revealing their identities [5].
- *Risks and Dangers:* Accessing the dark web carries certain risks. Malware, scams, phishing attempts, and other cyber threats are prevalent. Engaging in illegal activities on the dark web can lead to legal consequences, as law enforcement agencies actively monitor and investigate these platforms [9].

III. Purpose and Objectives of the Research

The purpose of research on the dark web is to gain a deeper understanding of this hidden part of the internet and its various aspects. The objectives of such research may include:

- *Exploration and Documentation:* Research aims to explore and document the structure, functionality, and operation of the dark web. This includes investigating the technical aspects, such as the software and protocols used for access, as well as the organization and dynamics of darknet marketplaces and hidden websites.
- *Analysis of Illicit Activities:* The dark web is known for facilitating illegal activities, and research seeks to analyze and understand the extent, nature, and impact of these activities. This involves studying the types of illicit goods and services traded, the methods of operation, and the associated risks and consequences.
- *Understanding the Dark Web Ecosystem:* Research aims to provide insights into the ecosystem of the dark web, including its users, communities, and communication channels. This involves examining the motivations of individuals engaging in dark web activities, the social dynamics, and the development of norms and rules within this hidden environment.
- *Impact on Society and Law Enforcement:* Research on the dark web explores the implications for society, law enforcement, and cybersecurity. This includes understanding the challenges faced by law enforcement agencies in detecting and combating dark web-related crimes, assessing the effectiveness of existing strategies, and identifying potential areas for improvement.
- *Privacy, Ethics, and Policy Considerations:* Research on the dark web also delves into the ethical considerations surrounding privacy, surveillance, and online freedom. It examines the balance between individual privacy rights and the need for law enforcement and explores the policy implications related to regulating the dark web.
- *Development of Countermeasures:* Research aims to contribute to the development of effective countermeasures against dark web-related risks and threats. This includes studying cybersecurity measures, techniques for tracking and identifying illicit activities, and strategies for mitigating the harm caused by the dark web.
- By conducting research on the dark web, scholars, policymakers, and law enforcement agencies can gain valuable insights into this hidden online landscape. The knowledge gained from such research can help inform policies, improve cybersecurity measures, and

enhance law enforcement efforts to combat illegal activities while also addressing privacy concerns and safeguarding individual rights.

IV. Technical Aspects of the Dark Web

The dark web relies on several technical aspects to provide anonymity and concealment. Here are some key technical components and mechanisms of the dark web [11] [12]:

- *Onion Routing:* The primary technology behind the dark web is onion routing, which anonymizes internet traffic by encrypting and routing it through a network of volunteer-operated relays. The most widely used implementation of onion routing is Tor (The Onion Router). When using Tor, the user's internet traffic is encrypted and passed through multiple relays, each layer of encryption being peeled off at each relay, similar to peeling layers of an onion. This makes it difficult to trace the origin or destination of the communication.
- *Tor Network:* The Tor network is a decentralized network of volunteer-operated relays that facilitate the anonymity of the dark web. The relays are distributed worldwide, and each relay only knows the previous and next hop in the communication chain, ensuring that no single relay has complete knowledge of the entire communication path.
- *Hidden Services:* Hidden services, also known as onion services, are websites or online services hosted on the dark web that can only be accessed through Tor. These websites have .onion domains and are designed to provide anonymity to both the users and the service operators. Hidden services use Tor's encryption and routing mechanisms to ensure that the traffic remains within the Tor network and that the website's actual location remains hidden.
- *Encryption and Anonymity:* Encryption plays a crucial role in securing communications on the dark web. Tor uses multiple layers of encryption to protect the data transmitted between relays and hidden services. This ensures that even if someone intercepts the traffic, they cannot decipher the content. Additionally, the use of onion routing and decentralized relays adds an extra layer of anonymity, making it challenging to identify the source or destination of the communication.
- *Accessing the Dark Web:* To access the dark web, users typically utilize special software like the Tor browser. The Tor browser is a modified version of the Firefox web browser that is configured to connect to the Tor network. It enables users to browse websites hosted on the dark web and access hidden services.
- *Additional Privacy Tools:* In addition to Tor, there are other privacy tools and networks that are used in conjunction with the dark web. These include Virtual Private Networks (VPNs), which can add an extra layer of encryption and conceal the user's IP address, and other anonymizing networks like I2P (Invisible Internet Project) that provide similar anonymity features.

V. Cybercrime on the Dark Web

The dark web is known for hosting various illegal activities and facilitating cybercrimes. Some common types of cybercrimes associated with the dark web include [13] [14] [15] [16] [17]:

- *Illegal Marketplaces:* Dark web marketplaces provide a platform for the buying and selling of illegal goods and services, such as drugs, firearms, stolen data, hacking tools, counterfeit money, and more. These marketplaces often operate using cryptocurrencies to maintain anonymity.
- *Hacking Tools and Services:* The dark web is a hub for hackers offering hacking tools, exploit kits, malware, and hacking services. Cybercriminals can purchase these tools and services to carry out attacks on individuals, organizations, or even entire computer networks.
- *Stolen Data and Identity Theft:* The dark web is a major marketplace for stolen personal information, including credit card details, login credentials, Social Security numbers, and

more. Cybercriminals engage in identity theft, financial fraud, and other illegal activities using this stolen data.

- *Gambling:* Gambling on the dark web uses bitcoin, despite being a trade that takes place both on and off the dark web. Many renowned Bitcoin gambling sites have blacklisted U.S.-specific IP addresses due to severe regulations and prosecutions by the U.S. government. However, users of the dark web are able to gamble at will using their existing IP addresses.
- *Distributed Denial of Service (DDoS) Attacks:* The dark web hosts forums and marketplaces where individuals can purchase DDoS attack services. These attacks involve overwhelming a target's website or network with an excessive amount of traffic, rendering it inaccessible to users.
- *Cyber Extortion and Ransomware:* The dark web is a platform where cybercriminals offer ransomware-as-a-service (RaaS) and engage in cyber extortion. They may distribute ransomware to encrypt victims' files and demand a ransom in exchange for decryption keys.
- *Child Exploitation:* Disturbingly, the dark web is also known for hosting websites and forums related to child pornography and child exploitation. Law enforcement agencies actively work to combat these heinous activities.
- *Proxying:* Because the dark web lacks the hypertext transfer protocol (https), which is normally present in standard Uniform Resource Locators (URL), users are more vulnerable to proxying attacks. Therefore, the security measures that are associated with https are skipped. When a hacker intervenes between a website and a user, this is known as proxying. The hacker deceives the users into thinking that the source of the website they have altered is legitimate. On such a website, a typical transaction made using an untraceable cryptocurrency like bitcoin will defraud the user while the hacker moves the money. Popular dark web group chat Black Death frequently switches its URL.
- *Terrorism:* A terrorist organization must have secret communication in order to function. The dark web satisfies the demand for terrorism to outfit an anonymous network that is accessible yet hidden from the public Internet. The dark web is the greatest platform for promoting terrorism since it makes it simple and untraceable to shut down sites used for recruiting, funding, and propaganda.
- *Financial Fraud:* There are various forms of financial fraud on the dark web. The most prevalent kind of financial fraud on the dark web is phishing, in which a person is directed to a website that seems similar to one they want to visit. The website is different, though, and the services it claims to offer could be fake. Since dark web sites frequently alter their domains and aesthetic appearances, it might be challenging to recognize a phishing site because there is no permanent structure that resembles a conventional site. Financial fraud on the dark web cannot be used against the opposing party, unlike surface web fraud, where you might file a complaint and pursue legal action against some convicted person.

VI. A Mechanism for Dark Web Access

Accessing the dark web involves a specific mechanism that differs from accessing the regular surface web. Here is a general overview of the access mechanism for the dark web [18] [10] [19] [12] as shown in Fig. 2:

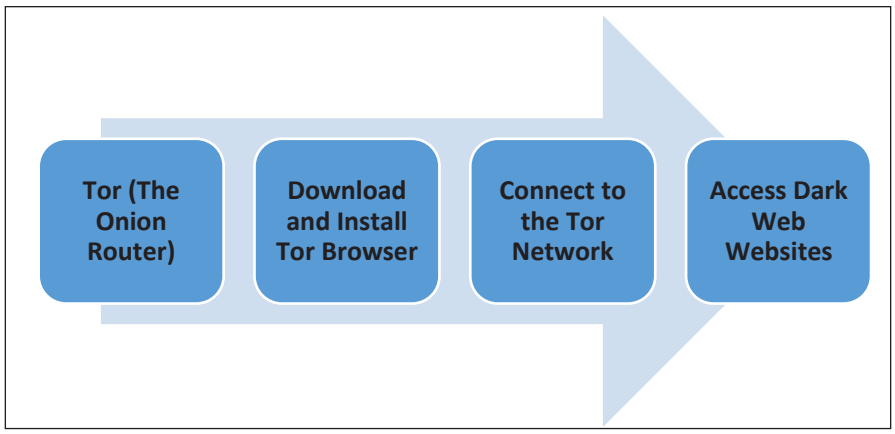

Fig. 2: Mechanism for Access of Dark Web

- *Tor (The Onion Router):* The most common method for accessing the dark web is through the use of Tor. Tor is free and open-source software that enables anonymous communication by routing internet traffic through a network of volunteer-operated servers. This network of servers, known as the Tor network, helps protect the identity and location of users by encrypting and bouncing their traffic through multiple relays.
- *Download and Install Tor Browser:* To access the dark web, you need to download and install the Tor Browser, which is a modified version of the Mozilla Firefox browser that is specifically configured to work with the Tor network. The Tor Browser routes your internet traffic through the Tor network, making it difficult to trace back to your actual location.
- *Connect to the Tor Network:* Once the Tor Browser is installed, launch it and connect to the Tor network. The browser will establish a connection to the network, and you will be assigned a new IP address that helps preserve your anonymity.
- *Access Dark Web Websites:* With the Tor Browser connected to the Tor network, you can now access dark web websites by entering their .onion URLs directly into the browser's address bar. Dark web websites use the .onion domain extension and are not indexed by search engines.

Using onion routing, web traffic is encrypted and redirected over Tor's onion network. Data is safeguarded by multiple layers of encryption before being sent through a group of network nodes known as onion routers. Each router (or node) "peels away" a layer of encryption in order for the data to arrive at its destination fully decrypted [20].

Encrypted data is routed anonymously across the three global proxy layers that comprise the Tor circuit. Let's examine the three tiers of network nodes in more detail:

- *Entry Node:* Tor Browser initially establishes an arbitrary connection with an entrance node that is well-known to the public. Data is added to the Tor circuit by the entering node.
- *Middle Nodes:* All the data is encrypted here. The data is then routed through a succession of nodes that gradually decrypt it. Each middle node only knows the identities of the intermediate nodes that come before it and after it, maintaining anonymity.
- *Exit Node:* After the final layer of encryption has been removed, the decrypted data travels through an exit node to leave the Tor network and get to its destination server.

In order to encrypt and decode traffic, Tor Browser routes web traffic through an entry node (blue), middle node (green), and exit node (orange), as depicted in Fig. 3.

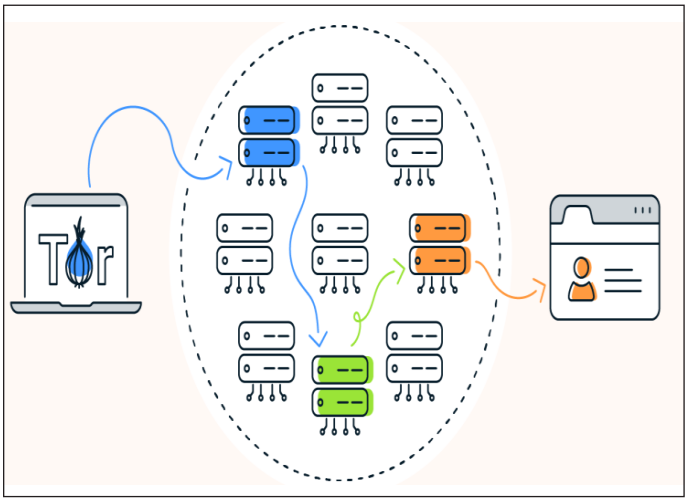

Fig. 3: The Three Global Proxy Layers [20]

It's important to exercise caution and follow best practices when accessing the dark web. Here are a few additional tips:

- Be cautious about the websites you visit and the activities you engage in. The dark web is known for illegal and illicit activities, and engaging in such activities can have serious legal consequences.
- Keep your Tor Browser up to date to benefit from security updates and patches.
- Avoid downloading files or running scripts from untrusted sources, as they may contain malware or compromise your anonymity.
- Remember that anonymity on the dark web is not foolproof, and there are potential vulnerabilities that could be exploited. It's important to educate yourself about potential risks and take necessary precautions.

VII. Conclusion

The darker portion of the Internet, known as the "dark web," is frequently used by users to carry out certain tasks covertly and without leaving any evidence. The explicit classification under the specific categories of crimes demonstrates that the dark web is a hub for illegal operations like child pornography, the trafficking of weapons, drugs, and proxies, among others. The major factor allowing these pervasive illicit activities to serve as a gateway to the criminal world is the anonymity offered by this platform. The huge sites accessible under the dark web are held by a variety of risky organizations, including espionage, terrorists, and thieves. These organizations may decide to prey on any weak individuals or international companies in order to benefit. Law enforcement finds it difficult to control the exploitations within all times boundary national and regional because to the untraceable nature of the crimes committed due to the borderless nature of the Internet. The dark web's benefits and drawbacks can be summed up as being determined by the user's goals. Therefore, it is imperative that internet users exercise caution when utilizing the internet to avoid becoming victims of these unlawful activities on the dark web.

References

[1] C. M. S. Steel, "Stolen identity valuation and market evolution on the dark web," *Int. J. Cyber Criminol.*, vol. 13, no. 1, pp. 70-83, 2019, doi: https://doi.org/10.5281/zenodo.3539500.

[2] M. Kadoguchi, H. Kobayashi, S. Hayashi, A. Otsuka, and M. Hashimoto, "Deep self-supervised clustering of the dark web for cyber threat intelligence," in *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2020, pp. 1-6.

[3] A. M. H. Taha, D. Ariffin, and S. S. Abu-Naser, "A systematic literature review of deep and machine learning algorithms in brain tumor and meta-analysis," *J. Theor. Appl. Inf. Technol.*, vol. 101, no. 1, pp. 21-36, 2023.

[4] A. Bloomenthal, "What is the dark web and should you access it?," 2022. Accessed: Jul. 14, 2023. [Online]. Available: https://www.investopedia.com/terms/d/dark-web.asp

[5] J. Saleem, R. Islam, and M. A. Kabir, "The anonymity of the dark web: A survey," *IEEE Access*, vol. 10, pp. 33628-33660, 2022.

[6] J. Hall, "ExtremeTech explains: All about the dark web, and how to use it | Extremetech," 2017. Accessed: Jul. 14, 2023. [Online].

Available: https://www.extremetech.com/internet/245086-deep-dive-dark-web-how-to-use

[7] R. Elangovan, "The dark web: Hidden access to internet today," in *Encyclopedia of Criminal Activities and the Deep Web*. IGI Global, 2020, pp. 129-139.

[8] Cyber IFF, "The layers of the web – surface web, deep web and dark web." Accessed: Jul. 14, 2023. [Online]. Available: https://ifflab.org/the-layers-of-the-web-surface-web-deep-web-and-dark-web/

[9] B. Mohammed, "Dark web access, hidden services and security challenges," 2022.

[10] M. Faizan, and R. A. Khan, "Exploring and analyzing the dark web: A new alchemy," *First Monday*, 2019.

[11] S. Sobhan et al., "A review of dark web: Trends and future directions," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2022, pp. 1780-1785.

[12] H. Zhang, and F. Zou, "A survey of the dark web and dark market research," in *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, 2020, pp. 1694-1705.

[13] S. Kaur, and S. Randhawa, "Dark web: A web of crimes," *Wirel. Pers. Commun.*, vol. 112, pp. 2131-2158, 2020.

[14] J. Besenyő, and A. Gulyas, "The effect of the dark web on the security," *J. Secur. Sustain. Issues*, vol. 11, no. 1, 2021.

[15] E. F. dos Reis, A. Teytelboym, A. ElBahraw, I. De Loizaga, and A. Baronchelli, "Identifying key players in dark web marketplaces," *arXiv Prepr. arXiv2306.09485*, 2023.

[16] D. Georgoulias, J. M. Pedersen, M. Falch, and E. Vasilomanolakis, "A qualitative mapping of Darkweb marketplaces," in *2021 APWG Symposium on Electronic Crime Research (eCrime)*, 2021, pp. 1-15.

[17] M. Chawki, "The dark web and the future of illicit drug markets," *J. Transp. Secur.*, vol. 15, no. 3-4, pp. 173-191, 2022.

[18] F. T. Ngo, C. Marcum, and S. Belshaw, "The dark web: What is it, How to access it, and Why we need to study it," *J. Contemp. Crim. Justice*, vol. 39, no. 2, pp. 160-166, 2023.

[19] D. Kavallieros, D. Myttas, E. Kermitsis, E. Lissaris, G. Giataganas, and E. Darra, "Using the dark web," *Dark Web Investig.*, pp. 27-48, 2021.

[20] D. Ghimiray, "Dark web browser: What is Tor, Is it safe & How to use it | Avast," 2022. Accessed: Jul. 14, 2023. [Online]. Available: https://www.avast.com/c-tor-dark-web-browser