IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13330

The Dark Web: An Examination of the Internet's Shadowy Areas

Mr. G. Balaji[1], Mrs. P. Menaka, M.C.A., M.Phil., (Ph.D.,)[2]

Department of Information Technology, Dr. N. G. P. Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Assistant Professor (SG), Department of Information Technology, Dr. N. G. P. Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: There are two primary parts of the Internet: the "Deep Web" and the "Surface Web." The Deep Web consists of unindexed pages, while the Surface Web consists of all publicly accessible and indexed websites. Because it contains hidden content on the World Wide Web, the "dark web" makes up the largest portion of the Deep Web. Certain software, authentication, and settings are required in order to use it. A multi-layer encryption method called the Onion Router, or TOR, safeguards user confidentiality and privacy. Numerous studies and surveys indicate that most internet users think the deep web and the dark web are interchangeable. To shed light on this and analyze the structure of the Internet, this article explores the current composition of the Internet and that section of the World Wide Web, which includes the Surface Web, Deep Web, and Dark Web. This phrase highlights the benefits of utilizing the Tor browser in the dark web and its useful applications while outlining the differences between the deep web and the dark web.

Keywords: Dark web, deep web, encryption, TOR, anonymous, privacy, access.

INTRODUCTION

Everybody uses the Internet on a daily basis. The "Deep Web to" and the "Surface Web" are the two online building pieces. The Surface Web, which is accessible for indexing by search engines like Google, Bing, Yahoo, and others, is made up of websites like YouTube, Facebook, Wikipedia, Amazon, and others. The "Visible Web" is another name for the Surface Web. However, the problem is not with the Internet. Just 4% of the whole internet is accessible to the general public through the Surface Web [1]. On the internet, there is a wealth of legally accessible content. 96% of the Internet is made up of hidden websites that are not accessible to the general public. The deep web is located in this peculiar area. The same goes for compelled access to data, including private accounts or internet banking. "Hidden networks" provide consumers with privacy [2]. Your name and other personal information will be made public if these websites are indexed, making it possible for anybody to find the information through a search. To preserve secrecy, pages with authentication protection are not indexed. Deep web authentication is used to access these websites. Some people refer to a portion of the Deep Web as the "Invisible Web," or the "Dark Web." The Dark Web is inaccessible to the general public, with only 45,000 dark web sites accounting for 0.01% of the total Internet [3, 4].

One term for the concealed content on the WWW (World Wide Web) is the "dark web." occupant. It makes use of the Internet, but it needs specific software, permissions, configurations, etc. It provides privacy and is not indexed by search engines. Darkness The page can only be seen by internal browsers with specific anonymizing software installed, such as Subgraph, Water fox, TOR (The Onion Router), I2P (Invisible Internet Project), and others. This image is from the Surface Web. The encrypted internet can be used by both high and low performers. This is a fact for both buyers and businesses. The easiest way to access the dark web is through TOR. It can be applied to both legitimate and illicit activities. The freedom of speech of journalists and whistleblowers, data sharing globally to safeguard privacy, and illicit applications of the dark web, such as drug sales, credit card theft, gambling, etc., are examples of legitimate usage. [5]. The dark web and the surface web work together. It functions in the same way as Clearnet. Its webpages resemble the Surface Web. For instance, it features business websites that resemble Flipkart or Amazon, which sell or buy goods, and Wikileaks, which is equivalent to Wikipedia on the Surface Web. It transfers traffic (HTTP and FTP) and between networks using the corresponding TCP/IP protocol application. Benefits and HTML pages make up its content. The dark web is notorious for illicit activities and is regarded as a risky location

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025
DOI: 10.17148/IJIREEICE.2025.13330

where drug dealing and other illicit activities occur. This can be a highly safe way to browse the internet if privacy is a concern [6].

THE DEEP WEB IS NOT THE SAME AS THE DARK WEB

The deep web and the black web are different, despite the common misperception that they are interchangeable. For user protection, the deep web is purposefully not indexed and unavailable to conventional search engines. On the other hand, the black web is a section of thedeepwebthathasbeenpurposefullyde-indexedinordertoprotectuserprivacy. It's odd that the black web is only accessible through one browser. Using the dark web exposes you to strange servers. The TOR network retains everything that offers users the same degree of security and privacy.

THE DEEP WEB

The deep web is not as dark and is much the same as it appears beneath the surface. The deep web lists every website that is not indexed, preventing search engines from returning it to us [7]. Because they are user-specific and don't require indexation for every URL, the deep web also contains a portion of the legitimate mainstream network, like Amazon, IMDB, and Netflix. The majority of individuals are unaware that they are using the deep web. Some websites, such as Facebook and Instagram, are also categorized as deep web because they may be accessed via the application program's user interface. The deep web contains all of the information that is not accessible by conventional search engines. Although its precise dimensions are uncertain, it is anticipated to be 400–500 times larger than the Surface Web. Accessing data from the deep web is difficult for conventional search engines like Google, mostly because of problems with naming conventions and inconsistent data. Since access to material on anonymous websites frequently requires login credentials, indexing these websites becomes challenging. These websites have time limits and are inaccessible after a predetermined amount of time. There is an infinite amount of intellectual content available on the deep web. Websites and pages that are not immediately accessible during standard internet searches are included in the deep web. This covers anything that needs a login, like online financial services and personal accounts. Because it safeguards
Private information and confidentiality, the deep web is extremely significant and safe. In daily life, it is essential. It offers customers privacy and security [8].

THE DARK WEB

The Dark Web is a smaller, more restricted subset of the Deep Web that is mostly used for illegal and informative purposes. The Dark Web uses TOR encryption to provide as a platform for private communication [9]. It is located in the lowest reaches of the internet. It is accessible via an anonymous browser that has to be verified and authenticated. Not all deep webs are dark webs, even though all dark webs are deep webs.

Getting Onto The Dark Web: A Summary Of TOR:

Websites that are hidden or unindexed on the Internet are referred to as the "dark web." In a specific network, it exists, but in a normal network, it cannot be detected. ICICC 2020, the International Conference on Innovative Computing and Communication The primary means of accessing the Dark Web is the TOR browser, also known as The Onion Router. TOR was primarily created for a variety of unique uses. The US Naval Research Laboratory created TOR in the 2000s [10]. The creation of TOR was intended to give US military personnel working abroad secrecy. Tor is a technique that uses many layers of encryption. The term "Onion Router" comes from its multiple layers, which resemble an onion. The multi-layered structure of TOR allows one to know which device it is traversing next and which one it has already passed through, but not the source or destination devices. Before being sent consecutively to the following device, data packets are first forwarded at each device by unwrapping their current receiving layer. The data saved in the subsequent device will be extracted by the current device. It has no knowledge where the data packets are coming from or leaving, but it is aware of the data path from which it received the data and the location from which

DOI: 10.17148/IJIREEICE.2025.13330

it is sending the data packet. This is the fundamental onion routing standard. Data packets that lack a network origin or destination are therefore untraceable. Address systems composed of randomly generated keys represented by address suffixes are used by TOR to control "hidden sites". The onion TOR is the most straightforward way to access dark websites. Website URLs are altered to prevent exposure and Distributed Denial of Service (DDoS) attacks, and TOR URLs are typically complicated and challenging to remember [11, 12]. If one of these browsers is installed on your computer, you can access dark websites. It is important to remember that the majority of filthy and nefarious dark websites require passwords and invite-only access.

HOW TOR WORKS

TOR operates using the "Onion Routing" technological model, in which user data is encrypted before being transmitted via a number of relays inside the TOR network. Layered encryption is used to protect the user and hide their identity. It works by using an intermediary relay circuit to go around the connections between the user's device and the desired location. They are run exclusively by volunteers who are prepared to donate their data talents for any reason, and they may be located anywhere in the world. When anonymity and network speed are the top concerns, more relays stand out because of the massive data transfers that each relay has [13]. User monitoring gets increasingly challenging as the number of relays increases.

HOW IS THE DARK WEB OPERATING

Users of the Dark Web frequently visit TOR websites. The onion domain is used to address TOR sites. The TOR browser's main objective is to provide anonymous access to the Internet's dark web. Every email address or website serves as a Dark Web node or entrance point [14]. This node or entry point establishes a connection to the website's actual storage server. These nodes, which are connected in a way that protects the user's identity when they browse the dark web page, provide access to the network. Locations and identities are hidden by a complex encryption technology, rendering them untraceable. The next node in the network that leads to the destination has the ability to decrypt the sent data. It is secure and privacy is preserved. Because of the intricacy of this system, neither the node path nor the information levels can be replicated. Because of the great degree of anonymity, users do not receive any information about the host, and websites are unable to monitor their IP address or location. On the Dark Web, user-to-user communication is highly encrypted, enabling private file sharing, blogging, and conversation. Every connection is secure and encrypted. Network access cannot be restricted. On the dark web, the site is anonymous due to connections and encryption.

Fraudsters and other criminals choose to establish their presence in this hidden online realm because of the increased level of anonymity on the Dark Web, which makes browsing safer. Dark web servers are made to avoid storing data that might identify a person. Because dark websites cannot be searched, they offer a high level of security. On the black web, web browsing is extremely slow [15].

FEATURES OF THE DARK WEB AND ITS USES

Data sent over web-based applications and the surface portion of the Internet are extremely susceptible to security lapses and other threats [16]. However, there are several significant benefits that the Dark Web offers, including user privacy when using the Internet, anonymity and secrecy, sharing information with internet censorship, buying restricted commodities, freedom of speech, etc. These characteristics may be found in dark web apps like bitcoin, the most widely used cryptocurrency for transactions, and dark web markets, sometimes referred to as crypto markets, which are used exclusively for TOR-based product sales. Even while using TOR to access the dark web guarantees user anonymity, there are a few requirements listed to further protect identification.

Characteristics of the Dark Web:

Following is a discussion of the dark web's various features.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13330

- **Privacy when using the Internet:** The dark web has just as many websites as the high web. These websites include those for video games, businesses, blogs, social media, movies, email services, and more.

  This acts as a very comprehensive data source. It is applicable in both legal and illegal settings.

- **Anonymity:** Users can safely surf dark websites and are granted privacy. The dark web can be used to access unindexed websites that don't return any search results. A high degree of anonymity is provided by the multi-layer encryption technology, which hides user IDs and locations and makes them untraceable.

  - **Purchase of Restricted Items:** It is acceptable to buy some products from the Dark Web. For instance, several Asian and Middle Eastern nations may for bid the use of some medications that are permitted in Europe, such as pain relievers and sleeping medicines.
  - **Exposing abuses of power:** Anything that could upset government and governance can be covered by journalists and political campaigns on the Dark Web. infringes upon someone's privacy. Since these countries do not like to disclose their information to the public, information is a potent weapon in their arsenal. In this context, the Dark Web is crucial for fostering a safe channel of communication both domestically and internationally.
  - **Freedom of speech:** This directly relates to privacy, allowing people to freely express their opinions on any topic without fear. Bullying is accepted in some countries, allowing everyone to exercise their right to free speech.

Conditions to Preserve Anonymity:

- Never reveal your real name or photographs.
- To prevent being tracked, always use distinct, anonymous passwords, accounts, and false identities.
- When transacting, always utilize a private Bit coin dark wallet.
- To prevent your IP address from being revealed, refrain from using JavaScript, installing browser extensions, and turning off cookies.
- To prevent browser finger printing, never resize the TOR browser window.
- When using a TOR browser to open documents, always unplug from the Internet.

APPLICATIONS FOR THE DARK WEB

Darknet Market:

A darknet marketplace, sometimes referred to as a crypto market, is a dark web selling or marketing website that uses Tor, I2P, or Freenet to sell goods because these browsers conceal users' location and identities. Guns, drugs, weapons, illegal commerce, credit card fraud, cyberweapons, counterfeit currency, and other illegal and legal goods are all dealt in on this black market. Gareth Owen of the University of Portsmouth proposed the Darknet Market as the second most popular Tor dark web site in December 2014. On the darknet market, Bitcoin is utilized for anonymous transactions, and a dark wallet protects both the buyer and the seller. Drugs, weapons, explosives, human organs, fake money, falsified documents, and more can all be found on the darknet market.

Bitcoin Promotion:

One well-known cryptocurrency is Bitcoin. It is a digital payment system that is decentralized. Cryptography is used. On the dark web, it is used to make anonymous payments. Without the involvement of an intermediary, it can be transmitted from one user to another Peer to Peer over the Bitcoin network. There is no government or central bank involved in a bitcoin transaction. Bitcoin was created by Satoshi Nakamoto and debuted in 2009. Bitcoin allows users to conduct business anonymously. Users were able to connect with illicit operations as a result.

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025
DOI: 10.17148/IJIREEICE.2025.13330

CONCLUSION

The dark web is unable to discriminate between malevolent and legitimate users because of its characteristics, such as anonymity. To overcome this obstacle, law enforcement organizations must implement technology that protects user privacy while successfully capturing offenders. Investigating fake websites rather than fraudulent users is an efficient way to accomplish this. It is not wrong or illegal to browse the dark web, but it is wrong to engage in unlawful activity. It makes it possible to connect with those who have interests and facilitates more communication. Governmental ethical hackers have the ability to install de- anonymization software on users' computers.

REFERENCES

[1]. Humburt G. Illuminating the dark web. April 1, 2017; 50(04):100-5; Computer.
[2]. Bhushan B, Saxena S. The Dark Web: An Exploration of the Internet's Darkest Side.2020. http://dx.doi.org/10.2139/ssrn.3598902
[3]. The Dark Art of Anonymity by Henderson L. Tor. Hammer, Mark (2015).
[4]. Bitcoin AM. Unlocking Digital Cryptocurrencies, Andreas M. Antonopoulos–K.: NGITS, 2014.
[5]. Rai AK, Bhushan B, Jha VK, and Sinha P. A survey of security flaws, attacks, and defences in wireless sensor networks at different OSI reference model layers. International Conference on Signal Processing and Communication (ICSPC), July 28, 2017 (pp. 288-293). IEEE.
[6]. Retzkin S. Practical Dark Web Analysis: Discover what happens on the Dark Web and how to use it. Packt Publishing Ltd., Dec. 26, 2018.
[7]. Wilson C, Carman M, Dalins J. A classification model for law enforcement regarding criminal motivation on the dark web. Digital Investigation, March 1, 2018, 24:62–71.
[8]. Tandon A, Narayan S, Bhushan B, Sharma M. Security attack classification and analysis for IEEE 802.15, as well as WSNs. 4 criteria: An examination. Third International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall) Sep. 15, 2017 (pp. 1–5). IEEE.
[9]. Alegre E, Biswas R, and Fidalgo E. Perceptual hashing and image classification techniques are used to identify service domains on the TOR dark net. Dec. 13, 2017: 8th International Conference on Imaging for Crime Detection and Prevention (ICDP 2017)
[10]. Kaushik I, Bhushan B, Singh A, Sharma A, and Sharma N. classification of web-based application attacks. July 5, 2019: 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (Vol. 1, pp. 1231-1235). IEEE.
[11]. Pospisil F, Lightfoot S. Privacy and surveillance on the deep web. Tech. Rep. 2017 May 5, ResearchGate, Berlin, Germany.
[12]. Senker C. Cybercrime and the Dark Net: Exposing the Internet's shadowy underworld. Arcturus Publishing, September 12, 2016.