Ali *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 4 issue 3 Year 2020

The Unseen Web, an Enormous Mass of Internet

Sundus Munir[1], Afrozah Nadeem[2], Syeda Binish Zahra[3], Sadia Kousar[4]
sundusm1@gmail.com[1], afxnadeem@gmail.com[2],
binishzahra@gmail.com[3], sadiakousar@gmail.com[4]
Lahore College for Women University[1]
University of Engineering and Technology[2,4]
National College of Business Administration & Economics (NCBAE)[3]

Abstract:

Deep web is the part of the internet; it holds 99% of the internet rest of the internet is known as surface web and it is access able by standard search engines, Deep web is famous by different names and can be called as invisible and hidden web but it can't be accessed by the standard exploratory engines this is due to the un indexed contents by common exploratory engines. Deep web content is invisible under HTML form. Deep web provides anonymous internet platform for hackers, government agencies and others. Due to this no one can trace the location of the user and don't have any kind of information about the web surfing of the user. Dark web is the part of Deep web, the reason behind it commonly used for the black market i.e. Drug sale, ammunition sale, and many other illegal activities. It is the consist of millions of websites some of which are very informative. While on the other hand some of the portion is legal to visit and rest is illegal. These websites can be accessed by using the popular tools, i.e. TOR, I2P which provide anonymity. About 2 million people use the TOR browser to browse deep and dark web.

Keyword: Surface web, Invisible, Deep Web, Anonymity

1. Introduction

Most people consider that they have complete access to the Internet. But they even don't know that the internet which they have access is just 1% and is known as "Surface Web". The leftover internet is 99% and is known as "Deep Web". The resources in Deep and Dark web are not indexed in common search engines like yahoo and google. The Dark Web is a fragment of Deep Web and is not index able so it can't be accessed by simple search engines but can be searched by [1]. Harvest engines. Deep web contains many contents like online forums, baking services, chat room services and many more and these services can be used by paying payment. But the dark web is not index able due to its materials and some other reasons [2]. Dark web is famous for the black market of drug selling, Ammunitions, Pornography, selling of credential information's and exchange of virtual currency and for many other things [3]. Some people use it in a bad way and others have a positive point of view. Its use is dependent on the mentality of users like criminal use it for criminal activities like cyber terrorism and journalists use it to gather some hidden information about some politics or any other issue which they want to expose in front of people [4]. The leading reason for the usage of Deep web is secrecy, deep web provides anonymous internet so hackers, government agencies and no one can trace the location of the user [5][6]. Only 32% content has been legal and 68% are illegal on deep web [7]. Users can access the Dark web by using the special browsers like TOR, FREENET and I2P they provide anonymous access to the resources of deep and dark web.

Deep web and dark web have enormous mass of internet and according to rough estimate it contains 7500 terabyte data [8]. About 2million peoples use the TOR browser or other networks to browse deep and dark web [9]. It consists of different levels nobody can access it completely [10]. It is divided into different levels on the basis of its content's danger level. Following are the different levels of the web.

• Common Web or internet

We usually use it daily and we are well known to it. Mostly it contains the contents which are "Open to the Public".

• Surface Web

It is also known as invisible web it is only 0.03% of internet It provides services such as Reddit, Digg, E-mail, chat board MySQL databases and social enabling contents are found here. The Surface web contains about 4.5 billion websites which are indexed by different search engines. The Surface web contains 19 Terabyte of information.

• Bergie Web

It has FTP Servers (4chan), honeypots, loaded webservers and google locked results. The Proxy is required for further access.

• Deep Web

It consists of the following things, heavy jailbait, Gore, On the Vanilla Sources, celebrity scandals, VIP Gossip, Hackers, Script kiddies, Raid information, Blue Prints, Virus Information, XSS Worm scripting, Mathematics research and many other information.

• Charter web

It is categorized into two parts. The first part can be accessed by using TOR. It contains information like hidden wiki, banned video, books, movies, Trade of Rare animals, Human trafficking, Personal records, billion dollar deals and black market. The second part can be accessed by modifying a hardware information which is a "Closed Shell System", it contains hardcore CP, World war 2 experiments and Atlantis Location [11].

• Marina's Web

This layer is having a lot of information about the secret documentation of government and many organizations. You will be the lucky person if you got access to it.

• (?)

This layer lies in between 5th and 7th layers. At this point people are not aware that they are in the attention of someone and it can be very dangerous. For example, individuals can reach at your destination to kill you.

• The Fog/virus soup

The best way to describe the level 7 is relating it with a war zone. Where the creator of it is trying to approach the 8th level, but preventing other people to access it.

• The Primarch system

This is the last level of the web. It's impossible to have direct access to that level. The Primarch system is some unknown thing which is controlling the internet all over the time. Even government and organizations have no control over it. It was unintentionally discovered in 2000's during deep web scan [12]. It is the "Final Boss of the Internet"

Effect on Privacy and Business

The Deep and dark web provide iceberg of the internet each and every thing here can be sold out like from your personal information to the big critical documentations. It is the black market for the drugs, selling of personal information, deals of ammunition. Deep web or dark web itself is not safe anonymity of search and identity is provided by TOR, I2P, FREENET etc [13]. Your information and identity can be compromised because deep web is full of hackers. Hackers always try to access user's information who uses this web frequently. Therefore, you are not secure while browsing deep or dark web.

It can provide anonymity but does not assure privacy it can have large impact on confidentiality [14][15]. To protect privacy one must not surf, deep and dark web and also use precautionary measure to save data from being going out into deep web.

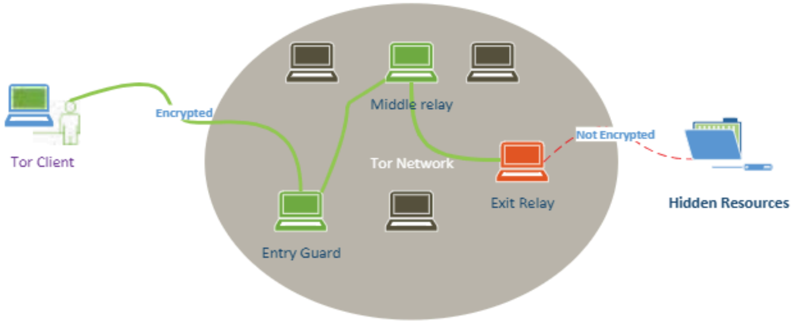
Following measure can be done to save data from being stolen.

- Assures that the web you are visiting or your own website is encrypted with an SSL certificate [16].
- Create backup of all data and information, so that in case of any attack it can be recovered.
- Educate people and employs about the cyber security [17].
- Use dual authentication factor, and choose strong password [18].
- Don't put personal information on the web.

Anonymous systems for accessing Deep Web

☒ TOR Browser:

Tor browser basically works on the basis of the onion method in which data that is to be sent by user, first encrypted and then send through different sources in the Tor network. Data is encrypted in multi layers of browser. The Tor is a type of browser that removes the identifying information so that original source cannot be traced, makes it easy to protect the user identity.



⊠ Operational Working

Tor browser uses three different layers [19].

In first step data is entered by using an entry node from the user side, then it enters in a Tor node and finally spits outs user data through the final exit node.

In 2nd step Tor browser services gets users IP address and guess the country and language automatically, but when using Tor, you will often appear to be in a physical position halfway just about the world.

If the user exists in a system that blocks Tor or need to access a web service that blocks Tor, you can also construct Tor Browser to use bridges. Like Tor entry or exit nodes, bridge

IP address is not shown publicly so it's difficult for web services and government to get these IP addresses and block them.

⊠ Features:

- Tor browser is simple to use as other browsers.
- It is high speed network of Onion Router [20].
- It can be downloaded and used on different types of operating systems.
- Tor browser only access the Onion web sites that are only available in the Tor network.
- Government agencies have the information about which sites users have visited, how many times, how long and from where all these services are provided by Tor to their users
- It sends data through different virtual routers; current router only has information of one backward and one forward router so it's become difficult to track the location and identity of the users.

⊠ I2P:

12p is a mostly used internet tool that makes the usage of internet services pretty easy. It's basically created to access the un accessible portion of the internet. I2P provides the short developer guide to make a website over the network. It works as a layer over the internet which create possibilities for the users to exchange the data [21].I2P can be used to create a web service or to use the web services. The network has no central point to store the information. Its development starts in 2003 and updated time to time.

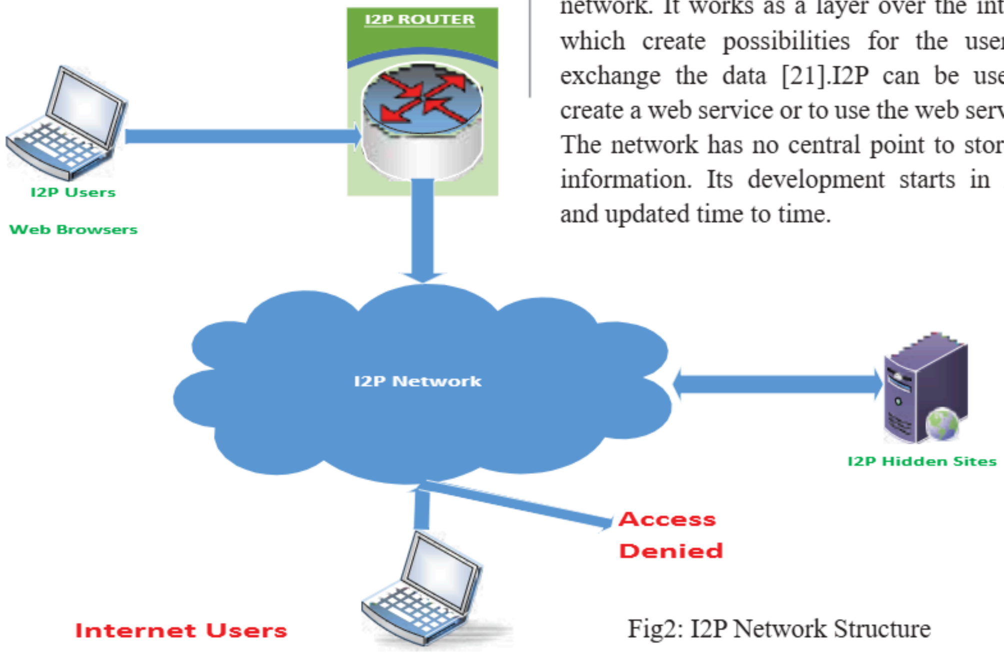


Fig2: I2P Network Structure

☒ Operational working:

12P network consist on different virtual routers. A router can be defined as a piece of instruction that enables the services to communicate with one another. In this network sender and receiver don't interact directly with one another instead of direct communication their data passed through different routers. Each sender and receiver over the internet work as a router as well. Hence this type of communication cannot identify the users.

☒ Features:

- Data cannot be extracted from the network and cannot access outside the network.
- It can perform the same activities like internet but without disclosing the private information of users.
- Different types of tools are available to access the services of browsers but 12P creates its own tools to avail the services of network. Therefore, this feature makes it much faster than other browsers.
- Sending message peer to peer used less spaces so it's difficult for the attacker to attack on it.
- Updating is done with time to time that increases its usage abilities.
- A major setback of this network is that it is still considered as an unexperienced network.

☒ Freenet

Freenet browser is a secret key based file sharing system with the aim of sharing information without knowing the actual source [22]. Creator of this browser starts project with the goal of sharing information secretly and for freedom of speech. When a user sends the information over Freenet network, it's difficult to find out the destination where information is being stored. Information also moves over the Freenet network according the demand of users.

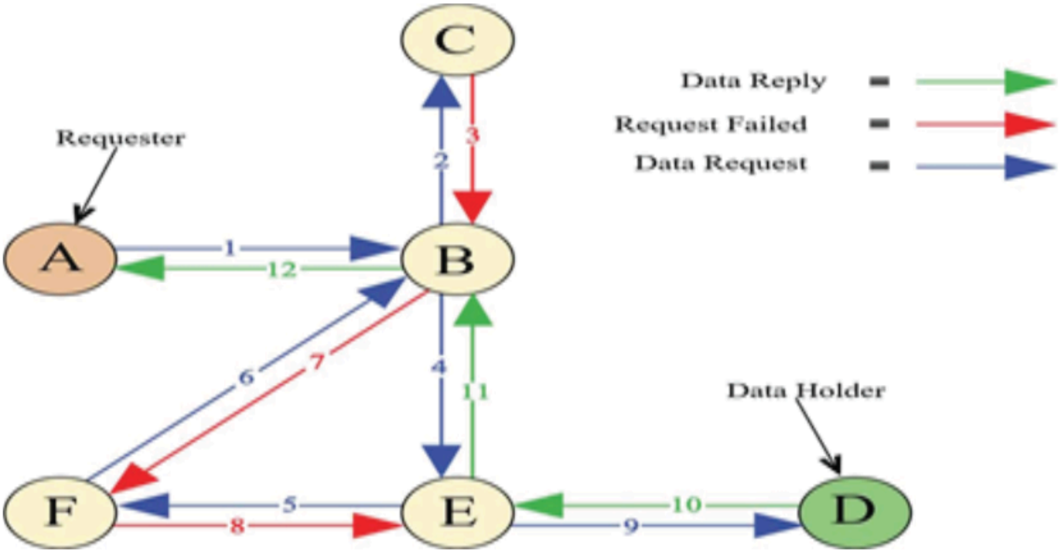


Fig3: Freenet Network Structure

☒ Features:

- Freenet keeps files in well-organized way against some secret key. Each file stored over the network have a unique key. Whenever user need to get the file he will provide that key to the network and get the that particular file in return. Once a file is submitted to it, it's contents as well as content type cannot be changed furthermore and it has TCP/IP protocol [23].
- Running network is implemented with the help of java language which executes on windows, Linux etc. Freenet network system provides unsigned files and message sharing facilities.
- This network can only access that data which has already stored in it. Hence it is simpler in use as compared to other networks.
- Freenet provides peer to peer connections by protecting the privacy of both users, one who is sending the files and 2nd who is retrieving that files. Data stored by the user saved in the form of pieces over the network, while getting that stored those pieces are found and combined.

☒ Architecture:

Freenet network works in the form of modules. These modules use "Freenet client protocol" for programs to use. Different applications used multiple services for sending files and sharing messages. As it contains a secret key for a file hence the stored file is encrypted, no one can access it using nodes of Freenet network without knowing that decrypted key. Getting the data from network is time consuming procedure it compares the key node to node. When it finds the related file or data, it stops checking the nodes of network. Freenet follow the stack concept for data storage.

Comparison:

Following is the comparison of three different anonymous networks of deep and dark web through which unseen web can be accessed [24]

Table1: Comparison of TOR, I2 P, Freenet

Sr #	TOR	I2P	Freenet
1	Tor browser basically works on the basis of the onion method in which data that is to be sent by user, first encrypted and then send through different sources in the Tor network.	12P is a network consist on different virtual routers. A router can be defined as a piece of instructions that enables the services to communicate with one another.	Freenet browser is a secret key-based file sharing system with the aim of sharing information without knowing the actual source you can also create sites.
2	Tor ultimately route the traffic to the different random routers present in network to provide anonymity to all kind of users.	In this network sender and receiver don't interact directly with one another instead of direct communication their data passed through different routers.	Freenet protect the privacy of both users, one who is saving the files and 2nd who is retrieving that files.
3	Single router has just the information of forward and its backward router so due to this reason user identity or location cannot be traced	It has tunnel services it provides two tunnels to its users one is inbound (Receive message) other is outbound (Send Message)	It is decentralized and store pieces of data on user hard drives and data pass through different nodes and this make difficult to track the location of the users.
4	It provides client server, multi layered and end to end data encryption.	I2p also has the peer to peer, multi layered and end to end data encryption of user communication.	It has the same feature as tor and i2p has like peer to peer, multi layered and encryption.

☒ Legal or illegal?

Tor, I2p and Freenet browsers are legal to use. Different countries have different rules related to the usage of these browsers [25]. China has banned the secrecy services of these browsers. Most countries working hard to stop citizens from using these networks.

Many authorities' hates these networks because by using services of deep web make it is easy for the reporters to report corruption or other illegal activities done by the politicians. Sophisticated users supporting Tor for freedom of expression, communication and publish around the world. These types of users provide bandwidth to the network.

If you are investigating a person related to you or paying role to resolve a legal dispute and that it's not good for your privacy, then the usage of this browser might be the right solution.

Pros and Cons of Deep and Dark Web

- Private information can be shared without government courier finding out.
- That information can be accessed which is blocked in a particular region.
- Deep and Dark web also provides a display space for against the law actions.
- Provides a platform for trading of harmful products like Drugs, weapons, fake passports, eBooks and hacking tools.
- Traders don't know that they will get the same material what they order.
- The User has to follow the correct steps in order to access the deep and dark web otherwise it can be privately dangerous for the user.
- Another major advantage of dark web is it contains a strange community, where people can share their experiences and give advices.
- Deep and Dark web provides "no physical contact" service

Conclusion

This paper embraces an outline of deep, dark web and comparison of three networks Tor, I2P, Freenet, to create consciousness about the unseen web and the operation of three different networks which provide anonymity to its users. Benefits and hindrances of unseen web to us and how much adverse effect it has on our privacy. Unseen web is the place where you can sell and buy each and every thing without being tracked by government and intelligence organizations. Deep web is the part of the internet; it holds 99% of the internet rest of the internet is known as surface web and it is accessible by standard search engines, Deep web is famous by different names and can be called as invisible and hidden web. Many authority's hatred these anonymous networks because their services make it easy for the reporters to report corruption or other illegal activities done by the politicians. Sophisticated users use Tor for freedom of expression, communication and publish their point of view around the world. These types of manipulators provide bandwidth to the network. This paper also informs us that which network is safer and more anonymous. I2P and Tor both are analogous to each other and provide anonymity where Freenet also provide anonymity but it has decentralized database with its application and is even more useful as an anonymous network.

References

[1] Steve Pederson, "Understanding the deep Web in 10 Minutes," BrightPlanet, March, 11, 2013.

[2] K. Finklea, "Dark Web Kristin Finklea Specialist in Domestic Security," Dark Web, 2017.

[3] S. Petersb, “Contents :Monograph on DARK WEB,” no. April, pp. 1–16, 2002.

[4] V. Vilic, “Dark web, cyber terrorism and cyber warfare: Dark side of the cyberspace,” Balk. Soc. Sci. Rev., vol. 10, no. April, pp. 7–25, 2017.

[5] “Surface Web, Deep Web,Dark Web a Subset of the Deep Web (Non - Indexable) That.”

[6] M. Overton, “The Dark Web Dark Web , Dark Net , What you need to know …,” 2015.

[7] S. Bindal and H. S. Muktawat, “Deep Web,” no. March 2010, 2014.

[8] Michael K. Bergman, “The Deep Web: Surfacing Hidden Value,” 2001. [Online].Available:https://quod.lib.umic.edu/j/jep/3336451.0007.104?view=text;rgn=main.

[9] U. T. Ocean and T. D. Web, “InfoSec Reading Room Under the Ocean of the Internet - The Deep Web,” p. 22, 2016.

[10] P. Ameya, S. Sagar, and S. Yadav, “Introduction to Deep Web,” Deep Learn. with Python, pp. 1–5, 2017.

[11] W. Paper, “THE DARK WEB & THREAT INTELLI.”

[12] “The Primarch system.”

[13] B. Shavers and J. Bair, “Hiding Behind the Keyboard,” Hiding Behind the Keyboard, pp. 223–228, 2016.

[14] S. Lightfoot, “Surveillance and privacy on the deep web,” no. March, pp. 0–27, 2018.

[15] M. Chertoff and T. Simon, “The Impact of the Dark Web on Internet Governance and Cyber Security,” Glob. Comm. Intrnet Gov., vol. 6, no. 6, 2015.

[16] “SSL Certificate for web pages.” [Online]. Available: https://www.globalsign. com/en/ssl- information-center/what-is- an-ssl-certificate/.

[17] B. M and C. V, “Cybercrime in the Deep Web,” pp. 24–31, 2015.

[18] A. Amin, I. ul Haq, and M. Nazir, “International Journal of Computer Science and Mobile Computing TWO FACTOR AUTHENTICATION,” Int. J. Comput. Sci. Mob. Comput., vol. 6, no. 7, pp. 5–8, 2017.

[19] Emin Çalışkan, Tomáš Minárik, Anna-Maria Osula “Technical and legal overview of the Tor (anonymity network).” .

[20] R. W. Gehl, “Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network,” New Media Soc., vol. 18, no. 7, pp. 1219–1235, 2016.

[21] F. Astolfi, J. Kroese, and J. Van Oorschot, “I2P - The Invisible Internet Project,” 2015.

[22] M.Godwin,“Freenet Documentation.”[Online].Available: https://freenetproject.org/pages/documentation.html.

[23] R. Kamath, “S . D . M COLLEGE OF ENGINEERING AND TECHNOLOGY Submitted by Roshan Kamath DEPARTMENT OF COMPUTER SCIENCE ENGINEERING,” pp. 1– 12, 2009.

[24] N. Negi, “Comparison of Anonymous Communication Networks-Tor , I2P , Freenet,” Int. Res. J. Eng. Technol., vol. 4, no. 7, pp. 2542–2544, 2017.

[25] D. S. Rudesill, J. Caverlee, and D. Sui, “The Deep Web and the Darknet: A Look Inside the Internet’s Massive Black Box,” Ssrn, no. August, 2015.