IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

Dark Web: The Uniluminated Side of the World Wide Web

Asoke Nath[1*], Romita Mondal[2]

[1]Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, India
[2]Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, India

Corresponding Author: asokejoy1@gmail.com

Available online at: www.ijcseonline.org

Accepted: 18/Jan/2019, Published: 31/Jan/2019

***Abstract*-**The Dark Web is a part of the World Wide Web that exists on dark-net whose content is intentionally hidden, and cannot be accessed using normal search engines and require some specific browsers such as Tor browser. Dark web uses network such as Tor, I2P.While tor provides anonymity of users and make them untraceable, I2P provides anonymous hosting of websites. As the dark web hides the user's identity and maintains secrecy, it can be used for legitimate purpose as well as illicit purpose. From smuggling of drugs and weapons to other illicit items, from hacking other's information to using those for forging, from counterfeiting money to using crypto currency, dark web can play a number of roles in malicious activity. On the other hand, government and legitimate authority use dark web for military application such as online surveillance, sting operation and to track the malicious activities. This paper describes dark web emphasizing on how it is accessed, how the tor network (onion routing) and I2P work to hide user's identity, how one can use TOR to access dark web, recent technological development, details on usage of dark web i.e. how different malicious activities are done using dark web, how the terrorist groups are using darkweb, how the legitimate authorities are using dark web to unveil some user's identity and to stop the illicit activities and the future scope of dark web.

***Keywords* -** Dark Web, Tor, I2P, Tor browser, Surface Web, Deep Web, Silk Road.

I. INTRODUCTION

Internet and World Wide Web (commonly known as WWW) are two frequently used words in our daily life. But how many of the internet users actually know about the ''UNILUMINATED'' side of the ''Internet'' or very precisely ''The Dark Web''. This dark area of the Internet or the dark Web is characterized by the unknown—unknown breadth, depth, content, and users [1].

The Dark Web is a part of the World Wide Web that exists on dark-net whose content is intentionally hidden, and cannot be accessed using normal search engines and requires some specific browser such as Tor browser. The Dark Web is accessed for both legitimate purposes and to conceal criminal or otherwise malicious activities. The extensive use of Dark Web for illegal practices has made it a den of mystery. Taking an eye-opening example of a notorious dark website - "The Silk Road". The Silk Road was an online global bazaar for illicit services and contraband, mainly drugs. Vendors of these illegal substances were located in more than 10 countries around the world, and contraband goods and services were provided to more than 100,000 buyers. It has been estimated that the Silk Road generated about $1.2 billion in sales between January 2011 and September 2013, after which it was dismantled by federal agents [1]. Though the dark web activities were going on, the exposure of this Silk Road website sheded light on the dark web.

Rest of the paper is organized as follows, Section I contains the introduction of Dark Web, section II contains accessing methodologies, section III contains literature review, section IV contains results and discussion, section V contains conclusion and future scope, and section VI contains the references.

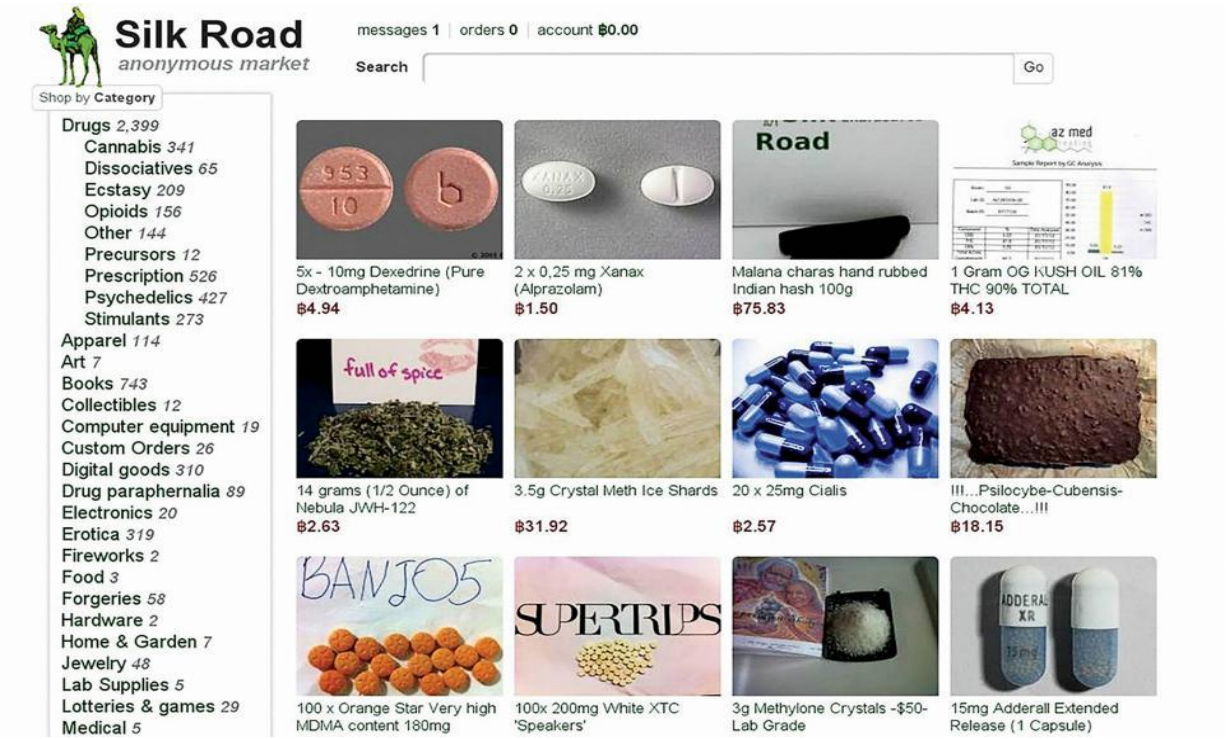

Figure 1: Silk Road Website

Layers of the Internet:

Actually, the internet comprises every single server, computer, and other device that are connected together in a network of networks. In conceptualizing the World Wide Web, some may view it as consisting solely of the websites accessible through a traditional search engine such as Google. However, this content—known as the "Surface Web"—is just one portion of the World Wide Web. The other two portions are Deep Web and Dark Web.

a) Surface Web: The surface web is actually what many users think as the Internet and uses daily. The portion of the World Wide Web that is indexed by search engines and can be accessed easily, is known as the surface web. It consists only 10 percent of the information that is available on the Internet. The Surface Web is simply the tip of the iceberg.

b) Deep Web: The deep web is a portion of the World Wide Web whose content is not indexed by any search engine and can be accessed using direct URL. Information on deep web includes content on private intranet(such as networks used at government agencies, corporate office, educational institutions etc),banking sites, cloud based accounts(Google Drive) that requires username and password for authentication or websites that produces content as a result of a search query or form. It is estimated that the deep web is 4000 to 5000 times larger than the surface web but the growing usage of deep web can actually make a large increase in the statistics [1].

c) Dark Web: The dark web is a portion of the deep web that the users can not access without using special browser. Contents of the dark web are intentionally hidden. Users and website operator of dark web becomes untraceable.

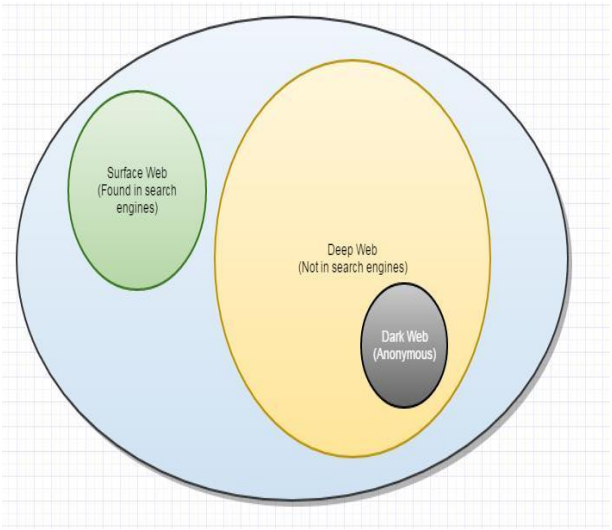

Figure 2: Layers of the Internet

People often use the two terms Deep Web and Dark web interchangeably. But they are not the same. Dark web is just a little portion of the deep web. There are some differences that separate the concept of deep web with dark web.

- Deep web contents are not indexed by search engines such as Google, yahoo and cannot be found by just searching through the traditional browsers. While dark web contents are intentionally hidden and cannot be accessed by any traditional search engine.
- Deep web contents can be accessed using search engine (Google, Yahoo) and direct link. It does not require any special browser. While dark web contents can only be accessed using special browser with specific configuration such as TOR browser.
- The contents of deep web are not illegal while a majority of contents in dark web is illegal.

Contents of deep web include information on private intranet used by government offices, private companies, banks. Databases of different educational institutes, libraries are also stored in deep web. Cloud based system (Gmail, Google Drive) information are stored in deep web which are protected by user name, password. On the other hand, content of dark web includes illegal sites for selling and buying of drugs, weapons, money laundering, counterfeiting, hacking groups, forums for discussions etc.

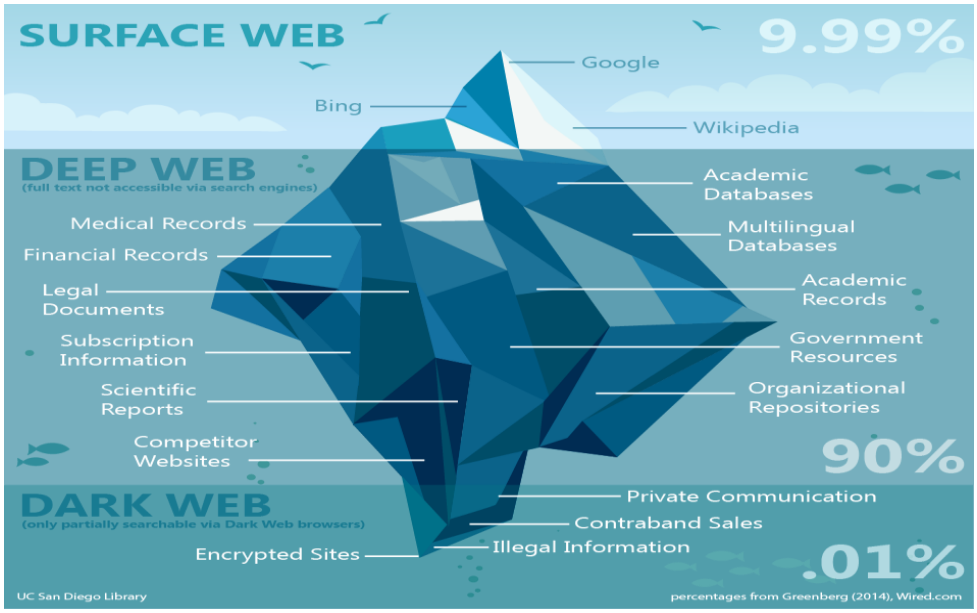

Figure 3: Iceberg image of the layers

II. ACCESSING METHODOLOGIES

Dark web uses small friend to friend, peer to peer network as well as large network such as TOR(The Onion Routing Project), I2P(Invisible Internet Project).

TOR (THE ONION ROUTER):
Tor is the most popular dark web network. Tor provides anonymous browsing facility by hiding the identity of the users and the hidden websites hosted on Tor. Tor protects users against traffic analysis which is a common form of internet surveillance. Knowing the source and destination of the internet traffic, an eavesdropper can infer who is talking to whom over a public network. Tor reduces the risk of both simple and sophisticated traffic analysis [2]. It distributes a transaction over several places on the Internet, so the source and destination cannot be linked by any single point.

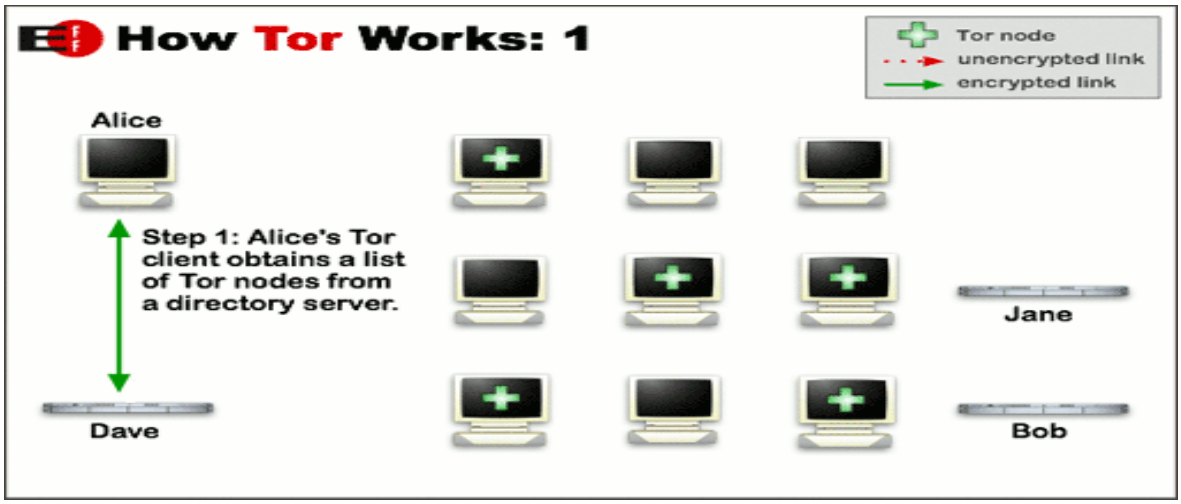

Figure 4: How TOR works (a)

Instead of taking direct route, data packets on Tor network take a random pathway through several relays, so no observer at any single point can identify the source and destination of the data packet [2]. In order to create a private network path with tor, the user's software incrementally builds a circuit of encrypted connection through relays on the network. Tor uses three relays. The circuit is extended one hop at a time, so each relay only knows the identity of the immediate antecedent and descendant. The complete path taken by a data packet is not known to any node. The client uses separate set of encryption keys for each relay so the encrypted data can be decrypted only by the intended node.

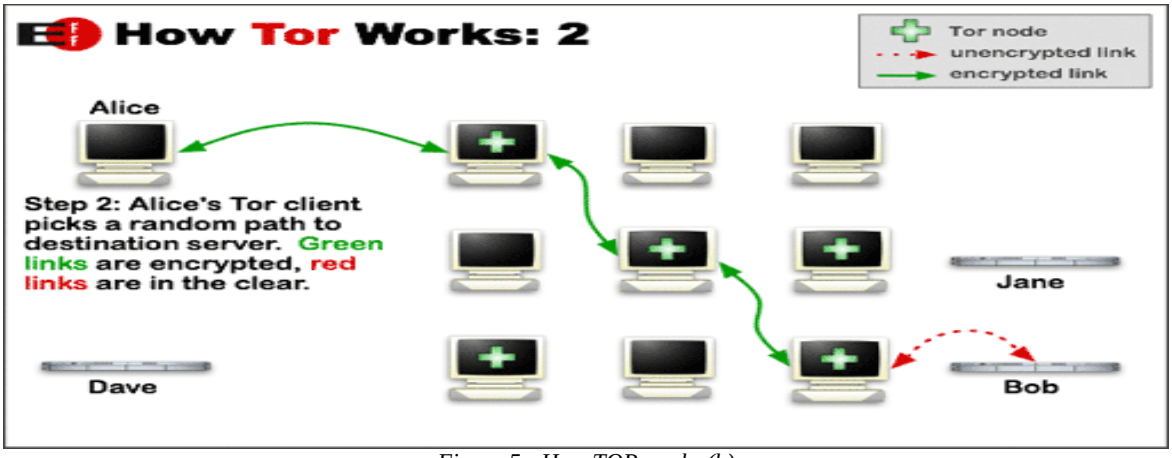

Figure 5: How TOR works (b)

After the circuit is established, data can be exchanged and several different types of software application can be used over the network. Tor only works for TCP streams. The Tor software uses the same circuit for connection that occurs within the same ten minutes [2]. After that it establishes a new connection. Hidden services on tor uses .onion domain.

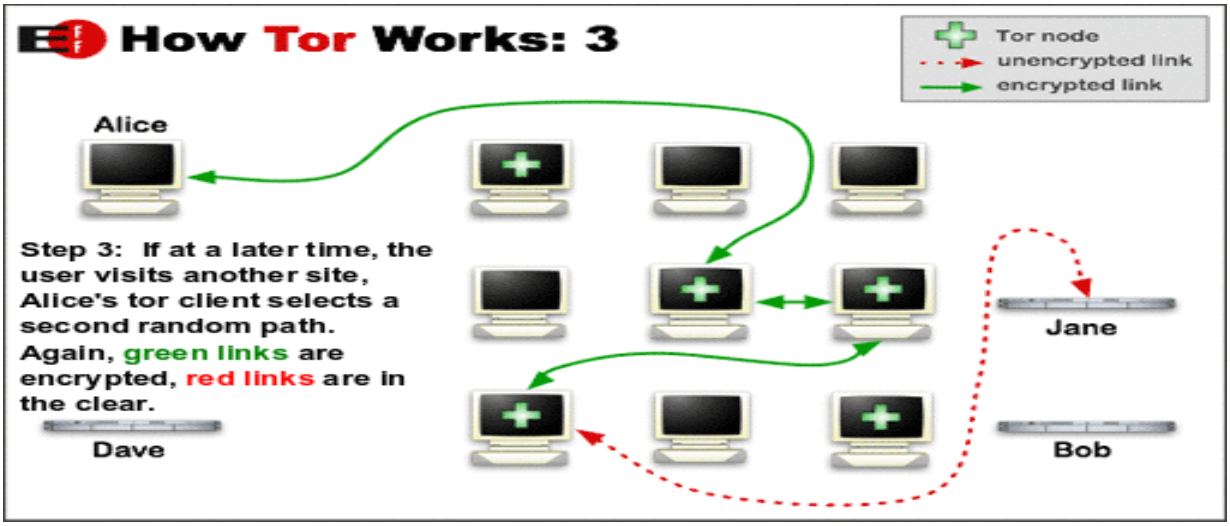

Figure 6: How TOR works(c)

I2P (Invisible Internet Project):

I2P is another popular anonymous darkweb network. Just like Tor, it also provides anonymous browsing facility. Anonymous connections are achieved by encrypting user's traffic and sending it through a volunteer run network. All communication is end to end encrypted (four layers of encryption are used when sending a message). As Tor hidden services use .onion domain, hidden services on I2P use .i2p domain. To anonymize the messages sent, each client application uses I2P "router". I2P Tunnel is currently used to let people run their own anonymous website (eepsite) by running a normal web server and pointing an I2PTunnel 'server' at it, which people can access anonymously over I2P with a normal web browser by running an I2PTunnel HTTP proxy (eepproxy). A tunnel is a directed path through a selected list of routers [3]. Each router uses layered encryption method that is only one router can decrypt information in each layer. Decrypted information contains the IP address of the next router along with the encrypted original message [3]. Each tunnel has a starting point known as Gate and an endpoint [3]. Messages can be sent in one direction using tunnel. Inbound and Outbound tunnel are used to send message in both direction. While an inbound tunnel is used to send message to the creator of the tunnel, an outbound tunnel is used to send message from the creator of the tunnel. This two tunnels are used together to create a two way communication. I2P network database (netDb), a custom structured distributed hash table to find other clients inbound tunnels. This database contains information on public keys, transport address of a router, and the necessary data to contact intended (the gateway which enables a destination, the lifetime of the tunnel, a public key pair to encipher messages). I2P is used for normal web browsing, email, file sharing, real-time chat, secretly hosting websites, blogging and forums etc.

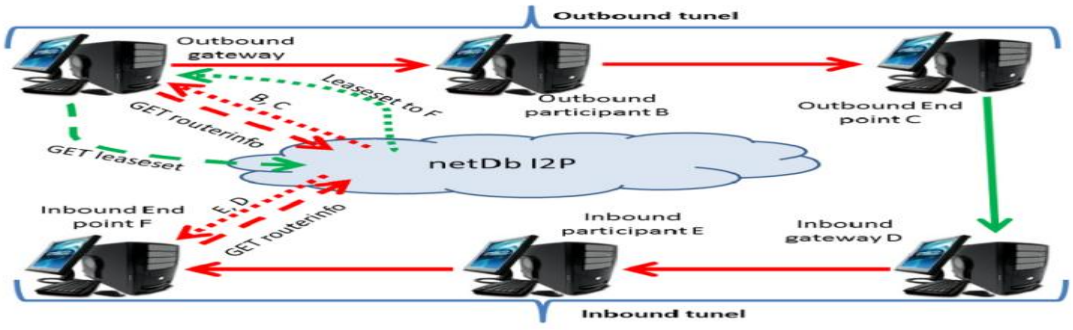

Figure 7: I2P network, source: Jerzy kosinski

III. LITERATURE REVIEW

Dark web hides the identity of the users and host of the hidden websites. This anonymous browsing advantage of dark web is leading its use to different illegal activity. While many people use dark web for only maintaining privacy, a major portion of the dark web users use it for illegal purpose. Extensive research work has been going on in past few years to minimize the crime by identifying and revealing the identity of the illegal sites hosted on dark web. Defense Advanced Research Projects Agency (DARPA) launched a program in 2014, called Memex. Their aim is to create a search index to help legal authorities indentify human trafficking operations online. According to them, Commercial search engines such as Google or Yahoo searches websites based on their popularity and indexes around 5 % of the entire Internet, but Memex aims to provide a better search result by sweeping through all the websites that are ignored by commercial search engines and on the deep web as well as dark web [4]. They have used Apache Tika system which lets users understand any file and the information contained within it. When Tika examines a file, it automatically identifies what type of file it is – like an image, audio or video. Once a file's type is identified, Tika uses specific tools to extract its content.
Several research works have been done to develop dark web crawlers for automatic categorization and indexing of websites on dark web.

ATOL present a framework for automated analysis and categorization of .onion websites in the dark web ecosystem. In this project, the researchers have developed a large-scale dark web crawling infrastructure called "OnionCrawler" that acquires new onion domains on a daily basis, and crawls and indexes millions of pages from these new and previously known .onion sites. It stores this data into a research repository designed to help better understand Tor's hidden service ecosystem. The analysis component of this framework is called Automated Tool for Onion Labeling (ATOL) which introduces a two-stage thematic labeling strategy: (1) it learns descriptive and discriminative keywords for different categories, and (2) uses these terms to map onion site content to a set of thematic label[5].

Another researcher Janis Dalins has proposed the use of AI tools with machine learning capability to develop a darkweb crawler that will help the law enforcement to get the information about illegal websites in dark web[6]. The project aimed to develop a classification system to train algorithms to target only the illegal contents, rather than legitimate use of anonymous browsing .

While the majority of transactions are traceable to individuals or entities in the real world, the use of crypto currency such as bitcoin has allowed for anonymous exchange of money. The use of cryptocurrency in dark web is growing rapidly. Block chain technology provides total anonymity. A block chain is a decentralized public ledger which keeps immutable record of the transactions on the network .This record is stored across several users (decentralized) which adds a level of security and reliability. Block chain does not require a centralized authority to verify the transaction[7].

The TOR project has recently released its next generation version. A significant set of changes have been made to their anonymity network which involves next generation crypto algorithms, improved authentication schemes, and redesigned directory. They have increased the size of the onion addresses and also made them completely private. It will help them better to combat against leaks and cyber attacks.

IV. RESULTS AND DISCUSSION

The key feature of dark web is anonymity. Dark web helps users to browse internet privately. There are many darknet available to access dark web but TOR is the most popular and heavily used network. TOR provides anonymity to user and websites hosted on TOR by hiding the identity or more specifically the IP address, so that users can access it without the fear of getting caught. The method of using TOR to access the dark web is described below.

Step 1: Use a virtual private network (VPN), which keeps NO LOGS, fast performance and is compatible with TOR. The VPN will give the user a fake IP address, in another country if the user likes, so even if Tor is compromised then the trace just leads back to somewhere else that can't be linked to the user[8].
The other benefit of using a VPN is to prevent hackers stealing user identity, personal files and photos from user's computer.

Step 2: Dark web cannot be accessed by just using a common browser like "Internet Explorer" or "Google Chrome". The dark web browser called TOR browser has to be downloaded. Now close all of your browsing windows and all apps connecting to the World Wide Web like Google Drive, Skype, One Drive, etc[8].
Then open VPN app and connect to another location other than the current location. Then using any normal browser download TOR.
TOR Official Website: https://www.torproject.org/download/download.html.

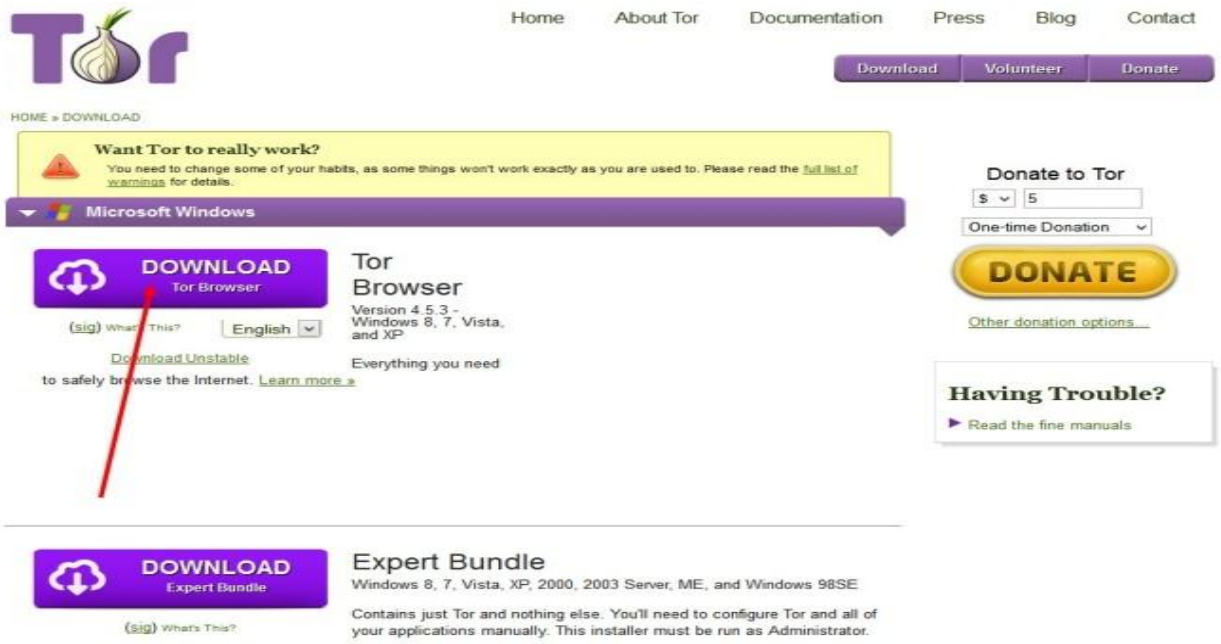

Figure 8: TOR browser download page

Step 3: When the download is complete, double-click the downloaded file, choose the destination folder (the folder where you want to extract tor browser), and choose extract [8] .

Step 4: Start TOR Browser. Open the folder where you extracted TOR browser and double-click "Start Tor Browser". The TOR start page will open in a browser window [8].

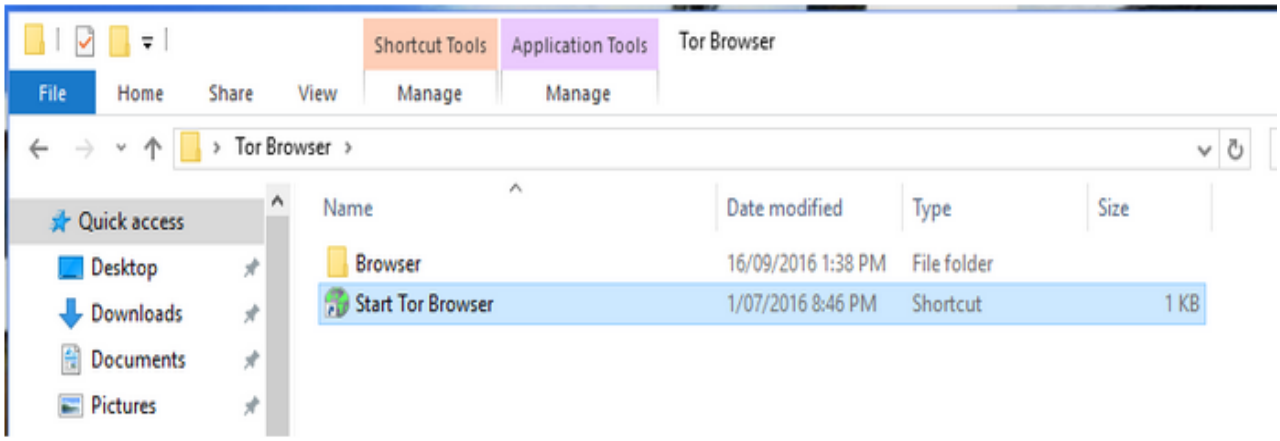

Figure 9: Start TOR browser

Step 5: Close any currently open browser window. This ensures that no public information from your previous browsing sessions will be available when you connect to Tor. Connect to Tor. Once your VPN is turned on and no browser windows are open, open Tor and then click Connect. This will open the Tor home page.

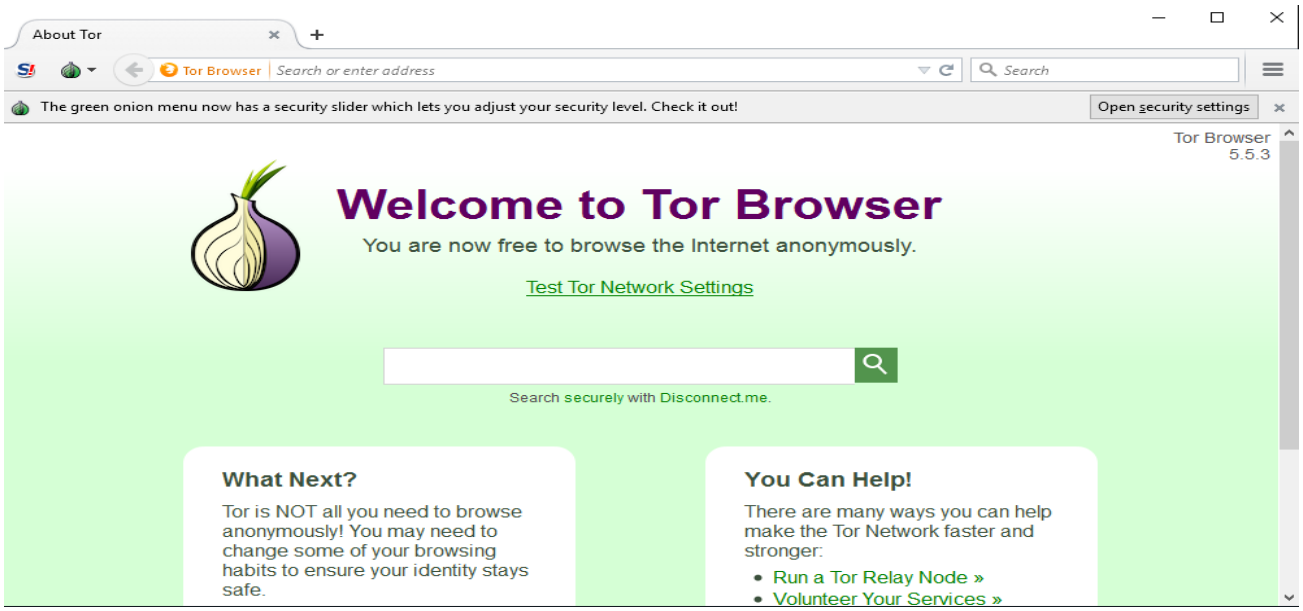

Figure 10: Homepage of TOR browser

Step 6: Change your Tor security settings. On the Tor home page, click the onion icon in the upper-left corner of the page, then drag the slider to the top. This will ensure that tracking scripts and other forms of browser monitoring cannot be loaded [8].

Step 7: Open a Dark Web search engine. Common (and comparatively safe) Dark Web search engines are as follows:

- Torch – It is a commonly used Dark Web search engine with over one million indexed hidden pages. Found at http://xmh57jrzrnw6insl.onion%20/.
- DuckDuckGo - Allows the user to surf both the surface web and the Dark Web. Found at https://duckduckgo.com/[9].
- notEvil – It uses a Google-like interface and blocks ads. Found at http://hss3uro2hsxfogfq.onion%20/.
- WWW Virtual Library - The oldest search engine until now, containing historical sources and other academic information. Found at http://vlib.org/.

- Avoid the Hidden Wiki and the Onion URL Repository when browsing the Dark Web; both of these search engines often link to illegal content.

Step 8: Browse the Dark Web using your preferred search engine.

There are many websites on TOR which host illegal contents. While many websites are used for smuggling drugs, weapons ,some websites host child abusive content. There are many websites for money laundering, counterfeiting, selling and buying of stolen personal credentials. Websites of different terrorist groups, hacking groups are also there. Forums are available for users to discuss different issues anonymously.

Users of TOR communicate with each other using email service, anonymous real-time chat room such as The Hub and Onion Chat, or personal messaging using TOR messenger. Bitmessage and Ricochet are other personal messaging options available on TOR.

Hidden Wiki is a website that contains a directory of hidden .onion sites categorized as websites for drugs, weapons, child abusive content, crypto currency sites, social networking sites, whitsleblowing sites such as wikileak etc.

A major disadvantage of Tor is its slow speed because all TOR traffic is sent through multiple relays and there can be delays in any one of the intermediate node. Speed is reduced when more users are simultaneously using TOR network.

An alternative of using TOR is TOR2WEB. This software allows users to access content on TOR hidden services from a standard browser without being connected to the TOR network. Users can access content on websites without installing and running TOR browser. But it doesn't provide the same anonymity to user which is provided by TOR. If users of tor2web access sites containing illegal content, they could be more easily detected by law enforcement.

The dark web is used for legal as well as illegal operations. Many researchers have sheded light on the illegal and legal use of dark web. Some illegal use of dark web is as follows:

- Darknet markets- Commercial darknet markets are used for selling drugs, weapons and other contraband items. The Silk Road was one famous darknet market for

selling drugs which was shut down by FBI in 2013 and its owner Ross Ulbricht was arrested. After that a second website The Silk Road 2 was developed which was also shut down in 2014. AlphaBay and Hansa are two other popular darknet markets. They were shut down in 2017.

- Hacking- Hackers use dark web for the advantage of anonymous browsing. Many hackers sell their services either individually or as a part of a group. Some groups are xDedic, hackforum, trojanforge, Mazafaka, dark0de, and TheRealDeal.

- Crypto Currencies- There are numerous carding forums, PayPal, Bitcoin trading websites .Users pay for the drugs and other contrabands using bitcoin crypto currency. Other crypto currencies such as Monero, Litecoin, and Zcash are gaining popularity.

- Illegal child sexual content-A December 2014 study by Gareth Owen from University of Portsmouth found that the most commonly hosted type of content on Tor was child abuse videos. Pedophiles use this websites.

- Terrorism: Notorious terrorist groups such as ISIS uses dark web to hire members, to communicate with them, to plan attacks and raise fund. According to a study, there are at least some real and fraudulent websites claiming to be used by ISIL (ISIS) including a fake one seized in Operation Onymous. ISIS and different jihadist groups use Telegram an encrypted mobile app to broadcast their message to the members of the group[10]. They use bitcoin to collect donations across the globe and use that money to buy weapons.
  Dark web is also used for human trafficking, whitsleblowing, gambling, money laundering. According to recent news, some website in dark web is providing stolen academic research papers.

Some legal use of dark web is as follows:

- Law Enforcement- while the dark web is believed to be heavily used for illegal work, law enforcement authorities use dark web to identify the illegal works and stop them. In 2013, the FBI took down the Silk Road website, the largest online black market. After one month when another website 'the silk road 2.0' came online, the FBI shut down that.

- Military- Military may use the dark web to study the environment in which it is operating and to discover any activities going around that can harm the troops. Tor can be used by military for taking down a website or denial of service attack or intercepting enemy communication or to plant disinformation about troops movement and target to puzzle the enemy.

- Journalist- journalists use dark web to communicate with whistleblowers to get sensitive data and to anonymously write about politically sensitive issues.

- Citizens of some country such as china (which imposes several restrictions on the use of Internet and use of Google, Facebook and other popular sites) use dark web to access them secretly.

V. CONCLUSION AND FUTUR SCOPE

Dark web has always been an interesting topic for researchers. Though it is strengthening its roots hiddenly, it is still not known to a majority of internet users. This paper focuses on providing information on dark web, how anonymity in dark web is achieved through TOR and I2P network, accessing dark web using TOR browser, recent technological developments. While the dark web is just a small portion of the deep web, the activities going on there is a matter of stress. As the dark web is becoming a breeding ground for criminal activities, law enforcement is trying to deanonymize websites and expose the faces behind those websites. Taking into account the future scope of dark web it can be said that the dark web will become even darker. Number of dark web user is increasing day by day. Terrorist groups ISIS, Al-Qaeda and other jihadist groups in Libya and Syria are spreading their activities through dark web. They are using it for hiring members across the world, secretly communicating among themselves, and planning attacks. Recent reports have shown that terrorist groups have used dark web for planning different attacks in Paris, Iraq and Iran. They are using bitcoin to accept donation and using the money to collect arms and other explosive materials. Bitcoin and Litecoin are popular everyday payment currency on dark web. As Bitcoin remains the gold standard in the dark web, litecoin is emerging as a second popular currency to dominate the dark web market. Selling and purchase of stolen credit card details, cloned credit cards, medical details, passport details etc are emerging as new crime in dark web which is a major threat to the society. The activities of whitsleblowers are increasing day by day using dark web. After the shutdown of three major darknet market (silk road, AlphaBay and hansa) by law enforcement, the hosts of darknet markets are strengthening the security of their websites to make it difficult for law enforcement to track the sites. Tor is also developing new tools to overcome the flaws in the security of the existing system. It can be concluded that the use of darkweb is not at all illegal as long as the user doesn't involve in any kind of illegal activity. People can use it for anonymously browsing through the internet without revealing their identity. The rising percentage of criminal activities in dark web indicates that it is hard to completely eradicate these crimes. But the law enforcement is conducting several operations to curb these crimes. As it seems difficult to eradicate crimes on

dark web, we hope that it will be eradicated with the invention and use of new technologies.

REFERENCES

[1] K Finklea, "Dark Web", Congressional Research Service, 2017.
[2] https://www.torproject.org
[3] J. Kosinski, "Deepweb And Darknet- Police View", Archibald Reiss Days 2015, Belgrade, Vol.III, 2015.
[4] https://www.darpa.mil/program/memex
[5] 5.S.Ghosh,P.Porras,V.Yegneswaran,A.Gehani,A.Das,"ATOL- A Framework for Automated Analysis and Categorization of the Darkweb Ecosystem", The AAAI-17 Workshop onArtificial Intelligence for Cyber Security,WS-17-04.
[6] Nadine Cranenburgh, "what lurks on the dark web? New research uses ai to shine light", 20-04-2018,https://www.createdigital.org.au/dark-web-new-research-ai/
[7] "Immunity on the Dark Web as a Result of Blockchain Technology", https://codeburst.io/immunity-on-the-dark-web-as-a-result-of-blockchain-technology-6693eb087bdd
[8] Tarquln," How to Access Notorious Dark web anonymously (10 step guide)", DarkWebNews, 6 November 2018 ,https://darkwebnews.com/help-advice/access-dark-web/
[9] "how to acess notorious dark web anonymously", https://www.wikihow.com/Access-the-Deep-Web
[10] G.Weimann,"Going Dark: Terrorism on the Dark Web", Studies in Conflict & Terrorism Vol.39,Issue.3,pp.195-206, 2016.
[11] V.Vilic,"Dark Web, Cyber Terrorism and Cyber Warfare: Dark Side of The Cyber Space", Balkan Social Science Review, Vol.10,pp. 7-25, 2017.
[12] M.Chertoff, T.Simon," The Impact of the Dark Web on Internet Governance and Cyber Security",Global Commision Of Internet Governence, paper series.(6), 2015.

Authors Profile

Dr. Asoke Nath is working as Associate Professor in Department Of Computer Science , St. Xavier's College (Autonomous), Kolkata. He is engaged in doing research work in the field of Cryptography and Network Security, Steganongraphy, Visual Cryptography, Quantum Computing, Big Data Analytics, Data Science, Green Computing, Li-Fi Technology, Mathematical Modeling in Social Networks, MOOCS, etc. He has published more than 239 research articles in International Journals and Conference Proceedings.

Romita Mondal is currently pursuing M.Sc. in Computer Science (2017-2019) from St. Xavier's College (Autonomous) Kolkata. She has received her B.Sc. degree in Computer Science in 2017 from Narasinha Dutt College under Calcutta University. Currently she is engaged in doing research work in ATM security.

