ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Darknet: A Class of Networks to Share Anonymous Digital Content

Ganesh.I.Rathod[1], Dipali.A.Nikam[2]

Assistant Professor, Dept. of C.S.E, Dr.J.J.Magdum College of Engineering, Jaysingpur, Maharashtra, India

Assistant Professor, H.O.D, Dept. of C.S.E, Dr.J.J.Magdum College of Engineering, Jaysingpur, Maharashtra, India

ABSTRACT: Darknet refer to a class of network that aims to guarantee anonymous and untraceable access to Web content and anonymity for a site. Nowadays internet users are showing more and more interest in anonymous communication, so privacy and anonymity problem have come out. This anonymity can be achieved through Darknet. In this paper, we initially understand the Darknet and later we discuss three popular Darknets, i.e. The Onion Router (TOR), Invisible Internet project (I2P) and Freenet. At the last, we understand how communications takes place in Darknet and have a look around the darker and the brighter side of the Darknet.

KEYWORDS: Darknet, Surface Web, Tor, I2P, Freenet.

I. INTRODUCTION

On the internet, when we search, using a search engine like Google, it generally returns us some millions of pages for every keyword typed. We can try to estimate internet's size by thinking of how many websites would be there, if people are using 'n' number of keywords to search for information. This portion of internet is just what is visible to us, but there exists, within the countless websites, an internet that is way beyond the scope of search engines and general browsing. This is what we call as the Darknet, Deepnet, Deep Web, Invisible Web or Hidden Internet. Darknets refer to a class of networks that aims to guarantee anonymous and untraceable access to web content and anonymity for a site. The purpose is to hide not only the communications themselves but the fact that information is being exchanged. Although the term "Darknet" has no formal definition, it was popularized in the paper [1], which defined Darknet as "a collection of networks and technologies used to share digital content".

"The darkweb"; "the deep web"; beneath "the surface web" or "Blackholes" termed in [4] – the metaphors alone make the internet feel suddenly more incomprehensible and unknown. Other terms circulate among those in the know [23]: Darknet, invisible web, dark address space, murky address space and dirty address space. All these phrases more or less go along the same meaning, in a sense, they are all part of the same picture: beyond the limits of most people's online lives, there exists a vast other internet out there, used by millions but it is been largely ignored by the media and properly understood by only a few computer experts.

II. LITERATURE SURVEY

To understand Deep Web, let us briefly know about the Surface Web, that is nothing but our regular net. The so-called **Surface Web**, which all of us use, consists of data that search engines can find and then offer up in response to your queries. But traditional search engine sees only a small amount of the information that's available, while rest of it is buried in what's called as the **Deep Web or Darknet**. In most part of our paper the term Deep Web is used rather than Darknet. So, the Dark Web is a bit like the Web's id. It is private. It is anonymous. It is powerful. It unleashes human nature in all its forms, both good and bad. The Deep Web consists of data that we won't locate with a simple Google search. No one really knows how big the deep Web really is, but its thousands of times bigger that the surface Web or Opennet. This data isn't necessarily hidden on purpose. It's just difficult for current search engine technology to find and make sense of it.

The Deep Web is enormous in comparison to the surface Web. Today's web has millions of registered domains. Each of which, can have thousands of sub-pages, many of which are not catalogued, and thus fall into the category of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Deep Web. More statistical details can be found in [13].To understand why so much of information is out of sight of our search engines, we should have a bit of background on searching technologies and paper [2], provides good knowledge about it, but we'll in this paper we will have a quick look at it . Search engines generally create an index of data by finding information that is stored on web sites and other resources. This process means using the automated **spiders** or **crawlers**, find web pages by following links on different web pages, and from those pages they follow more links until they have indexed, a very good portion of the web to be displayed on Google. But here's the shocking news: this portion accounts for only about one percent (1%) of all the pages that are out there on the Internet. In fact, it is predicted that the amount of content search engines are unable to itemize is 500 times bigger than the content we are able to see on the Surface Web. Surface Web is the web we use every day, the sites we can get to from Google, Bing or Yahoo. Google alone covers about 8 billion pages, so imagine the subject matter that is not covered by Google, if it accounts for just one percent. Web crawlers are unable to reach the deep areas of the internet for a number of reasons, including technical barrier that make indexing efforts difficult and data incompatibilities. Search engines most common weaknesses include password-protected sites that need registration and login, such as our e-mail, e-banking or a company's private database. They also cannot crawl dynamic content, which is nothing but anything that changes automatically without the user having to manually refresh the page. A chat room is a good example of the dynamic content, where the user sits and the content constantly updates without needing anybody's interaction. There are also sites that simply do not want to be found by search engines; these sites intentionally prohibit spiders from crawling, much like hanging the 'Do Not Disturb' tag outside our hotel room.

There are many millions of sub-pages strewn throughout millions of domains. There are many internal pages with no external links. There are unlisted or unpublished blog posts, picture galleries, file directories, and untold amounts of information that search engines just cannot see. Here's just one example. There are many independent newspaper web sites online, and sometimes, search engine crawlers index a few of these articles on those websites. That's particularly true for important news stories that receive a lot of media attention. A quick Google search will undoubtedly reveal many dozens of articles on, for example, World Cup Cricket teams. But if we are looking for a more hidden story, then we have to go directly to a specific newspaper website and then browse or search for the content we are looking for. This is especially true as a news story becomes old. The older the story, the more likely it is stored only on the newspaper's archive, which is not visible on the surface web. Subsequently, that news may not appear readily in search engines, so it counts as part of the Deep Web [13]. As we can see just from our newspaper example, there is immense value in the information drained away in the Deep Web. The Deep Web is an endless repository for a mind-reeling amount of information. There are financial information's, engineering databases; pictures, medical papers, illustration's etc. And the Deep Web is only getting deeper and more complicated. For search engines to increase their effectiveness, their programmers must find out how to go into the Deep Web and bring data to the surface. Somehow they must not only find useful information, but they must find a way to present it without staggering the end users. Using Deep Web valuable information can be obtained, for example, construction engineers could potentially search research papers at multiple universities in order to find the latest and greatest in bridge-building materials. Doctors could quickly locate the latest research on a specific disease. The potential is unlimited. Yet there's a darker side to the Deep Web too, that is troubling to lot of people for a lot of reasons.

The Deep Web may be a shadow land of untapped potential, but with a small amount of skill and some luck, we can illuminate a lot of useful information that many people worked to archive. On the Darknet, where people purposely hide information, they would prefer it if you left the lights off. The bad thing, as always, gets most of the headlines. We can find illegal goods and activities of all kinds through the Dark Web that includes human trafficking, selling drugs, stolen credit card numbers, child pornography, weapons, copyrighted media and anything else we can think of. But we won't find this information with a Google search. These kinds of Web sites require us to use special software's, such as **The Onion Router**, more commonly known as **Tor**. Some other popular examples of darknets are **I2P** (Invisible Internet Project) and **Freenet**. So in the further section, we try to provide a brief idea about these darknets that is Tor, I2P & Freenet. We also try to understand the communication taking place in Darknet compared to our regular net. Finally, in the last section we give a darker as well as the brighter side of Darknet.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

III. POPULAR DARKNETS

The interest in hidden communication has been acquiring more and more attention from internet users as privacy and anonymity problem have come out. So, this online anonymity can be achieved through three popular Darknets such as Tor, Invisible Internet project (I2P) and Freenet. Note that, I2P & Freenet have not yet reached the same adoption that Tor has but present suitable technical features that could lead them to become possible alternatives in the future.

A. The Onion Router (Tor)

The Tor was originally developed by the U.S. Naval Research Laboratory and it was introduced in year 2002 [15]. It allows for anonymous communications by exploiting a network of volunteer nodes, responsible for routing encrypted requests so that the traffic can be hidden from network surveillance tools. The Tor network is comprised of three different types of nodes: directory servers, exit relays, and internal relays. When we connect to Tor, the first thing our client does is obtain a current list of relays from one of the trusted directory servers. The addresses of these directory servers are included with the basic configuration files transported with the client.

After obtaining a list of currently operational relays from the directory servers, our client then determines the optimal route for our traffic across the Tor network and finally exits from an exit node. This circuit created consists of our computer, the relay to which we are connecting and multiple internal relays before reaching an exit node. Note that this is relatively different than that of traditional IP forwarding that occurs between routers on the internet. Conventional IP routers find a best possible route on a per-packet basis; there are no "stateful" circuits from an IP outlook. In short, for the life of a circuit, all of our traffic will follow the same route within the Tor network and they exit at the same point.

During the circuit creation process, our client exchanges cryptographic keys with the first relay into which it is connected and then its starts encrypting traffic back and forth. Later each hop in transit between the various relays is encrypted using those relay's cryptographic keys. We can visualize this as layers of encryption being wrapped around our data: this is where the phrase "Onion Routing" comes from when describing the type of network Tor establishes. Finally, our encrypted traffic is decrypted at the exit relay where it is then forwarded out onto the regular internet. This is one of the ways that Tor helps to keep our privacy online – each exit node is aggregating traffic from many other Tor users and putting it out onto the internet all at once. Our traffic becomes a small stream in the very large of data coming from and entering back into any given exit node. It is also important to note that our exit node only knows which intermediate node to send receiving data back to (this is also true for each internal circuit). This means that our identity and the content of our traffic are cryptographically divided – our entry node knows who we are but doesn't know what we are doing and our exit node knows what we are doing but doesn't know who we are. All the relays in between only know one thing, that is to forward the encrypted payload to the next relay on the circuit. Assuming that the content of our traffic does not open our identity, this permits us to browse the internet completely anonymously. The fig 1 from [24], illustrates how every layer of the "test" packet is peeled away one at a time on its way to the web server.

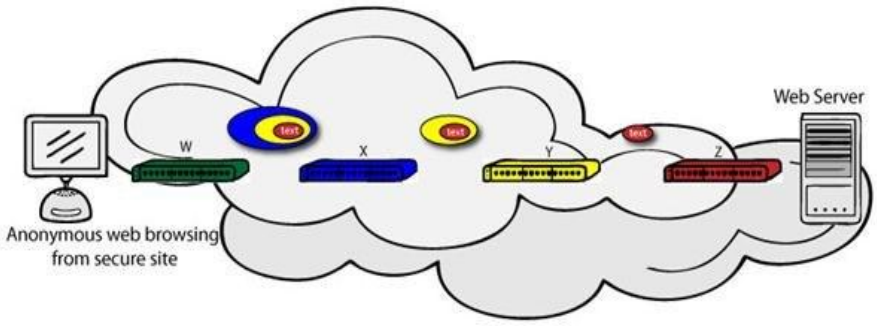

Fig.1. Example of Tor

Tor also allows us to run and access what are called as the "hidden services." These are nothing but the servers that are accessible only from Tor network itself. Among the various hidden services are various blogs, email servers, and forums. We will see in coming section , how I2P provides a better framework for providing these hidden services, but

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

if someone's primary goal is to access our regular internet services in an hidden fashion, then Tor is an essential tool in one's armoury.

B. Invisible Internet project (I2P)

Tor network has some restrictions in a sense that it is built on a centralized system. To overcome this constraint, developers have come up with a distributed alternative for file-sharing which was then followed by the look of peer-to-peer networking (P2P). And later followed by a new project called as the Invisible Internet Project (I2P) [10]. I2P was designed as a hidden peer-to-peer (P2P) distributed communication layer that is able to run on any traditional internet service. The I2P developer's concept was to implement a unique idea for distributed P2P anonymous systems, which provide their users a better anonymity and security [9].On the surface, I2P provides the same benefits that Tor does. Both allows anonymous access to online content, both makes use of a peer-to-peer-like routing structure, and both of these operate using layered encryption. However, I2P was basically designed to provide a different set of benefits. As we saw above, the primary use of Tor is enabling anonymous access of the internet with hidden services as an additional benefit to it. On the other hand, I2P was designed from day one to be a true "darknet.".Its primary goal is to be a "network within the internet", with traffic staying contained in its borders. As many other software's that are designed to protect user's anonymity, I2P also allows the implementation of an additional layer of encryption model and a certain routing system known as "Garlic routing". Garlic routing is quite similar to Tor's onion routing. The main difference with onion routing is that Garlic routing extends onion by bundling different messages together. All data that are transmitted through the tunnels are fully encrypted and message can be decrypted only by the receiver's router.

The important components in I2P network are: router, tunnels and NetDB.

Router: Routers are just simple software that participates in the network.

Tunnel: Tunnels are unidirectional path through several routers, which means that the sending path and the receiving path are different. (Example for Alice and Bob want to communicate through I2P, they actually require four tunnels). Tunnels get expired after certain amount of time. Tunnels are checked every time to remove the failing tunnels. The default lifetime is set to ten minutes (10 min). The length of a tunnel hop usually changes. Tunnels could be exploratory or client. There are two types of tunnels (inbound tunnels and outbound tunnels) that is been proposed by I2P [11]. Below fig 2 from [11], gives a clear picture of it.

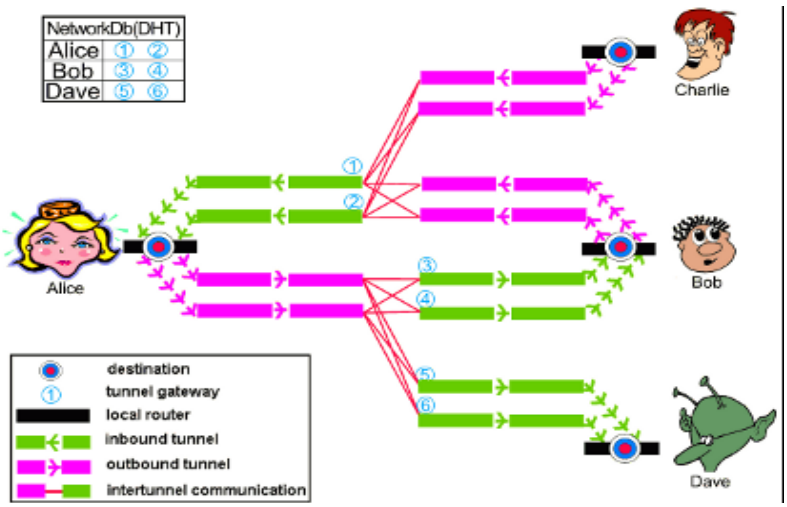

Fig.2. I2P tunnels overview

Inbound tunnels and outbound tunnels are automatically built when I2P is started. Also, it is important to notice that connections to tunnels are only valid for nodes over which I2P has installed paths. As given in figure 2, the first tunnel is a tunnel gateway and the last tunnel is the tunnel exit point or endpoint.

NetDB : The network database called NetDB is one of the key concept of I2P, it is comprised of a pair of algorithms that makes the sharing of metadata possible [12].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

I2P routing is differently than Tor. I2P performs packet based routing as opposed to Tor's circuit based routing. This has the advantage of allowing I2P to dynamically route around congestion and service interruptions in a similar manner to the internet's IP routing. This provides great amount of reliability and redundancy to the network itself. Additionally, I2P does not depend on a trusted directory service to get route information. Instead of that, network routes are formed and constantly updated dynamically, with each router constantly evaluating the other routers and sharing what it finds. Finally, I2P forms two independent simplex tunnels for traffic to traverse the network to and from each host as opposed to Tor's formation of a single duplex circuit. This provides the additional advantage of only disclosing half the traffic in the case of an in-network eavesdropper. From the perspective of application-level, there is a fundamental difference between the I2P and Tor networks as well. Tor functions by providing us a proxy on our local machine that we must configure our applications to use. In contrast, I2P is basically used by applications that are written specifically to run on the I2P network only. These include, but are not limited to, file sharing, instant messaging, email and distributed storage applications.

C. Freenet

Freenet has been formed since 2000 and it can be considered as the predecessor of I2P. Freenet is a distributed content sharing system, where users can both insert and retrieve files [21]. As a popular peer-to-peer anonymous network [14], Freenet aims to provide the anonymity to both content publishers and retrievers. Unlike I2P, Freenet implements a pure Distributed Hash Table (DHT) [22], in the form of an unstructured overlay network. It means that every node is responsible for a subset of the resources available in the network and serves them collaboratively when it receives a request. Further, nodes maintain a list of neighboring nodes, usually only known and trusted neighbors, to increase security. This is also called as the "small world principle". Data and nodes are known by a key, usually represented with a hash value. When looking for a resource, a request will pass across all of a node's neighbors in order of preference (i.e., basically to the nodes whose key is closest to the resource key).

Due to its adopted approach, Freenet is more suitable to serving static contents such as static sites and does not cope well with dynamically generated web pages or other forms of internet services (e.g. mail, IRC etc). When compared with I2P and Tor, Freenet provides less flexibility in terms of hosted services, being limited to serving only static content without, for example, server-side scripting. The range of services that can be implemented on top is smaller. However, this does not mean that Freenet cannot be a suitable platform to host simple marketplaces or exchange information related to malicious activities.

IV. COMMUNICATIONS IN DARKNET COMPARED TO CLEARNET

To differentiate between the regular internet and Darknets, the term "Opennet or "Clearnet" termed in [16] is considered, which refers to the normal, publically accessible internet at large. Darknets function inside the internet, and are dependent on it to function, but their design theories and goals dictate that they operate under fundamentally different principles than that of the Clearnet. This may be explained by highlighting how the two networks communicate. When a Clearnet or Opennet user at home opens an URL (for e.g. ww.google.co.in) in their web browser, data is first sent to their router. This is then forwarded to their ISP's routing infrastructure, which is in turn transmitted to the next router. This continues until the last hop, which is the server that hosts the requested page, which then services the request – in this case, displaying the Google India homepage. The path that the data takes from the home PC to the web server can be seen by running tools such as tracerout, on the originating computer. Although the exact route that data takes may change over time, depending upon the routing principle of the network infrastructure, it is likely that subsequent paths will not change greatly. All data transmitted through this method is unencrypted, allowing for interception, data alteration or observation, as can be seen in the figure below.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

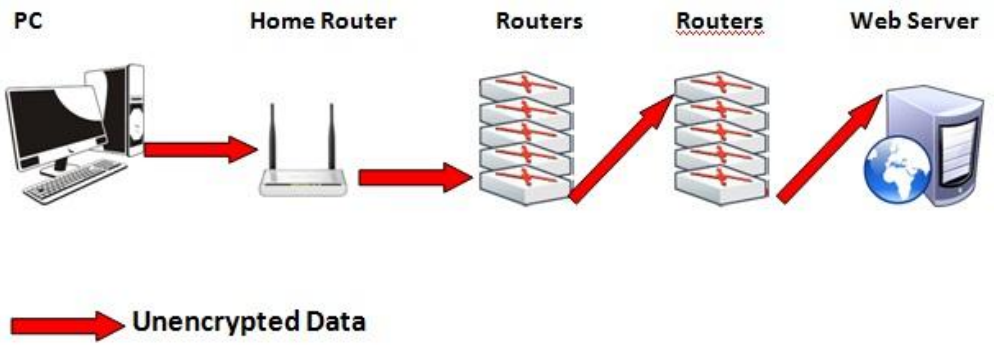

Fig.3. Data routing across the Clearnet.

When a user of the Tor Darknet accesses the same above website, data is first sent to the Tor routing software installed on their PC. This software produces encrypted tunnels to one or more Tor entry relays. Data is transmitted from the Tor software through a tunnel to the Tor entry relay, which has itself encrypted tunnels to other Tor relays.

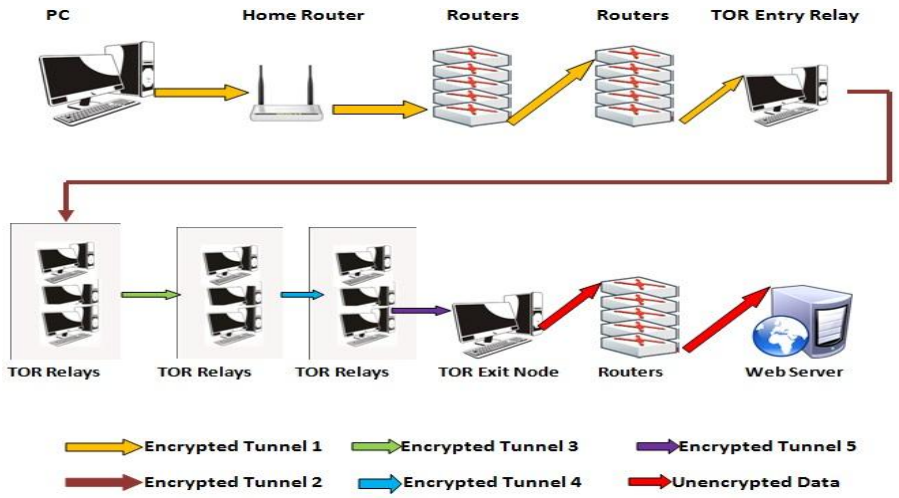

Fig.4. Data routing across TOR

Data is forwarded to a various other Tor relays, before it arrives at a Tor exit point or exit node, which is an exit point from Tor into the Clearnet. From here onwards data will traverse Clearnet paths to the server, which then services the request. The actual path that the data took inside Tor cannot be predicted, but only the Clearnet route, that the data took into Tor and the route it took when it exited Tor can be seen. All data sent via Tor is encrypted in such a way that the original data source and destination cannot be predicted, and the data cannot be changed, as seen in the fig 4.

V. DARKER & BRIGHTER SIDE OF DARKNET

Most of the Darknet is misused for criminal purposes. This is just because it offers almost full anonymity to criminals. They are to; sell services such as, assassin services, porn of all types, credit card fraud, journalists who want to work without the possibility of getting jailed for speaking truth, assassins and thieves can openly post their resumes and contact information, selling banned drugs etc.

That is why Darknet is dangerous. So, in spite of all these criminal activities authorities hesitate to put a complete break on Darknet software's because, according to the article, popular Darknet Tor was initially created by the US military base for hidden communication. They still dump government files on the Darknet, which is not open to general public. There are hidden intranets where they store these files and people who have passwords can only access these files. Since various governments are themselves using the Darknet, they do not consider it practicable to order Tor to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

shut it down, which gives offenders, a free hand. They can create and host anonymous websites offering just about anything but is not searchable from our normal web, nor can the regular mainstream browsers open such sites as they are not dependent on traditional DNS servers. All the Darknet has **.onion** domains that can be accessed only through Tor browser and a few more projects that are able to utilize Tor networks. But the simplest way to get into the Darknet is the Tor browser.

The Darknet itself has ominous overtones. But, not all the darker side is bad. The Darknet is a home to alternate search engines, file storage, E-mail services, file sharing, chat sites, social media, whistle blowing sites and news outlets. Darknet is desired by governments to allow to operate in full anonymity, of course this aspect has been exploited by criminals, hack activists and other normal people who wish to defend their privacy, for this reason various agencies and institutes of few countries have promoted project to develop new monitoring systems and at same time they have started a misinformation campaign against this parallel and hidden world. The governments want us to stay away from hidden web, because they cannot spy on us, the crime is present in Darknet as well as in the Clearnet, of course the anonymity granted by Darknet could encourage criminal activities but at same time it represent an obstacle to the criminal that for example wish to steal sensible information of the users or spy on them.

Need for Darknet: With news of intelligence agencies surveillance practices, it has become vital to keep critical and important documents secret. It can also be a solution for research of sensitive topics, hidden military communication and safe submission of sensitive documents to police, governments etc. Journalist community can make a maximum use of the Darknet because it is safer than any other privacy measure. But, before frequently using Darknet, a good cyber security infrastructure has to be implemented. Darknet exists in order to provide amazing services to people and organizations that require anonymity to release their information or communicate without any fear. It is time to realize the good and the bad of technology in order to use it very well judiciously and constructively.

Darknet search engines may not offer up personalized search results, but they do not track our online behavior or either does not offer up an endless stream of advertisements. For citizens living in countries with violent or oppressive leaders, the Darknet offers a more secure way to communicate with like-minded individuals. Unlike Twitter or Facebook, which are easy for determined authorities to monitor, the Darknet provides deeper cover and a degree of safety for those who would plot to undermine politicians or corporate overlords. So although the Darknet has its murkier side, it has great potential, too.

VI. CONCLUSION

This paper has tried to provide a brief overview on Darknet and discussed three popular darknets such as Tor, I2P and Freenet. Darknet is a large field of research and development that steadily continues to grow. The interests and demands of the general public are increasing all the time. The source for this demand may be all the lawsuits against users of file sharing applications, and in some countries, the outlawing of such applications. But not only individuals with a liking for file sharing want anonymous networks. Human rights activists fight for the right of freedom of speech without unmotivated eavesdropping by the government and journalists want to protect their sources. In many western countries, laws permitting such eavesdropping or wiretapping by government authorities is already in place, or will soon be. Equally much as the topic of anonymous communication is controversial, it also shows the creativity of a group of dedicated individuals to fight back against laws and authorities by the means of technology. It is therefore ironic that Onion Routing originates from the US Navy Research lab. Most anonymous systems is however created and developed by individuals or academic institutions. Tor and I2P are two systems we believe will still be in use in the following years. They have proven to be working and are constantly gaining popularity.

REFERENCES

[1] Biddle, England, Peinado, & Willman, "The Darknet and the Future of Content Distribution," Microsoft Corporation, 2002.
[2] Monica Peshave, "How Search Engine Work and a Web Crawler Application",2005,www.micsymposium.org/mics_2005/papers/paper89.pdf.
[3] Gildas Nya Tchabe and Yinhua Xu, "Anonymous Communications: A surveyonI2P".https://www.cdc.informatik.tudarmstadt.de/fileadmin /user_upload / Group_CDC /Documents / Lehre/SS13/ Seminar/CPS/ cps2014_ submission_4.pdf.
[4] K. Kinjal N. Patel, "Internet Worm Detection Using Distributed Blackhole Networks", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 1, January – 2014.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

[5] Abdelberi Chaabane, Pere Manils, and Mohamed Ali Kaafar. Digging into Anonymous Trac:"A Deep Analysis of the Tor Anonymous Network". In Proceedings of the 2010 4th International Conference on Network and System Security, NSS '10, Washington, DC, USA, September 2010. IEEE Computer Society.
[6] Dingledine, R., Mathewson, N., Syverson, Tor: "The second-generation onion router". In: Proceedings of the 13th USENIX Security Symposium (August 2004)
[7] Herrmann, M. and Grotho_, C.: Privacy Implications of Performance-Based Peer Selection by Onion Routers:"A Real-World Case Study Using I2P". In the Proceedings of the 11th Privacy Enhancing Technologies Symposium (PETS 11). Waterloo, ON, Canada, July 27 - 29, 2011.
[8] B. Guanyu Tian, Zhenhai Duan, Todd Baumeister, Yingfei Dong, "A Traceback Attack on Freenet", http://www.ee.hawaii.edu/~dong/traceback/1569649421.pdf.
[9] Michael Herrmann and Christian Grotho, "Privacy-Implications of Performance-Based Peer Selection by Onion-Routers": A Real-World Case Study using I2P. http://grothoff.org/christian/i2p.pdf.
[10] J. Jrandom, I2P Anonymous Network: Technical Introduction, Retrieved on December 13, 2010, from Anonymous Network.,http://www.i2p2.de/techintro.html.
[11] wiki.ubuntuusers.de/i2p.
[12] TMA2012-LNCS.pdf.http://hal.archives-ouvertes.fr/docs/00/63/22/59/PDF/TMA2012-LNCS.pdf.
[13] Michael. K. Bergman, "The Deep Web: Surfacing Hidden Value", White Paper- BrightPlanet - Deep Content, Monday, September 24, 2001.
[14] C. Callanan, H. Dries-Ziekenheiner, A. Escudero-Pascual, and R. Guerra. Leaping over the firewall: A review of censorship circumvention tools. Report by Freedom House, Apr. 2011.
[15] Vincenzo Ciancaglini, Marco Balduzzi, Max Goncharov, and Robert McArdle, "Deepweb and Cybercrime". A Trend Micro Research Paper.
[16] Symon Aked, Christopher Bolan and Murray Brand, "Determining What Characteristics Constitute a Darknet" 11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013
[17] Zantout, B.C. and Haraty, R.A: "I2P Communication System". In the Proceedings of 10th International Conference on Networks (ICN 11). Saint Maarten, the Netherlands Antilles, January 23 - 28, 2011: 401 - 409.
[18] Chen, X.-W. Chu, A.L. Jia, and J.A. Pouwelse. "Inequity of sharing ratio enforcement in Darknet": Measurement and improvement. In Proceedings of the 14th International Conference on High Performance and Communications (HPCC'12). Liverpool, UK, 2012.
[19] Xiaowen Chu, Xiaowei Chen, "Dissecting Darknets: Measurement and Performance Analysis", http://www.comp.hkbu.edu.hk/~chxw/papers/darknet_preprint.pdf.
[20] Michael Bailey, Evan Cooke, Farnam Jahanian, Andrew Myrick, Sushant Sinha, "Practical Darknet Measurement", http://mdbailey.ece.illinois.edu/publications/ciss06_final.pdf.
[21] Freenet. https://freenetproject.org/.
[22] https://www.cs.rutgers.edu/~pxk/rutgers/notes/content/dht.html.
[23] http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet.
[24] http://null-byte.wonderhowto.com/inspiration/anonymity-darknets-and-staying-out-federal-custody-part-two-onions-and-daggers-0133474/
[25] http://www.thewindowsclub.com/darknet-deepnet.