iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48588

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

Dark Web

Anmol Chauhan[1], Navpreet Singh[2]
Jagan Institute of Management Studies

Abstract: ***In today's world, we are all connected to the Internet in one way or another. It has become an integral part of daily routine or lifestyle. The Dark Web is like a hidden cache on the internet commonly used to store and access personal information. However, there have been numerous reports of the site being abused for criminal and illegal activities. In this article, we will present a comprehensive look at the Dark Web and the different browsers used to access the Dark Web. Learn different aspects of the Dark Web like features, pros, cons and browsers will be discussed. It also presents a complete view of the different attack, mining and rock types. There are different types of crimes and incidents on the dark web discussed so that readers are aware of these types of activities and take appropriate measures to protect them.***
Keywords: Internet, Dark Web, Dark net, TOR, Onion Road.

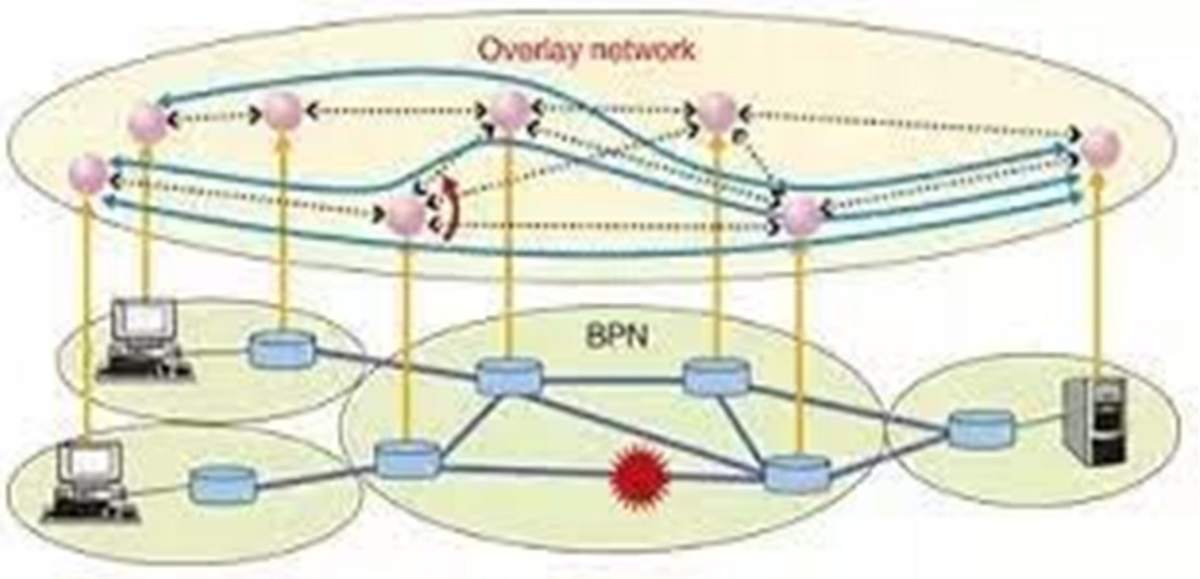
I. INTRODUCTION

As the Internet continued to grow in the mid to late 90s, it transformed a lot around the globe. The main problem is that the Internet is no longer designed with factors like privacy and anonymity in mind.

But, some people are very concerned about their privacy and in the mid-1990s one such group of people became the federal government of the United States. As long as you have an internet connection, you can communicate with anyone. A team of scientists and mathematicians working for one of the divisions of the United States Navy, known as the Naval Research Laboratory (NRL), has pioneered the innovation of the latest generation. called Onion Routing. The biggest change happened with the immediate form of communication within. With the development of the times, digitization has ended with the technology of various types of attacks. So the whole batch can be tracked or traceable. Web protection has become one of the major issues when most users go online to fulfill their desires.

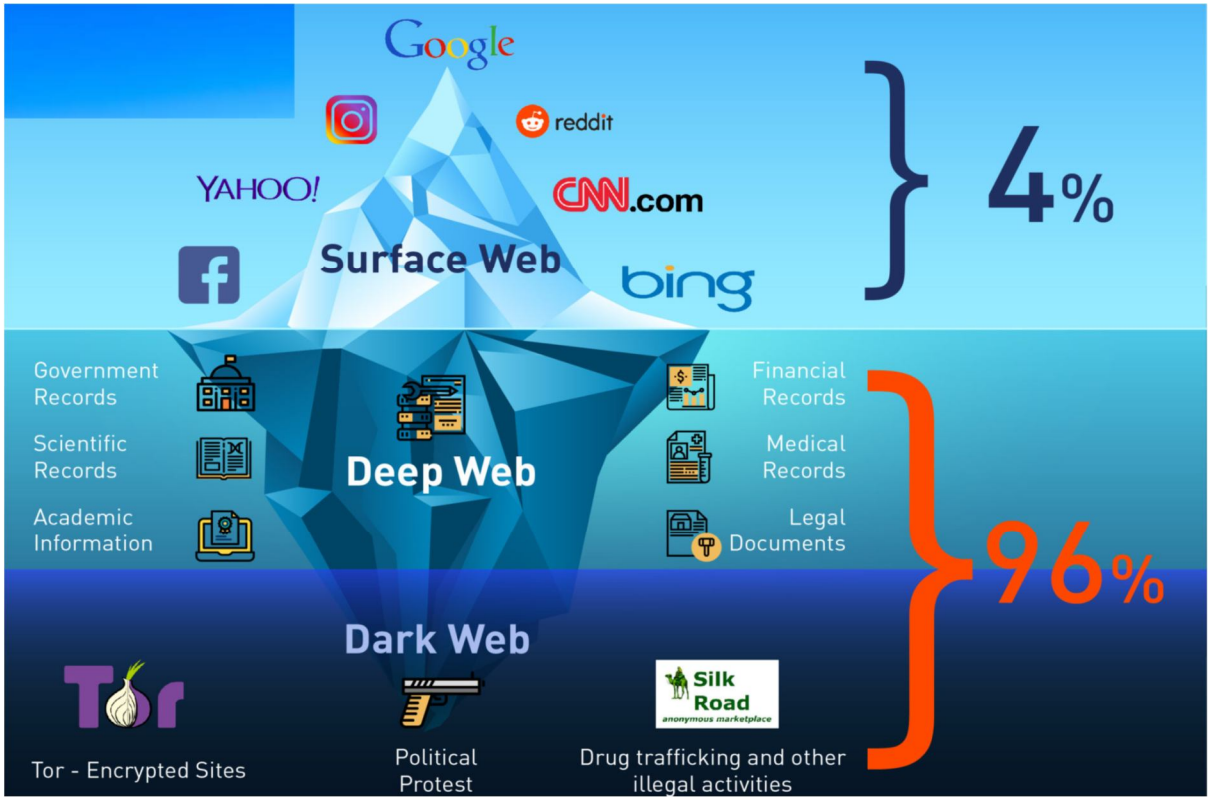
Allow blind connections where the source and location are not determined by a third party . This is achieved by constructing an overlay network. A network overlay is a network built on top of another network. Here in our case the network is the Internet. In this case, the traffic goes through the overlay network, as shown in Figure 1.

Fig. 1 Overlay network



©IJRASET: All Rights are Reserved

Fig. 2 Layers of internet



Networks that use onion routing are classified as Darknet. By meeting in all these different darknets, the Dark Web was born. The folks at the NRL soon realized that for the network to be truly anonymous, it had to be accessible to everyone, not just the US government. As a result, NRL was forced to release its onion process community under an open source license and become the Onion Router (TOR).

A. Structure of Internet

The World Wide Web (www) has three parts namely Surface Web, Deep Web and DarkWeb as shown in Figure 2. Surface Web, also known as Visual or Visual Web, is easily accessible to the public through web search engines. standard.

Only 0.03% of results are available on most web search engines. Deep Web works with most websites and is not widely available in the community. Also known as hidden or hidden web. It is estimated that 96% of the Internet is a dark, deep web. It is used for covert purposes. One of the most insightful examples of the web is: Netflix, online banking, email, dynamic pages and insights, and all are password protected or a fee wall. The Dark Web also refers to content from the World Wide Web but is not more of a web element as it is and is not available to most of the browsers used to access the web above. He began his development with the help of the US military, which he used as a means of communication with spy devices placed remotely outside his adopted son. The dark web is the part of the web that is largely illegal and disruptive. The Dark Web is also used as an illegal platform for terrorism, hacking and fraud, theft and fraud, child pornography and more. It is the Dark Web that is part of the Deep Web. The Dark Web provides hidden services that end in action

B. Elements of the Dark Web

There is a contract process and tools used to create the Dark Web. The important elements of the Dark Web are the browser for accessing Dark Web files, the encryption process to encrypt the data, the virtual private network for data transmission, and the routing algorithm [5]. Access to the dark web is important for anonymity. It is not enough to browse for anonymity, but also to use a good virtual private network (VPN). Nord VPN or Ghost VPN for free. NordVPN acts as a personal VPN service provider. Contains

macOS, Windows, and Linux desktop apps for iOS and Android. In the case of Phantom VPN, so is internet usage, it is not tracked and securely stored by ISPs, online snoopers and advertisers.

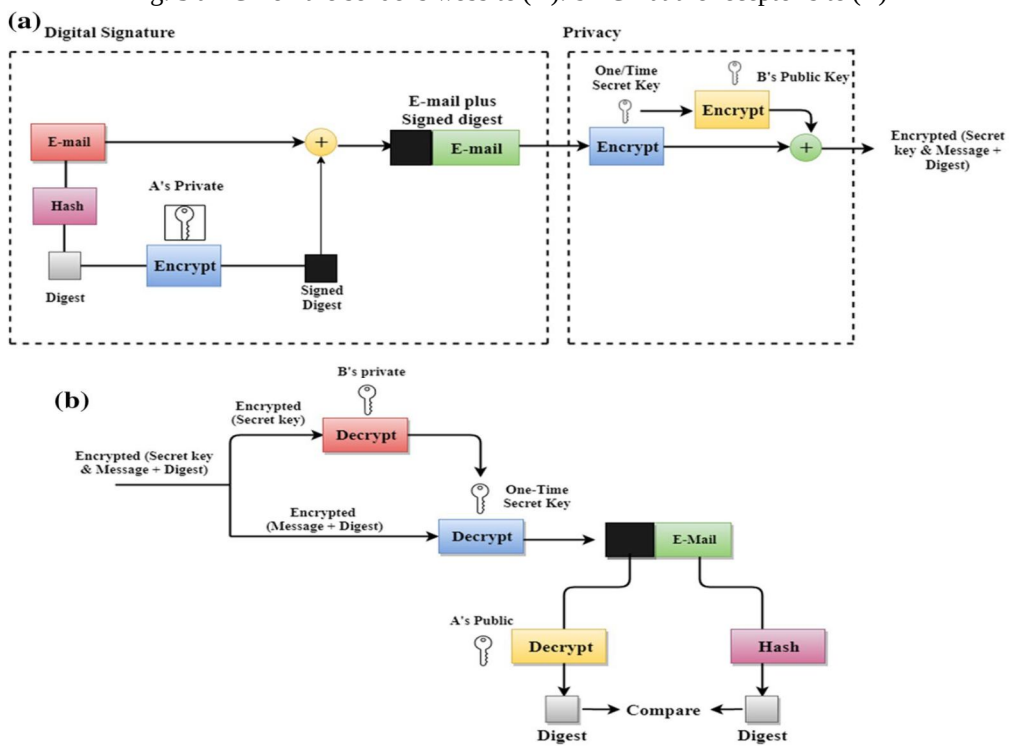
Encryption is a key feature used on the Dark Web. Multiple layers of complexity Encryption uses the TOR browser and a random path is used to protect your identity. If the web is dark and you don't want to use a particular intermediary communication system, this data is available to third parties. This means that you should not share any information that could be problematic if a third party gets involved. Anonymity solves this problem in most cases. But the problem persists because a third person can still read the messages you send or receive. Then the encryption process known as Pretty Good Privacy (PGP) [6] takes effect

It is a strong encryption technology that always protects all kinds of sensitive information or communications.

Designed to provide security features such as integrity, authenticity, confidentiality, and non-disclosure. PGP is basically based on unequal crucifixion. In unequal encryption, two different keys i.e. public key and private key are used to encrypt and decrypt data. This is the public key for anyone Public key. In this type of encryption, when someone nails a message with your public key, only you can remove the encryption and read it.

PGP can also be used for authentication purposes. To prove authenticity, PGP works differently. It uses a combination of hashing and encryption for public keys. Ensure security, using a combination of private key encryption and public key encryption. Thus, a private key, a hash function and two public-private keys are used in the digital signature as shown in Figure 3

Fig. 3 a PGP on the sender's website (A). b PGP at the receptor site (B)



Using PGP encryption has many advantages. First of all, details are always protected as they cannot be viewed or stolen by anyone on the internet. Insights or data can be shared securely over the internet. Deleted messages or other sensitive information cannot be recovered once they have been deleted. Second, emails or messages cannot be infected by invaders. This encryption method verifies the sender's details so that it is not verified by a third party. Easy to use. Confidentiality is ensured using symmetric block encryption. Electronic signatures provide a guarantee. Provides compression using the base 64 encoding system.

There are many browsers designed to access the Dark Web. A detailed discussion of various browser features has been presented in the program. 3.2. The most used browser on the Dark Web is Onion Route (TOR)

Created by Paul Syverson, Michael G. Reed and David Goldschlag at the US Naval Research Laboratory in the 1990s.

TOR is written in C, Python, and Rust. TOR alpha version was released on September 20, 2002. It works with lane technology [7]. In this way, the user's data takes precedence over the code and the data is transmitted over the different transmission lines (central

computer) existing in the network. Therefore, it generates multi-line based encoding. Multiple transfers can be a result of extra bandwidth and won't change it's very difficult to track any user.

By default there are three transfers when discrete shared communication is described below -

1) *Protection and Intermediate Relay:* Protective and Central Relay also known as Goless Forwarding as if shown in Figure 4. It is the basic transmission that makes up the Tor circuit. In between, the handover does not act as a secure handover or a handover exit, but acts as a secondary location between the two. The transfer of security guards must be quick and stable. It requires little hosting effort. Originally the actual IP address of the client or user trying to connect to the TOR circuit, obviously There are websites where security personnel are currently being directed, their contact details can be seen.
2) *Switch Output:* This is the final Tor Circuit relay. Move the outgoing traffic to where it's going. The client will only see the IP address of the output relay instead of the actual IP address. Each node has only information about its predecessor as well as its interest (Figure 5).
3) *Bridging:* As mentioned earlier, TOR users will only deal with forwarded IP addresses. However, TOR can still be blocked by governments or ISPs by blacklisting TOR addresses and public IP addresses. Bridges are less dangerous and require lower bandwidth performance.

C. *Browsers: A Way to Access the Dark Web*

The browser acts as a gateway to the Dark Web . Table 1 presents typical browser variants for accessing the Dark Web and their pros and cons. The underlying router protocol used in a particular browser and its features are also listed in the table.

Fig. 4 Relays used in Dark Web

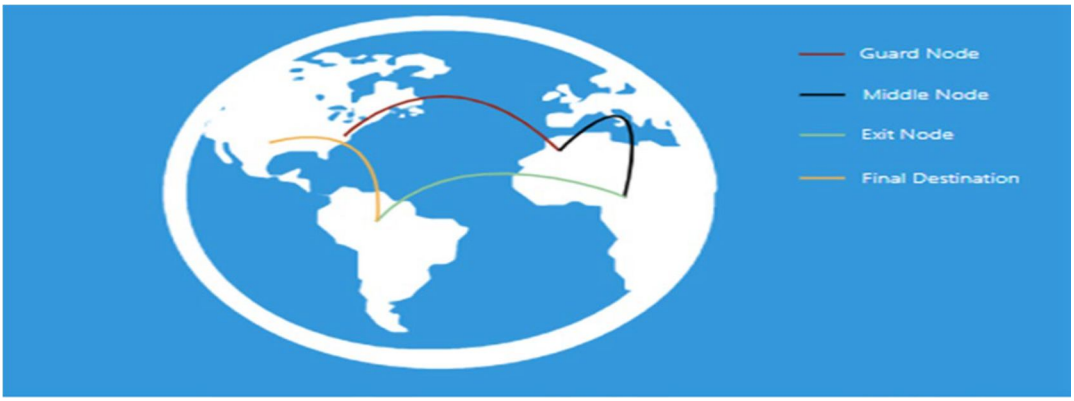
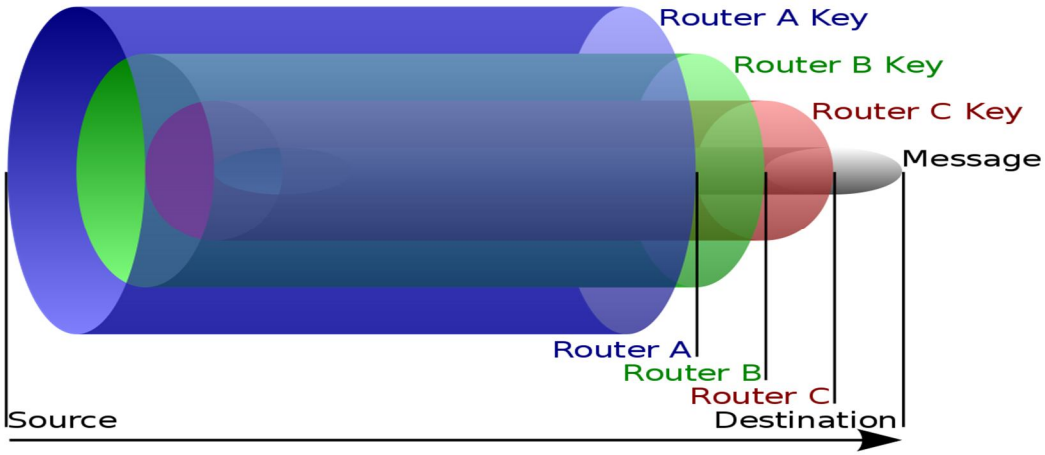


Fig. 5 Data flow in onion routing



II. LITERATURE

Internet layers extend beyond local content that many people can easily access in their everyday searches. Some of the content is from the Deep Web, content that is not displayed by traditional search engines like Google. The long corners of the Deep Web, sections known as the Web, contain intentionally hidden content. The dark web can be used for legal purposes and to conceal criminal activity or other harmful ways. It is the exploitation of the Dark Web through illegal activities that has benefited officials and policymakers.

People can access the Dark Web using special software like Tor (short for Onion Router). Tor relies on a volunteer computer network to provide web users through another user's computer network that the first user cannot track traffic. Some developers have developed tools - such as Tor2web - that can allow anyone to access Torhost content without downloading and installing the Tor software, although accessing the Black Web in this way can be difficult. may have some effect. While on the Dark Web, users often navigate through links such as "hidden Wikis", which categorize web pages, like Wikipedia. People can also search the dark web using comprehensive search engines, search the deep web, or more specifically look for illegal items like drugs, illegal guns, or counterfeit money. On the Dark Web, individuals can communicate through channels such as secure email, web chat, or Tor-hosted private messages. While tools like Tor aim for anonymity and content, researchers and security experts are constantly developing ways to identify or "reveal" certain hidden services or individuals.

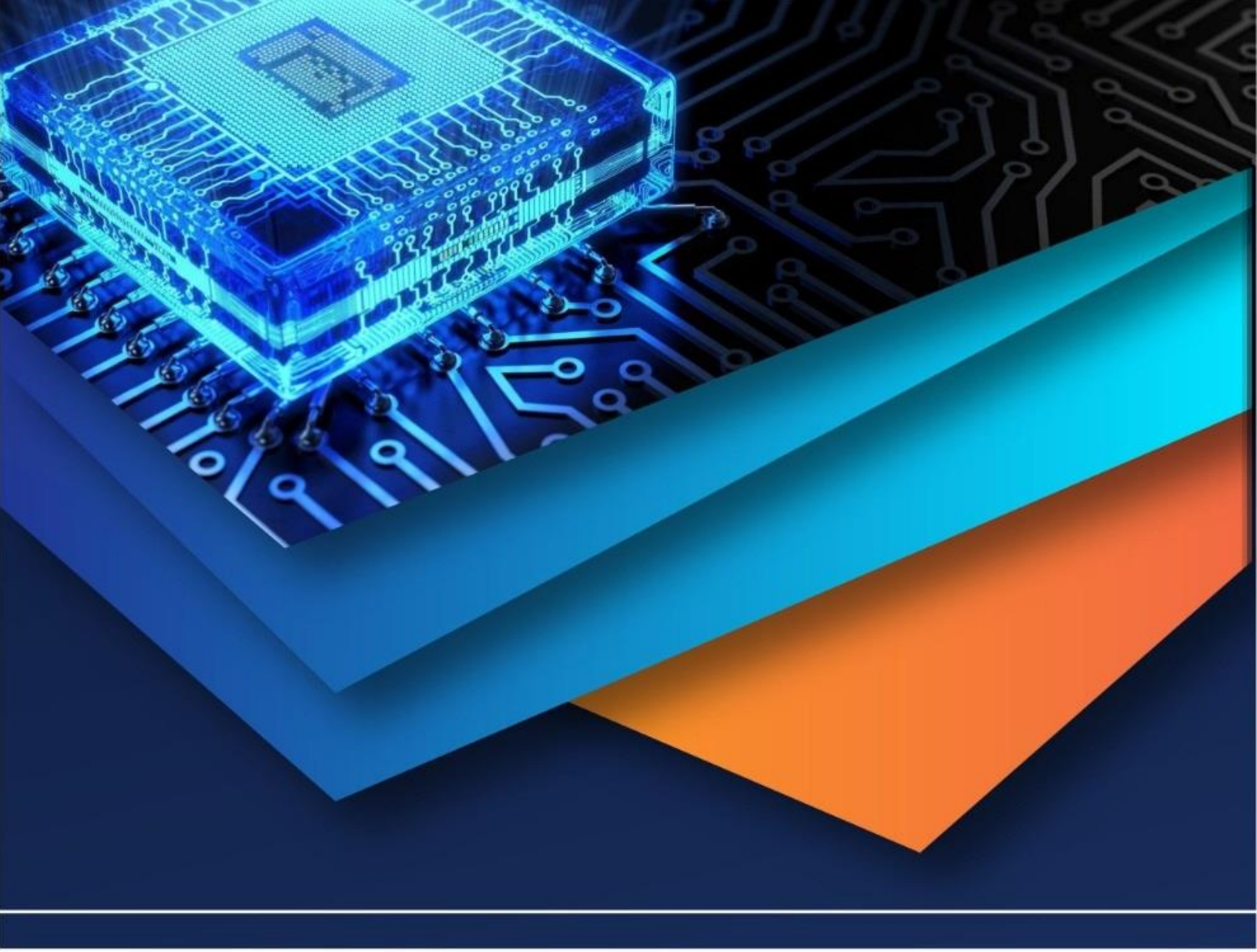
Unknown exchanges like Tor have been used for illicit and illegal activities ranging from maintaining privacy to selling illegal goods – especially those purchased with Bitcoin or other digital currencies. They can be used to prevent bans, access to blocked content, or to maintain the security of sensitive communications or business plans. However, the list of evil figures, from criminals to terrorists to state-sponsored spies, can also use cyberspace, and the Dark Web can serve as a forum for discussion, collaborate and act.

III. CONCLUSION

The dark web is a part of the internet that is often used by users to perform some tasks in a hidden way without leaving a trace. It has become a hotbed of criminal activities such as child pornography, arms trafficking, drug trafficking and onion processing, etc. The main reason for these activities is the anonymity provided in this forum. There are several attacks launched on this platform and the ransom is made in the form of a small amount on the Dark Net. It is also used by the governments of different countries for privacy purposes. See all Dark Web attacks, abuses, browsers, and different instances. It can be concluded that the pros and cons of the Dark Web depend on the intentions of the users.

REFERENCES

[1] https://en.wikipedia.org/wiki/Dark_web
[2] Ciancaglini, V., Balduzzi, M., & Goncharov, M. [Online]. Retrieved December 20, 2019, from https ://www.trend micro .com/vinfo /pl/secur ity/news/cyber crime -and-digit al-threa ts/deep-web-and-cyber crime -its-not-all-about -tor.
[3] Mirea, M., Wang, V., & Jung J. (2019). The not so dark side of the darknet: a qualitative study. Security Journal, 32, 102–118.
[4] Mirea, M., Wang, V., & Jung, J. (2018). The not so dark side of the darknet: A qualitative study. Security Journal, 32, 102–118.
[5] https://www.cumanagement.com/articles/2019/05/introduction-dark-web
[6] https://www.investopedia.com/terms/d/dark-web.asp
[7] https://www.cumanagement.com/articles/2019/05/introduction-dark-web



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)