# Introduction of Dark Web

Praveen Dominic, Department Of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
E-mail id - praveen.dominic@Galgotiasuniversity.edu.in

***Abstract:-The Internet as a whole is a network of numerous computer networks and their vast infrastructure. The network is made up of open websites using search engines such as Google, Firefox, etc. Dark Internet is a part of the Deep Web. It can be reached via TOR. Actors on Dark Web pages are anonymous and secret. Anonymity, anonymity and the probability of non-detection are three considerations offered by special browsers, such as TOR and I2P. In this article, we're going to analyze and produce findings on the effect of the Dark Web on various realms of society. The number of average anonymous users of the Dark Web (using TOR) in both Kosovo and the world is provided for a period of time. The effect of secret resources websites is seen and the findings are obtained from the search engines of Ahimia and Onion City Dark Web. Anonymity is not absolutely confirmed on the Dark Internet. TOR is committed to it and planned to carry out secret tasks.***

***Keywords: Anonymity, Dark Web, Privacy, TOR, I2P.***

## . INTRODUCTION

A lot of people believe that the Web and the web are synonyms. In addition, there are two separate definitions with similar elements. The Internet requires numerous networks and their vast infrastructure.[1] It allows a million computers to be linked by establishing a network on which each device can communicate with other computers as long as it is linked to the Internet. The web (medium) offers access to information. In terms of conceptualization, web content is made up of open web pages via search engines such as Google, Firefox, etc. This material is referred to as the "Internet top".[1]

Another component of the Internet is the Deep Web, which applies to a subset with its contents where it is used for various technical purposes. It contains information on private networks and intranets (agencies, institutions, businesses, corporate websites, etc.), web lookup pages or forms searches. Broad Web is also segmented as the Dark Web. Its content is intentionally hidden and cannot be accessed by standard web browsers. The owners of the Dark Web pages are anonymous and secret.[2] Apps are accessible on the Dark Web to exchange low-risk and undetected (anonymous) info. Access by users anonymously is important for the Dark Web, and has recently been sponsored by the encryption tunnel for surveillance security. The TOR project was initiated in 2002 by the US Naval Research Laboratory to allow anonymous online communication. Invisible Internet Project (I2P) is another network on the Web with data at its edges that is used for secure communication, information encryption, etc.[3] This guarantees more efficient and reliable networking TOR allows users to channel their traffic via "server machines" in such a manner that traffic is not tracked back to the original users and that their identity is concealed. To transfer data from one layer to another, TOR has built "relays" on computers that hold information via tunnels all around the world. Dark web can be accomplished by means of open and cooperative nodes of other network communities (TOR or I2P).[4] TOR has the name of the program that we run on the device and the data network that controls and supports its connections. This allows users to access websites via virtual tunnels where individuals and organizations can share data through public networks without violating their privacy.[4]. Figure 1 shows the in introduction of dark web.

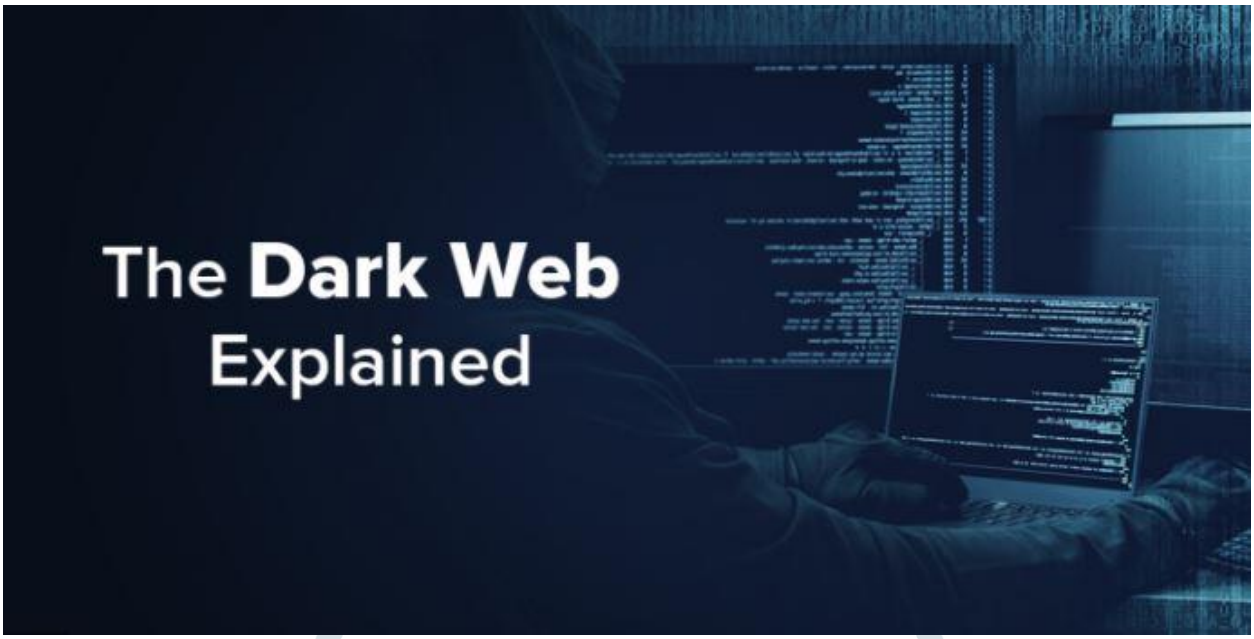


**Fig.1: Introduction of Dark Web**

## RELATED WORK

The sharing of arms and the incidence of child pornography was conveniently carried out with the aid of the Dark Web. The delivery of network information with the aid of the TOR network and consumers can conveniently afford an encrypted method anonymity. As a consequence, in order to perform an in-depth analysis, the numerous works of literature allow for the enhancement of study, and hence the TOR routing with the other concepts is given with the aid of the numerous US intelligence systems.[5] It not only allows the Dark Network mechanism to be used for a legitimate reason, but also for an illegal reason. The privacy of the program, with an adequate review of the network trackers, is conveniently depicted for the purpose of evaluating the data, and study is also continued with the aid of the ISI testing frameworks.. The behavior of the literature review is based on a thorough analysis of the different aspects of the Dark Web, which is clarified in an acceptable manner. The work also serves to explain the important aspects of the study carried out by the researcher. In another study by Barnett et al., the function of spiders (defined as software programs that are used to transverse information on the World Wide Web) and the ease of access that can be obtained through the registration process are studied and thus the exact and required information on the various forms can be easily collected. Social network analysis (SNA) is an subject of interest and is being performed for the purpose of obtaining graph-based approaches, making it possible to evaluate the network structure by representing the structure or population power.[5] The effect of social connections is commonly represented by the use of social networks, making it easier for real life networks to do so. Specific SNA methods have been developed for the analysis of forum posting and website connections. The primary focus is on understanding the "remote networks" and their particular characteristics. Detailed coding systems have been developed to identify militant websites and terrorism content.

Sentiment and impact analysis allow the detection of violent and extremist sites that present significant threats. Terrorism Informatics is referred to as the use of specialized knowledge processing, research methods and methodologies to store, incorporate, handle and interpret the diversity of intelligence relevant to terrorism for international / national security purposes. The methodology is drawn from fields such as computer science, arithmetic, astronomy, economics, social sciences, etc. Figure 2 portrays the types of dark web.

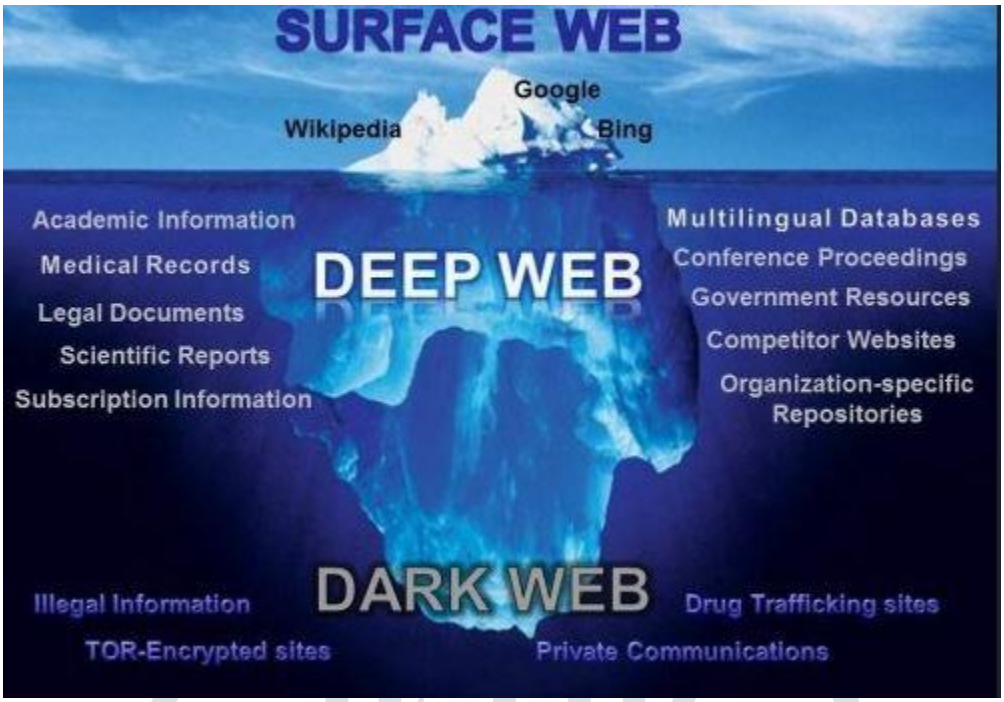


**Fig 2. Types of Dark Web**

*Techniques, Attributes, Accessing and Communication in the Dark Web:*

Anonymity in the Dark Web is derived from the Greek word "anonymia" which refers to the hiding of personal identity from others. If we take some activity on the site, our fingerprints are recorded as data on the Internet. If the Internet Protocol address cannot be registered, we may assume that anonymity is assured. The TOR client, via volunteer server networks, pushes Internet traffic all over the world.

This makes it easier to hide information from consumers and to prevent the risk of tracking behaviors. Dark Web also has detrimental consequences by encouraging criminals to commit cybercrime and mask their traces. T is perceived to be an effective medium for governments to share classified information, for journalists to circumvent censorship, and for activists to "hide" from repressive regimes. Onion technology1 facilitates secure communication across a network of computers. Messages are sent encrypted (using asymmetric encryption) and distributed to each of the network nodes.[6]

*Online Privacy in the Dark Web:*

Used to allow private, anonymous and secure communications and activities for specific purposes. Within the following, some examples are provided that they relate to the elements listed above:

Anti-censorship and political activities to prevent censorship and to access other destinations or materials that are blocked in one way or another, TOR finds this to be an effective method. It allows people to access information that could be inaccessible in other areas of the world. To avoid this, some governments have developed regulations to use the TOR or to restrict access to the TOR for limited time periods.[6]

Sensitive communications:-. When individuals choose to view confidential information for personal or business reasons in chat rooms or forums, this is allowed by TOR. It is intended to shield children online (i.e. Internet browsing) from violence (i.e. secret IP addresses of their devices). This device can be used by companies to shield their ventures and to fence spies away from them.[6]

TOR may be used by journalists to connect anonymously with whistleblowers and dissidents. Individuals have the ability to connect and exchange confidential information with TOR outlets, e.g. the Strongbox in New York. Edward Snowden used Tail (an encryption operating system) which is running in TOR. Reported and reported to journalists for the release of secret information

Leaked information: - When individuals choose to view confidential information for personal or business reasons in chat rooms or forums, this is allowed by TOR. It is intended to shield children online (i.e. Internet browsing) from violence (i.e. secret IP addresses of their devices). This device can be used by companies to shield their ventures and to fence spies away from them.[6]

*Dark Web in the Government, Military and Intelligence:*

Thanks to the anonymity of Tor and other applications such as I2P, the Dark Web can be a platform for sinister online actors. Nonetheless, as noted, there are a variety of ways in which the research and use of the Dark Web can have benefits. This refers not only to individuals and companies wanting personal anonymity, but also to other government sectors — namely law enforcement, military, etc. Anonymity on the Dark Web can be used to protect enemies from military command and field control systems for detection and hacking. The military can use the Dark Web to research the world in which it operates, as well as to uncover activities that pose an operational risk to the military. For example, evidence shows that the Islamic State (IS) and the associated groups are trying to make use of it. The Department of Defense (DOD) will track these operations in its war against the IS and use a range of strategies to thwart terrorist plots.

TOR tools may be used by the military to perform secret or covert computer network activities, such as a website launch or denial of service attack, or to capture and obstruct enemy communications.[7]

## CONCLUSIONS

Dark Web networks such as TOR have created a wide variety of ways for criminal individuals to trade legitimate and illicit "goods" anonymously. Dark Web is a growing commodity, especially in the field of illegal resources and activities. Protection processes should be proactive in resolving these problems and taking steps to remove them. This paper explores the effect of the Dark Web, the secrecy and confidentiality of the Dark Web, and the findings show anonymous users daily the amount of this Internet section for the Kosovo area as well as the world as a whole, and the effect of secret resources websites on the Dark Web.

**REFERENCES**

[1] R. W. Gehl, “Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network,” *New Media Soc.*, 2016.

[2] H. Chen, W. Chung, J. Qin, E. Reid, M. Sageman, and G. Weimann, “Uncovering the Dark Web: A case study of Jjihad on the Web,” *J. Am. Soc. Inf. Sci. Technol.*, 2008.

[3] G. Hurlburt, “Shining Light on the Dark Web,” *Computer (Long. Beach. Calif).*, 2017.

[4] J. R. Harrison, D. L. Roberts, and J. Hernandez-Castro, “Assessing the extent and nature of wildlife trade on the dark web,” *Conserv. Biol.*, 2016.

[5] K. J. Navara and R. J. Nelson, “The dark side of light at night: Physiological, epidemiological, and ecological consequences,” *Journal of Pineal Research*. 2007.

[6] P. K. Jonason, M. Lyons, H. M. Baughman, and P. A. Vernon, “What a tangled web we weave: The dark triad traits and deception,” *Pers. Individ. Dif.*, 2014.

[7] R. H. Nilsson *et al.*, “The UNITE database for molecular identification of fungi: Handling dark taxa and parallel taxonomic classifications,” *Nucleic Acids Res.*, 2019.