Int. Jrl. of **Human Computations & Intelligence**
Vol. 02, Issue 04, 2023
ISSN: 2583-5696



ORIGINAL RESEARCH

# A Connotation and Measurement of Dark Web in Factual Environment: Analysis and Observations

**C. Gowthami[1] . T Suresh[1] . J Sheik Mohamed[1] . N Ch S N Iyengar [2]**

[1]Sreenivasa Institute of Technology and Management Studies (SITAMS)
Jawaharlal Nehru Technological University (JNTU) Anantapur
Chittoor, Andra Pradesh, India
[2] Department of Computer Science and Engineering
Sreenidhi Institute of Science & Technology, Hyderabad, Telangana, India

Received: 20 April 2023 / Revised: 18 May 2023 / Accepted: 05 June 2023

DOI: 10.5281/zenodo.8026951

**Abstract:** The dark web refers to a part of the internet that is not accessible through traditional search engines or web browsers and can be accessed through special software, such as Tor. The Tor browsers allows users to browse the web anonymously. The dark web is often associated with illegal activities, such as buying and selling of drugs, weapons, and stolen data, as well as the exchange of sensitive or confidential information. It's important to note that not everything on the dark web is illegal, but it is a place where anonymity and privacy are highly valued. It's also important to be cautious when accessing the dark web, as there are many risks associated with it, including the potential for scams, hacking, and other criminal activities. However, it can also be used for legitimate purposes such as anonymous communication, privacy protection, and access to restricted information. However, it is important to note that not all activities on the Dark web are illegal, and some users access it for privacy reasons. The dark web contains a variety of information that may be dangerous to children, since children are curious about the dark web, it has attracted many children who might be at risk. Purpose of dark web is to hide the identity. The dark web can be dangerous if you aren't careful about what you view. Even through the dark web may be used in illegal way but still the dark web can be utilized with positive notion.

***Keywords:*** Dark Web, TOR Browser, Anonymity, Child protection, Legitimate.

## I. INTRODUCTION

The dark web is the hidden collective of internet sites only accessible by a specialized browser. It is used for keeping internet activity anonymous and private, which can be helpful in both legal and illegal applications. The dark web's history can be traced back to the 1990s when the US Navy developed Tor network to protect government communications. The network used a technique called "Onion routing" to encrypt and route internet traffic through a series of servers, making it difficult to

trace the origin of the communication. In 2002, the Tor project was released as open-source software, making it available for public use. The dark web quickly became a popular destination for people seeking anonymity online, including journalists, activists, and whistle-blowers. As a result, law enforcement agencies around the world have been working to crack down on illegal activities on the dark web. Despite efforts to combat illegal activities, the dark web remains a significant part of the internet and is used by millions of people worldwide for legitimate purposes. It gives all users anonymity, and the US government finally gave it to various civil rights to organisations. The Tor network strength comes from the fact that it cannot be shut down from any single location. Even if you turn of the American servers, the rest of the network continues to function.

**Fig.1: Dark web**

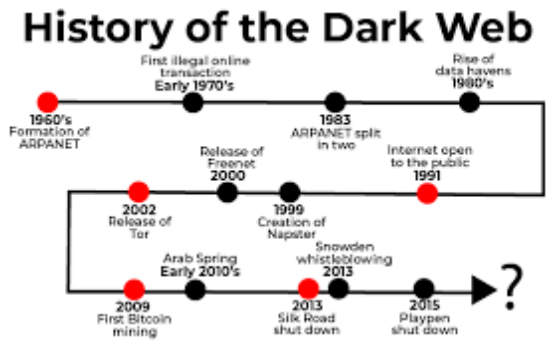


**Fig. 2: History of Dark web**

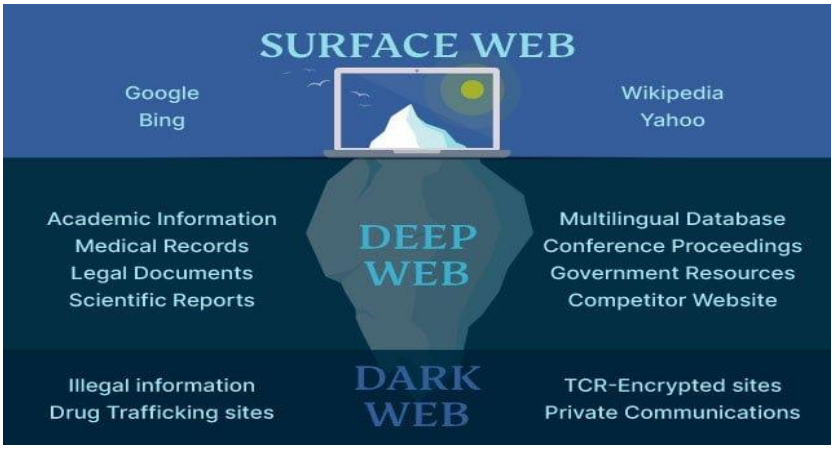

**Fig. 3: Types of webs**

**Surface Web:** This is part of the dark web that is indexed by search engines and can be accessed through standard web browsers like Google Chrome, Safari, and Firefox. When we go to the websites like facebook.com or amazon.com, we are only looking at the surface of it and can only see the information that is visible to the user in front them. We can't see what's going on "behind the scenes".

**Deep Web:** The Deep web allows users to view information that is normally hidden behind the closed doors, it cannot be accessed using standard web browsers. It includes websites and online platforms that are intentionally hidden and require specific software such as Tor browser to access. The deep web is often used for legitimate purposes, such as anonymous communication and protecting privacy. It can be used for private data and pages of companies, universities, libraries, hospitals, governments, international organisations.

**Dark Web:** The dark web is the section of the internet that can be accessed via a special browser called Tor (the onion router) and VPN. It is also known as the darknet or the unregulated internet. It cannot be accessible through standard browsers. Dark web websites do not end in .com or .org, even if Tor is used. Instead, URLs are typically made up of a jumble of letters and digits. They end with the. onion suffix. Dark websites URLs change frequently, making them more difficult to locate than most other platforms on the internet. It is a online marketplaces that operate on the dark web and are often associated with illegal activities, such as the buying and selling of drugs, stolen data, and other illicit goods and services. Darknet markets require specific software, configurations, and payment methods to access and operate, and they are often heavily monitored by law enforcement agencies.

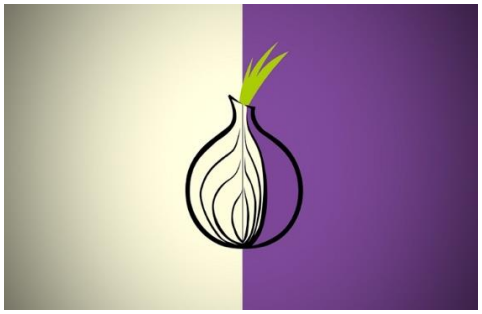

**Fig. 4: Tor Browser**

**Tor Browser:** The Tor Browser is a free and open-source web browser that allows users to browse the internet anonymously and access websites that are not indexed by traditional search engines. The dark web is a small part of the deep web that is not accessible through regular browsers and requires a special software such as Tor to access. It's important to note that while Tor network provides some anonymity, it is not completely secure. Users should still take precautions to protect their privacy and security while using the Tor browser on the dark web, such as avoiding clicking on suspicious links or downloading unknown files. The Tor browser works by routing web traffic through

a series of servers. This makes it difficult for anyone to trace the user's internet activity back to the physical location or identity. The Tor browser also includes security features such as blocking tracking cookies, protecting against browser fingerprinting, and encrypting all data transmitted between the user and the website they are visiting.

**Working of Tor:** Tor (The Onion Router) is a free and open-source software that enables users to browse the internet anonymously and securely. The Tor network consists of volunteer-operated servers, also known as nodes, which are spread around the world. When a user connects to the Tor network, their internet traffic is encrypted and sent through a series of randomly selected nodes, each of which only knows the IP address of the previous and next nodes in the chain. This multi-layered approach to encryption and routing is often compared to the layers of an onion, hence the name "Onion Router." The first node in the chain is called the entry node, and it receives the user's encrypted traffic. It only knows the user's IP address, not their actual location or identity. The entry node then passes the traffic to a randomly selected middle node, which further encrypts the traffic and forwards it to another randomly selected middle node. This process is repeated several times, with the traffic passing through multiple middle nodes, before reaching the exit node. The exit node decrypts the traffic and sends it to the intended recipient, such as a website or other online service.

Because of the multiple layers of encryption and routing, it is extremely difficult for anyone, including governments and internet service providers, to track a user's online activity or identify their real IP address. Tor can be used to bypass censorship, protect user privacy, and access the dark web. However, it's important to note that Tor is not 100% secure, and there are still potential vulnerabilities that can be exploited. For example, if a user logs into an account that contains personally identifying information or uses a website that is not encrypted with HTTPS, their identity could be revealed. Therefore, it is important to use Tor in conjunction with other security measures and exercise caution when browsing the internet.

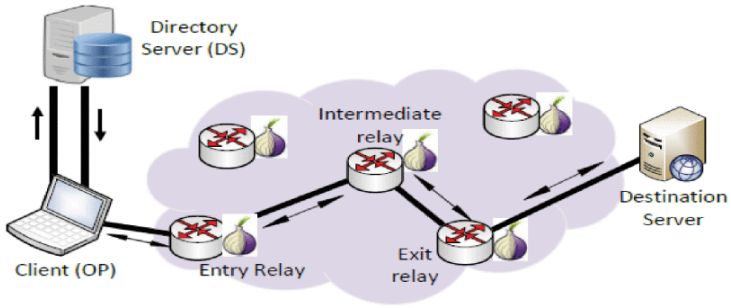


**Fig. 5: Working of Tor**

## II. WORKING OF DARK WEB

Internet The dark web operates using a variety of anonymous networks, such as Tor (The Onion Router), I2P (Invisible Internet Project), and Freenet. These networks use encryption and layered routing to provide anonymity to users and keep their activities hidden from prying eyes. When a user

connects to the dark web using a special software, the software encrypts their internet traffic and sends it through a series of nodes or relays, which are operated by volunteers around the world. These nodes are responsible for decrypting and forwarding the user's traffic to the next node in the network, until it reaches its final destination.

Because each node in the network only knows the previous and next node in the chain, and not the full path of the user's traffic, it is very difficult for anyone to trace the user's activities back to their real-world identity. On the dark web, users can access websites and services that are not available on the regular internet, such as anonymous marketplaces for buying and selling illegal goods and services, forums for discussion of sensitive topics, and encrypted communication channels for messaging and file sharing.

While the dark web can be used for legitimate purposes, it is also a haven for illegal activities such as drug trafficking, weapons sales, and human trafficking. Law enforcement agencies around the world are constantly working to track down and shut down these illicit activities on the dark web. The 'Dark Web' use complex systems that anonymise a user's true IP address, making it very difficult to work out which websites a device has visited. It is generally accessed using dedicated software, the best known is called Tor (The Onion Router). Around 2.5 million people use Tor every day.

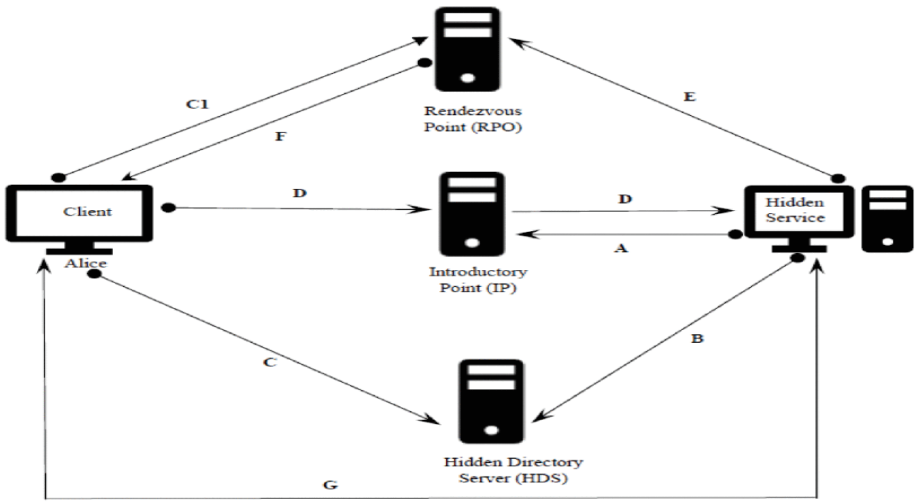


**Fig. 6: Working of Dark web**

**Legal Uses of the Dark Web**

While using the dark web may seem suspect on the surface, it is perfectly legal, and there are many legitimate uses of Tor and anonymous browsing. For example, in countries where government surveillance may be used to spy on and oppress political dissidents, the dark web is often a place for communication that avoids government censorship and scrutiny. Despite these added layers of security, users should still be cautious using the dark web and take proper security measures, such as periodically updating their security software, browsing with a robust VPN, and avoiding the use of a standard email address.

There are also some legal uses. Here are a few examples:

- **Whistleblowing:** The Dark Web can provide a more secure platform for individuals who wish to share sensitive or confidential information with the public or media without fear of retaliation.
- **Privacy:** The Dark Web can provide a level of privacy for individuals who wish to browse the internet without being tracked or monitored by their ISP or government agencies.
- **Research:** Some academic researchers use the Dark Web to study online communities, behaviour, and trends that are not accessible through normal internet channels.
- **Journalists:** The Dark Web can provide a more secure platform for journalists to communicate with sources and to research sensitive topics.

It is important to note, however, that while these uses are legal, the Dark Web is still a highly unregulated and potentially dangerous environment. Users should always take necessary precautions to protect themselves and their personal information.

**Illegal Uses of the Dark Web**

Given its anonymous nature, the dark web is also used for illicit and even illegal purposes. These include the buying and selling of illegal drugs, weapons, passwords, and stolen identities, as well as the trading of illegal pornography and other potentially harmful materials. Several sites hosting illegal material have been discovered by government agencies and shut down in recent years, including Silk Road, Alpha Bay, and Hansa. The dark web's anonymity has also led to cybersecurity threats and various data breaches over the last few decades

There are many illegal activities that take place on the Dark Web, due to the anonymity it provides and the difficulty of tracing illegal activities. Here are some examples of illegal activities that occur on the Dark Web:

- **Illegal drug trade:** The Dark Web is notorious for its drug markets, where people can buy and sell illegal drugs anonymously.
- **Weapons trade:** The Dark Web is also home to marketplaces where people can buy and sell illegal weapons, including firearms, explosives, and other dangerous materials.
- **Hacking services:** The Dark Web is a hub for hackers who offer their services to anyone willing to pay, including hacking into email accounts, websites, and even bank accounts.
- **Child pornography:** The Dark Web is home to illegal marketplaces and forums where people can share and trade child pornography.
- **Fraud and scams:** The Dark Web is also known for its marketplaces where people can buy and sell stolen personal information, such as credit card numbers and login credentials.

It is important to note that these activities are illegal and can lead to serious consequences if caught by law enforcement. It is strongly advised to avoid any involvement in illegal activities and to take necessary precautions to protect personal information while browsing the Dark Web.

**Legitimate uses in Dark Web**

While the Dark Web is often associated with illegal activities, there are also legitimate uses for this part of the internet that are important to note. Here are some examples of legitimate uses for the Dark Web:

- Circumvent Government Censorship
- Anonymous Email Services
- Visit news outlets
- Anonymous collaboration with journalists
- Contact CIA Anonymously
- Access to Academic Research
- Use Ad-Free Search Engines
- Secure Your Cryptocurrency Wallets
- Access social media
- Listen to online radio
- Find niche content
- Participate in forums and chat boards

**Types of threats in Dark Web**

The Dark Web is a highly unregulated and anonymous environment, making it a breeding ground for various types of threats. Here are some examples of threats that exist on the Dark Web:

- **Cyber-attacks:** The Dark Web is a hub for hackers who offer their services to anyone willing to pay. These hackers can launch cyber-attacks on individuals, organizations, and even governments, causing damage and stealing sensitive information.
- **Malware:** The Dark Web is also a place where people can buy and sell malware, which can infect computers and steal personal information, such as login credentials and financial information.
- **Fraud and scams:** The Dark Web are known for its marketplaces where people can buy and sell stolen personal information, such as credit card numbers and login credentials. These marketplaces can also be used to conduct fraud and scams, such as fake product listings or investment opportunities.
- **Illicit drug trade:** The Dark Web is infamous for its drug marketplaces, which can be a threat to public health and safety.

- **Child exploitation:** The Dark Web is home to illegal marketplaces and forums where people can share and trade child pornography, which is a serious threat to the safety and well-being of children.
- **Illegal weapons trade:** The Dark Web is also home to marketplaces where people can buy and sell illegal weapons, including firearms, explosives, and other dangerous materials, posing a threat to public safety.

It is important to note that the Dark Web is a highly unregulated and potentially dangerous environment, and users should take necessary precautions to protect themselves and their personal information.

**How to access the dark web safely**

Accessing the Dark Web safely requires taking several precautions to protect your personal information and privacy. Here are some steps you can take to access the Dark Web safely:

- **Use a reliable VPN:** A virtual private network (VPN) can help protect your online privacy and keep your internet traffic encrypted, making it more difficult for others to monitor your online activity. Make sure to choose a reputable VPN provider with a no-logging policy.
- **Use Tor browser:** Tor is a free and open-source software that allows users to access the Dark Web anonymously. It encrypts your internet traffic and bounces it through a network of relays, making it difficult for anyone to track your online activity. Make sure to download Tor from the official website.
- **Use a trusted search engine:** While the Dark Web is not indexed by mainstream search engines, there are several Dark Web search engines available. Make sure to use a trusted search engine, such as Torch or DuckDuckGo.
- **Do not share personal information:** Avoid sharing any personal information, such as your real name or address, on the Dark Web. Use a pseudonym instead.
- **Be cautious of links and downloads:** The Dark Web is a high-risk environment, and there are many malicious links and downloads that can infect your computer with malware or steal your personal information. Avoid clicking on links or downloading files from untrusted sources.
- **Use caution when interacting with others:** Be cautious when interacting with others on the Dark Web, as it can be difficult to determine who you are communicating with. Avoid sharing sensitive information and be wary of anyone who asks for personal information or money.

It is important to note that accessing the Dark Web can still be risky, even with these precautions. Users should use their best judgment and take necessary precautions to protect themselves and their personal information.

**The safeguard your child from the dangers of the Dark Web:**

- Using a virtual private network to add an additional layer of security to your child's online activities is a good idea (VPN).
- Please notify the CEOP if your child comes across something disturbing or concerning. Make them aware that those who use the dark Web to remain private may have complex motives for doing so, which may endanger them

**Protecting the children from the dark web:**

Protecting children from the dark web is a serious concern for parents and caregivers. Here are some steps you can take to help keep children safe:

- Encourage them in physical exercise
- Take children on a trip
- Monitor child's internet usage
- Use parental control app
- Have a conversation with your child
- Spend time with your children
- Reduce your internet use
- Motivate them to participate in extra activities
- Keep all electronic and gadgets in common spaces
- Limit technology access
- **Educate children about online safety:** Teach children about the potential dangers of the internet and the importance of protecting personal information. Make sure they understand the risks associated with visiting unknown websites, engaging with strangers online, and sharing personal information.

- **Use parental controls:** Many internet service providers offer parental controls that can block access to certain websites, limit the amount of time children spend online, and monitor their online activity. You can also use software such as Net Nanny, Qustodio, or Kaspersky Safe Kids to monitor and limit access to certain websites.
- **Monitor their online activity:** Keep an eye on your child's online activity by monitoring their browsing history, social media accounts, and online interactions. You can also use software to track their activity and receive alerts when they visit certain websites or engage in certain behaviours.
- **Set ground rules:** Establish rules for internet use, such as not sharing personal information, not engaging with strangers online, and not visiting unknown websites. Make sure children understand the consequences of breaking these rules.
- **Keep communication open:** Encourage your children to talk to you about their online activity and any concerns they may have. Let them know they can come to you if they see something that makes them uncomfortable or if they have questions about something they have seen online.

- **Limit access to devices:** Consider limiting the amount of time children spend online by setting time limits or restricting access to devices. You can also restrict access to certain apps or websites on devices to ensure they are not accessing the dark web.

It's important to remember that no system is fool proof, and there is no guarantee that your child will never stumble across something they shouldn't see online. However, by taking these steps, you can help reduce the risks and keep your child safe.

**Advantages of Dark web:**

There are some potential advantages to using the dark web for legitimate purposes, such as:

- **Anonymous communication**: The dark web can provide a level of anonymity that is not possible on the regular internet. This can be useful for journalists, activists, and others who need to communicate sensitive information without fear of reprisal.
- **Access to information**: The dark web contains a wealth of information that is not available on the regular internet. This can include academic papers, research, and other resources that may be difficult to find elsewhere.
- **Protection from surveillance**: The dark web can protect users from government surveillance and other forms of monitoring. This can be important for individuals living in countries with repressive regimes or for those who are concerned about privacy and security.
- **Access to marketplaces**: While there are certainly illegal marketplaces on the dark web, there are also legitimate marketplaces where users can buy and sell goods and services anonymously. This can be useful for people who live in countries with restrictive trade policies or for those who want to buy or sell items without revealing their identity.
- It is important to keep in mind that the potential advantages of the dark web are outweighed by the potential risks and dangers. It is not a place for casual browsing or exploration and should be approached with caution and a thorough understanding of the risks involved.

**Disadvantages in dark web:**

The dark web is often associated with illegal activities and can be a dangerous place. Here are some of the disadvantages of using the dark web:

- **Illegal activities:** The dark web is notorious for illegal activities such as drug trafficking, weapons sales, and human trafficking. Engaging in these activities can put users at risk of arrest, violence, and other dangers.
- **Cybersecurity risks:** The dark web is not subject to the same cybersecurity standards as the regular internet, which can make it vulnerable to hacking and other cyberattacks. Users may be at risk of having their personal and financial information stolen.

- **Scams and fraud**: There are many scams and fraudulent activities on the dark web, such as fake marketplaces, phishing scams, and pyramid schemes. Users can lose their money and personal information to these scams.
- **Exposure to disturbing content**: The dark web contains a lot of disturbing and illegal content such as child pornography, violent videos, and extremist materials. Exposure to this content can be traumatic and harmful.
- **Lack of regulation**: The dark web is not regulated in the same way as the regular internet, which can make it difficult for users to seek recourse if they are scammed or harmed in any way.
- It is important to keep in mind that the risks and dangers of the dark web far outweigh the potential advantages. Users should approach the dark web with caution and a thorough understanding of the risks involved.

## III. Conclusion:

In today digital's age, protecting children from the dark web is critical. Since children cannot differentiate between good and evil, parents have to direct and protect their children. It is vital to protect your child from dangers of dark web. You can also monitor and track your children's online behaviour using various parental control software available on the market. The dark web is a hidden part of the internet that can be associated with illegal activities. While there may be legitimate uses for it, users should exercise caution and take precautions when accessing it to protect their online privacy and personal information. This includes using a VPN, a secure browser, enabling two-factor authentication, avoiding revealing personal information, avoiding illegal activities, and staying informed about potential threats and changes. It is important to understand the risks involved and to take appropriate measures to protect yourself if you choose to access the dark web. Overall, you must understand that the dark web is not a place where your child can wake up one day and declare, "I'm going there". So as a parent you must be aware of the dark web. I've listed a few guidelines for parents to protect their children from the dark web, and if you are concerned about your children, you can use the rules listed above.

## References:

1. Biryukov, A., Pustogarov, I., & Weinmann, R. P. (2014). Content and popularity analysis of Tor hidden services. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.
2. Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the Dark Web: A case study of Jihad on the Web. Journal of the American Society for Information Science and Technology. https://doi.org/10.1002/asi.20838
3. Chakravarty, S., Ktait, A., & Dube, A. (2019). A comparative study of darknet markets. Journal of Money Laundering Control, 22(1), 68-81.
4. Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. New Media and Society. https://doi.org/10.1177/1461444814554900
5. Harrison, J. R., Roberts, D. L., & Hernandez-Castro, J. (2016). Assessing the extent and nature of wildlife trade on the dark web. Conservation Biology. Https://doi.org/10.1111/cobi.12707

6. Hurlburt, G. (2017). Shining Light on the Dark Web. Computer. https://doi.org/10.1109/MC.2017.110 [5] Jonason, P. K., Lyons, M., Baughman, H. M., & Vernon, P. A. (2014). What a tangled web we weave: The dark triad traits and deception. Personality and Individual Differences. https://doi.org/10.1016/j.paid.2014.06.038
7. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.
8. McCoy, D., Pitsillidis, A., Vern Paxson, S., Weaver, N., & Kreibich, C. (2012). Measuring the utility of security signals with respect to internet routing events. Proceedings of the ACM SIGCOMM Internet Measurement Conference.
9. Martin, J., & Malik, M. (2019). Cryptocurrency-enabled crime: An analysis of cryptocurrency-related cybercrime and money laundering. Journal of Financial Crime, 26(2), 282-299.
10. Navara, K. J., & Nelson, R. J. (2007). The dark side of light at night: Physiological, epidemiological, and ecological consequences. In Journal of Pineal Research. https://doi.org/10.1111/j.1600- 079X.2007.00473.X
11. Ahmed, S. T., Kumar, V. V., Singh, K. K., Singh, A., Muthukumaran, V., & Gupta, D. (2022). 6G enabled federated learning for secure IoMT resource recommendation and propagation analysis. Computers and Electrical Engineering, 102, 108210.
12. Ahmed, S. T., & Basha, S. M. (2022). Information and Communication Theory-Source Coding Techniques-Part II. MileStone Research Publications.
13. Raja, D. K., Kumar, G. H., Basha, S. M., & Ahmed, S. T. (2022). Recommendations based on integrated matrix time decomposition and clustering optimization. International Journal of Performability Engineering, 18(4), 298.