Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

# A Survey on Tor's Multi Layer Architecture and Web Implications in Dark Web

**Noman Aqeel**[1]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
nomanaqeel773@gmail.com

**Absar Alam**[2]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
absaralam5122002@gmail.com

**Zahir Bhatti**[3]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
zaheerbhatti514@gmail.com

**Ammar Amir**[4]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
haisamamir015@gmail.com

**Hamayun Khan**[5]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

**Bilal Hassan**[6]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
bilal.hassan@superior.edu.pk

## Abstract

The Tor network is a fundamental element of the dark web that provides users with secure and shadowy access to data and communication. Originally tor was developed for privacy and protection purposes but later it turned into a platform where both legal and illegal activities are done. The study looks into the architectural components of Tor, onion routing, encryption layer, and node structure that facilitate obscurity. Moreover, it explores both the positive and negative sides of the network, examining how its architecture works and supports illegal activities. Law enforcement investigates the activities, highlighting the challenges in balancing the benefits of the network against the need to tackle security risks. By reviewing recent research, technical advancement, and structural study, this paper presents a deep understanding of the Tor network in enhancing privacy, security, and unidentified communication. Also highlighting the related risks, challenges, and ethical considerations

**Keywords:** Tor network, Dark web, onion routing, privacy protection, law enforcement, ethical considerations

## Introduction

The Tor network stands for The Onion router, this network is Resilient identity-concealing that is built for online privacy and security. Firstly it is developed by the U.S Naval Research Laboratory in the 1990's for securing military communication and activities. With time, or becomes an open-source network. It allows users to use the internet without revealing their identities and locations [1, 3]. This feature makes the tor an essential browser for business holders to secure privacy. The access to Tor Onion services consists of multiple phases. The initial step revolves around finding onion addresses, which is challenging due to their complex and unidentified nature once the onion address is acquired, the next step is to establish a tor circuit with onion services at the node within the tor network. However, these onion services may experience internet interruption due to which the last node hosting the onion routing fails [4, 7]. Once the network is established to a specific node user gets access to several services. These services include web services like HTTP and HTTPS, email servers, and instant messaging application features with unidentified networks, as well as SSH servers that give secure and private networks for communication. The network considers nodes related to crypto currency activities [8, 11].

Understanding how onion services work on the Tor network and where the criminals find these onion addresses enables us to monitor their illegal activities. Without proper knowledge of the Tor browser, it is dangerous and somehow difficult to access onion services. There are a lot of hackers available to look at who's connection is weak so they can hack their secure network. With time, tor routing become a backbone of the dark web for illegal activities because of its anonymity [12, 15]. This paper, a detailed discussion of Tor's architecture, multilayered encryption and various nodes within the network, societal implications and challenges, black-market transactions, difficulty of policing illegal activities on the dark web while respecting legal activities [16].

## Overview of the Dark Web and Tor's Role

### Understanding the Dark Web

The Internet is divided into 3 main layers: the surface web, the deep web, and the dark web. Surface consists of only 4% of the whole internet that we normally use in our daily life, including websites, and search engines like Google and Bing. The deep web consists of only 90% of the whole internet and includes content that is not accessible by search engines including private databases, military networks, academic journals, etc. The dark web consists of only 6% of the whole internet that is no longer secret from the world, it contains data that need some special permissions to access them [17, 21].

The dark web is a subset of the deep web that is hidden and can be accessed through specific unidentified networks like Tor (the onion routing) [22]. The dark web is specially designed for complete undetectable identity. The dark web uses complex encrypted protocols and doesn't use standard URLs, it uses ".onion" addresses that build only developed for Tor.

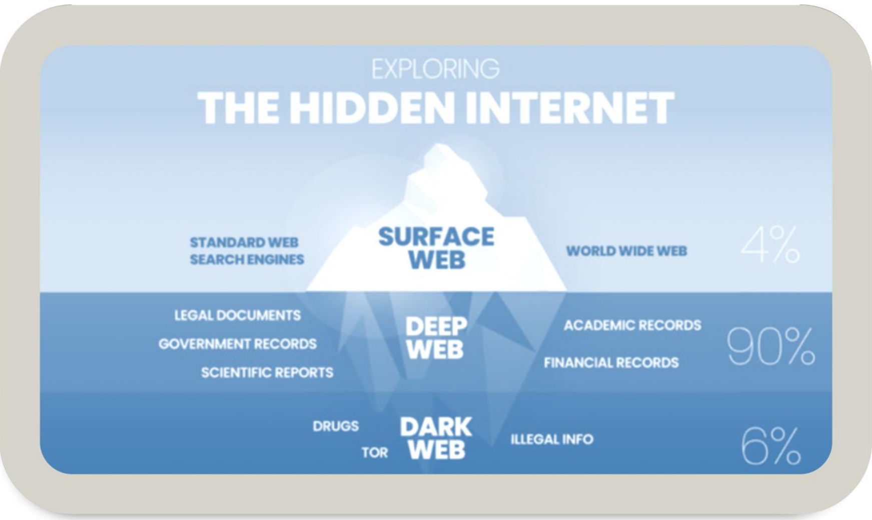


**Figure 1.** Overview of the Internet Layers [22]

This special encryption makes it difficult for outsiders to crack the network. Daily, a wide range of activities is done on the dark web, including legal forums and resources for prohibited marketplaces where illegal services and goods like drugs, murders, etc are exchanged. All of these markets use the browser to hide their identity and can openly do dealing and illegal transactions while the surface web is open, clean transparent for everyone, and easily trackable. It depends on us for what purpose we use the dark web: for privacy protection or illegal activities [23, 25].

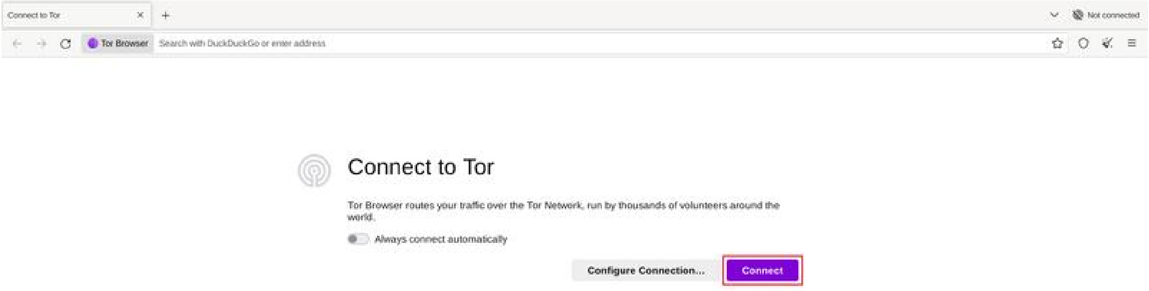
**The Purpose and Evolution of Tor**

The basic purpose for developing the Tor network is for secure and private communication for government and military use. In the early 2000's tor was launched as an independent platform, due to its privacy protection feature tor gained popularity [26]. Tor's significance has increased in the past twenty years. Tor users are increasing day by day who depend on the untrackable identity of the users. Tor has focused on increasing its network security also updating their functionality to meet the exact requirements of those people who need anonymity. Later tor became a criminal base hub to operate their illegal activities on the dark web and no one can track them [27].

**Architecture of the Tor Network**

Decentralization relies on millions of volunteer-run servers, called nodes and they act as a bridge, helping to maintain an unidentifiable and secure connection [28]. Tor is designed with considering these keys

- **Deployability:** it should be easy to implement for real-world use.
- **Simple Design:** security and protocol settings should be simple and user-friendly
- **Usability:** difficult system features like anonymity, likely few users who compromise their identity. Thus usability is important for maintaining security.
- **Flexibility:** The protocol must be adaptable and well-defined.



Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

Always connect automatically

Figure 2. Architecture of the Tor Network [29]

### Onion Routing and Multi-Layered Encryption

The basic technology used for Tor's anonymity is onion routing. This method includes encapsulating data in many layers of encryption, each presenting a layer of an onion. When data or information is passed through the Tor network, the passes through a series of volunteer-operated nodes, called onion routers. Every node decrypts only one layer of encryption, revealing its next location in the path, and ensuring that user identity and that specific data are hidden [30].

Onion routing is one of the best methods for protecting anonymity because it divides data into many stages, on every stage data is encrypted and decrypted sequentially as it passes through the network. This approach prevents everybody from accessing any information from the data passage. This way onion routing protects users' data and identity. According to the Tor project research, this layered method can prevent any surveillance and interception but some loopholes exist like at end nodes from where data exits and re-enters the open internet. Every node in the network knows its predecessor and successor. Network security is enhanced by limiting the number of data packets available on any single node [31, 35].

### Node Structure and Roles

The Tor network is made up of main three types of nodes, each node type has its specific role play in maintaining the anonymity of the network [36].

**Entry Nodes**: The entry node is also known as the guard node, the first node connects the user's device to the Tor network. This node has the user's IP address but doesn't know the final location of the data. Every node works as a first node and encrypts at every node. This is the first layer of anonymity for users.

**Relay Nodes:** Once the data is passed through the entry node, it enters into the relay node, which acts as an intermediate point in the Tor network. It doesn't have the first and the last node information of the data, they only know the information of the preceding and next nodes in the node chain of the network. Relay nodes increase user privacy or anonymity by re-encrypting the data sent to the next node and the network is decentralized and difficult to trace [37].

**Exit Nodes:** The exit node is the last in the node chain network and it is responsible for passing the data from the network to its final location on the open internet. Exit nodes have data in unencrypted form but it isn't the first node or main source of the data. Still, it maintains the anonymity of the user. This point is the weakest part of the tor network.

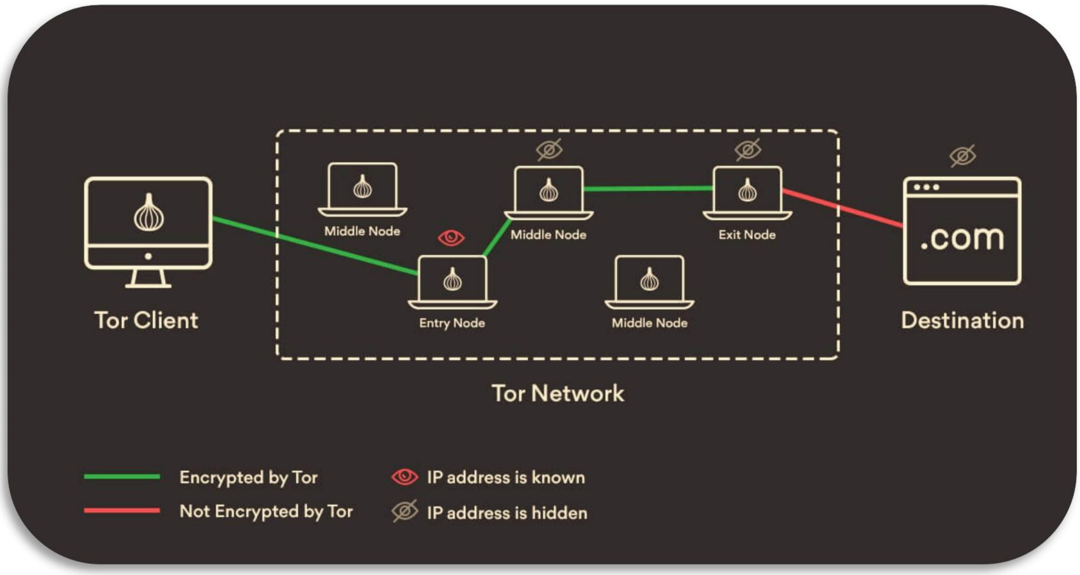


**Figure 3.** Onion Routing Process [38]

**Traffic Flow, Latency, and Bandwidth Challenges**

A Tor network is a multi-layered encrypted network due to which data needs to pass through many nodes to reach its final destination, this architecture results in latency and bandwidth limitations. At every node, data is re-encrypted which naturally slows down the data transfer time. According to studies average latency on a tor network is higher than a normal web browsing, due to this some users use surface web for regular internet activities [39].

Bandwidth limitation is also a big challenge for onion routing networks. Nodes are operated by volunteers, and the overall capacity of the network may be constrained by the bandwidth of these volunteer-operated nodes. This may slow down the connection during high traffic. To handle these problems the project has launched many performance-enhancing techniques which include load balancing and minimum path selection. These measures have reduced the latency and bandwidth issues [40].

### Content and Activities on the Dark Web via Tor

### Legitimate Uses of Tor

The Tor network supports privacy, security, and freedom of expression. Especially, in those regions where restrictions are applied by their governance and 24-hour surveillance. Here, surveillance means "keeping an eye on someone" and censorship means "controlling what people can see or say". Its core mission is to give people a secure way to connect and communicate [41].

**Activism and Free Speech:** when governments stop us from free speech. Then people use Tor to share information safely and will share protests organize and also coordinate with each other. Tor provides a secure environment for people who identify with injustice

**Journalism and Whistleblowing:** For Journalism and Whistleblowing Tor is an important tool that is very helpful to share securely communicate and sensitive information. Journalism especially, research on corruption and sensitive topics. It protects their identity and saves receive their sensitive data. Whistleblowing platforms like SecureDrop facilitate document sharing and are hosted on the Tor Network to protect user identities [42].

**Censorship Resistance:** When censorship internet spreads anywhere at that time Tor can work as a gateway. Most of the users can use websites, and social media platforms and reach new sources to access blocked websites by using Tor.

Studies show that Tor internet usage increased during political and users seek wrong and unfiltered information. In the end, Tor censorship promotes freedom of information by resisting censorship [43]. Users utilize Tor Internet societal value to promote open access to information and protect individual from surveillances. Especially, in those environments where fundamental freedom is very less.

### Illicit Activities Enabled by Tor

Tor is a valuable tool for privacy and freedom. However, some individuals and groups use it for illegal activities. Dark-Web which is accessible through Tor,

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

built a marketplace of illegal goods and services. A secure to transfer the transactions without revealing their identities [44].

**Dark Web Marketplaces:** the dark web marketplace is very popular and famous for illegal things like drugs, guns, etc. These places can work freely. Systems that make it very hard for police to track them. Many or most of the markets have been shut down but new dealers come on tor for illegal activities.

**Cybercrime and Hacking Services:** The dark web has sites where buying and selling tools are available for crime. It is a huge cybercrime economy market, where stolen credit cards, personal data, hacking tracks, etc are sold [45].

**Human Trafficking and Illegal Services:** The dark web also hosts illegal services like human trafficking.  While most of the websites are scams, provide other services. Law enforcement has taken strong action against these criminal activities, but the tracking method remains a challenge to breaking down Tor's network..

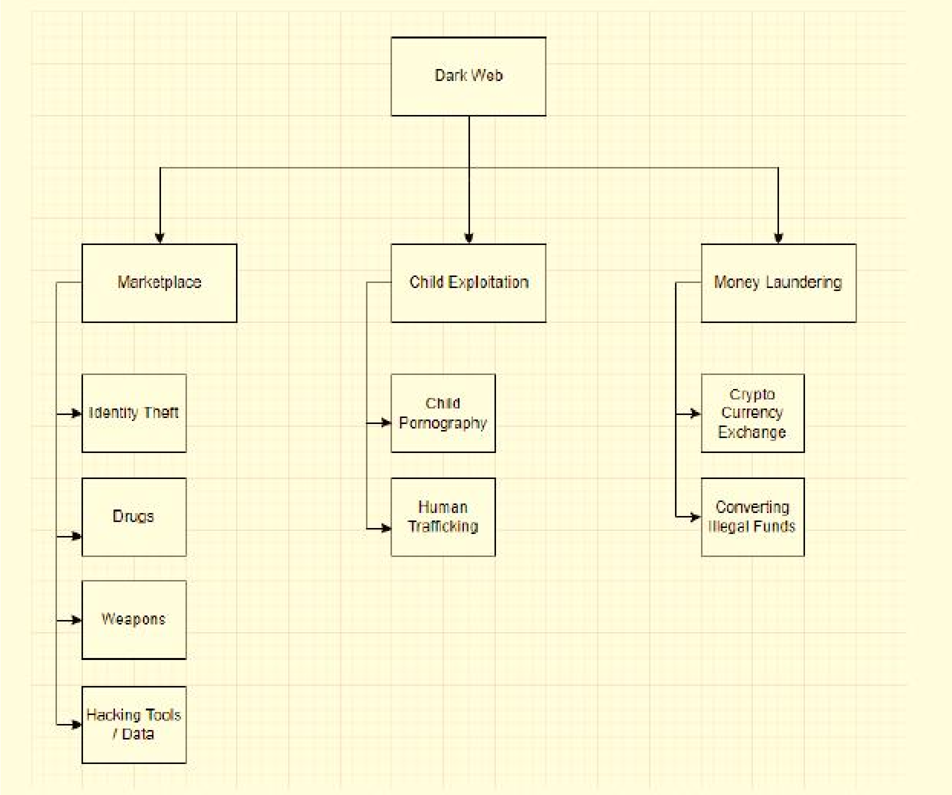


**Figure 4.** User Demographics on the Tor Network [46]

**Crypto-currency and Anonymous Financial Transactions**

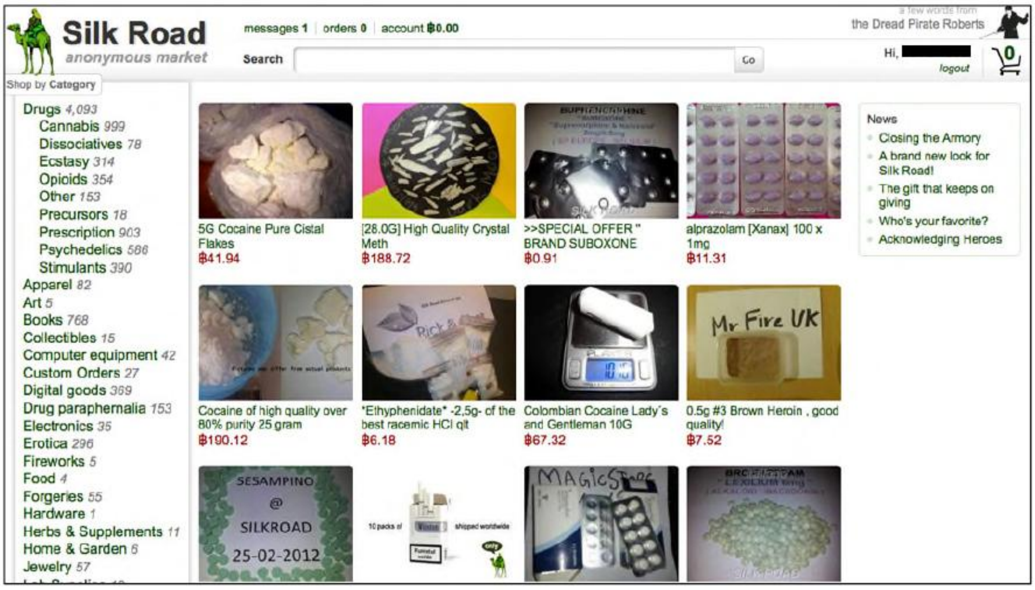
Cryptocurrencies like Bitcoins [47] are also very widely used on the dark web. These digital currencies are nontrackable that's why criminals use them for their illegal business transitions.

**Legitimate Financial Transactions:** Some people use crypto-currencies on the dark web for good reasons too. They help online journalists, protect privacy, and donate to some free speech causes. These transactions are private and secure on the Tor network.

**Facilitating Illicit Transactions:** The main and wide use of crypto-currency on the dark web is for illegal activities. Bit-cons are the most widely used but Monero is used to buy drugs, weapons, and stolen and personal data information.

The crypto-currencies and Tor have made transactions easier, helping both illegal and legal markets.

One of the famous markets place for drugs: Silk Road



5G Cocaine Pure Cistal Flakes
฿41.94

[28.0G] High Quality Crystal Meth
฿188.72

>>SPECIAL OFFER " BRAND SUBOXONE
฿0.91

alprazolam [Xanax] 100 x 1mg
฿11.31

Cocaine of high quality over 80% purity 25 gram
฿190.12

'Ethyphenidate' -2,5g- of the best racemic HCl qlt
฿6.18

Colombian Cocaine Lady's and Gentleman 10G
฿67.32

0.5g #3 Brown Heroin , good quality!
฿7.52

News
- Closing the Armory
- A brand new look for Silk Road!
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes

**Figure 5.** Legitimate uses of TOR [48]

**Privacy and Security Implications of Tor**

**Benefits of Privacy and Anonymity**

Tor privacy features are vital in today's digital era, where online tracking is effortless and common. Tor also provides important and informative benefits for society:

**Freedom of Expression and Privacy Protection**: Tor protects freedom of privacy especially, in those countries where surveillance is rigorous. It allows people to raise their voices for their rights without fear of arrest. Freedom of speech is everyone's right. Tor provides a safe way of communicating with each other and getting information without revealing your identity.

**Protection Against Tracking and Surveillance:** Tor protects your online tracking and finding by governments. On the other hand, Websites and the Internet collect your personal data for targeted ads and some hackers hack your data for blackmailing purposes. Tor network hides your personal information and IP address.

**Empowering Vulnerable Populations:** Tor protects vulnerable groups, such as activities and personal communication with each other, by providing a safe online space. Tor helps you access information, and communication without any fear of hacking and protected from surveillance [49].

**Security Challenges and Vulnerabilities**

The network has vulnerabilities that can compromise user's privacy. So regular updates and caution are very crucial for users.

**Exit Node Risks:** Tor exit nodes can monitor the data that passes through the devices and capture unencrypted data like login and passwords.[2] Exit nodes are the last and important steps before data leaves Tor's network. Tor recommends to use HTTPs to prevent yourself from this risk. [21]

**Traffic Analysis Attacks:** This method involves analysis of data flow patterns to reduce information about the origin, destination, and actual content of that information. Research has shown that advanced traffic analysis can reveal Tor users under specific conditions. These types of attacks are done by professional hackers who have access to my nodes in the network.

**Vulnerabilities in User Behavior:** By using Tor you do not completely hide. If you log into personal accounts or share personal information, you can easily track and show your own identity. To stay safe ensure all these vulnerabilities when you are on Tor and must follow guidelines.

**Law Enforcement Approaches and Countermeasures**

**Detection and Monitoring Techniques**

Law enforcement applies many methods to detect and monitor users to see their identity but is very difficult to track anonymous identities and to shut down their illegal activities from the dark web [16].

- **Traffic analysis:** it involves related data that is entering and exiting the

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

tor network, trying to identify their source.

- **Deep packet inspection:** DPI is a technique that identifies patterns between the exit node and the source in the tor traffic but cannot decrypt the data. It may block access to tor with strict internet controls.
- **Honeypots:** these are nodes that are operated by law enforcement, usually an exit node, to monitor the unencrypted data of criminals.
- **Exploring vulnerabilities:** deploying malware or operational weaknesses in tor services like exit nodes

## Ethical Considerations and the Future of Tor

### Privacy vs. Security: Ethical Dilemmas

The Tor Network demonstrates the complicated balance between public security and the human right to privacy. On one side Tor serves as an important for the journalists and activists to express their thoughts freely and safely by hiding their identity and by being anonymous. On the other side, there is a vital role of Tor features in promoting and facilitating criminal acts and creating hindrances for the government and cybercrime to track the person and handle these kinds of activities. So, because of these concerns, there is a question mark regarding privacy rights and security.

### Privacy as a Fundamental Right

The basic and most fundamental right of human is to control and manage their personal information and communication [8][9]. Especially in this society that is always under the supervision and data collection. The Tor network proclaims this right by providing a platform that protects every user from incursive tracking either from the government or from corporations, especially in nations where there is no independence of speech. For many, Tor is requisite for freedom of speech that would be restricted otherwise. Security, protection, and privacy rights provided by the Tor are vital for sustaining democratic independence, individuals' autonomy, and human rights.

### Security and the Social Responsibility to Prevent Harm

There are lots of challenges for law enforcement agencies to monitor all the illegal activities occurring on the dark web including drug dealings, and human smuggling that take place via networks like Tor. If it is untreated and consistently neglected then it will lead to widespread harm to the public safety. Supporters of supervision assert that access to these anonymous networks led citizens to criminal activities. In this view, limiting the complete anonymity on platforms like Tor is necessary to track, investigate, and ultimately demoralize illegal activities to maintain order and social security.

### Ethical Dilemmas of Surveillance

While considering the supervision there is an ethical difference between privacy and security. Advocates of privacy contend that surveillance not only invades individual rights but can also create an environment of fear and self-censorship. In this view, people will remain within their limit of expression and behaviour online because they know they are being monitored even if they are involved in any kind of illegal activity or not. This creates a threatening and alarming effect that weakens free speech and the social fabric of democratic societies will be damaged. So, there is a challenge lies in achieving a balance where privacy rights will be respected without compromising security.

### Technological Limitations and Abuse Potential

Ethical concerns rise as the Tor browser tries to regulate through surveillance technologies or "backdoors". Any step or measure that weakens Tor's encryption leads to risk to the security of all users, including the ones using it for authentic purposes i.e. law enforcement agencies, and higher officials of the defense system of any nation or country. There is also a risk of its usage in such a way that these surveillance technologies may be misused by the government's authoritarian or any private entity that will cause harm to the population. Law enforcement wants more ways to track threats and privacy supporters want strong protections to avoid misuse of the Tor browser.

Ultimately, to balance safety and privacy for the protection of people and keep everyone safe both sides need to work together because both privacy and security are vital for a functional democratic society.

### The Future of Tor and Anonymous Networks

The role of the Tor network is expected to grow as surveillance technologies and online tracking continue to advance. Tor's future will depend on new privacy technologies that are evolving day by day by changing in the social opinions and how people view the balance between the privacy and security.

### Emerging Privacy Technologies

These are the following features and technologies that will play a vital role in the advancement of the Tor browser: Advancement in the encryption method and the technologies that are used for the protection by enabling Tor to offer technologies that provide even stronger protections.

For example: There are both challenges and opportunities for Quantum computation, otherwise, it has the potential to create challenges by breaking the current encryption method. It also led to the development of new stronger architecture having stronger encryption that protects against these risks. The newly emerging protocols like "zero-knowledge" prove that they will allow for verification without figuring out user information, thereby strengthening privacy on Tor and other anonymous networks. These technologies play a vital role in pushing Tor to evolve in such order by keeping the advancements in digital security and more specifically comparison to the alternatives like i2p.

### Increased Surveillance and Regulation

As cybercrime becomes more advanced and evolves day by day so there is a need for the government must take strict action the regulate unidentified networks that are working online and involved in many criminal activities. It would be the better step to make internet safer by implementing restrictions on the Tor browser and many other service providers that report many suspicious activities.

In developed and developing countries where security is the primary concern, they already increasing their oversight of online traffic. If there were proper regulations for Tor then there would be a great impact on the networks structure and architecture and the ability to maintain it anonymity.

### Wider Adoption and Decentralization

With time, the awareness and importance of data privacy have increased, as there are many tools in the market to protect their information. With the trend towards anonymity, people started accepting these networks and also used by the public. Technologies like blockchain and distributed networks play important roles in updating the Tor network. More people adopt these privacy-protected networks and more digital freedom. However, this user anonymity may create new problems for governance.

### The Role of AI and Machine Learning

Integration of artificial intelligence and machine learning technologies is expected a significant impact on the improvement of the Tor network. It may help the Tor network to reduce its limitations and remove its loopholes [10]. On the other hand, these technologies will also be used by governance to monitor the network, which means it introduces a new privacy threat for users.

This problem is mainly focused on the future development or updating of the Tor network.

**Conclusion**

In the world where many are watching the Tor network plays an important role in keeping our online activities private and protecting our communication from tracking. In this paper, the complete architecture of the Tor Network has been examined especially the principles of onion routing and multiple-layer encryption to protect the user identity. By using volunteer-operated systems or servers Tor helps people to access the information without showing who they are and from where they are accessing to protect their identity. Especially, in the modern era where everything is being monitored and everyone is continuously under the digital surveillance and data collection of everything we do online.

Many valid and authentic uses of Tor are highlighted in this analysis including free expression even in a restricting environment, freedom of speech for the journalists, and helping activists to express themselves. On the other hand, Tor's anonymous features have led to illegal activities on the dark web, such as dealings of illegal goods, illegal weapons, black-market transactions, and cybercrime that cause substantial challenges for law enforcement. All the ethical issues regarding the usage of Tor are primarily discussed in this paper, focusing on the clash between people's right to privacy and the need for security. There is a challenge arising from the argument about privacy vs security for finding the equality that respects both individual rights and the safety of the broader public.

The new technologies that are strictly involved in protecting privacy, increasing surveillance efforts, and a global demand for stronger data protection will affect the future of Tor's Network. Many modern and advanced technologies like Quantum encryption and Zero Knowledge proofs can make Tor stronger at keeping users anonymous by regulating it towards new operational models that might lead to changes in How Tor operates. Eventually, the Tor network will play an important role in conversations about privacy, digital rights, and the bond of surveillance, working as both the key protector of digital freedom and the point for ethical discussion.

In conclusion, the role of Tor in the internet is more important now than ever. It characterizes all the challenges we face today in the era of technologies technically called the "Digital Age" where there must be a balance between privacy rights and security needs, where this technology can help people but can also create challenges for rules and regulations. Technology can be a savior to sort this out but it has become an expensive nightmare for the norms, law enforcement, and legalized systems. The Future of Tor and Anonymous Networks: The answer will have a huge effect on our privacy, security, and freedom over the internet. Do understand the dual-sided nature of the Tor network as both the promise and peril of private communication, but its short- and long-term evolution will be one part of our online privacy future.

**Funding Statement:** The authors received no specific funding for this study.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] Shehreyar Nawaz, Hamayun Khan, Wajiha Salman, Umer Shahid, Momin Latif Khokhar, M Zaid Iqbal, & Abdullah Hamid. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of Engineering Sciences, 2(4), 85–114

[2] Hoang, D. H., & Nguyen, H. D. (2018). A PCA-based method for IoT network traffic anomaly detection. In2018 20th International Conference on Advanced Communication Technology (ICACT), 381-386. IEEE.

[3] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson,

R. (2016). Threat analysis of IoT networks using artificial neural network intrusiondetection system. In2016 International Symposium on Networks, Computers and Communications (ISNCC), 1-6. IEEE.

[4] Blanco, R., Malagón, P., Briongos, S., & Moya, J. M. (2019). Anomaly Detection Using Gaussian Mixture Probability Model to Implement Intrusion Detection System. InInternational Conference on Hybrid Artificial Intelligence Systems, 648-659. Springer, Cham.

[5] Muhammad Abdullah, Hamayun Khan, Ayesha Shafqat, Muhammad Daniyal, Muhammad Bilal, & Muhammad Anas. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross – Platform . Spectrum of Engineering Sciences, 2(3)

[6] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey.ACM Computing Surveys (CSUR),41(3), 1-58.

[7] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[8] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[9] Muhammad Waleed Khawar, Hamayun Khan, Wajiha Salman, Samra Shaheen, Ariba Shakil, Fatima Iftikhar, & Khawaja Muhammad Ismail Faisal. (2024). Investigating the Most Effective AI/ML-Based Strategies for Predictive Network Maintenance to Minimize Downtime and Enhance Service Reliability. Spectrum of Engineering Sciences, 2(4), 115–132

[10] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[11] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[12] K. Benzekki, A. El Fergougui, and A. E. Elalaoui, Software-defined networking (SDN): A survey, Secur. Commun. Netw., vol. 9, no. 18, pp. 58035833, 2016.

[13] Ahmad, S., Lavin, A., Purdy, S., & Agha, Z. (2017). Unsupervised real-time anomaly detection for streaming data.Neurocomputing,262, 134-147.

[14] Akhi, A. B., Kanon, E. J., Kabir, A., &Banu, A. (2019).Network Intrusion Classification Employing Machine Learning: A Survey. (Doctoral dissertation)Department of Computer Science and Engineering, United International University, Bangladesh.

[15] Alizadeh, H., Khoshrou, A., &Zuquete, A. (2015). Traffic classification and verification using unsupervised learning of Gaussian Mixture Models. In2015 IEEE international workshop on measurements & networking (M&N). 1-6. IEEE. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task

Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1,  pp. 2097-2113, Sep. 2023

[16] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[17] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[18] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[19] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[20] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[21] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[22] M. S. Abdul Razak, S. P. A. Gothandapani, N. Kamal, and K. Chellappan, “Presenting the Secure Collapsible Makerspace with Biometric Authentication”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 1, pp. 12880–12886, Feb. 2024.

[23] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185,  July. 2018

[24] Amangele, P., Reed, M. J., Al-Naday, M., Thomos, N., & Nowak, M. (2019). Hierarchical Machine Learning for IoT Anomaly Detection in SDN. In2019 International Conference on Information Technologies (InfoTech). 1-4. IEEE.

[25] Anderson, J. P. (1980). Computer security threat monitoring and surveillance.Technical Report, Fort Washington, PA, James P. Anderson Co.

[26] Aung, Y. Y., & Min, M. M (2018). An analysis of K-means algorithm based network intrusion detection system. Advances in Science, Technology and Engineering Systems Journal,3(1), 496-501. Bauer, F. C., Muir, D. R., &Indiveri, G (2019). Real-Time Ultra-Low Power ECG Anomaly Detection

[27] Bhati, B. S., Rai, C. S., Balamurugan, B., & Al-Turjman, F. (2020). An intrusion detection scheme based on the ensemble of discriminant classifiers.Computers & Electrical Engineering,86, 106742.

[28] Bhattacharyya, D. K., &Kalita, J. K. (2013).Network anomaly detection: A machine learning perspective. CRCPress.

[29] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[30] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[31] Jawad Ahmad, Hamayun Khan, Wajiha Salman, Muzamal Amin, Zain Ali, & Shumail Shokat. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133–149

[32] Khan, A. Yasmeen, S. Jan, U. Hashmi, "ENHANCED RESOURCE LEVELING INDYNAMIC POWER MANAGEMENT TECHNIQUEOF IMPROVEMENT IN PERFORMANCE FOR MULTI-CORE PROCESSORS" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[33] Abdul Rafay, Hamayun Khan, Wajiha Salman, Gulzar Yahya, & Uzair Malik. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150–165

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[34] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[35] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[36] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[37] Ibrahim Akmal, Hamayun Khan, Ayesha Khushnood, Fatima Zulfiqar, & Eman Shahbaz. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of Engineering Sciences, 2(3)

[38] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[39] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[40] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[41] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[42] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[43] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[44] Mian Muhammad Abdullah, Hamayun Khan, Sabestean, Muhammad Farhan, Farhan Khadim, & Hafiz-ul-Asad. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of Engineering Sciences, 2(3)

[45] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[46] Haripriya, L.A., Jabbar, M., &Seetharamulu, B. (2018). A Novel Intrusion Detection System Using Artificial Neural Networks and Feature Subset Selection. International Journal of Engineering and Technology, 7(4), 181. http://doi.org/10.14419/ijet.v7i4.6.20458

[47] Aaraiz Naveed, Hamayun Khan, Zaeem Imtiaz, Wahaj Hassan, & Uneeb Fareed. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of Engineering Sciences, 2(3)

[48] Hafiz M. Saqlain Khan, Hamayun Khan, Ch. Muhammad Akhtar Hayat, Hassan Tayyab, & Kashif Ali. (2024). An Enhanced Cost Effective and Scalable Network Architecture for Data Centers. Spectrum of Engineering Sciences, 2(3).

[49] M. Shahzar Nasir, Hamayun Khan, Ahmad Qureshi, Arslan Rafiq, & Taha Rasheed. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of Engineering Sciences, 2(3)