JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
SICAIET
2024

Research Article
Collection: Artificial Intelligence and Emerging Technologies

A Review: Performance and Security Based Comparative Analysis of Well-Known Stealth Services

Shagufta Faryad[1], Ijaz Ali Shoukat[1], Erssa Arif[1], Muhammad Rehan Faheem[2], Muhammad Kashif[3], and Amina Nawaz[1*]

[1]Riphah International University, Faisalabad, Pakistan.
[2]Department of Computer Science, The Islamia University of Bahawalpur, Pakistan.
[3]Southwest Jiatong University, China.
[*]Corresponding Author: Amina Nawaz. Email: aminach375@gmail.com

Academic Editor: Salman Qadri **Published:** February 01, 2024

Abstract: In the digital landscape of privacy-concerned era, anonymous or Stealth Services (SSs) offer a promising future for entities who wish for obscurity and solitude in their communication. The elevating paramount of privacy concern consistently increasing the usage of SSs and affected individuals day by day. Some SSs being the hot stakes of cyber world needs to be analyzed more critically. We categorize, analyze and synthesize the comprehensive analysis of six prominent SSs (Tor, I2P, Freenet, Riffle, Lokinet and JAP) to commence their in-depth comparative evaluation metrics in multiple aspects. Analytical and performance based scrutiny elucidates the diverse approaches, their architectures, security features, flaws and associated attacks. The synthesized examination offers a nuanced aspect towards SSs and enlightens the way for future developments in cyber security and secrecy. Performance and security based evaluation reveals that Tor incur performance bottlenecks while decentralized SS I2P enhances security with compromised throughput. Likewise, the Freenet and JAP offer more data resilience but suffer from transparency and scalability issues. Although, Riffle and Lokinet are innovative paradigms of SSs but both have more complexity and other trade-offs. The valuable insights will help the researchers and decision-makers navigate the complexities of the digital life, facilitating a deeper understanding of the challenges involved in selecting a secure communication network and offering improved stealth solutions.

Keywords: Anonymous; Stealth services (SSs); Tor; Riffle; I2P; Lokinet.

1. Introduction

In today's ubiquitous surveillance era, security and privacy has become the hot concerns for individuals. The pervasive nature of personal autonomy accentuates the robust security and privacy focused solutions. Digital foot printing and identity theft proliferation urging the necessity for deploying the more secure network that can preserve the intimacy of the personal and professional communications and data. This paramount has influenced the people to use ultra-secret networks that anonymize and secure their data as well as conceal their identity and communication while going through the public network.

Influenced users often utilizes such kind of networks which offers them anonymity, identity protection and secrecy alike features. Stealth services (SSs) or the anonymous services such as Tor, I2P, Freenet, Lokinet, Riffle and Jondonym (JAP) being at the forefront are widely used in the dark web (DW) to conceal one's identity during communication over the civic network. Figure 1, Classify the stealth services under different categories. Previously significant research has been done over there to illuminate the susceptibilities and dark sides of these SSs but specifically analytical and statistical evaluation of these services has yet to be focused. This review aims to disclose diverse Stealth Services (SSs) evolving around,

their classification, architecture and intrinsic features besides in depth examination from several facets has also been done to enlighten the way for effective stealth solutions.

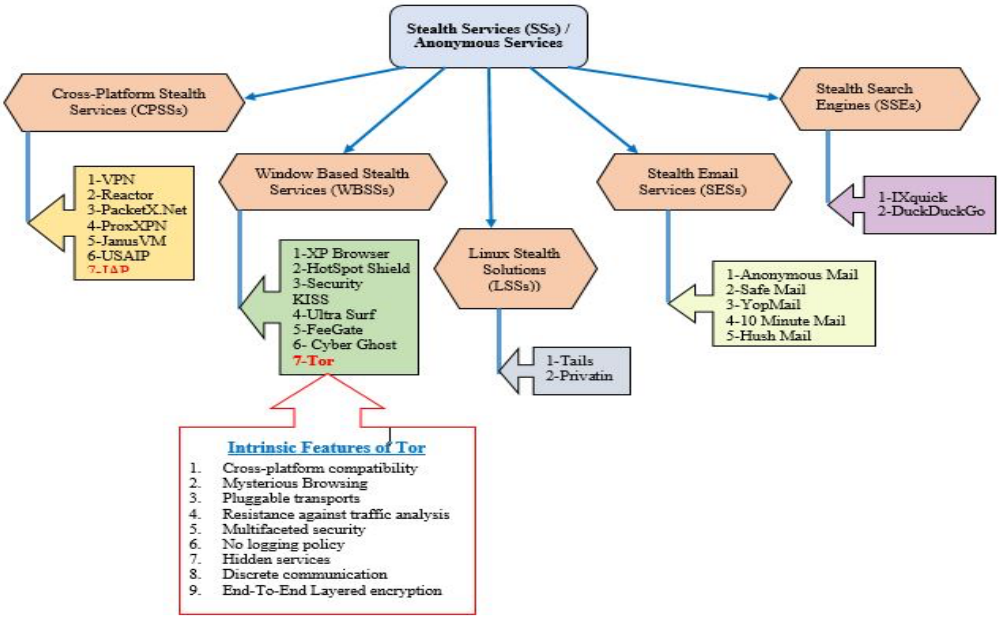


Figure 1. Classification of Stealth Services (SSs)

Section II confer about cutting-edge Stealth services (SSs), likewise Comparative Evaluation in section III will reveal multidimensional Statistical and analytical examination of these Stealth services (SSs). Later Section IV, presenting crux will enlighten the future research perspectives. The thorough analysis offers an inclusive outlook on secure systems, paving the way for advancements in cybersecurity and privacy. These insights will guide researchers in navigating the intricacies of digital life, letting them to better understand the difficulties in choosing a safe communication system and providing improved solutions for stealth and security.

2. Cutting-Edge Stealth Services

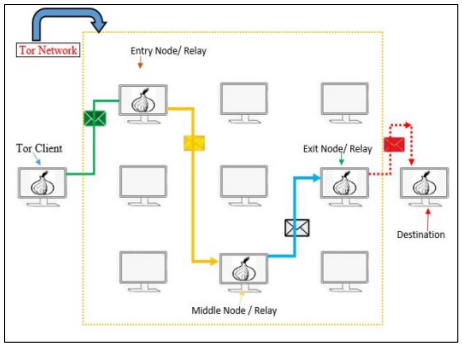
This section Elaborate the six cutting-edge Stealth Services (SSs) leverage with advance cryptographic techniques and efficient data communication protocols. Enlightening how these hidden services can embrace the need of obscurity and privacy in this ubiquitous.

2.1. Tor Network

Tor termed as "The onion Router" was the early source established by U.S Navy in almost 1990 to communicate secret data and bypass the areas restrictive internet policies. Eventually, Tor became open source widely used network in order to provide free censorship, secure platform to activists, dissidents and a protected way to exchange secret data [1]. Innovative adoption and revolutionary integration of Tor network has much guaranteed the privacy of its users and provides the new landscape of online communication. With the ever growing necessity of numerous world anonymous communication for those individuals concerned about more security and privacy became a must [2].

The obvious anonymous routing network Tor, routing the traffic through multiple volunteer servers makes the communication decentralized, obscure and more secure for the privacy concerned entities [3]. Anonymity is guaranteed via advance layered encryption using multiple securing protocols and manifold encryption ciphers e.g. AES, RSA etc. [4]. Exertion is offered to protect the source and destination even from every node where it's being routed. The Onion Routing Protocols comprised of layered encryption, dynamically established circuits and the End-To-End encryption technologies (e.g. HTTP, TLS) ensures data integrity and secrecy at every relay or node making the Tor more secret network.

Websites hosted within the Tor and web-server's addresses are registered with onion domain (e.g. "name. Onion") a character string of 16-bits [5]. The Tor network works with IP masking and multi-layered encryption elaborated in the Figure 2 (a), Figure (b). In spite of positive uses, Tor doesn't guarantee hundred percent security due to the vulnerabilities and illicit activities (e.g. child erotic abuse materials etc.) allied with the said network [6].



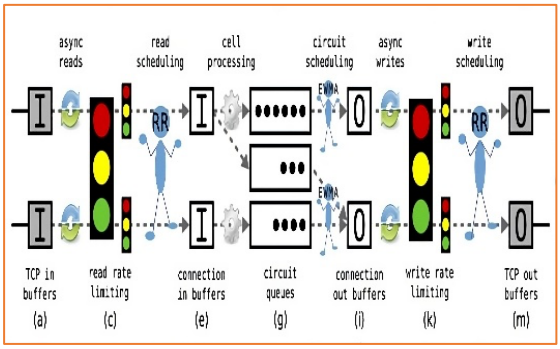
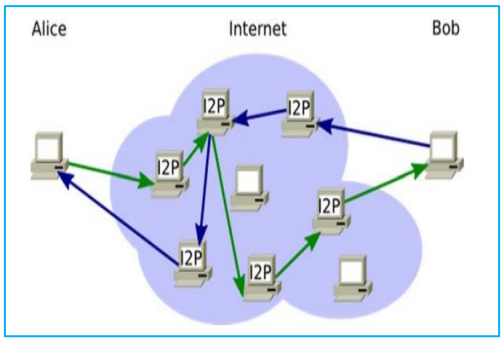


Figure 2. (a) Tor Architecture outer Layout **Figure 1. (b)** Tor's Inner Layout [17]

2.2. I2P Network

I2P termed as "Invisible Internet Project", a peer-to-peer network promising the anonymity and protecting one's identity utilizing it [7]. I2P Network encompasses through several nodes, clients partaking their bandwidths and keeping the record of theirs peer's performance. For each stretch, client needs to inaugurate an encrypted, unidirectional short-lived tunnel to establish a secure path for communication where data (garlic cloves) transferred can't be seen at any stage [7]. "Garlic Clove" refers to bundle the individually encrypted messages into a single clove/message that ensures the overall security of an individual's message [10].



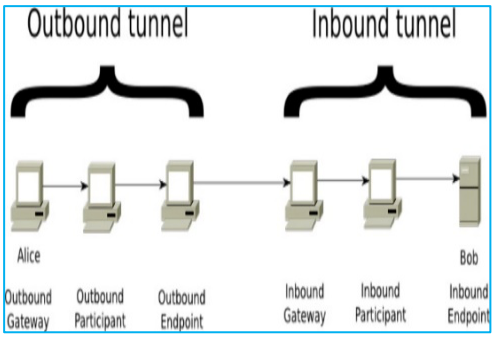


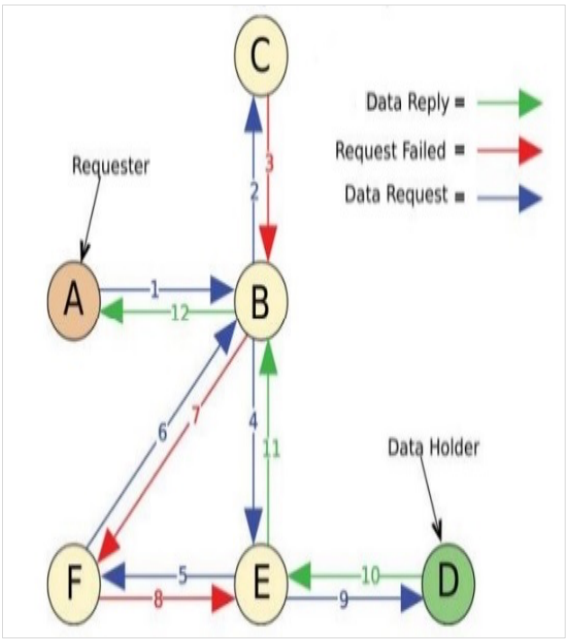
Figure 3. (a) I2P Network architecture [11] **Figure 3. (b)** I2P tunnel Layout [5]

Unlike Tor, In I2P network data packets passes through numerous nodes ensuring secrecy before reaching the intended destiny shown in Figure 3(a). The tunnel layout designed inside I2P network and its working architecture can be seen in Figure 3 (a), Figure (b). The I2P network not only hides the sender but also aims to fleece the receiver identity too [10]. The IP address anonymity of both sender and the receiver remain intact but the location identifiers can reveal a node. Peer nodes utilize the selection technique to maintain its speed, performance, and sustainability [7, 5].

2.3. Freenet

Another anonymous and decentralized P2P communication service is offered by Freenet. It works on the principle of decentralization and allows retrieving data only if you know the encryption key. In this network each node subsidize its storage as well as the bandwidth for the fragment of encrypted data in the network and retains a "Routing Table" comprises of the addresses of other nodes. Each node in the network acts as a router manager [5]. All the communication is made obscure using the tunnels and garlic routing mechanism shown in Figure 4 (a). Freenet being a decentralized SS has specific nodes layout architecture explained in Figure 4 (b).

End-to-End encryption assures the anonymity of source and destination. Every node must have the knowledge about internal and external tunnels that helps the user to save their information and data globally in a database named as netDB. Freenet uses proxy chain to communicate the request to the next node where every node only knew about the preceding and forwarding node but have no knowledge about the originating node [5, 12, and 18].



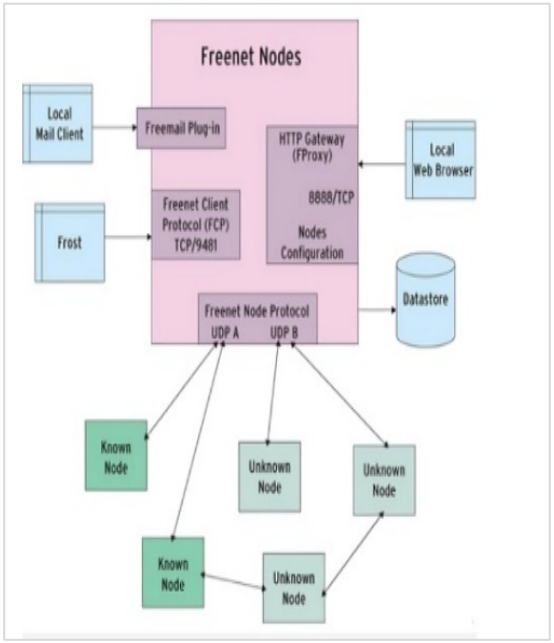


Figure 4(a). Freenet Architecture [11] **Figure 4(b).** Nodes Layout in Freenet [19]

The destination node is capable of peeling out all the encryption layers from the garlic clove using their corresponding keys. In spite of all the protected mechanisms anonymity is still questionable and might be open to several attacks [10].

2.4. Riffle

A secret network that emerges anonymity to only sanctioned group of users over a trivial set of deceptive servers. Riffle uses the mixture of both upstream and downstream communication intends to provide effective computations and optimal bandwidth. In setup stage, Riffle users utilizes three sets of encryption algorithms coupled with the servers, with an incorporating key that diffuses the definite disruption. Simple protocol like Diffie-Hellman is castoff for Private Information Recovery (PIR) [5, 24, and 26]. Figure 5(a), Figure (b) explains the deployment model and Testbed layout of Riffle network.

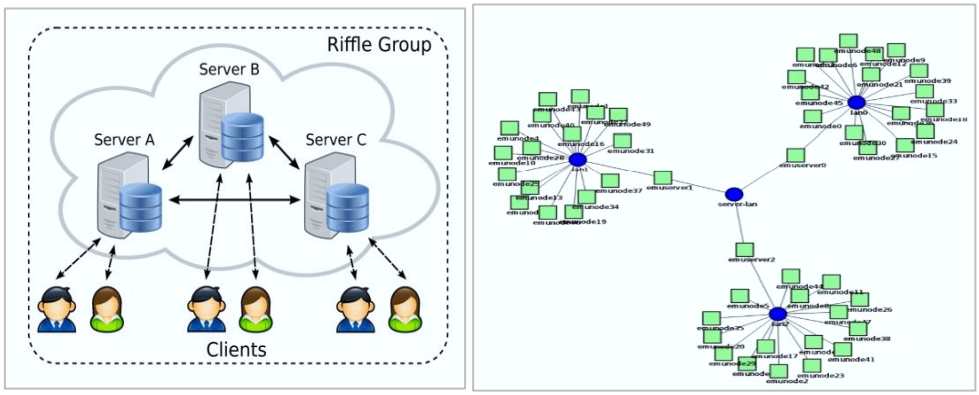


Figure 5. (a) Riffle Deployment Model [20] **Figure 5. (b)** Testbed Layout of Riffle [20]

2.5. Loki-net

An obscure, fully distributed and open source SS that facilitates its users to communicate secretly is referred as "Lokinet". Loki-communication has low latency feature uses LLRA protocol to send and receive data packets without any disruption. The hybrid solution among Tor and I2P provides fully incentivized environment to all its nodes [21] [22] [23] [27].

2.6. JAP (Java Anon Proxy)

JAP termed as "JonDo" or "Jondonym" leverage the communication transmit data packets through numerous "mixes" over the civic network to protect from surveillance and being traced. User dependent

path selection among several mixes termed as "mix Cascades" makes the JAP more flexible SS for anonymity seekers [25] [29].

2.7. Intrusion Classification Taxonomy

This section explains the intricacies and intrusion classification taxonomy of different SSs. All the attacks that are possible under the umbrella of prescribed SSs are shown in the Figure 6.

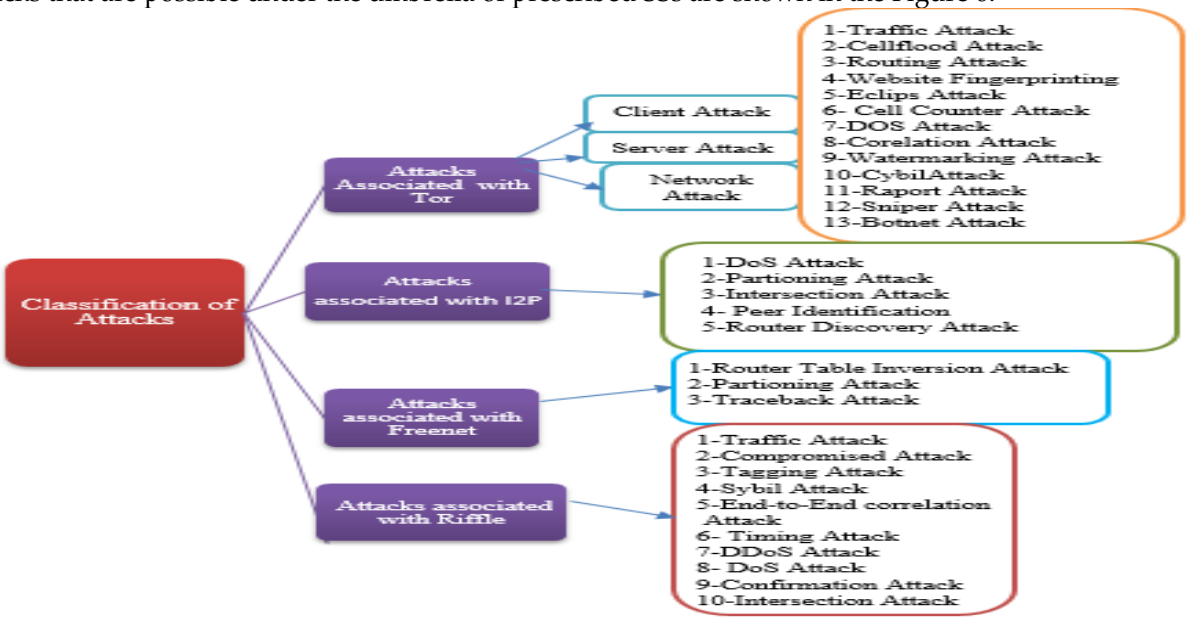


Figure 6. Intrusion Classification Taxonomy [5] [12]

3. Comparison Matrices of Anonymous Networks

This section explores and investigates the several aspects of SSs. An analytical and comparative examination provides the in-depth insights about performance and design oriented landscapes as well as facilitates to mitigate the associated attacks.

Table 1. Analytical Evaluation of SSs

Analytical Parameters	Tor	I2P	Freenet	Riffle	Loki-net	JAP	References
Distribution	Partially Decentralized	Decentralized	Decentralized	Partially Decentralized (Mixnet)	Fully Decentralized	Centralized	[5] [12] [13] [27] [29] [30] [31] [33]
Node Incentive	Volunteered	Volunteered	Volunteered	Unknown	Incentivized	Unknown	[5] [12] [13]
Load Balancing	Yes using (TLBM)	No	No	Yes	Better Load Balancing	Not Available	[27] [29] [31]
Complexity	Reduced	Increased	Moderate	More Complex	Moderate	High	[5] [12] [13]
Architecture	Onion Routing	Garlic Routing	Decentralized	Mix-network	Mixnet, DHT and SDN	Mix of Onion Routing & Mix-network	[27] [29] [23] [24] [25] [26] [31]
Switching	Circuit Switching	Packet Switching	Message Passing Technique	Packet Switching	Packet Switching	Tunneling	[25] [26]
Scalability	High	Suitable Enough	Low	Low	Moderate	Moderate	[5] [12] [13]

Performance of stealth services influenced by multifaceted factors (e.g. throughput, bandwidth consumed, response time etc.). A deep statistical performance analysis on these SSs results the Table 2. Table 3. Explains the bilateral evaluation of Tor and Freenet while Figure 7. Presents the facts about Geo-location Based Servers of SSs. The security aspects of these SSs is considered under Table 4.

Table 2. Performance Analysis among SSs [5, 12, 13, 15, 16, 20-27, 29, 30, 31, 32, ss33]

Performance Parameters	Tor	I2P	Freenet	Riffle	Loki-net	JAP
Bandwidth Consumption	16 MB/Sec	>128KB/Sec	Variable	100 KB/Sec (per user)	Not mentioned in DHT	>128 KB/Sec
Degree of Anatomization	0.77 (Aggregated)*	0.71(Aggregated)*	Not Available	Not Available	Not Available	0.625 (Aggregated)*
Expected Speed	200 KB/Sec to 8MB/Sec	50 KB/Sec to 300 KB/Sec	Variable	100 KB/per client	100 MB/Sec	30-50 KB/Sec
Throughput	Moderate to High	Lower	Low to moderate	Higher	Moderate to High	Moderate to High
Response Time	Medium	Faster	Variable	Fastest	Faster	Variable
Traffic type	Basically Http, (Mix of TCP, UDP)	(Mix of TCP, UDP)	UDP	(Mix of TCP, UDP)	All Type of traffic	(Mix of TCP, UDP)
Transfer Protocols	TSL, HTTPS, SOCKS	12CP, 12NP & Others	Protocols (used in Message Passing)	Mixnet	UDP, ICMP	TCP and UDP
Estimated Nodes	7000+	2000+	30000+	Variable	1700+	Not Disclosed
Latency	Low	High	Low	Low	Low	Low

Table 3. Bilateral Evaluation among Tor and Freenet

Performance	Tor	Freenet	Ref
Avg. Degree of Connection	2.982	18.362	[30] [33]
Avg. Path Length	4.630	2.965	
Clustering Coefficient	0.279	0.264	
Diameter	16	6	

Figure 7. Geo-location Based Servers of SSs

The above elaborated SSs (Stealth Services) are assessed and compared on the basis of information security grounds governed by the NIST agency [28]. Security parameters (e.g. confidentiality, availability etc.) of SSs are demonstrated as: "*" is used to climax "Provides only in some circumstances" and "✔" is used to indicate "Yes/provides".

Table 4. Comparative Evaluation on Security Grounds

Anonymous Services / Proxies	Confidentiality	Integrity	Availability	Reliability	Anonymity	Hidden Services	Traffic Analysis Resistance	References
Tor	✔	✔	*	*	✔	✔	✔	[5][12][13] [14][15][31] [30] [33]
I2P	✔	✔	*	*	✔	✔	✔	[5][12][13] [14][15]
Freenet	✔	✔	*	*	✔	✔	*	[16][19]
Riffle	✔	✔	*	*	✔	*	*	[20][24]
Loki-net	✔	✔	*	*	✔	✔	*	[21][22][23] [27]
JAP	✔	✔	*	*	✔	*	*	[25][29]

4. Conclusions

The entire comparative examination underscores the realm of Stealth Services (SSs). Classification taxonomies of well-known SSs are provided with their associated at-tacks besides their architectures and working methodologies. Stealth services (SSs) nuanced their interplay between security and performance to achieve the high anonymity with efficient throughput. Analytical and security based evaluation reveals that Tor being the robust SS incur performance bottlenecks. The decentralized SS I2P enhances security but compromises throughput. Likewise the Freenet provides more data resilience, yet suffers scalability issues. Although, Riffle and Lokinet are innovative paradigms of stealth solutions but fires more complexity and other trade-offs. JAP provides anonymity with more intricacies of transparency. However, these SSs need to be analyzed on other technical grounds that can foster the expansion of more diverse nature SSs with a high degree of integrity and security aligned with efficient throughput.

References

1. N. Dutta, N. Jadav, S. Tanwar, H. K. D. Sarma, E. Pricop, N. Dutta, et al., "Tor—the onion router," in *Cyber Security: Issues and Current Trends*, 2022, pp. 37-55.
2. Sobhan, S., Williams, T., Faruk, M. J. H., Rodriguez, J., Tasnim, M., Mathew, E., ... & Shahriar, H. (2022, June). A review of dark web: Trends and future directions. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1780-1785).
3. Saleem, J., Islam, R., & Kabir, M. A. (2022). The anonymity of the dark web: A survey. *IEEE Access*, 10, 33628-33660.
4. M. H. Javed, "Tor Network Architecture, Anonymity and Hidden Services," doi: https://doi.org/10.31224/3054, 2023.
5. M. Hosseini Shirvani and A. Akbarifar, "A Comparative Study on Anonymizing Networks: TOR, I2P, and Riffle Networks Comparison," *Journal of Electrical and Computer Engineering Innovations (JECEI)*, vol. 10, no. 2, pp. 259-272, 2022.
6. Gannon, C., Blokland, A. A., Huikuri, S., Babchishin, K. M., & Lehmann, R. J. (2023). Child sexual abuse material on the darknet. *Forensische Psychiatrie, Psychologie, Kriminologie*, 17(4), 353-365.
7. Chen, B., Xu, C., Cai, W., & Xia, Y. (2023, September). Narrowing Down the Secrets of the Internet-A Review of Privacy Leakages and Prevention Methods. In 2023 9th International Conference on Humanities and Social Science Research (ICHSSR 2023) (pp. 87-95). Atlantis Press.
8. https://www.researchgate.net/figure/Accessing-an-I2P-Eepsite_fig3_221655653
9. I2P Project, "I2P Routing," [Online]. Available: https://trac.i2p2.de/attachment/wiki/Content/i2prouting.png.
10. Erdin, E., Zachor, C., & Gunes, M. H. (2015). How to find hidden users: A survey of attacks on anonymity networks. *IEEE Communications Surveys & Tutorials*, 17(4), 2296-2316.
11. Zeinalipour-Yazti, D. (2003). *Information retrieval in peer-to-peer systems* (Doctoral dissertation, University of California, Riverside). Available: http://www.cs.ucr.edu/~csyiazti/papers/cise2003/cise2003.pdf.
12. Haraty, R. A., Assi, M., & Rahal, I. (2017). A Systematic Review of Anonymous Communication Systems. *ICEIS (2)*, 211-220
13. Zhang, J., Duan, H., Liu, W., & Wu, J. (2011). Anonymity analysis of P2P anonymous communication systems. *Computer Communications*, *34*(3), 358-366.
14. Erdin, E., Zachor, C., & Gunes, M. H. (2015). How to find hidden users: A survey of attacks on anonymity networks. *IEEE Communications Surveys & Tutorials*, *17*(4), 2296-2316.
15. Li, B., Erdin, E., Gunes, M. H., Bebis, G., & Shipley, T. (2013). An overview of anonymity technology usage. *Computer Communications*, 36(12), 1269-1283.
16. Le Blond, S., Choffnes, D., Zhou, W., Druschel, P., Ballani, H., & Francis, P. (2013). Towards efficient traffic-analysis resistant anonymity networks. *ACM SIGCOMM Computer Communication Review*, *43*(4), 303-314.
17. Jansen, R., Syverson, P., & Hopper, N. (2012). Throttling tor bandwidth parasites. In *21st USENIX Security Symposium (USENIX Security 12)* (pp. 349-363).
18. O. Odegbile, "Freenet: Distributed Anonymous Information Storage and Retrieval System."
19. https://www.linux-magazine.com/Issues/2008/91/Freenet
20. A. H. Kwon, D. Lazar, S. Devadas, and B. Ford, "Riffle: An efficient communication system with strong anonymity," in Proceedings of the 2015 *IEEE Symposium on Security and Privacy* (SP), 2015, pp. 447-462.
21. K. Jefferys, S. Harman, J. Ross, and P. McLean, "Private transactions, decentralised communication," 2018.
22. https://csilinux.com/tor-vs-lokinet-a-comprehensive-comparison-mobile/
23. M. Chaieb and S. Yousfi, "LOKI Vote: A Blockchain-Based Coercion Resistant E-Voting Protocol," *in Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020*, Dubai, United Arab Emirates, November 25–26, 2020, Proceedings, vol. 17, pp. 151-168, Springer International Publishing, 2020.
24. A. H. Kwon, D. Lazar, S. Devadas, and B. Ford, "Riffle: An efficient communication system with strong anonymity," in Proceedings of the *IEEE Symposium on Security and Privacy*, 2015.
25. N. Dutta, N. Jadav, S. Tanwar, H.K.D. Sarma, and E. Pricop, "Being Hidden and Anonymous," in *Cyber Security*: Issues and Current Trends, Studies in Computational Intelligence, vol. 995. Springer, Singapore, 2022, https://doi.org/10.1007/978-981-16-6597-4_2.
26. H. Zhang, B. Cho, E. Seyfe, A. Ching, and M.J. Freedman, "Riffle: Optimized Shuffle Service for Large-Scale Data Analytics," in EuroSys '18: 13th *European Conference on Computer Systems*, April 23–26, 2018, Porto, Portugal. ACM, New York, NY, USA, pp. 15, https://doi.org/10.1145/3190508.3190534.
27. https://oxen.io/blog/lokinet-speed-and-scale
28. https://www.nccoe.nist.gov/publication/1800-26/VolB/index.html#security-characteristic-analysis
29. S. Pape and D. Harborth, "Acceptance Factors of Privacy-Enhancing Technologies on the Basis of Tor and JonDonym," in *Human Factors in Privacy Research*, pp. 299-320, Cham, Springer International Publishing, 2023.
30. V. Duddu, D. Samanta, and D. V. Rao, "Fuzzy graph modelling of anonymous networks," in *Soft Computing Applications*: *Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018)*, vol. II 8, pp. 432-444, Springer International Publishing, 2021.

31. J. Bergman and O. B. Popov, "Exploring Dark Web Crawlers: A Systematic Literature Review of Dark Web Crawlers and Their Implementation," in IEEE Access, vol. 11, pp. 35914-35933, 2023, doi: 10.1109/ACCESS.2023.3255165.
32. I. Karunanayake, N. Ahmed, R. Malaney, R. Islam and S. K. Jha, "Darknet Traffic Analysis: Investigating the Impact of Modified Tor Traffic on Onion Service Traffic Classification," in IEEE Access, vol. 11, pp. 70011-70022, 2023, doi: 10.1109/ACCESS.2023.3293526.
33. J. Saleem, R. Islam and M. Z. Islam, "Darknet Traffic Analysis: A Systematic Literature Review," in IEEE Access, vol. 12, pp. 42423-42452, 2024, doi: 10.1109/ACCESS.2024.3373769.