SoK: Invisible Internet Project (I2P)

Jubin Raj Nirmal
40235087
j_nirmal@live.concordia.ca

Riya Vinodbhai Patel
40224858
p_riyavi@live.concordia.com

Sanchit Smarak Behera
40230269
sa_beher@live.concordia.ca

Abstract

I2P is a powerful open-source technology that allows anonymity and encryption over internet communication through its decentralized message-oriented mix net. It has the potential to provide a secure means of communication for individuals in situations where anonymity is crucial. However, its use may also pose challenges in real-time environments where it may provide means for malware to exfiltrate data. Nevertheless, the need for anonymous communication systems has become increasingly important, and I2P provides a valuable solution for anonymity and privacy online. This paper presents a Systemization of Knowledge (SoK) on the Invisible Internet Project (I2P). It evaluates I2P using UDS (Usability Deployability Security) Evaluation Framework (with TOR as an alternative) and Cognitive Walkthrough. The cognitive walkthrough evaluates I2P's usability by examining the user's ability to achieve their goals while using it. Finally, we conclude the evaluation of I2P based on UDS and the Expert Review.

I. INTRODUCTION

The Invisible Internet Project (I2P) [1], an open-source software project, aims to make online communication anonymous and secure [2]. Clients can interface secretly and namelessly over this circulated network without revealing their identity [3]. I2P is a famous choice for individuals that need protection and namelessness while talking on the web [2]. It started as an alternative to TOR, a popular anonymity network [4].

I2P has the following key features:

- Unknown Correspondence: a secure communication platform that lets users send and receive messages without telling anyone who they are or where they are.
- Architecture with Dispersion: uses a globally distributed network of nodes managed by volunteers.
- Security: End-to-end encryption guarantees that only the intended recipient can read or intercept the messages.
- Independent Organization: Unlike conventional VPNs, I2P is a self-contained network that operates solely within the I2P network.
- Namelessness Administrations: offers an assortment of obscurity administrations, for example, secure email, mysterious web perusing, and record sharing.
- Free Software: I2P is an open-source project that suggests anyone can examine and change the source code.
- Resistant to Attacks from Sybil [2] [3]: Sybil attacks, in which an attacker creates many nodes in a network to gain control or influence over it, are protected by built-in security features in I2P.

The main components of I2P include the router, Socket API for messaging (SAM), I2P Messenger, I2P Browser, I2P Snark, and I2Pd [3].

- Router: The central element of an I2P network is the router—which controls how requests and messages are routed through the network [2]. Additionally, the router has a user interface for configuring and managing the network.
- SAM (Socket API for messaging): I2P applications connect to I2P networks using the SAM (Socket API for Messaging) protocol. Provides a socket-based API for sending and receiving messages over I2P networks [2].
- I2P Messenger: I2P Messenger is an email platform built on an anonymous and secure I2P network [3]. Users can send and receive emails without revealing their location or identity.
  I2P Messenger is an instant messaging program based on the I2P network. Provides anonymous and secure messaging between I2P users.
- I2P Browsers: I2P Browser is a customized version of Firefox configured to work with I2P networks. Through the I2P network, users can access the internet anonymously [2].
- I2P Snark: I2P-Snark is his network-based I2P BitTorrent client. Through the I2P network, users can download and distribute files anonymously [3].
- I2Pd: I2Pd is a C++-based execution of an I2P router. Its lightweight and practical design makes it ideal for low-power devices [2], such as routers and embedded systems.

I2P works by making a worldwide organization of volunteer-run hubs spread out over the globe. These hubs communicate with one another to create mysterious online communication conceivably [4]. When a client sends a message or asks through I2P, the message is scrambled and steered through numerous hubs, sometimes recently reaching its goal. The term "burrowing" alludes to steering over numerous hubs. When a client initially enters the I2P organization, they lay out an affiliation with a "switch" center, which fills in as the organization's section. The switching hub gives the client a one-of-a-kind address, alluded to as a "goal," which is utilized to recognize the client inside the I2P arrangement. This address's long string of characters closes with ".i2p," which stands for Web Convention. The message is scrambled and sent to the target address when a client wishes to send a message or ask another client about the I2P arrangement. Before arriving at its objective, the message is coordinated through a progression of hubs. The message is unscrambled by each hub within the way, uncovering the address of another hub within the burrow. The message is unscrambled and passed on to the arranged recipient by the passage's final center.

It is troublesome for anybody to hinder or follow the association since the routing strategy employments different hubs. Moreover, the burrow guarantees that every hub has yet to get to the whole directing way since each hub, as it was, knows the addresses of the nodes preceding and taking after it.

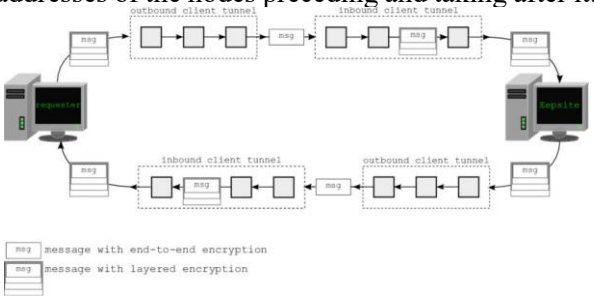

Figure 1: I2P Working Mechanism

In addition, I2P provides several anonymous communication services, including file sharing, secure email, and anonymous web surfing [3]. These functionalities are added to the I2P organization's center steering instrument, giving it a flexible stage for mysterious web correspondence [2].

II. EVALUATION

UDS (Usability Deployability Security) may be a high-level technique utilized to assess a program based on three key angles:

Usability, deployability, and security. Usability is the ease with which clients can work and explore a chunk of the program. This incorporates angles such as user interface plan, ease of utilization, and availability. A computer program with tall convenience is natural, simple to memorize, and essential to utilize. The term deployability depicts how uncomplicated it is to introduce and set up the program on different distinctive frameworks and stages. This covers framework necessities, establishment methods, related costs, and program compatibility. Security here implies a program's measures to fight off dangers such as hacking, malware, and data breaches. This incorporates viewpoints such as get to control, encryption, and verification. A program with tall security is created to supply strong security against these dangers and is planned from the ground up with security in intellect. [5]

Analyzing and assessing computer programs based on these three variables makes a difference in engineers and clients deciding the qualities and restrictions of a specific program. A program that does well in all three is likely to be solid, simple to utilize, and secure, essential for ensuring that program ventures are successful and broadly received by clients.

Evaluating I2P technology will assist us in understanding how well it works, considering its usability for users who make use of it for anonymity, its deployability for decentralized deployment and maintenance, and finally, its security against different attack vectors. An evaluation assessment of I2P based on the UDS evaluation framework is carried out with a famous alternative, TOR (The Onion Routing), which provides almost similar features. The evaluation framework is as follows.

Usability:

I2P is intended to be user-friendly, having a straightforward and apparent user interface. The interface offers a variety of essential tools and features that are easy to use, making it simple for users to communicate and exchange data anonymously over the Internet. However, the user interface may not be as polished as some other software and may require some technical knowledge or expertise to utilize it efficiently. Here are some Usability criteria to be considered-

1. Memory-wise effortless: The system should require the least amount of effort from the users to perform tasks.

2. Scalable for users: The system should be scalable, so it may support many users and adapt to meet their needs.
3. Easy adaptability: The system should be flexible, allowing the users to tailor their experience and meet their demands.
4. Ease of use acquisition: The system should be uncomplicated to learn so that new users may rapidly become proficient at using it.
5. Coherence of interface: The system should be consistent in its design and operation so that users can easily predict how it will perform in various situations and scenarios.

Deployability:

I2P is available for various operating systems, including Windows, Linux, and macOS. With step-by-step instructions for each platform, it is simple to install and set up. I2P can also be installed on mobile devices using third-party applications, which makes it versatile. Additionally, I2P is designed to be compatible with other software and systems, making it easy to integrate into existing infrastructure. Here are some deployability criteria to be considered-

1. Easy installation across platforms: The system should be effortless to install across distinct platforms.
2. Smooth system compatibility: The system should be able to function accurately with different operating systems and software.
3. Minimal cost per User: The cost acquired by each user using the system should be negligible.
4. Mature: The system should be stable and mature, with a proven history of robust deployments and ongoing development and maintenance.
5. Open-source availability: The system should be available under an open-source license, with the source code freely accessible for modification and redistribution.

Security:

I2P places a high focus on security, using many levels of encryption and anonymity to safeguard the users' privacy. I2P employs end-to-end encryption, which ensures that data is only accessible to the sender and receiver. Additionally, I2P uses a distributed network design architecture, which helps to protect against attacks and data breaches. However, it is essential to note that no system can be a hundred percent secure, and users should take necessary precautions to protect their data. Here are some Security criteria to be considered-

1. Resilient to guessing attacks: The system should be able to resist attacks that involve the guessing of passcodes, passwords, encryption keys, or other sensitive information through an exhaustive search and other means.
2. Resistance to physical observation: The system should guard against attacks that involve observing the network traffic or hardware devices (routers and servers) to obtain access or steal sensitive data.
3. Protection against identity and location: The system should be designed not to compromise the user's identity and location against attacks.
4. Protection against protocol-level attacks: The system should protect the users against attacks that exploit vulnerabilities in the network protocols, such as Sybil attacks and Buffer overflow attacks.
5. No trusted third party: The system minimizes the reliance on trusted third parties for security and privacy.

	Usability					Deployability					Security				
	Memory-wise effortless	Scalable for users	Scalable for users	Ease of use acquisition	Coherence of interface	Easy installation across platforms	Smooth system compatibility	Minimal cost per User	Mature	Open-source availability	Resilient to guessing attacks	Resistance to physical observation	Protection against identity and location	Protection against protocol-level attacks	No trusted third party
I2P	●	●	◒	◒	◒	●	◒	●	◒	●	●	●	●	●	●
TOR	●	●	●	◒	◒	●	●	●	●	●	●	●	●	●	◒

Table 1: Evaluation Framework

The above table shows the evaluation framework considering usability, deployability, and security of two famous technologies used for anonymity and privacy over the internet, I2P and TOR. Evaluating I2P standalone would yield more results once compared with at least one other technology, so we decided on TOR.

Taking into consideration, memory-wise effortless, I2P received a full dot because the design makes use of minimal system resources and runs efficiently even on low-end devices; on the other hand, TOR also received a full dot because it utilizes minimal resources, is memory efficient and does not slow down user's system or the internet connection [6]. Now, scalable users, I2P is scalable and also handles a large number of users without compromising on performance. TOR also received a full dot because it is built to support many users and can handle a significant amount of traffic [7]. Now for easy adaptability, I2P provides some flexibility but may require technical knowledge to customize the user

experience fully. On the other hand, TOR received a full dot because it is flexible and allows users to customize their experience through various settings and configurations [6]. Now for ease of user acquisition, I2P received a half dot because while it has a user-friendly interface, it still may require some technical expertise to use it efficiently.
Moreover, TOR also received a half dot because it may be easy for some users but may require technical knowledge [7]. Finally, for the coherence of the interface, I2P received a half dot because the interface may not be as polished as other software, but it is consistent in design and operation [1]. Moreover, TOR also got a half dot for the same reason as I2P [8].
Coming to deployability and easy installation across platforms, I2P and Tor received a full dot because of the ease of installation and usage across multiple platforms, such as Windows, Linux, and Mac OS [9]. For d2, Smooth system compatibility, I2P received a half dot because while it may work well with various systems, there may be issues with specific configurations, and some users have reported difficulties with compatibility [10] [11]. While on the other hand, Tor received a full dot because it is more mature than I2P, and its initial development started in the mid-1990s [12]. Now for d3, Minimal cost per user, both I2P and TOR received full dot because they are open-source, free-to-use software. Now for d4, Mature, I2P received a half dot because it may have been around for many years, but it is still not as well established in comparison to TOR and is not as reliable or rampantly used. While on the other hand, TOR being a mature technology, received a full dot; it has been around for over a decade and is rampantly used and trusted. Finally, for d5, Open-source availability, I2P received a full dot because it is entirely open-source, which means that users can inspect the code, modify and contribute to the development of I2P. Also, TOR being open source too, received a full dot.
Coming to security, for Resilient to guessing attacks, both I2P and TOR earned a full dot because it uses robust encryption algorithms and techniques such as Perfect Forward Secrecy (PFS) and Diffie-Hellman (DH) to protect sensitive information and prevent brute-force attacks [9]. Now for Resistance to physical observation, I2P earned a full dot because of the use of encryption to protect network traffic and prevent eavesdropping. Also, it has measures in place to prevent attacks on hardware devices. For example, I2P nodes can be configured to function on devices without public IP addresses, which makes them challenging to locate and attack [1]. On the other hand, TOR also received a full dot as it has encryption in place for network protection and eavesdrop prevention. For protection against identity and location, Both I2P and TOR earned a full dot due to their garlic and onion routing, respectively [6]. For protection against protocol-level attacks, both I2P and TOR earned a full dot. I2P and TOR both have measures in place to protect against various types of attacks that exploit vulnerabilities in the network protocols; I2P makes use of a reputation system to identify and block malicious nodes that tries to disrupt the network [13], whereas TOR has a directory system to maintain a list of known relays and prevent Sybil attacks [8]. Finally, for No trusted party, again, both of them received full dots because they are decentralized systems that minimize reliance on trusted third parties, users communicate directly with each other, and no presence of central authority for monitoring and controlling the network.
After evaluating I2P and Tor utilizing the UDS criteria, it is plausible to conclude that both systems have benefits and drawbacks. One advantage of I2P is that it is entirely open-source, which means it has support from developers around the globe which may help I2P mature with time as a technology. It also offers excellent security against protocol-level assaults and has a low cost per user. It may, however, have compatibility concerns with some platforms and is still regarded as less mature than Tor. Tor, in contrast, has a more established and dependable network with excellent system compatibility and a good track record for privacy and anonymity protection. It is also easier for the typical person to operate. However, considering its reliance upon a limited number of centralized exit nodes and awareness of timing attacks, it might be less vulnerable to specific attacks.
I2P and Tor offer robust identity and location security, utilizing distributed systems that eliminate reliance on trusted third parties. Ultimately, user-specific requirements and priorities influence the decision between the two.

III. USER EXPERIENCE

A study by [6] evaluated the I2P user experience and found that while users were generally satisfied with the level of privacy and anonymity offered by the network, they also reported usability issues. They were related to the system's complexity and the network's slowness. Research suggests that improving the user-friendliness of the network could make it more accessible to more users.
In addition to user studies, expert reviews of I2P were also conducted. One such review by [7]

evaluated the privacy and anonymity features of I2P. It concluded that the network provides robust security and anonymity but also identified several usability issues related to installation and configuration problems. The review suggests that improving the user experience during installation could make I2P more accessible to more users.
Overall, the I2P user experience regarding privacy and anonymity is positive, but usability issues related to complexity and speed have been reported. Experts have also identified usability issues related to installation and configuration. Improving the usability of I2P can make it more accessible to more users.

IV. COGNITIVE WALKTHROUGH

I2P (Invisible Internet Project) is a mysterious arranged layer that permits secure and private communication over the web. Here are six core tasks [8] that can be performed on I2P:

1. Effectively Setup and configure I2P:
   The primary step is to introduce and design I2P on your PC. This incorporates downloading and introducing the I2P computer program, designing your browser to utilize the I2P intermediary, and arranging the I2P switch settings.
2. Effectively Browse I2P destinations:
   Once I2P is arranged, you can browse websites facilitated on the I2P organized namelessly. These websites are not perceptible on the standard web and can, as it were, be gotten to through the I2P arrangement.
3. Effectively Send and get mysterious mail:
   Through its coordinates mail client, I2P too offers mysterious email communication. This client permits you to send and get emails without unveiling your personality or IP address.
4. Effectively Have your claim location on I2P:
   You construct an I2P location and set it up to function on the I2P organize in case you need to have your claim mysterious location on the I2P arrange. This incorporates setting up security shields, building and arranging the site and advancing the site among I2P clients.
5. Effectively Take part in I2P communities:
   I2P offers an assortment of gatherings and communities where clients may communicate and exchange data. You will sign up for these communities, take some of the discussions, and post your possessed substance.
6. Successfully Use I2P for record sharing:
   You can share files with other I2P clients utilizing mysterious record sharing, which I2P backs. This prevents you from disclosing your character or IP address. To share records over the I2P arrange, users can utilize an I2P record-sharing program like "iMule."

Here are the eight guidelines [9] for performing a cognitive walkthrough on I2P:

1. The client ought to have the Control and Opportunity:
   Clients ought to be able to choose the programs and administrations they need to utilize and control their I2P settings and inclinations. Moreover, they must be able to change their I2P inclinations and settings rapidly.
2. Client encounters must be Consistency, and Standards:
   All I2P applications and administrations need to have a uniform see and feel. Furthermore, it should utilize a standardized lexicon and naming to form it essential for consumers to comprehend.
3. The client ought to be able to identify the Error:
   If there are any mistakes or issues, I2P needs to offer clear mistake messages and allow clients criticism. Furthermore, it ought to join shields against client mistakes, such as demands for affirmation sometime recently carrying out pivotal errands.
4. The client ought to be able to Acknowledgment over Recall:
   I2P should be made so clients can rapidly distinguish what they seek without memorizing detailed data. To demonstrate its various assignments, the I2P switch interface, for occurrence, ought to utilize clear and reasonable symbols and names.
5. Clients' ought to be comfortable with the terminology utilized in any interface exchanges or documentation:
   I2P's task-permitting capabilities got to be versatile and viable. It should empower clients to personalize the interface to meet their needs and offer accessible routes or hotkeys for habitually utilized highlights.
6. Clients' ought to be adequately comfortable with the interface to continue utilizing it:
   I2P ought to have a simple, aesthetically satisfying, and instinctive plan. It needs to dodge cluttered client interfacing and offer an easy-to-use interface.
7. Offer assistance and documentation:
   In arrange to help clients in carrying out assignments and investigating issues, I2P ought to offer clear and basic documentation and help apparatuses. These can be client gatherings, FAQs, and instructional exercises.

8. Client Input and Emphasis:
   To improve the client encounter ceaselessly, I2P should advance client criticism and iteration. This might involve getting client input through overviews or client testing, at that point, executing that input to upgrade the program and administrations.

Detailed cognitive walkthrough using the four primary core tasks and eight guidelines for the I2P software:

Task 1:

1. The client ought to have the Control and Opportunity:
   The I2P software allows users to choose which applications and services to use and customize their I2P settings and preferences. The router interface provides clear and easy-to-use settings for users to configure their network preferences.
2. Client encounters must be Consistency, and Standards:
   The I2P website has clear and consistent instructions for downloading and installing the software.
   The software's consistent design and layout may vary depending on the application or service bug used.
3. The client ought to be able to identify the Error:
   The I2P website provides clear instructions for troubleshooting common installation issues.
   The software provides clear error messages if the installation fails and provides guidance on resolving any issues.
4. The client ought to be able to Acknowledgement over Recall:
   The I2P website has a clear and intuitive layout, with links to download and install the software easily visible.
   The software has a straightforward installation wizard with step-by-step instructions for users.
5. Clients' ought to be comfortable with the terminology utilized in any interface exchanges or documentation:
   The recommendation to use more descriptive and intuitive labels for options and settings will help ensure that the language and terminology used in I2P match the real world.
   Clients' ought to be adequately comfortable with the interface to continue utilizing it:
6. The I2P software has a minimalist design, with only essential information and options presented during installation. The router interface has shortcuts or hotkeys for frequently used functions and allows users to customize the interface to suit their needs to some extent.
7. Offer assistance and documentation.
   The I2P website should provide clear and concise documentation on downloading, installing, and configuring I2P.
   The software should have built-in help resources, such as tutorials and FAQs, to assist users with common issues.
8. Client Input and Emphasis:
   The I2P community should encourage user feedback and suggestions for improving the software and services.
   The development team should continually iterate and improve the software based on user feedback and suggestions.

Task 2:

1. The client ought to have the Control and Opportunity:
   The user has control over their I2P network connection. They can change router parameters such as bandwidth use and network interface setup through the router console.
2. Client encounters must be Consistency, and Standards:
   All I2P apps and services follow the same network connection procedure. The I2P router only must be started once to connect to the I2P network automatically. The user can access many I2P applications and services once connected.
3. The client ought to be able to identify the Error:
   I2P has safeguards in place to stop connection issues. For instance, I2P will display an error notice and information on how to fix the problem if the user's network interface setup is incorrect. In addition, I2P has a connection wizard to help users set up connections.
4. The client ought to be able to Acknowledgement over Recall:
   The I2P network connection process is a simple one that consumers may easily understand. The I2P router only must be started once to connect to the I2P network automatically. The user can access several I2P applications and services once connected.
5. Clients'' ought to be comfortable with the terminology utilized in any interface exchanges or documentation:
   The method users can use to join the I2P network is flexible and effective. The software has a connection wizard to help users establish connections, and the router console lets them

change the router and network interface configuration settings.

6. Clients' ought to be adequately comfortable with the interface to continue utilizing it:
   The I2P interface may vary from user to user.
7. Offer assistance and documentation.
   I2P offers instructions and support materials to help users connect to the network. The program has a connection wizard and extensive online documentation covering everything from router installation to typical problems.
8. Client Input and Emphasis:
   I2P offers users several alternatives to give feedback and get assistance with any problems they run into. Users can post queries in the help forum on the I2P website and get answers from other community members.

Task 3:

1. The client ought to have the Control and Opportunity:
   When utilizing the I2P program, users have some discretion and freedom, although it is constrained. Users can change settings and preferences, but there is little help for going back and undoing changes if necessary.
2. Client encounters must be Consistency, and Standards:
   The I2P software's inconsistent behavior and design make it challenging for users to get the most out of the interface.
3. The client ought to be able to identify the Error:
   Users may find recognizing and handling potential problems challenging because the I2P software only sometimes prevents errors or provides clear error signals.
4. The client ought to be able to Acknowledgement over Recall:
   The I2P software does, in part, rely on human memory and recall since, to operate it correctly, users must be able to memorize specific configuration options and jargon.
5. Clients'' ought to be comfortable with the terminology utilized in any interface exchanges or documentation:
   Users may need help comprehending the meaning and function of some functions since the language and terminology used in the I2P software and documentation frequently do not correspond to the real world.
6. Clients' ought to be adequately comfortable with the interface to continue utilizing it:
   Users should feel at ease and confident using the anonymous email interface, which is meant to be straightforward, intuitive, and user-friendly.
7. Offer assistance and documentation.
   Although some help and documentation are available to users, its scope is constrained, and it only sometimes offers precise instructions on how to use the product efficiently.
8. Client Input and Emphasis:
   Users can access tools like the bug tracker and help forum on the I2P website to report issues and get assistance. How receptive the development team is to user suggestions and problems still need to be made evident.

Task 4:

1. The client ought to have the Control and Opportunity:
   Users have some control and freedom while using the I2P software, but it is limited. Users can adjust settings and configurations, but there is limited guidance on undoing or correcting actions if needed.
2. Client encounters must be Consistency, and Standards:
   The process for hosting a site on I2P is consistent across all I2P services and applications. The user can navigate the process easily and understand the terminology used.
3. The client ought to be able to identify the Error:
   The user gets clear error messages if they encounter problems while hosting their site on I2P. Before performing critical actions, the system should also have mechanisms to prevent user errors, such as confirmation prompts

.

4. The client ought to be able to Acknowledgement over Recall:
   The process for hosting a site on I2P is designed in a way that makes it easy for the user to recognize what they are looking for without having to remember specific details or commands. For example, the I2P site hosting interface should use simple and intuitive icons and labels to indicate its functions.
5. Clients' ought to be comfortable with the terminology utilized in any interface exchanges or documentation:
   The terminology used in the site hosting process is easy to understand and consistent with standard web hosting terminology. Any documentation or help resources should be clear and concise.
6. Clients' ought to be adequately comfortable with the interface to continue utilizing it:

The terminology used in the site hosting process is easy to understand and consistent with standard web hosting terminology.

7. Offer assistance and documentation.
   The user is provided with clear documentation and helpful resources on how to host their site on I2P. This could include tutorials, FAQs, and user forums.
8. Client Input and Emphasis:
   The user is encouraged to provide feedback on their experience hosting their site on I2P, which could be used to improve the process.

V. ETHICAL CONSIDERATION

There are different moral issues raised by unknown frameworks like Pinnacle and I2P that should be considered. One of the primary concerns is the potential for these technologies to facilitate illegal activity. In some research, a combination of network traffic analysis and digital techniques is used to identify and analyze I2P traffic association with illegal activities, which includes drug trafficking, hacking, and child pornography. I2P was found to be being used for a range of criminal activities [9].

VI. CONCLUSION

To conclude, the Systemization of Knowledge (SoK) on the Invisible Internet Project (I2P) has comprehensively evaluated I2P's strengths and weaknesses in providing secure and anonymous online communication. The UDS Evaluation Framework of I2P and its Cognitive Walkthrough has provided a holistic evaluation of I2P's security, usability, and deployability. I2P offers a high degree of security and privacy for its users. However, its usability may require technical knowledge, and its deployability may need improvement to achieve broader adoption, considering it is less mature than TOR.

Given the increasing importance of anonymous communication systems, I2P provides a valuable solution for situations where anonymity is crucial. However, its maturity might positively change its usability and deployability. However nevertheless, future research on I2P should be considered to identify the issues and further evaluate its effectiveness in providing secure, usable, and private communication over the Internet. In conclusion, I2P's potential to provide secure and anonymous online communication is significant, and its development and adoption should continue to be supported.

VII. REFERENCES

[1] "I2P," [Online]. Available: https://geti2p.net/en/.

[2] S. Kumar, "Design and implementation of anonymous communication system using i2p," International Journal of Computer Science and Mobile Computing, 5(9), 77-87, 2016.

[3] K. Murphy, " A comprehensive review of the invisible Internet project," Journal of Computer Science and Engineering, 2(2), 51-56, 2020.

[4] A. &. K. S. J. Jøsang, "The invisible internet project: anonymous communication for everybody," In Computer Security--ESORICS 2018 (pp. 655-673). Springer International Publishing., 2018.

[5] C. H. C. v. O. F. S. Joseph Bonneau, "The quest to replace passwords: a framework for comparative evaluation of Web authentication schemes," 15 JJ Thomson Avenue Cambridge CB3 0FD United Kingdom, 2012.

[6] B. C. A. F. Shirazi, "A Survey on Tor and I2P," IARIA, 2014.

[7] M. K. U. P. M. Z. I. A. N. D. Afzaal Ali, "TOR vs I2P: A Comparative Study," IEEE, 2016.

[8] [Online]. Available: https://www.torproject.org/.

[9] B. Z. a. R. A. Haraty, "I2P Data Communication System," IARIA, 2011.

[10] [Online]. Available: https://www.reddit.com/r/i2p/.

[11] [Online]. Available: https://i2pforum.net/.

[12] [Online]. Available: https://en.wikipedia.org/wiki/Tor_(network)/.

[13] K. A. &. D. Gaastra, "Blockchain-based Sybil Attack Mitigation: A Case Study of the I2P Network," University of Amsterdam, 2018.

[14] C. Z. Y. &. C. S. Yao, "Understanding the User Experience of the Tor and I2P Anonymous Communication Networks.," Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 2362-2373. doi: 10.1145/2858036.2858311., 2016.

[15] V. H. J. &. M. C. Mavroudis, " Security and Usability Review of Tor and its Variants.," Proceedings of the 2017 Symposium on Usable Privacy and Security (SOUPS 2017), 211-226. doi: 10.1145/3136826.3136841., 2017.

[16] O. Husain, "What Is I2P? How Does It Work? And How to Use It Safely?," ProPrivacy, 2022.

[17] C. &. P. P. Lewis, "Cognitive walkthroughs: A method for theory-based evaluation of user interfaces," Proceedings of the SIGCHI conference on Human factors in computing systems, 105-112, 1991.

[18] M. W. &. W. H. Behnam Bazli, "The dark side of I2P, a forensic analysis case study," Systems Science & Control Engineering, 5:1, 278-286, DOI: 10.1080/21642583.2017.1331770, 2017.