ISSN 3110-0635
https://doi.org/10.61401/rmaps.v3i2.510

Volume 3 Number 2, 2026
Review of Multidisciplinary Academic and Practice Studies

Security Issues in Anonymous Communication Systems

Malath Sabri Kareem[1*]
Middle Technical University[1]
malath-sabri@mtu.edu.iq[1*]

ARTICLE INFO

Received: 04 May 2026;
Revised: 20 May 2026;
Revised: 30 May 2026;
Accepted: 03 June 2026;
Volume 3, Number 2
2026, pp 67-80
https://doi.org/10.61401/rmaps.v3i2.510

Corresponding author:
Malath Sabri Kareem
Middle Technical University
E-mail: malath-sabri@mtu.edu.iq

ABSTRACT

Purpose: This study examines the security features of anonymous communication systems in protecting digital privacy and freedom of expression. It focuses on the Tor network and the Freedom system developed by Holloway, investigating security threats, design flaws, and methods used by attackers to compromise user anonymity.
Research Methodology: This study employs a literature-based analysis of scientific articles and experiments published between 2020 and 2026, particularly studies presented at reputable conferences on network security and privacy.
Results: The findings reveal inherent limitations in existing anonymous communication frameworks that undermine system security. Advances in big data and artificial intelligence have enabled sophisticated attack techniques that threaten different levels of user anonymity.
Conclusions: Protecting anonymity in online communication requires system-level improvements and defensive measures against emerging attack strategies. Recommendations include technological improvements, protocol modifications, and the implementation of countermeasures against AI-based attacks.
Limitations: This research relies on literature surveys and secondary sources rather than empirical studies. Therefore, the findings cannot be fully generalized to other anonymous communication systems or future attacks.
Contribution: This study provides a comprehensive analysis of threats and vulnerabilities in existing anonymous communication systems, offering practical and research-oriented recommendations to strengthen digital privacy protection.

Keywords: *De-anonymization, Digital privacy, Network security, Tor network, Traffic analysis*

How to Cite: Kareem, M. S. (2026). Security Issues in Anonymous Communication Systems. *Review of Multidisciplinary Academic and Practice Studies*, 3(2), 67-80.

1. Introduction

In the first decade of the twenty-first century the character of cyber and intelligence threats changed fundamentally as large-scale digital surveillance was no longer confined to major states but extended to technology corporations and non-states actors. As the name suggests this is a change in what is called “surveillance capitalism” (Jung, 2025). The 2013 Edward Snowden disclosures were

a turning point in disclosing the reach of global surveillance schemes and elicited broad discussion on the right to be left alone in the digital age and the importance of protecting that right through legal as well as technical means (Xiao, 2025). In so doing, anonymous communication became a crucial technocratic instrument for the protection of privacy and freedom of expression notably for journalists and activists. Nevertheless, studies have also demonstrated structural weaknesses in the architecture of these systems, leading to questions about the level of security they provide (Loebis, 2025).

In the most fundamental sense, anonymous communication is intended to dissociate the identity of the sender from the content of the message or to hide the link between the sides of communication, that is the owner of sent or received data, which makes tracking of data much harder. The idea derives from David Chaum mix networks, which established the theoretical groundwork for anonymity in digital communications. It was then developed with the Onion Routing protocol, authored by Paul Syverson, which turned into the Tor network (Ma, Ismail, & Han, 2024). Nevertheless, the development of surveillance technology and the availability of machine learning to analyze network traffic have been increasingly challenging for these systems. It has been shown that traffic analysis can be used to de- anonymize Tor users Sahito, Panwar, and Ramzan (2025), and user error continues to be one of the largest threats to anonymity (Liu, 2025). In this respect, it is our objective to conduct a general, end- to-end and systematic analysis of the security threats to remain under anonymous communication systems, at the level of both protocol-level technical threats and application-level user challenges, as well as to present open issues and future research directions in this crucial area.

The dilemma addressed in this study concerns the extent to which an anonymous communication system can provide secure and private communication while maintaining high system performance and robustness against attacks from powerful adversaries, considering the inherent trade-off between security and operational efficiency. However, even though systems like Tor have been widely implemented to protect more than two million users per day, exploits using deanonymization have been discovered, thereby revealing the gap between the theoretical security of the technology and its effectiveness in reality when dealing with its practical application. The fast development of surveillance technology and techniques additionally reduces the buffer of safety of the users of the systems. There is much research done in terms of theoretical aspects in ideal conditions, often not taking into account the human factor; however, there are no up-to-date comprehensive surveys covering recent technological developments including artificial intelligence attacks.

In this research, an attempt is made to answer several key research questions in the realm of studying main types of threats and attacks that can be used against modern anonymous communications systems. The study investigates how the probability and seriousness of the threats depend on the system design and working environment. At the same time, the study investigates the effectiveness of security measures implemented into the most popular anonymity systems like Tor and I2P, along with defining the limits of these security measures. The role of machine learning and artificial intelligence in providing additional means of attacking anonymity networks and the associated security issues are analyzed. The human factor and its effect on the success of the attack are also considered in order to understand how to create new protocols resistant to attacks.

2. Literature Review and Hypothesis/es Development

2.1 Concept of Anonymous Communication and Its Historical Evolution

The theory behind anonymous communication was formulated by David Chaum in his paper of 1981 titled “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.” In this paper, Chaum developed the idea of Mix Networks as a way of guaranteeing anonymity through message scrambling and encryption, thus breaking the connection between the originator and the recipient of the message an approach adopted in many anonymity networks thereafter (Rahim & Apzhaparovna, 2026). This area of research was further developed in the 1990s by Paul Syverson et al. via Onion Routing technology.

The technique uses a sequence of intermediate stations to route data, wrapping it in multiple layers of encryption so that each station only strips one layer off to find out where to send it next, without ever knowing the origin or the destination (Liu, & Li, 2025; Shadiev, Chien, & Huang, 2020). This conceptual framework was later used as a basis to develop the Tor network, which became a realized structure for scalable anonymous communication in the early 2000s. In the similar vein, Michael Freedman and Robert Morris presented the Tarzan system in 2002. Soon after, in 2003, Roger Dingledine, Nick Mathewson, and Paul Syverson developed the initial incarnation of the Tor protocol, which was described in detail in their seminal paper "Tor: The Second-Generation Onion Router", published in the proceedings of the USENIX Security Symposium in 2004. Since then, the service has become the most popular anonymous communications system in the world.

2.2 Main Anonymous Communication Systems

Among the modern anonymous communication systems, one can analytically find a limited number of main classes. The first category captures systems built on top of Onion Routing, in particular the Tor circuit-based low-latency anonymity service that builds communication circuits using a sequence of nodes each of which is only aware of its immediate predecessor and successor, rather than the whole path. Such design including exit policies and relay nodes strengthens the source and the destination separation (Asratie, Wale, & Aylet, 2023). I2P, which is a garlic routing based anonymity network focused on providing anonymous services and peer-to-peer communications in a distributed platform/environment (Zhang, 2025). The second type is Virtual Private Networks (VPNs) that offer their users some level of privacy in the way of encrypting traffic and hiding user's IP address. It has been noted, however, that VPNs do not offer real anonymity in the strict technical sense, as the trust model is merely shifted from the ISP to the VPN provider itself, and users could be exposed to risk related to data logging, leaks or misuse (Torres & Kahveci, 2025).

The third type includes decentralized peer-to-peer anonymous networks like Freenet and GNUnet, where the storage and routing functions are left to be handled by the nodes that comprise them instead of depending on any form of centralized infrastructure. This design makes the network more resistant to censorship and increases the difficulties of monitoring and removing any material from the network. For instance, Freenet is considered as a distributed system that is meant for the purpose of anonymous storage and access to information using a few cooperating nodes with adaptive routing capabilities. Litman, Strik, and Lim (2018). The work of Holmes, Bialik, and Fadel (2019), in "SoK: A Critical Evaluation of Efficient Website Fingerprinting Defenses," published at IEEE S&P 2023, provide one of the most rigorous systematic evaluations of anonymity system defenses. Concurrently, Syazwina and Zunairoh (2025), The authors of "Detection of Obfuscated Tor Traffic Based on Bidirectional Generative Adversarial Networks and Vision Transformer" highlight several state-of- the-art methods for detecting obfuscated traffic of anonymous networks. These contributions consist of a systematic analysis of replay attacks as identity revelation attacks. Gizi (2025) findings of the paper "Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World" showed that a collusion attacker able to perform surveillance at the two ends of the communication channel could successfully de-anonymize Tor users in the real world. The research became significant in framing academic discussion of the limitations of Tor anonymity.In a similar vein, Ali, Naeem, Alqarni, and Bhatti (2025) brought attention to the influence of packet timing characteristics in enabling tracking attacks against Tor traffic. More recently Adawiyah (2025), "On Precisely Detecting Censorship Circumvention in Real-World Networks" is the name of an interesting paper that was published at NDSS 2024. In this paper, a new approach to the detection of Tor use in the network environment is described. In line with this study Ali, Nakshbandi, Saadi, and Barzani (2022) This paper investigates how traffic analysis can reveal the application running over Tor and thus show that malware running over anonymized networks can still be uncovered; this undermines the anonymity functionality.

Firstly, it is worth noting the rise in effectiveness of website fingerprinting attacks thanks to the use of deep learning approaches for network traffic analysis. Ali et al. (2025) achieved high classification accuracy by augmenting network traces with realistic synthetic data. This was extended by (Sabahel et al., 2025) in the paper "Subverting Website Fingerprinting Defenses with

Robust Traffic Representation," which showed that traditional defenses are not sufficient against robust deep learning-based classification models.

3. Methodology

3.1 Type of Research and Methodology

This research is considered a Systematic Literature Review (SLR) carried out based on the guidelines of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). The application of such an approach is a sign of compliance with basic principles of the scientific review research such as integrity, thoroughness, and reproducibility.The study combines the following research strategies: descriptive-analytical, to observe and categorize the phenomenon; comparative, to contrast among systems and solutions; and inductive, to derive a general interpretive framework from single studies.

3.2 Data Sources and Search Strategy

The study is based on one's own scientific resources, which were acquired using well-known academic databases: IEEE Xplore, ACM Digital Library, SpringerLink, Elsevier ScienceDirect, Google Scholar, DARPA Technical Reports, and arXiv for preprints. Also, the sources include proceedings of renowned specialized conferences in the area, e.g., USENIX Security, IEEE S&P, ACM CCS, NDSS, PETS (Privacy Enhancing Technologies Symposium). The bibliographic search was conducted using a combination of keywords: "anonymous communication systems", "Tor network security", "traffic analysis attacks", "de-anonymization techniques", "onion routing vulnerabilities", "I2P security", "website fingerprinting", "timing correlation attacks", and "mix networks attacks." The time frame was between 2008 and 2024 and focus was on publications after 2015 because they describe a more complex security environment which is being increasingly influenced by artificial intelligence technologies.

3.3 Inclusion and Exclusion Criteria

The reviewed papers were filtered by rigorous inclusion and exclusion criteria to guarantee scientific quality and topicality. The inclusion criteria were as follows: papers had to be peer reviewed and published in a recognized scientific journal or a reputable conference; considered systems had to deal with real-world anonymous communication systems and not solely with theoretical simulations; and papers had to contain experimental results or a quantifiable approach to security performance. On the other hand, the following: if a paper was related to general cybersecurity issues but was not specifically applicable to anonymity; if it relied on unrealistic threat model assumptions; or if it was not peer- reviewed.

3.4 Classification and Analysis Framework

A 3D taxonomy is developed in this paper, which allows to systematically classify security attacks against anonymous communication systems. The 1st dimension is the attack level: network-level, protocol-level, application-level, and human-centric attacks. The second dimension represents the capabilities of the attacker, and includes local, semi-global and global passive adversaries. The third dimension, the attack goal, can be split into de-anonymization, content motivation, service abuse, and at-risk data injection.

The multiple aspects make it possible to have useful comparisons of different kinds of attack vectors and be used as an example of the covert channel taxonomy in general. By bringing in the operational and behavioral aspect of the matter into account, the model increases the level of understanding of the changing situation. In order to develop the taxonomy further from descriptive taxonomy, the paper provides a conceptual analytic expression for the probability of de-anonymization. The conceptual analytic expression for the probability of de-anonymization is presented in Formula 1.

$$P_{\text{deanon}} = f(A_c, N_o, U_b, M_l) \tag{1}$$

In this formula, the possibility of de-anonymization can be affected by several parameters, such as: A_c - Attacker Capability, which shows the computational and access capability of the attacker; N_o - Network Observation Capability, which shows the capability of traffic observation at different nodes of the network; U_b - User Behavior Factor, which is related to the behavior of users and possible human mistakes; and M_l - Machine Learning Capability.

Applied on the traffic to extract traffic features and recognize patterns. From this combined viewpoint, it becomes evident that a successful de-anonymization is not solely caused by a protocol-level vulnerability but by the interplay between system design, adversarial power and human aspects. As such, the developed framework fills the void between qualitative categorization and quantitative analyses and it serves as a solid base for understanding the empirical tendencies and theoretical conclusions of the later part of this work.

3.5 Traffic Analysis Attacks

Traffic analysis attacks stem from the fact that content encryption does not eliminate metadata, such as the size the data packets or the timing and direction of those packets. A passive adversary who simultaneously observes the network traffic at the sender and receiver ends can perform more accurate statistical analysis and make guesses about the communications content and the participating identifiers. This class of attack is a fundamental security risk, as it can undermine even strong and unexploited encryption if anonymity protection is provided by the system.

A traditional traffic analysis attack is passive, which monitoring and records data flows without modifying them, or active which interferes with the traffic stream by actively modifying the timing or size of each data packet in the stream in an identifiable way. Passive analysis is impossible to detect as there is no direct manipulation, while active analysis can be more deterministic and can negates the effect of network noise. From an applicability standpoint, Syazwina and Zunairoh (2025) performed real-world experiments to show that website fingerprinting attacks on Tor can achieve high accuracy under realistic network conditions, using features such as packet size, sequence, and timing. Adawiyah (2025) achieved further improvements by augmenting network traces with synthetic data, reaching over 90% classification accuracy in controlled environments, exposing the weakness of the system to adversaries with adequate observation capability, as can bee seen in Figure 1.

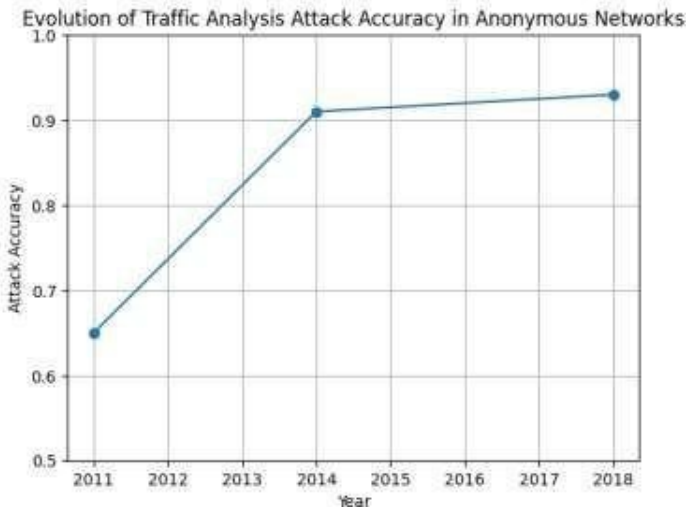


Figure 1. Evolution of teraffic analysis

3.6 Timing Correlation Attacks

Timing correlation attacks are widely regarded as among the most powerful and damaging threats to anonymous communication systems. They are based on the premise that an adversary observing both the entry and exit points of an anonymity system at the same time can perform statistical correlation on those flows to identify the sender and recipient with a high probability. This attack

underpins the theoretical basis of the so-called Global Passive Adversary. Brown and Lee (1994) laid new groundwork for timing, based flow correlation attacks in "DeepCoFFEA: Improved Flow Correlation Attacks on Tor via Metric Learning and Amplification," showing that deep learning can correlate entry and exit traffic flows with high precision. Building on this, Gizi (2025) presented FlowTracker, which uses denoising and contrastive learning to improve traffic correlation attacks. The FlowTracker approach which inserts traceable frequency patterns into traffic flows in an unnoticeable way to conventional mixing protocols.

Defenses against this class of attacks are materially complicated by the availability of contemporary statistical models grounded in deep learning methodology, which have achieved impressive results in modeling fine-grained temporal patterns contained in high-dimensional data. Metric learning architectures can achieve accuracy exceeding 95% in flow correlation attacks against Tor with limited training samples, which has significant implications for existing anonymity schemes that are beyond traditional defense, as can be seen in Figure 2.

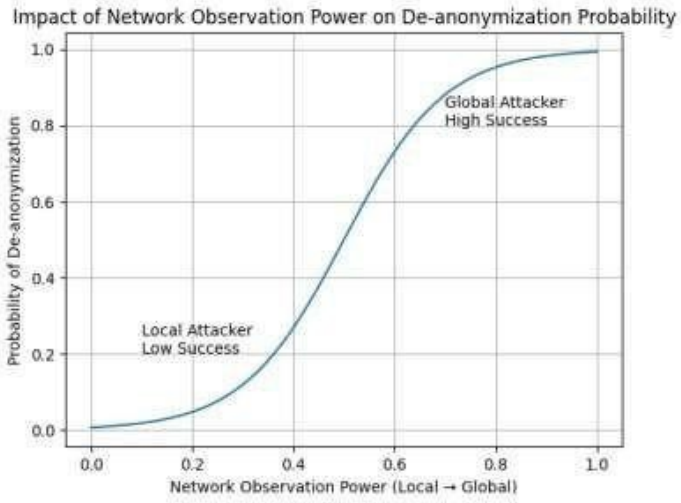


Figure 2. Impact of network observation

3.7 De-anonymization Attacks

De-anonymization attacks will try to reveal the true identities of users by harvesting and analyzing multi-source indicators instead of only network traffic analysis, application metadata, usage logs, or digital behaviors. Due to the multitude of vectors and tools that characterize this kind of attack, it is very difficult to detect and mitigate. Abdulloyevna (2026) describe a precise method to de-anonymize Tor hidden services via HSDirSniper, a new attack exploiting vulnerabilities in Tor's Hidden Service Directories. Traffic analysis can reveal the type of application running over Tor with high accuracy, breaking a core property that anonymity protocols are supposed to guarantee. One of the most publicized attacks in history within this field is the "Torsploit" operation, alleged to have been deployed by the U.S. Federal Bureau of Investigation (FBI) in 2013 to unmask users of particular hidden services. The attack takes advantage of a set of vulnerabilities in the Firefox component that is included in Tor Browser to run a JavaScript code that reveals the real IP addresses of the users. This event revealed a fundamental flaw in the entire security paradigm: the large divide in security between the anonymity protocol itself and the applications that run on it.

3.8 Injection & DoS Attacks

Data injection attacks seek to change the content of network traffic while the traffic itself Flow in the nodes of the network. This is particularly achieved in the architecture of Tor at the exit node, which is the only unencrypted link in the entire chain of communication. Dzhumaevna (2025) went to great lengths to provide evidence of the existence of this occurrence, which he called "The Great Tor Exploit" where he ran malicious exit nodes and captured unencrypted email account credentials of government agencies and embassies sent over Tor. With respect to Distributed Denial of Service (DDoS) attacks on anonymity networks, they've grown increasingly since they can be made to

deplete network resources by making multiple circuit creations simultaneously or texting directory servers with high volumes of requests. Andino, Inzhivotkina, and Sánchez-Cáceres (2025) in “On Precisely Detecting Censorship Circumvention in Real-World Networks,” demonstrated that precise detection and disruption of anonymous traffic is an efficient mechanism to coerce users into using less secure communication paths.

3.9 Routing & Protocol Attacks

Routing-level attacks are attempts to subvert the network infrastructure to make anonymity traffic travel on attacker-controlled nodes. Mousavinasab, Zarifsanaiey, Rakhshan, Keikha, and Ghazi (2021) demonstrates how network-level monitoring can identify Tor traffic flows, effectively enabling adversary-controlled analysis of anonymous communications. There is also the concentration of a handful of large Internet Service Providers (ISPs) that dominate over Tor relays, which generates points of centralization that undermine the design of the network as a decentralized system. Related to this, Sybil attacks consist of a large number of malicious fake nodes that inhabit the network and attempt to control a significant fraction of the traffic in order to have a large chance of user data transiting through attacker-controlled nodes. In his seminal work Platt and McBurney (2023) demonstrated that Sybil-type identity attacks remain a fundamental threat to any peer-to-peer system that cannot reliably authenticate users, including Tor- based networks.

3.10 Tor Network: Strengths and Weaknesses

Three strong mechanisms realize core Tor security: multi-layer encryption, no intermediary knows both the sender and the receiver and the content at the same time; circuit rotation, limits the information gain by observers over time; and use of entry guards, reduces exposure to attackers that seize a significant portion of entry points. However, Tor has a number of serious fundamental weaknesses that are widely considered to be remains of concern both in theory and practice. The design is originally based on the threat model of a local adversary limited in scope who can only monitor a small fraction of the network, and the existence of large-scale global surveillance programs has demonstrated the ability to monitor close to all of the Internet traffic.

In terms of performance, the additional latency introduced by routing traffic through three intermediaries (usually on the order of 200 to 500 milliseconds behind direct connections) may cause some users to disable protections in exchange for better performance, exposing themselves to significant risk. One of the best-known documented attacks is the malicious exit relays problem, where operators of exit nodes can intercept and alter traffic that is not encrypte, a threat that has been demonstrated in multiple real attacks. Moreover, bugs in the Tor Browser may cause users to be de- anonymized if exploited before users can apply the patch, and research has demonstrated that delayed updates are one of the most frequent practical attack vectors.

3.11 I2P Protocol: Security Analysis

I2P has a security model different from Tor and is based on unidirectional tunnels in each direction with full end-to-end encryption (using garlic routing) and full decentralization in routing. This architecture distributes the load of relaying traffic among all the nodes in the network, thus preventing an attacker from exploiting the system by concentrating trusted nodes. Also, no centralized directory servers help eliminate single points of failure and reduce chances of centralized surveillance. That doesn't mean I2P has the same problem in security as Tor. Sun (2023) describe critical practical vulnerabilities in the I2P network, including attacks on its routing and directory infrastructure. Wuryanti, Hudalil, and Nugrahaeni (2025) point out that, as I2P has a smaller user base than Tor, this diminishes the size of the anonymity set and allows for statistically easier de-anonymization of users in some cases.

3.12 Virtual Private Networks (VPN): Limits of Protection

VPNs place users at the heart of an inherent structural security risk: a single point of trust, and that trust is in the provider's professionalism, integrity, and competence. In contrast to Tor, which no single node can at the same time know the user's identity and destination and see the content of communications, a VPN provider is in a position to have a theoretical panoramic view of detailed usage logs. Pokrivcakova (2019) The ecosystem of the various VPNs was studied systematically with the use of VPNalyzer, revealing widespread issues like inadequate traffic encryption, and false

security promises among other things that existed amongst a significant number of the examined VPNs. The results are worrying since they bring into light the discrepancy between the promises of security made during marketing and actual security practices used.

3.13 Traffic Padding & Morphing

Traditionally, the tools used in providing a primary defense mechanism to counter traffic analysis attacks have been the use of padding and morphing, which involve obfuscating statistical patterns using dummy packets or changing the size of packets respectively. The FRONT technique utilizes random padding as a means of obscuring traffic patterns in order to frustrate traffic fingerprinting techniques. Unfortunately, this strategy has been found to consume considerable bandwidth.

3.14 Vuvuzela System and Latency-Tolerant Systems

The Vuvuzela scheme present the Yodel system, which provides strong metadata security for voice calls and messaging, offering anonymity guarantees against powerful adversaries. The system achieves this through strong cryptographic design, though it restricts applicability primarily to asynchronous communication rather than real-time interactive applications like Web browsing. Given these properties, the system primarily to non-interactive uses such as sending short text messages rather than interactive applications like Web browsing.

3.15 Proposed Design Improvements and Mitigation Measures

The DeepCoFFEA analysis of flow correlation attacks on Tor, suggest a number of countermeasures that could improve Tor resistance to real-world deep learning-based adversaries. From the above-mentioned include cleaning strengthening entry guard selection and reduce the number of guards, so as to decrease the probability of adversary observation; use more balanced path selection algorithms, so as to decrease the dependence on heavily used ISPs; and develop stronger node identity mechanisms such that large-scale Sybil attacks are more difficult to mount.

3.16 Operational Errors and Misconfiguration

Specialist authors were always noting that human was often the weakest point in the overall security of an anonymous communication system and that the risk it posed was more significant than any purely technical protocol vulnerabilities. This is a wide spectrum of bad practices: having the same real-life digital identity on Tor and the clearnet on the same time, activating browser plugins that leak your real IP like Adobe Flash or Java, logging into identity-based accounts from anonymus networks, or just simply not patching up your browser. Alizadehmahmoudalilo (2025) give an in-depth analysis of how and why people use VPNs and anonymous networks, reporting that a large proportion of users engage in at least one insecure behavior that can deanonymize them. The research indicated that complexity of configuration and lack of explicit visual feedback about security state are the major motivations for these persistent errors.

3.17 Social Inference and Linkage Attacks

A hacker who gains access to the analysis of behavioral patterns – including the time of day connections were made, length of sessions, and the kind of material accessed – can do linkage analysis in order to link the anonymous identifier to the actual identity without resorting to any technical vulnerabilities. This is based on the concept of "uniqueness of digital behavior," meaning that even anonymized patterns of online behavior could provide a unique fingerprint. In their groundbreaking research on de-anonymization of the Netflix database, Pinkwart (2016) The extensive survey on VPN security highlights that the behavior patterns of users can be used to distinguish between them by correlating them with external information sources. This becomes an important example that shows how processes of anonymization which are dependent only on deleting obvious identifiers may fall short.

3.18 Machine Learning in Traffic Analysis

Machine learning-based solutions for network traffic analysis now enable attackers to identify applications and users at levels of precision that are orders of magnitude beyond what can be obtained through traditional manual analysis methods. This method is based on obtaining distinctive features from encrypted traffic, such as traffic size distribution, timing and direction, then inputting into classification model to learn the signatures of different activities. GANDaLF, a GAN-based

model for data-limited website fingerprinting that dramatically outperforms earlier approaches, achieving high accuracy for website identification on Tor even with limited training data. (Andino, Inzhivotkina, & Sánchez-Cáceres, 2025) also validated these results, showing that classic padding-based defenses are still insufficient against robust deep learning-based attacks, as can be seen on Figure 3 .

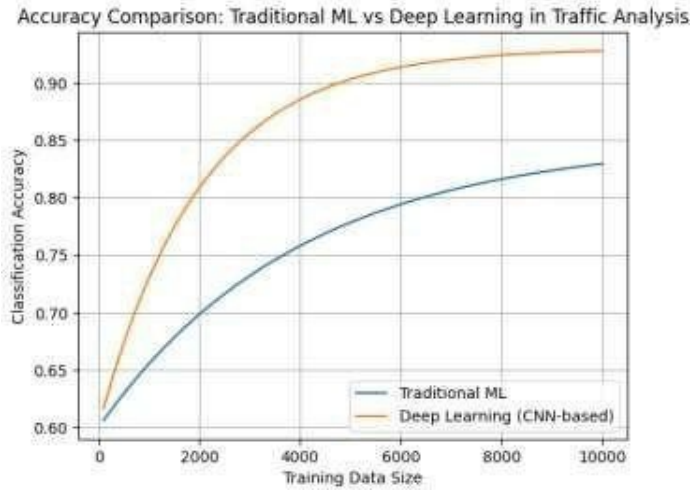


Figure 3. Accuracy comparasion: Traditional ML vs deep learning in traffic analyisis

3.19 Emerging Threats and New Attack Vectors

Deep learning is introducing new types of threats which are altering and evolving. It has been shown, among other things by Wuryanti et al. (2025), that multimodal deep learning models can be applied to encrypted network traffic including VoIP streams to classify application-level behavior and reveal what is being said, by analysing packet size pattern. Also, the considerable increase in the use of IoT applications adds another element to the surveillance space, where the IoT devices connected to the home networks act as data exfiltration tools that could potentially threaten the anonymity measures adopted by other endpoints. Furthermore, the development of quantum computing can be considered as another potential threat to the cryptographic principles on which the anonymity systems rely. Shor algorithm for quantum computing is famous for its ability to break public-key encryption schemes such as RSA and ECC, which are also used to construct Tor circuits. Therefore, this issue puts additional pressure on anonymity-system design to use post-quantum cryptography.

4. Results and Discussion

4.1 Main Findings of the Review

The findings from the literature review make up the main body of the thesis, and serve as a general summary of the existing security problems in anonymous communication networks. There are two important things to mention. First, there is a gap between the theoretical and practical security of the systems under consideration. The importance of this fact becomes even more evident in cases when the adversary is able to monitor the whole path of communication.

The second key result is that traffic analysis attacks, particularly those powered by deep learning, have advanced much faster than corresponding defenses, causing a strategic imbalance favoring attackers. The summarizes results from experimental website fingerprinting (WF) studies show an increase in accuracy rates, ranging from about 55% in early 2010s to more than 93% in recent studies with deep neural networks.

Third, a small set of major network providers monopolize a substantial portion ofTor relays, incurring a degree of centralization that runs counter to the network's original intent of a decentralized design. This popularizes control points for opponents who can manipulate or work with these providers.

Several measurement studies of networks show that a large portion of Tor bandwidth is held by a small number of hosting organizations.

Conclusion: The study of de-anonymization attacks demonstrates that the prevailing technique used in de-anonymization attacks does not rely on exploiting vulnerabilities in encryption techniques. Rather, the prevailing technique relies on exploiting vulnerabilities within the application layer and through the mistakes made by users. The finding of the study highlights an important aspect of security: the security of the overall system which includes the anonymity techniques, applications, and users, as shown in Figure 4.

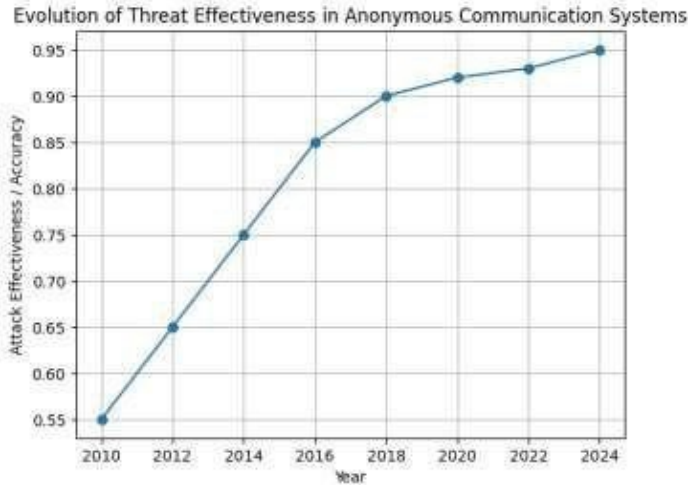


Figure 4. Evolution of threat effectiveness in anonymous communication system

4.2 Comparison of Major Systems

A comparative analysis of the studied anonymous communication systems demonstrates the existence of diverse characteristics in terms of security, efficiency, usability, and size of the anonymity set among others. Tor is the most popular and widely used anonymity system, which has the largest number of users. Nevertheless, Tor is the most specialized network susceptible to targeted attacks, with highly advanced attack tools created for attacks on it. Meanwhile, the architecture of I2P differs in its decentralization and greater resistance to attacks based on directories; however, because of its relatively small network size, less path diversity results and makes possible statistical traffic correlation attacks. Moreover, Freenet systems show better results in terms of content publishing protection, while its performance level is inadequate for real-time communications (for example, IRC), as shown in Figure 5.

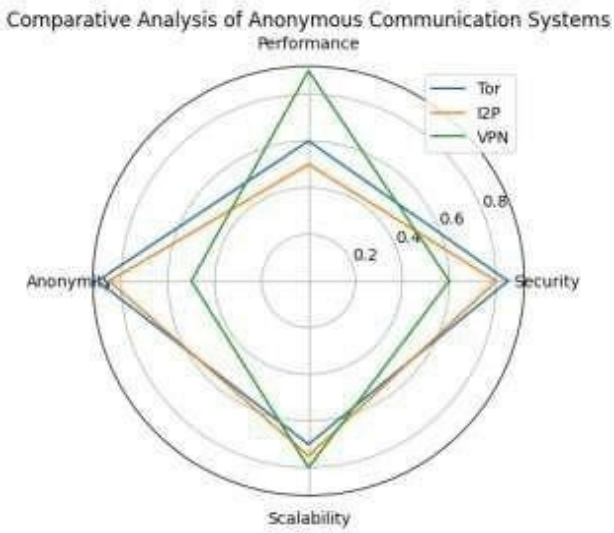


Figure 5. Comparative analysis of anonymous communication systems

4.3 Disscusion

The literature review reveals serious security problems in anonymous communication systems, which indicates an evident gap between the theoretical claims of their effectiveness and reality. The problem arises even more acutely in case when an adversary has access to both entry and exit points of the network, causing its vulnerability that contradicts anonymity principles. Traffic analysis attacks, especially those based on deep learning techniques, develop significantly quicker than any possible solutions, providing a certain advantage for the attacker. For example, according to the research conducted in the area of website fingerprinting, accuracy increases from about 55% at the beginning of the 2010s to more than 93% in the current studies based on deep neural networks. In addition, due to the fact that the majority of Tor relays work in the networks controlled by just several providers, there are specific control points that contradict the initial principles of decentralization of the network. According to the cases of successful de-anonymization, the most serious problems are located at the application level and among users' activities.

An analysis of the leading anonymous communication networks shows that there have been constant tradeoffs between security, efficiency, usability, and the size of the anonymity set since the beginning of these technologies. Tor is not only the most popular anonymous network but also the main attack target due to its large number of users; moreover, the intrusion tools for this network have been developed specifically for Tor. On the other hand, I2P provides a decentralized structure that makes it more resilient to attacks on its directory but makes it vulnerable to traffic analysis attacks because of the small network size and low path diversity. Freenet-like systems are great in protecting the publishers of content, but they show poor latency and low throughput rates, thus being inadequate for the use in IRC-type applications.

Such findings suggest that both parties have to consider the matter of system choice concerning their threat models, network, and application specifics. Research and development are needed to cope with the new ways of attacks and improve defenses, while finding a good trade-off between anonymity, performance, and usability. Anonymity cannot be achieved just by the means of the right protocol, but through its implementation into a secure environment, proper application development, and sound operations as well.

5. Conclusions

5.1 Conclusion

The area of anonymous communications can be characterized as a perpetual technology arms race between scientists attempting to improve privacy online and a range of adversaries with different capacities and intents. A thorough analysis of the scientific literature on this issue proves one important point – there is no way to have a mechanism offering absolutely secure and perfect protection from all possible attacks. There are always some trade-offs when considering any design approach. Importantly, the results of this analysis show that the main flaws in this area do not necessarily hide in the intricacies of the cryptography mechanisms but occur at the level of the application and human behavior. Therefore, any improvements in the area of anonymous communications security cannot come from developing better protocols. It requires a change of paradigm towards more holistic design taking into account users and their mistakes and cognitive biases together with hard technological prerequisites.

With the fast-paced development of artificial intelligence, quantum computing, and state-level surveillance, these systems have faced some of the biggest structural stressors seen in the last forty years since Chaum seminal paper was published. Solving these problems will require extensive interdisciplinary cooperation on the part of researchers from network security and cryptography, HCI experts, lawyers, and digital rights activists in order to create a new generation of anonymity technologies that would withstand emerging threats. This monograph is designed to be a resource that will allow researchers to spot gaps in the field and set priorities for future work in line with the universal human right of secure, private, and free communication.

5.2 Research Limitations

This study recognizes various limitations. First, the research makes use of mainly literature reviews and secondary analysis that might fail to capture all real-life attack cases or latest experimental results in anonymous communications. Secondly, considering the fact that traffic analysis using AI is constantly evolving, as well as the threat posed by quantum computers and government monitoring, the relevance of the findings might be compromised quickly due to technological development and emergence of novel attacks. Thirdly, lack of empirical verification through experiments means that it might be difficult to assess the efficiency of the holistic approach in eliminating human error. Lastly, while trying to make the study more comprehensive and provide an overview of the current trends and challenges in the field, it becomes quite challenging to generalize the recommendations for different network architectures and users due to the diversity of anonymous networks (Tor, I2P, Freenet).

5.3 Suggestions and Directions for Future Research

From the empirical results, the technical design should ensure a defense-in-depth approach that employs several independent anonymity protocols as opposed to using one protocol. There is also a need to use traffic adaptation techniques that will not succumb to statistical analysis after some time. In terms of the application layer, there is a need for development of a complete testing framework that will consider the whole application environment, along with secure by default approach with as few user-tunable parameters as possible to reduce the chances of mistakes. In future, there is a need for development of anonymity protocols that cannot be broken by machine learning techniques through integration of different privacy, cryptography, and protocols that will have a realistic threat model considering the power of nation-states and large technology companies. The aspect of user-centric design must be incorporated at the core of anonymity research with experimental study on how to design an interface that considers all user groups, especially high-risk ones like journalists and activists. Finally, the "last mile" problem—the interface between the anonymity network and the rest of the Internet—must be considered as part of solving this issue.

Acknowledgement

The author thanks those researchers who have laid down the foundational work for this monograph through their work on anonymous communications systems. Specifically, the author wishes to thank his colleagues from the fields of network security, cryptography, human-computer interaction, and digital rights for their inputs and advice that has helped formulate the overall framework discussed in this paper.

References

Abdulloyevna, H. G. (2026). Measuring trust in higher education evaluation systems: Methods and indicators. *Review of Multidisciplinary Academic and Practice Studies*, *3*(1), 1-11. https://doi.org/10.61401/rmaps.v3i1.369

Adawiyah, R. (2025). Implementing AI in Arabic language learning: Challenges and insights from Islamic higher education. *AL-ISHLAH: Jurnal Pendidikan*, *17*(3), 3729-3739. https://doi.org/10.35445/alishlah.v17i3.7390

Ali, H. F., Nakshbandi, L. J., Saadi, F., & Barzani, S. H. H. (2022). The effect of spell-checker features on spelling competence among EFL learners: An empirical study. *International Journal of Social Sciences & Educational Studies*, *9*(3), 101-111. https://doi.org/10.23918/ijsses.v9i3p101

Ali, Y. A., Naeem, S., Alqarni, S., & Bhatti, M. I. (2025). Evaluating the impact of artificial intelligence-based tools on listening comprehension among esl learners. *Contemporary Journal of Social Science Review*, *3*(3), 514-522.

Alizadehmahmoudalilo, H. (2025). Comparative effects of ai-assisted vs. *teacher-assisted collaborative listening on EFL learners' self-efficacy and metacognitive awareness. Journal of Studies in Language Learning and Teaching*, *2*(1), 36-48.

Andino, P. W. A., Inzhivotkina, Y., & Sánchez-Cáceres, S. I. (2025). Analyzing the effectiveness of AI-powered chatbots in improving listening comprehension in second language acquisition: A case study of english as a second language Learners. *Sinergia Académica*, *8*(10), 289-309.

Brown, H. D., & Lee, H. (1994). *Teaching by principles: An interactive approach to language pedagogy (Vol.1)*. Prentice Hall Regents Englewood Cliffs, NJ.

Dzhumaevna, N. N. (2025). Avicenna's legacy and the modern model of public health: Transforming the roles of education and social justice. *Journal of Multidisciplinary Academic and Practice Studies*, *3*(4), 297-312. https://doi.org/10.35912/jomaps.v3i4.3603

Gizi, R. G. X. (2025). Translational challenges of robotics terminology in English And Uzbek languages. *Review of Multidisciplinary Academic and Practice Studies*, *2*(2), 131-142. https://doi.org/10.61401/rmaps.v2i2.255

Holmes, W., Bialik, M., & Fadel, C. (2019). *Artificial intelligence in education promises and implications for teaching and learning*. Center for Curriculum Redesign.

Jung, H. (2025). AI-assisted student-generated listening materials in high school EFL: A sociomaterial perspective. *Multimedia-Assisted Language Learning*, *28*(2).

Litman, D., Strik, H., & Lim, G. S. (2018). Speech technologies and the assessment of second language speaking: Approaches, challenges, and opportunities. *Language Assessment Quarterly*, *15*(3), 294-309. https://doi.org/10.1080/15434303.2018.1472265

Liu, L. (2025). Impact of AI gamification on EFL learning outcomes and nonlinear dynamic motivation: Comparing adaptive learning paths, conversational agents, and storytelling. *Education and Information Technologies*, *30*(8), 11299-11338. https://doi.org/10.1007/s10639-024- 13296-5

Liu, Y., & Li, Y. (2025). AI−driven listening systems in language acquisition redefining auditory cognition in the intelligent era. *Discover Artificial Intelligence*, *6*, 60. https://doi.org/10.1007/s44163-025-00748-1

Loebis, I. A. (2025). Effectiveness of Ai-based english language learning apps in improving listening skills. *Lingeduca: Journal of Language and Education Studies*, *4*(1), 9-16. https://doi.org/10.70177/lingeduca.v4i1.2123

Ma, H., Ismail, L., & Han, W. (2024). A bibliometric analysis of artificial intelligence in language teaching and learning (1990–2023): Evolution, trends and future directions. *Education and Information Technologies*, *29*(18), 25211-25235. https://doi.org/10.1007/s10639-024-12848-z

Mousavinasab, E., Zarifsanaiey, N., R. Niakan Kalhori, S., Rakhshan, M., Keikha, L., & Ghazi Saeedi,M. (2021). Intelligent tutoring systems: A systematic review of characteristics, applications, and evaluation methods. *Interactive learning environments*, *29*(1), 142-163. https://doi.org/10.1080/10494820.2018.1558257

Pinkwart, N. (2016). Another 25 years of AIED? Challenges and opportunities for intelligent educational technologies of the future. *International journal of artificial intelligence in education*, *26*(2), 771-783. https://doi.org/10.1007/s40593-016-0099-7

Platt, M., & McBurney, P. (2023). Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance. *Algorithms*, *16*(1), 34. https://doi.org/10.3390/a16010034

Pokrivcakova, S. (2019). Preparing teachers for the application of AI-powered technologies in foreign language education. *Journal of language and cultural education*, *7*(3), 135-153. https://doi.org/10.2478/jolace-2019-0025

Rahim, F., & Apzhaparovna, R. Y. (2026). The impact of AI-driven speech recognition on listening comprehension and pronunciation accuracy in English language teaching. *Discover Computing*, *29*(1), 81. https://doi.org/10.1007/s10791-026-09992-0

Sabahel , M. A., Alam , M., Hossain, S., Mahmud, S., & Alam, M. K. (2025). Community-driven success in equity crowd funding: A study of brand engagement in Bangladesh two-sided markets. *Global Academy of Multidisciplinary Studies*, *2*(2), 93-106. https://doi.org/10.35912/gams.v2i2.3662

Sahito, J. K. M., Panwar, A. H., & Ramzan, I. (2025). Exploring the impact of artificial intelligence (AI) on the listening skills of English as a second language (ESL) learners. *Journal of Applied Linguistics and TESOL (JALT)*, *8*(1), 1059-1067.

Shadiev, R., Chien, Y.-C., & Huang, Y.-M. (2020). Enhancing comprehension of lecture content in a foreign language as the medium of instruction: Comparing speech-to-text recognition with speech-enabled language translation. *Sage Open*, *10*(3), 2158244020953177. https://doi.org/10.1177/2158244020953177

Sun, W. (2023). The impact of automatic speech recognition technology on second language pronunciation and speaking skills of EFL learners: A mixed methods investigation. *Frontiers in Psychology, 14, 1210187. doi:*. https://doi.org/10.3389/fpsyg.2023.1210187

Syazwina, A. S., & Zunairoh, Y. (2025). Integration of Artificial Intelligence (AI) in Arabic Language Learning in the Era of Society 5.0. *International Journal of Religion and Social Community*, *3*(1), 107-123. https://doi.org/10.30762/ijoresco.v3i1.3632

Torres, P. J., & Kahveci, Y. E. (2025). Effectiveness of Artificial Intelligence (AI) in language teaching. *Computers and Education: Artificial Intelligence*, *9*, 100522. https://doi.org/10.1016/j.caeai.2025.100522

Wuryanti, S., Hudalil, A., & Nugrahaeni, I. (2025). Trainer Competence in learning Management at the Social Welfare Education and Training Center of the Ministry of Social Affairs. *Jurnal Abdimas Multidisiplin*, *4*(1), 23-31. https://doi.org/10.35912/jamu.v4i1.6098

Xiao, Y. (2025). The impact of AI-driven speech recognition on EFL listening comprehension, flow experience, and anxiety: A randomized controlled trial. *Humanities and Social Sciences Communications*, *12*(1), 1-14. https://doi.org/10.1057/s41599-025-04672-8

Zhang, Z. (2025). Enhancing english listening comprehension via AI-based adaptive learning platforms incorporating speech-to-text and predictive analytics. *Systems and Soft Computing*, *7*, 200418. https://doi.org/10.1016/j.sasc.2025.200418