Review of Muldisciplinary Academic and Pratice Studies
ISSN: 3110-0635, Vol 3, No 2, 2026, 67-80 https://doi.org/10.61401/rmaps.v3i2.510

Security Issues in Anonymous Communication Systems

Malath Sabri Kareem
Middle Technical University
malath-sabri@mtu.edu.iq

Article History
Received on 4 June 2026
1st Revision on 6 July 2026
2nd Revision on 15 July 2026
Accepted on 3 August 2026

Abstract

Purpose: This study examines the security aspects of anonymous communication systems, which are critical for protecting digital privacy and maintaining freedom of expression online. It focuses on widely used systems, such as the Tor network and Holloway's Freedom protocol, analyzing vulnerabilities, systemic weaknesses, and the advanced attack techniques employed by adversaries to compromise user anonymity, including traffic analysis, de-anonymization, and timing correlation attacks.

Research Methodology: A literature-based analytical approach was employed, reviewing specialized scientific articles and experimental studies published between 2020 and 2026. Emphasis was placed on research accepted at prominent conferences in network security and privacy protection. The study synthesizes evidence on security threats, attack methodologies, and systemic vulnerabilities affecting anonymous communication systems.

Results: The analysis reveals persistent fundamental weaknesses in current anonymous communication systems, which continue to compromise security. Additionally, the application of big data and artificial intelligence has facilitated increasingly sophisticated attack strategies capable of penetrating multiple layers of anonymity. The study identifies both the limitations of existing systems and the emerging risks that users face.

Conclusions: Protecting anonymity in digital communication requires both system-level improvements and strategic countermeasures against evolving attack techniques. Recommendations include technical upgrades, protocol redesigns, and adoption of AI-resistant security measures to ensure the resilience of anonymous communication systems in the future.

Limitations: The study relies on literature review and secondary data rather than primary experimental validation. As such, conclusions may not fully generalize to all types of anonymous systems or evolving attack scenarios.

Contribution: This study provides a comprehensive analysis of current threats and vulnerabilities in anonymous communication systems, offering practical and research-oriented recommendations to strengthen digital privacy protection and to future-proof these systems against increasingly sophisticated attacks.

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 Muldisciplinary Academic and Pratice 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's 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 (L. 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. Despite the widespread use of systems such as Tor, which supports over two million daily users, vulnerabilities have been exploited through successful deanonymization attacks, revealing a gap between theoretical security guarantees and actual user protection in real-world conditions. The rapid evolution of surveillance technologies and network analysis tools further reduces the safety margin for system users. Much of the existing literature addresses technical aspects in idealized conditions, often neglecting human and behavioral factors, and there is a notable absence of updated comprehensive surveys that consider recent technological advancements, particularly AI-driven attacks.

This study seeks to answer several fundamental research questions. It investigates the main types of security threats and attacks targeting contemporary anonymous communication systems and examines how their severity and likelihood vary depending on system architecture and operational context. The study also explores the effectiveness of security mechanisms embedded in widely used anonymity systems, including Tor and I2P, and identifies the limits of these defenses. Additionally, it considers the role of machine learning and artificial intelligence in enhancing attackers' capabilities for network traffic analysis and de-anonymization, along with the security implications for user protection. Human and behavioral factors are analyzed to understand their impact on attack success and to inform the design of more resilient protocols. Finally, the study identifies pressing research directions and frameworks for developing anonymous communication systems that balance privacy, security, and operational efficiency

2. Literature Review and Hypothesis/es Development

2.1 Concept of Anonymous Communication and Its Historical Evolution

The theory underlying anonymous communication systems was introduced by David Chaum in his pioneering 1981 paper "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms." In that paper, Chaum proposed the use of Mix Networks for that purpose, an approach based on message permutation and encryption to break the relationship between sender and receiver, which is at the top of the pyramid in most later anonymity protocols (Rahim & Apzhaparovna, 2026). During the 1990s, this type of research was continued by Paul Syverson and others with the development of the Onion Routing protocol.

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 (Y. 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 consists of decentralized P2P anonymous networks like Freenet and GNUnet that rely on the participating nodes to handle storage and routing instead of the central infrastructure. This design improves defiance to censorship as well as the difficulty in tracking or taking down contents. For instance, Freenet has been called a distributed system for anonymous storage and retrieval of information using loosely cooperative nodes of small adaptiverouting while GNUnet seeks to construct a censorship robust and privacy protecting P2P network, contrary to the pragmatic and security issues raised in 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), in "Detection of Obfuscated Tor Traffic Based on Bidirectional Generative Adversarial Networks and Vision Transformer," demonstrated advanced techniques for identifying obfuscated anonymous network traffic. These contributions comprehensive study of replay attacks as identity revealing attacks.

Gizi (2025) in "Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World," which established that a coordinated adversary that monitors the traffic at both entry and exit of communication paths can successfully de-anonymize users in real-world deployments. This work proved pivotal in shaping the scholarly discussion on practical limits of Tor protection. In a similar vein, Y. A. 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), in "On Precisely Detecting Censorship Circumvention in Real-World Networks" at NDSS 2024, presented a novel approach to detecting Tor usage at the network level, demonstrating how adversaries can identify and disrupt anonymous traffic. In the same line, H. F. Ali, Nakshbandi, Saadi, and Barzani (2022) studied how traffic analysis can reveal the application running over Tor, showing that even malware using anonymous channels can be exposed, which breaks functional anonymity.

At the forefront, the use of deep learning for network traffic analysis has dramatically improved accuracy in website fingerprinting attacks. Y. A. Ali et al. (2025) achieved high classification accuracy by augmenting network traces with realistic synthetic data. This was extended by Sabahel , Alam , Hossain, Mahmud, and Alam (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 study is a Systematic Literature Review (SLR) that adheres to the preferred reporting items for systematic reviews and meta-analyses (PRISMA) in its protocol for analysing and reporting. The use of this protocol demonstrates a dedication to being open, complete, and reproducible, which are essential criteria of high-quality scientific review research. 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.

This multi-faceted approach facilitates meaningful comparisons between disparate types of attacks and can serve as a general covert channel framework for assessing additional security threats. By combining technical, operational, and behavioral views, the model facilitates a better understanding of the dynamic threat landscape.To be able to extend this taxonomy to more than descriptive classification, the contribution introduces a conceptual analytic expression that expresses the probability of de-anonymization as a function of several interacting parameters:

$$\mathrm{P\_deanon} = \mathrm{f(A\_c, N\_o, U\_b, M\_l)} \quad (1)$$

Then, in this expression, the de-anonymization probability is affected by the Attacker CapabilityA_c which models the computational power and access level of the adversary, the Network ObservationCapability N_o which models the traffic monitoring ability at different points over the network, the User Behavior Factor U_b which models the operational habits and possible human mistakes, and the Machine Learning Capability M_l which represents the level of analytical tool

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.

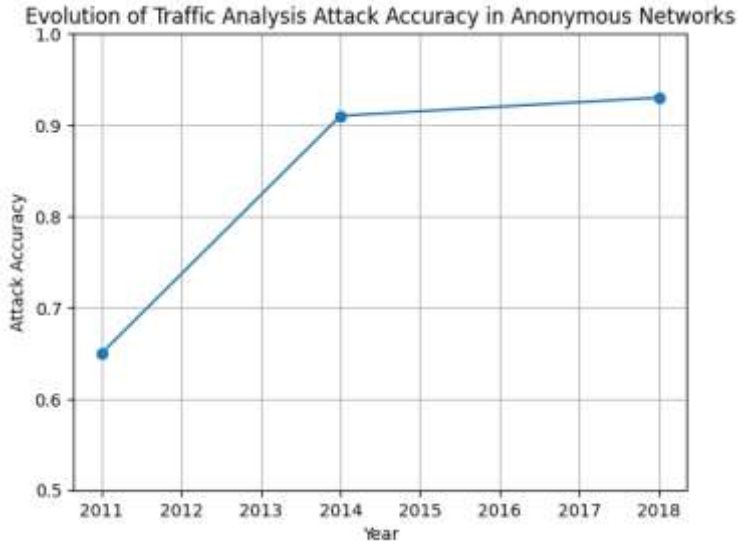

Figure 1. Evolution of teraffic analysis

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.

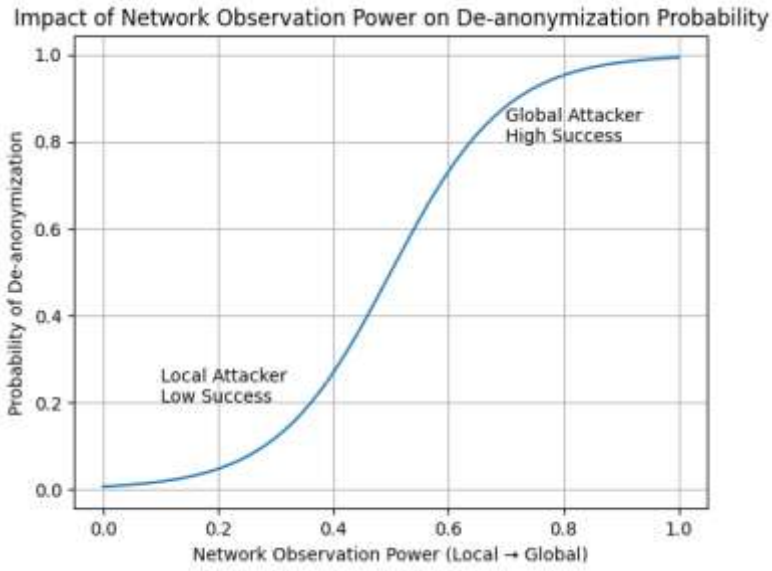

Figure 2. Impact of network observation

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 et al. (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 Xu & Zou (2021) [29] 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) conducted a systematic investigation of the VPN ecosystem via VPNalyzer, revealing widespread issues including inadequate traffic encryption and misleading security claims across a

significant portion of VPN services examined. These findings are alarming and call into question the gap between security assertions in marketing materials and actual application security practices.

3.13 Traffic Padding & Morphing

Padding and morphing have been early countermeasures against traffic analysis attacks, trying to remove statistical patterns by injecting dummy packets or lengthening/shrinking real packets. The FRONT scheme, which uses randomized padding to obscure traffic patterns and interfere with fingerprinting-based analysis techniques. Yet, this method has been shown to impose significant bandwidth overhead and may impair user experience under high-traffic scenarios.

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's 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

An attacker with access to behavioural pattern analytics, such as daily connection times, session lengths, and the kinds of contents accessed, can carry out linkage analysis to link an anonymous ID to a real ID even without any technical exploits. This forensic technique is based on the "uniqueness of digital behavior" principle that states that even online activity patterns when anonymized can turn into a unique and comparable fingerprint. In their seminal work on de-anonymizing the Netflix dataset, Pinkwart (2016) demonstrate in their comprehensive VPN security survey that user behavioral patterns can be leveraged to uniquely identify individuals when correlated with external data sources. This is a vivid illustration of how anonymization procedures based on simply dropping explicit identifiers and not taking into account the behavioural patterns can go awry.

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 et al. (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.

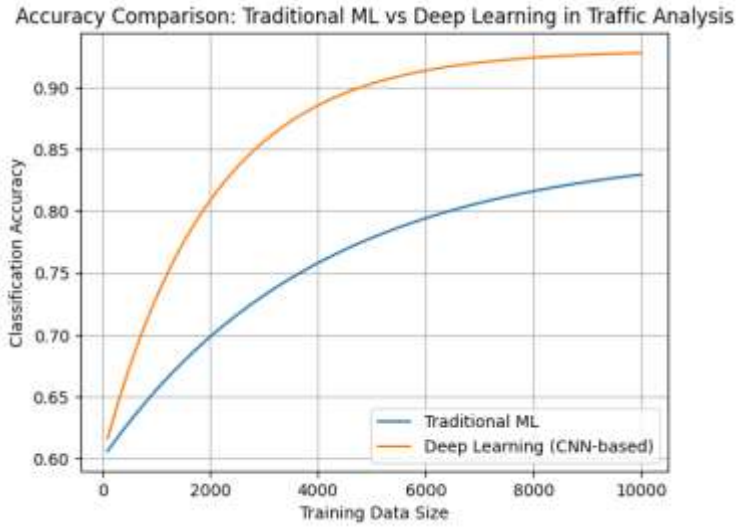

Figure 3. Accuracy comparasion: Traditional ML vs deep learning in traffic analyisis

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. Moreover, the enormous increase in Internet of Things (IoT) applications adds a new surface to the surveillance scene, with IoT devices in home networks acting as data exfil-tration sources that can compromise the anonymity masks employed by other end points. In addition, quantum computing development is a looming threat to the cryptographic base used in anonymity systems. Shor's quantum algorithm is known to break public-key cryptosystems like RSA and ECC (which are also used to construct Tor circuits). This puts an increasing strain on the design of anonymity systems in to move towards post-quantum cryptography to guarantee long term security.

4. Results and Discussion

4.1 Results

4.1.1 Main Findings of the Review

The findings of the literature review in this study are the contents of the main body of the thesis and show a generalized summary of the current security issues concerning anonymous communication systems. There are two important aspects; the first is a fundamental gap in what the theoretical development of these systems says about their security and how secure they really are. It is especially relevant when the adversary can observe the entire path both the entry and the exit of the network at the same time.

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's bandwidth is held by a small number of hosting organizations.

Conclusion The survey on reported de-anonymization attacks ultimately exposes that the dominating attack vector in practice is not attacking encryption protocols themselves, but rather exploiting weaknesses on the application layer and user operational mistakes. This conclusion implies a fundamental security axiom: the entire system must be secure, not just the anonymity protocols themselves, but also the application environments and the users, as can be seen in Figure 4.

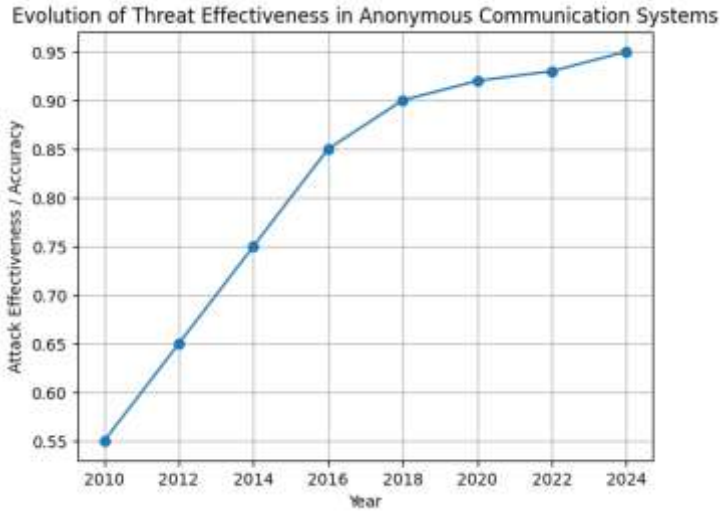

Figure 4. Evolution of threat effectiveness in anonymous communication system

4.1.2 Comparison of Major Systems

The comparison between the analyzed anonymous communication systems shows a heterogeneous picture where security, efficiency, usability, and anonymity set are subject to various trade-offs. # The Tor network is the best known and most widely used, therefore the largest number of users is on it. But it is also the most specialized attacked system, and sophisticated attack tools are developed for it. In contrast, I2P offers a significantly more decentralized model that is more resistant to directory-based attacks, though its smaller network size decreases path diversity and statistically aids traffic correlation attacks. At the same time, Freenet-based systems do the best job at protecting content publishers, but are too slow for real-time communications applications such as IRC, as can be seen in Figure 5.

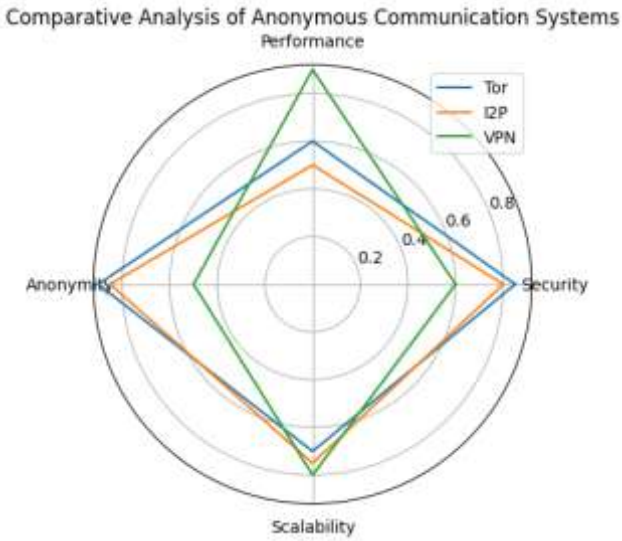

Figure 5. Comparative analysis of anonymous communication systems

4.2 Disscusion

The findings from the literature review reveal significant security challenges in anonymous communication systems, highlighting a fundamental gap between theoretical assurances and real-world performance. This gap becomes especially critical when adversaries can observe both entry and exit points of the network simultaneously, exposing vulnerabilities that undermine intended anonymity guarantees. Traffic analysis attacks, particularly those powered by deep learning, have advanced far more rapidly than corresponding defenses, creating a strategic advantage for attackers. Experimental studies on website fingerprinting indicate that accuracy rates have risen from around 55% in the early 2010s to over 93% in recent deep neural network–based studies. Additionally, the centralization of Tor relays under a small set of major network providers introduces critical control points that can be exploited, countering the network's original decentralized intent. Reported de-anonymization attacks emphasize that vulnerabilities are predominantly at the application layer and in user operational mistakes, suggesting that effective anonymity requires securing the entire system, including protocols, applications, and user behavior.

Comparative analysis of major anonymous communication systems highlights the inherent trade-offs among security, efficiency, usability, and anonymity set size. The Tor network, being the most widely adopted, hosts the largest user base but is also the most targeted, with sophisticated attack tools developed specifically against it. I2P provides a more decentralized design, offering better resistance to directory-based attacks; however, its smaller network size reduces path diversity, increasing vulnerability to traffic correlation attacks. Freenet-based systems excel at protecting content publishers but suffer from high latency and low throughput, limiting their suitability for real-time communication applications such as IRC. These differences underscore that no single system simultaneously optimizes all dimensions, and design choices inherently prioritize certain aspects of security and performance over others.

Overall, these findings suggest that both users and developers must carefully consider system selection based on specific threat models, network characteristics, and application requirements. Continuous research and innovation are necessary to address emerging attack vectors, improve defensive mechanisms, and balance trade-offs between anonymity, performance, and usability. Ensuring effective anonymity extends beyond protocol design to include secure application environments, user-centric design, and robust operational practices, emphasizing a holistic approach to maintaining privacy in anonymous communication networks.

5. Conclusions

5.1 Conclusion

The domain of anonymous communication can be described as an ever-evolving technological arms race between researchers aiming to improve digital privacy and a myriad of adversaries with different capabilities and incentives. A thorough Literature survey of this work shows the basic truth that no mechanism can offer absolute and perfect security from all types of attacks. There are tradeoffs inherent to every design paradigm. Importantly, this work also demonstrates that the most critical weaknesses are not necessarily buried deep within the details of the cryptographic protocols, but can often be found in the application layer and surrounding human behaviors. Therefore, an improvement in the security of anonymous communication systems cannot be brought about by devising better protocols per se, but rather by a paradigm shift, a shift towards a holistic design philosophy concerned with human users, their errors and cognitive biases, along strict technical requirements.

The rapid evolution of artificial intelligence, quantum computing, and government surveillance has placed these systems under some of the greatest structural pressures they have experienced since Chaum's seminal paper four decades ago. Tackling these challenges will require long-term, interdisciplinary collaboration among network security researchers, cryptographers, human-computer interaction experts, legal scholars, and digital rights advocates to develop a new generation of anonymity protocols that can resist an evolving threat environment. We hope this monograph serves as a consolidation point from which researchers and practitioners can identify key gaps and set priorities for moving forward, coherent with the basic human right to communicate securely, privately, and freely.

5.2 Research Limitations

This study acknowledges several limitations. First, the research is based primarily on literature surveys and secondary analyses, which may not capture all real-world attack scenarios or the latest experimental results from emerging anonymous communication systems. Second, the dynamic and rapidly evolving nature of AI-driven traffic analysis, quantum computing threats, and government surveillance means that findings may become outdated quickly as new technologies and attack vectors emerge. Third, the study does not include empirical testing or user-centered experiments, which limits the ability to assess the practical effectiveness of proposed holistic design strategies in mitigating human errors and operational vulnerabilities. Finally, while the work aims to provide a broad synthesis of major challenges and trends, the heterogeneity of anonymous systems (e.g., Tor, I2P, Freenet) makes it difficult to generalize recommendations for all network architectures and user populations. Future studies should incorporate experimental evaluations, cross-disciplinary validation, and longitudinal analyses to address these gaps.

5.3 Suggestions and Directions for Future Research

Based on the research findings, technical design should adhere to a defense-in-depth approach, integrating multiple independent anonymity protocols rather than relying on a single one, and implementing dynamic traffic adaptation techniques that resist long-term statistical analysis. At the application layer, it is crucial to develop comprehensive security testing frameworks encompassing the entire application environment and to prioritize "secure by default" solutions with minimal user-configurable options to reduce human error. Future research should focus on developing machine learning–resistant anonymity systems through cross-layer integration of differential privacy, cryptography, and protocol design, alongside more realistic threat modeling that simulates the capabilities of nation states and large technology companies. Additionally, user-centric design must be embedded at the core of anonymity research, involving experimental studies to optimize interface design and default settings for diverse user populations, particularly high-risk users such as journalists and activists. Finally, addressing the "last-mile problem" where anonymity networks interface with the public Internet is essential, requiring innovative methods to hide or segment exit-phase traffic to prevent monitoring and correlation attacks.

Acknowledgement

The author would like to express sincere gratitude to all the researchers whose work contributed to this monograph, providing foundational insights into anonymous communication systems. Special thanks are extended to colleagues in network security, cryptography, human-computer interaction, and digital rights advocacy for their guidance and discussions that informed the holistic perspective presented here. The author also appreciates the constructive feedback from peer reviewers, which helped refine the analyses and recommendations.

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. doi: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. doi: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. doi: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.

Asratie, M. G., Wale, B. D., & Aylet, Y. T. (2023). Effects of using educational technology tools to enhance EFL students' speaking performance. *Education and Information Technologies, 28*(8), 10031-10051. doi:https://doi.org/10.1007/s10639-022-11562-y

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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi:https://doi.org/10.1007/s40593-016-0099-7

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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi:https://doi.org/10.1016/j.sasc.2025.200418