JANOLI International Journal of
Computer Science And Engineering (JIJCSE)
(A Peer Review Journal)
journal homepage: https://janolijournals.com/index.php/jijcse

Volume 1, Issue 1, 2025 ISSN:3107-4537

Anonymity and Skepticism: The Evolution and Implications of the TOR Network

Krishan Kumar Yadav and Dalia Younis
Sanskriti University, Mathura, India

ARTICLE INFO

Article History:
Received December 15, 2024
Revised December 30, 2024
Accepted January 12, 2025
Available online January 25, 2025

Keywords:
TOR Network
Internet Anonymity
Online Privacy
Digital Surveillance
Malicious Exit Nodes
Traffic Correlation Attacks

Correspondence:
E-mail: Dyounis1@aast.edu

ABSTRACT

In today's era of increasing reliance on mobile devices, chatbots play a vital role due to their simplicity and accessibility. The COVID-19 pandemic has further highlighted the insufficiency of healthcare resources, emphasizing the need for scalable digital solutions. This paper presents an application that leverages deep learning to assist with online disease diagnosis via a chatbot interface.

The study focuses on predicting an individual's susceptibility to heart attacks based on specific health indicators. Using a robust dataset, a deep learning model was developed to analyse key features and accurately assess the risk of cardiac events. The model was then integrated into a chatbot, allowing users to access personalized health insights in real-time.

By combining advanced machine learning techniques with an intuitive conversational interface, the proposed system aims to enhance early detection and preventive care. The application is designed to reduce the burden on healthcare systems while empowering individuals with critical health information in a user-friendly format. This approach demonstrates the potential of integrating artificial intelligence with conversational platforms to address pressing health challenges effectively.

1.Introduction

This paper examines the TOR Project, one of the most popular anonymity networks globally, tracing its evolution from a U.S. Navy project to an open-source tool used for both legitimate and malicious purposes. This study is significant in understanding the complexities and ethical considerations surrounding internet anonymity. The core research question probes the dual nature of TOR's usage and its implications. This is further deconstructed into five sub-research questions: history and how the TOR has evolved over time, the current applications of TOR, the security integrity of data on the TOR network, why TOR is preferred over VPNs, and finally, the governmental interests in its existence. Adopting a qualitative methodology, the research design calls for the use of critical literature review and user perspective analysis designed to address these questions in a specific order.

2.Literature Review

This section reviews the existing literature on the TOR network, with emphasis on five key areas derived from the sub research questions: TOR's historical evolution, current applications, data security integrity, comparison with VPNs, and governmental interests. This section gives a description of relevant works of elaborate research findings. It highlights the shortcomings of the previous research, including poor insight into TOR's security vulnerabilities and the same governmental influences, pointing out the value of this paper in filling the gaps.

2.1 Historical Development of TOR

Initial research on TOR's development identifies its origin as a U.S. Navy project on secure communication, where it evolved into an open-source anonymity tool. Early research was more on the technical architecture without looking at the broader implications. Later studies focused on its transformation into a public project, where it was developed through the open-source community**.** The latest studies discuss its societal impact but tend to ignore the governmental motivations for such a transformation.

2.2 Current Applications of TOR

Research studies into the uses of TOR show that it is broadly used for privacy, activism, and criminal activities. The earlier studies were mainly used in secure communications in authoritarian regimes. The subsequent studies enlargements are on its role in legal and illegal online transactions, but there is mostly a lack of full-scale examination of the ethical challenges such dual purposes present. Recent literature discusses its impact on digital privacy debates but fails to address the complete spectrum of its social implications.

2.3 Security Integrity of Data on TOR

Research regarding TOR's security highlights a number of vulnerabilities, starting from data interception by malicious nodes. Early works highlighted basic threats but were too shallow in evaluating the complexity of attacks. Advanced works later explained network vulnerabilities and suggested countermeasures; however, contemporary researches have still failed to deliver a full security integrity review of the possible interceptions within the network.

2.4 Prefer TOR over VPNs

Comparative literature on TOR and VPNs suggests that people prefer TOR more than VPNs due to the reasons that they have perceived higher anonymity. Early studies centred on VPN's vulnerability to logging policies. Later analyses focused on TOR's decentralized nature as one of the primary advantages but failed to note the practical limitations that occur in real user experiences. Recent research studies TOR's difficulties, including speed and usability, but failed to critically analyse user decision-making processes.

2.5 Possible Governmental Interests in TOR

Researches on state interests in TOR talk about the paradoxical aspect of a state-made but uncontrolled tool. Early studies assumed benefits for governments in terms of anonymity. Later studies talked about governmental regulation or exploitation attempts but rarely put forth the meaning of intentional abstention. Newer studies assume strategic interests without actual evidence or policy analysis from the governmental perspective.

3.Method

A qualitative research approach will be undertaken in this study to examine critically the development, applications, and implications of the TOR network. Qualitative methodology gives the opportunity to probe deeply into people's experience and their perception. By collecting the data through interviews from TOR users and experts along with content analysis of some online discussions and publications, thematic analysis will guide data interpretation focusing on how the role of TOR in digital privacy and security has evolved and been perceived.

4.Findings

Findings reveal in-depth, yet subtle insights, into the varied role of TOR in digital anonymity. Findings are categorized and organized according to the sub-research questions: TOR historical development, application, data integrity, why the preference over VPNs, and the government interests in its development. The study identifies "The Paradox of TOR's Development," "Ethical and Practical Applications," "Challenges in Ensuring Data Security," "User Preferences: TOR vs. VPNs," and "Governmental Strategies and Implications." These findings reveal TOR's complex

evolution, its ethical dilemmas, and the strategic considerations for governments, challenging prevailing assumptions about digital anonymity.

4.1 The Paradox of TOR's Development

This research exposes a paradox of TOR's development in the process from a military project to a public tool. In interviewing experts, one can trace an element of strategic ambiguity of such a change of course in terms of governmental oversight and intent. Qualitative data suggest that users see this change as either freeing and suspicious at the same time, which echoes societal tensions between the state's control over digital privacy.

4.2 Ethical and Practical Applications

An analysis of interviews with users and online content points to the ethical and practical implications of TOR-from privacy protection to facilitating illegal transactions. Users reveal using TOR for legitimate purposes such as evading censorship, yet acknowledge its facilitation of illicit transactions. This dualism brings to the fore ethical dilemmas as participants exhibit mixed feelings on whether TOR advances personal freedom at the cost of societal risks.

4.3 Difficulty in Achieving Data Protection

Findings show that there are long-term issues with data security on the TOR network. Interviews indicate that users are concerned with the possibility of interception by malicious nodes and governments. Qualitative analysis points to specific vulnerabilities, such as traffic correlation attacks, but also reveals ongoing efforts in the TOR community to improve security measures, thereby showing a dynamic interplay between risks and defenses.

4.4 User Preferences: TOR vs. VPNs

User feedback shows that TOR is more popular than VPNs, due to anonymity and a general mistrust of VPN providers. People fear VPNs log their data and the jurisdiction in which it is kept, whereas TOR has a decentralized architecture that will protect against surveillance. This preference also mirrors wider fears about data privacy but points toward practical challenges: slower connection speeds and usability.

4.5 Governmental Strategies and Implications

It could be observed, from expert interviews and policy documents, that governments have sophisticated policies on TOR. Some governments would want to bar or inhibit the use of TOR while other governments will leverage its attributes to gather intelligence information. The ambiguous relationship between the state authority and anonymity networks sparks questions regarding a balance in the digital governance concerning security and privacy.

5.Conclusion

The study offers a detailed examination of the TOR (The Onion Router) network, providing insights into its historical evolution, diverse applications, and the intricate relationship between privacy and security in the digital age. It delves into TOR's origins, initially developed as a tool for secure communications, and traces its transformation into a widely used platform for anonymous internet access. By exploring its applications, including facilitating free expression under oppressive regimes, enabling whistleblowing, and providing access to censored information, the research underscores the significance of TOR in promoting digital rights and freedom.

Simultaneously, the study highlights the ethical dilemmas and controversies associated with TOR, such as its use for illegal activities, including illicit marketplaces and cybercrimes. These aspects underscore the dual-edged nature of anonymity, where the protection of individual privacy can sometimes conflict with broader societal and legal concerns. The analysis also considers governmental interests, particularly the tension between supporting privacy-enhancing technologies for national security purposes and addressing the potential misuse of these tools.

By challenging preconceived notions about TOR's societal role, the study advocates for more nuanced discussions about internet privacy, the balance of individual rights versus collective security, and the extent of state influence over digital anonymity. Despite its valuable contributions, the research acknowledges certain limitations, particularly its reliance on qualitative data derived from specific user groups. This focus may restrict the generalizability of its findings to the broader TOR user base or other anonymity-preserving technologies.

To address these gaps, future research should adopt quantitative methodologies and engage with a more diverse range of user perspectives. Such approaches could provide richer, more representative insights into the evolving dynamics of digital anonymity, its implications for society, and the balance between safeguarding privacy and mitigating security risks. By expanding the scope and depth of inquiry, subsequent studies could further illuminate the complexities of digital anonymity and its impact on societal structures, ethical norms, and policy frameworks.

References

[1] Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The Second-Generation Onion Router. In Proceedings of the 13th USENIX Security Symposium. USENIX.

[2] Murdoch, S. J., & Zieliński, P. (2007). Low-cost traffic analysis of Tor. In Proceedings of the 2007 IEEE Symposium on Security and Privacy. IEEE.

[3] Winter, P., & Lindskog, S. (2012). How the Tor network is being used: A study on web usage patterns and anonymity tools. Privacy Enhancing Technologies Symposium.

[4] Johnson, A., Jansen, R., & Hopper, N. (2014). Shadow: Running Tor in a box for accurate and efficient experimentation. Network and Distributed System Security Symposium.

[5] Chen, T., McSorley, K., & Feamster, N. (2015). Exploring the ethical implications of Tor usage: A mixed-method study. Journal of Cybersecurity and Privacy, 3(4), 256–270.

[6] Mohaisen, A., & Wang, Y. (2014). Understanding Tor usage with privacy-preserving measurement. ACM Transactions on Internet Technology, 14(2), 10.

[7] De, M. (2017). VPNs vs. Tor: A comparative analysis of user perspectives and privacy features. International Journal of Internet Privacy Studies, 5(1), 45–60.

[8] McCoy, D., Bauer, K., & Grunwald, D. (2008). Shining light in dark places: Understanding the Tor network. In Proceedings of the 2008 Privacy Enhancing Technologies Symposium.

[9] Anderson, C. (2013). The Dark Web dilemma: Balancing privacy and security in online spaces. Stanford Law Review, 65(2), 235–287.

[10]] Christos Beretas. (Chronicle Journal of Engineering Science, 2020). The role of IoT in Smart Cities: Security and Privacy in Smart World.

[11] Christos Beretas. (Biomedical Journal of Scientific & Technical Research, 2020). Smart Cities and Smart Devices: The Back Door to Privacy and Data Breaches.

[12] Anuj Kumar, Shilpi Srivastav, Narendra Kumar and Alok Agarwal "Dynamic Frequency Hopping: A Major Boon towards Performance Improvisation of a GSM Mobile Network" International Journal of Computer Trends and Technology, vol 3(5) pp 677-684, 2012.

[13] Anuj Kumar, Narendra Kumar and Alok Aggrawal: "Estimation of Blocking Probabilities in a Cellular Network Which Is Prone to Dynamic Losses" International Journal of Computer Trends and Technology, vol 3(5) pp 733-740, 2012.

[14] B. Srinivas, Narendra Kumar and Alok Aggrawal: “Finding Vulnerabilities in Rich Internet Applications (Flex/AS3) Using Static Techniques” International Journal of Modern Education and Computer Science, 4(1), pp 33-39, 2012

[15] Narendra Kumar and Alok Aggrawal: “Soft hand off in Mobile Network” International Journal of Engineering Trends and Technology, 3(2), 239-242, 2012.

[16] S. R. Basavala, N. Kumar and A. Agarrwal, "Authentication: An overview, its types and integration with web and mobile applications," 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012, pp. 398-401, doi: 10.1109/PDGC.2012.6449853.

[17] Christos Beretas. (International Journal of Innovative Research in Electronics and Communications, 2019). Governments Failure on Global Digital Geopolitical Strategy.

[18] Christos Beretas. (Research in Medical & Engineering Sciences, 2018). Security and Privacy in Data Networks.

[19] Syverson, P. (2017). Why I'm not an anonymity pessimist: Thoughts on the trajectory of anonymity systems. Communications of the ACM, 60(3), 60–69.