INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume08 Issue06, June-2023, pg. 13-16

Published Date: - 21-06-2023

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

SECURE NET: ENSURING PRIVACY AND TRUST THROUGH ANONYMOUS AND DISTRIBUTED AUTHENTICATION IN PEER-TO-PEER NETWORKS

Janaka Lavakumar

Department of Computer Engineering, University of Peradeniya, Sri Lanka

Abstract: In peer-to-peer (P2P) networks, ensuring privacy and trust is of utmost importance due to the decentralized nature of the communication. Traditional authentication methods often fall short in providing anonymity and robustness against malicious attacks. To address these challenges, we propose Secure Net, a novel framework that combines anonymous and distributed authentication mechanisms. Secure Net employs cryptographic techniques to protect user identities while enabling secure and reliable communication in P2P networks. By distributing the authentication process across multiple nodes, Secure Net mitigates the risk of single points of failure and enhances the overall resilience of the network. Through extensive evaluations, we demonstrate the effectiveness of Secure Net in safeguarding privacy, maintaining trust, and providing seamless authentication in P2P environments.

Keywords: Peer-to-Peer Networks, Authentication, Privacy, Trust, Anonymity, Distributed Systems, Cryptography, Resilience.

INTRODUCTION

Peer-to-peer (P2P) networks have gained significant popularity due to their decentralized architecture and efficient resource sharing capabilities. However, ensuring privacy and trust in P2P networks poses significant challenges. Traditional authentication methods often rely on centralized authorities or require participants to reveal their identities, which compromises privacy and opens the door to malicious attacks. Therefore, there is a pressing need for a robust authentication mechanism that guarantees anonymity, maintains trust, and ensures secure communication in P2P networks.

In this paper, we present Secure Net, a novel framework designed to address the authentication challenges in P2P networks. Secure Net leverages the power of anonymous and distributed authentication mechanisms to provide a secure and trustworthy environment for P2P communication. By combining cryptographic techniques with decentralized authentication protocols, Secure Net aims to protect user identities, prevent identity theft, and mitigate the risk of malicious activities.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume08 Issue06, June-2023, pg. 13-16

Published Date: - 21-06-2023

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

METHOD

Secure Net utilizes a multi-layered approach to achieve anonymous and distributed authentication in P2P networks. The core components of Secure Net are as follows:

Anonymous Identity Generation: Secure Net generates unique anonymous identities for participants in the P2P network. This process involves cryptographic techniques such as public-key cryptography and digital signatures to ensure the authenticity and integrity of the generated identities.

Distributed Authentication: Secure Net distributes the authentication process across multiple nodes in the P2P network. Each participating node acts as an authentication server, verifying the identities of other nodes based on the received authentication requests. This distributed approach eliminates the reliance on a single point of failure and enhances the overall resilience of the authentication system.

Trust Establishment: Secure Net incorporates trust mechanisms to establish and maintain trust among the participating nodes. Trust is established based on a combination of factors, including past interaction history, reputation scores, and recommendations from trusted peers. This trust-based approach helps identify and mitigate the risks associated with malicious or compromised nodes.

Secure Communication Channels: Once authenticated, Secure Net establishes secure communication channels between nodes using encryption algorithms and secure key exchange protocols. These measures ensure the confidentiality, integrity, and authenticity of the data exchanged between nodes, protecting against eavesdropping and tampering attacks.

To evaluate the effectiveness of Secure Net, we conducted extensive simulations and performance analysis. We measured various metrics such as authentication success rate, communication overhead, and resilience against different types of attacks. The results demonstrate that Secure Net provides robust authentication, maintains privacy, and establishes trust in P2P networks, making it a promising solution for secure and reliable communication in decentralized environments.

RESULTS

The evaluation of Secure Net yielded promising results, demonstrating its effectiveness in ensuring privacy, trust, and secure communication in P2P networks. The following key findings were observed:

Authentication Success Rate: Secure Net achieved a high authentication success rate, indicating its ability to accurately verify the identities of participants in the P2P network. The distributed nature of the authentication process contributed to the resilience of the system, reducing the chances of authentication failures due to single points of failure.

Volume08 Issue06, June-2023, pg. 13-16

Published Date: - 21-06-2023

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

Privacy Protection: Secure Net successfully provided anonymity for participants by generating unique anonymous identities. This safeguarded user privacy and prevented identity theft, as the actual identities of users remained hidden during the authentication process.

Trust Establishment: The incorporation of trust mechanisms in Secure Net facilitated the establishment and maintenance of trust relationships among participating nodes. The combination of historical interactions, reputation scores, and peer recommendations enabled the identification and avoidance of potentially malicious or compromised nodes, thus enhancing the overall trustworthiness of the network.

Secure Communication Channels: Secure Net ensured secure communication channels between authenticated nodes, employing encryption algorithms and secure key exchange protocols. This protected the integrity, confidentiality, and authenticity of the data exchanged, mitigating the risk of eavesdropping and tampering attacks.

DISCUSSION

The results highlight the significant advantages of Secure Net in addressing the authentication challenges in P2P networks. By combining anonymous and distributed authentication mechanisms, Secure Net strikes a balance between privacy, trust, and security. The distributed nature of authentication mitigates the vulnerabilities associated with centralized authentication systems, while the anonymity feature protects user identities and ensures privacy.

The incorporation of trust mechanisms in Secure Net enables nodes to make informed decisions about interacting with other participants, enhancing the overall reliability and trustworthiness of the P2P network. The secure communication channels provided by Secure Net ensure that sensitive information remains protected throughout the communication process.

It is important to note that while Secure Net demonstrates promising results, there are certain limitations. The performance of Secure Net can be influenced by network size, node churn, and the presence of malicious nodes. Further research and optimization are required to address these challenges and improve the scalability and resilience of Secure Net in larger P2P networks.

CONCLUSION

In conclusion, Secure Net offers a robust solution for anonymous and distributed authentication in P2P networks. By combining cryptographic techniques, anonymous identity generation, distributed authentication, trust establishment, and secure communication channels, Secure Net ensures privacy, maintains trust, and enables secure communication in decentralized environments.

The evaluation results demonstrate that Secure Net effectively verifies participant identities, protects user privacy, establishes trust relationships, and provides secure communication channels. However, further

Volume08 Issue06, June-2023, pg. 13-16

Published Date: - 21-06-2023

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

research and optimizations are necessary to address scalability and resilience concerns in larger P2P networks.

Secure Net has the potential to enhance the security and trustworthiness of P2P networks, making it a valuable contribution to the field of decentralized communication. With continued advancements and refinements, Secure Net can pave the way for more secure and privacy-preserving P2P applications and services.

REFERENCES

1. Ahmed, R., & Boutaba, R. (2010). A survey of distributed search techniques in large scale distributed systems. IEEE Communications Surveys & Tutorials, 13(2), 150-167. https://ieeexplore.ieee.org/abstract/document/5473882
2. Alawatugoda, J. (2017). Generic construction of an eCK- secure key exchange protocol in the standard model. International Journal of Information Security, 16(5), 541-557. https://doi.org/10.1007/s10207-016-0346-9
3. Alilwit, N. (2020). Authentication based on blockchain. Doctoral Dissertations and Master's Theses, EmbryRiddle Aeronautical University, (548).
4. Asif, M., Aziz, Z., Bin Ahmad, M., Khalid, A., Waris, H. A., & Gilani, A. (2022). Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. Sensors, 22(7), 2604. https://doi.org/10.3390/s22072604
5. Backx, P., Wauters, T., Dhoedt, B., & Demeester, P. (2002, October). A comparison of peer-to-peer architectures. In Eurescom Summit (Vol. 2). Citeseer.
6. Beverly Yang, B., & Garcia-Molina, H. (2003). Design a super-peer network. Data Engineering, 2003. Proceedings. 19th International Conference on, p, 49-60.
7. Bob, A., David, A., Greg, B., & Fred, E. (2005). The PGP trust model.
8. Bresson, E., Stern, J., & Szydlo, M. (2002, August). Threshold ring signatures and applications to ad-hoc groups. In Annual International Cryptology Conference (pp. 465-480). Springer, Berlin, Heidelberg.https://link.springer.com/chapter/10.1007/3-540-45708-9_ 30
9. Cramer, R., & Damgård, I. (1997, May). Linear zero- knowledge-A note on efficient zero-knowledge proofs and arguments. In Proceedings of the twenty- ninth annual ACM symposium on Theory of computing (pp. 436-445). https://dl.acm.org/doi/pdf/10.1145/258533.258635