



e-ISSN:2582-7219



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 11, November 2024



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521



6381 907 438



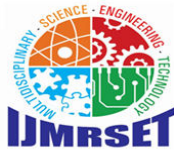
6381 907 438



ijmrset@gmail.com



www.ijmrset.com



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fortifying Highly Secure Data Communication between Decentralized Army Stations using Blockchain Technology

Shubham Gaikwad¹, Aditya Sawwase², Rohan Dahihande³, Prof. R. C. Pachhade⁴

Students, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahmednagar,
Maharashtra, India^{1,2,3}

Professor, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahmednagar,
Maharashtra, India⁴

ABSTRACT: The idea focuses on enhancing the security and reliability of data exchange between military units. Traditional methods of secure communication often involve centralized systems, which can be vulnerable to breaches and single points of failure. By utilizing blockchain technology, the implementing idea introduces a decentralized approach that ensures data integrity and security through a distributed ledger system.

In this system, blockchain provides a tamper-proof record of all communications, ensuring that data is encrypted, verified, and resistant to unauthorized access. This decentralized model eliminates the need for a central authority, reducing potential vulnerabilities and increasing the resilience of the communication network. As a result, the system aims to offer a more secure, reliable, and robust solution for confidential data transmission between army stations, enhancing operational security and efficiency.

KEYWORDS: Encryption, Decryption, Digital Hashing, Military information, Key Generation, Decentralize Data Storage System, Cryptographic Hashing, Blockchain Technology, etc.

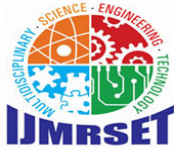
I. INTRODUCTION

In modern military operations, secure and reliable communication between army stations is crucial for effective coordination and mission success. Traditional communication systems often rely on centralized infrastructures, which can be susceptible to security breaches and operational failures. Such vulnerabilities can compromise sensitive data and disrupt critical military activities. Addressing these challenges requires a more resilient and secure approach to data communication.

The system aims to overcome these limitations by employing blockchain technology. Unlike traditional centralized systems, blockchain operates on a decentralized network of nodes that collectively manage and verify data transactions. This decentralized nature significantly enhances the security and reliability of communications by eliminating single points of failure and reducing the risk of unauthorized access.

By integrating blockchain technology, the idea ensures that all data exchanged between the two army stations is encrypted, immutable, and auditable. This approach provides a secure communication channel that is resistant to tampering and interception. As a result, military personnel can trust the integrity and confidentiality of their data, leading to improved operational security and more effective coordination between decentralized army units.

The subsequent sections will delve into the specific modules, methodologies, and anticipated outcomes, showcasing the idea's commitment to advancing the state-of-the-art in secure military communications.



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

- "A Secure Blockchain Enabled V2V Communication System Using Smart Contract" by Debashis Das, Sourav Banerjee, Pushpita Chatterjee, Uttam Ghosh (2023).
- Smart Contracts: Security Issues and Future Research Opportunities" by M. S. Ali, M. Vecchio, M. Pinchetti, and A. Antonelli (2021). This research examines the security vulnerabilities and potential of smart contracts. The use of smart contracts in automating security protocols for military communications is directly relevant to this system, providing a basis for implementing automated security measures.
- Blockchain-Based Secure Data Sharing for IoT Devices in Smart Home Environments" by Y. Zhang, J. Wen, D. Ma, and R. Zhang (2020). This paper investigates the application of blockchain for secure data sharing in IoT environments. The methodologies discussed can be adapted for secure data communication between decentralized army stations, particularly in enhancing data integrity and privacy.
- A Survey on the Security of Blockchain Systems" by L. Chen, L. Xu, Z. Shah, and Y. Gao (2020). This survey reviews various security aspects of blockchain technology, including cryptographic techniques and consensus mechanisms. The insights from this paper are crucial for understanding the security measures needed for a blockchain-based military communication system.
- Decentralized and Secure Communication for Military Applications Using Blockchain Technology" by J. Zhang et al. (2019). This study explores the use of blockchain technology in military communication systems. It demonstrates how blockchain can enhance the security and reliability of data transmission in decentralized military networks, providing a solid foundation for this idea's objectives.
- Blockchain Technology: Principles and Applications" by M. Pilkington (2016). This paper provides an in-depth overview of blockchain technology, discussing its foundational principles and various applications. It highlights the potential of blockchain for creating secure and decentralized systems, emphasizing its relevance for secure communication networks.

III. PROBLEM STATEMENT

Current centralized communication systems between army stations are prone to security vulnerabilities, single points of failure, and potential data breaches. These weaknesses can compromise the confidentiality and integrity of sensitive military information, leading to compromised operations and reduced trust in the communication network. There is a need for a more secure and reliable solution that can ensure safe, tamper-proof data exchange between decentralized army stations.

IV. OBJECTIVES

The primary objectives are to:

1. **To design and implement** a decentralized communication framework that enhances data security and resilience against cyber threats.
2. **To develop and integrate** advanced encryption algorithms to ensure confidentiality and integrity of sensitive military communications.
3. **To establish** a real-time data transmission system that minimizes latency and facilitates timely decision-making between army stations.
4. **To enable** seamless interoperability with existing military communication systems, allowing for easy integration and scalability.
5. **To implement** robust authentication mechanisms to verify user identities and prevent unauthorized access to the communication network.



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. PROPOSED SYSTEM

The proposed system design for this paper is meticulously crafted to address the critical security challenges inherent in military communication. The backbone of the design is a decentralized blockchain network, comprising nodes representing each army station, fostering a tamper-proof and transparent ledger. Smart contracts, powered by blockchain technology, automate data transactions, ensuring secure exchanges while upholding data integrity and authenticity. Advanced cryptographic techniques, including asymmetric encryption and zero-knowledge proofs, are integrated to fortify data confidentiality. Decentralized identity management enhances user authentication through blockchain verification and multifactor authentication.

Secure communication protocols, such as SSL and secure messaging, are implemented for encrypted data transmission, while real-time monitoring ensures threat detection. Immutable data storage on the blockchain guarantees data traceability and historical tracking. A user-friendly interface facilitates cross-agency collaboration, providing secure access control mechanisms for streamlined data sharing between army stations. Continuous monitoring and auditing mechanisms, including intrusion detection systems and regular transaction audits, contribute to proactive threat mitigation. Overall, this proposed system design harnesses the power of blockchain, cryptography, and secure communication protocols to create a robust framework that not only addresses the vulnerabilities of traditional military communication but also introduces innovative features for enhanced security, integrity, and efficiency in data exchanges between two army stations.

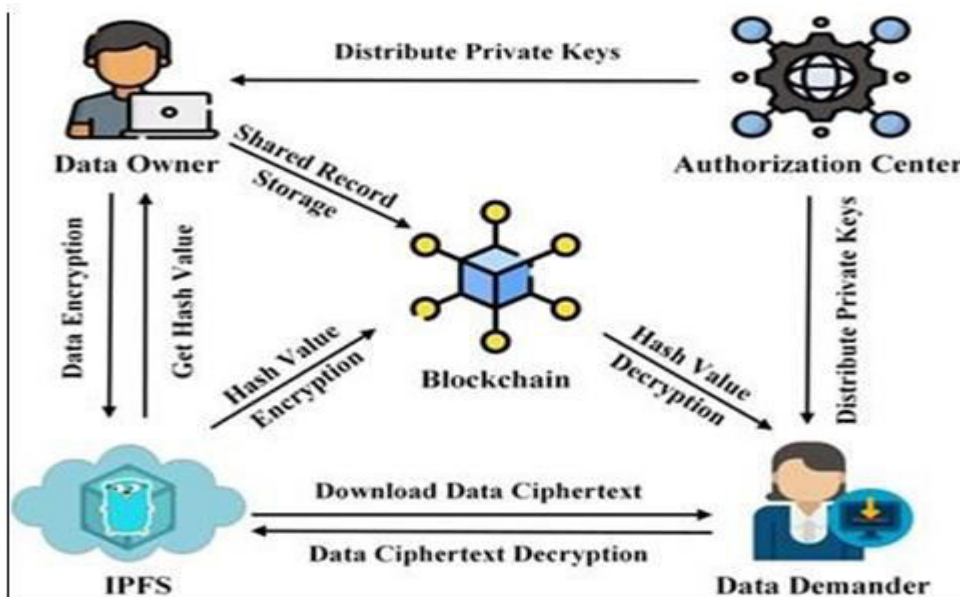
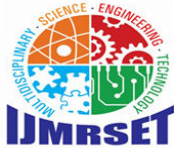


Fig.1: Proposed System Architecture

The proposed system leverages blockchain technology to establish a secure and reliable communication network between two decentralized army stations. By utilizing a decentralized ledger, the system ensures that all data exchanged between the stations is recorded in an immutable and tamper-proof manner. Each transaction is encrypted and added to the blockchain in a secure manner, creating a transparent and verifiable record of all communications. This approach significantly enhances the security of the data, making it resistant to unauthorized access and alterations.



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

ACKNOWLEDGMENT

We would prefer to give thanks the researchers likewise publishers for creating their resources available. We are conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

1. Wang, J., & Li, Y. (2022). "Resilient Communication Framework for Decentralized Military Operations." *IEEE Transactions on Mobile Computing*, 21(5), 2030-2042.
2. Khan, M., & Al-Riyami, A. (2021). "Decentralized Communication Systems for Tactical Military Operations." *International Journal of Advanced Computer Science and Applications*, 12(4), 132-139.
3. Pezeshki, S., & Sharif, M. (2021). "A Secure Communication Model for Military Wireless Networks Using Blockchain Technology." *IEEE Access*, 9, 99800-99810.
4. Sharma, R., & Kumar, V. (2021). "Performance Analysis of Secure Communication Protocols in Military Applications." *Journal of Information Security and Applications*, 57, 102693.
5. Mishra, A., & Kumar, A. (2020). "Challenges and Solutions in Secure Data Communication in Military Networks." *International Journal of Computer Applications*, 975, 8887.
6. Panda, S., & Roy, S. (2020). "Cybersecurity for Military Communication Systems: Current Trends and Future Directions." *IEEE Communications Surveys & Tutorials*, 22(4), 2331-2356.
7. Chen, T., Zhang, Y., & Xu, W. (2020). "Secure Communication Protocol for Military Wireless Networks." *IEEE Transactions on Information Forensics and Security*, 15, 2433-2446.
8. Liu, J., & Wang, Y. (2019). "A Review of Encryption Techniques for Secure Military Communications." *Military Communications and Information Systems Conference (MilCIS)*, 1-6.
9. Seyed, M. H., & Hoshmand, A. (2019). "Decentralized Security Architecture for Military Communication Systems." *Journal of Computer Networks and Communications*, 2019.
10. Hussain, A., & Iqbal, M. (2018). "A Survey of Secure Communication in Wireless Military Networks." *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 15(3), 233-246.
11. G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking Beyond Banks and Money*. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.
12. L. Luu et al., "A secure sharding protocol for open blockchains," *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 17–30.
13. Leible, S.; Schlager, S.; Schubotz, M.; Gipp, B. A review on blockchain technology and blockchain projects fostering open science. *Front. Blockchain* 2019, 2, 28
14. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* 2019, 36, 55–81.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com