IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203032

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

Shubham Gaikwad[1], Aditya Sawwase[2], Rohan Dahihande[3], R. C. Pachhade[4]

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, India[4]

ABSTRACT: The project 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, this project 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 project 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 secures approach to data communication .

The project 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 project 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 [7].
The subsequent sections will delve into the specific modules, methodologies, and anticipated outcomes, showcasing the project's commitment to advancing the state-of-the-art in secure military communications.

II. RELATED WORK

Several studies have explored the use of blockchain technology for secure communication in military and defense applications. Traditional military networks rely on centralized architectures, making them vulnerable to cyberattacks, data breaches, and single points of failure. Recent advancements in decentralized communication frameworks leverage blockchain's immutable ledger, cryptographic encryption, and consensus mechanisms to ensure tamper-proof and highly secure data exchange between military stations. Researchers have proposed smart contract-based authentication and zero-trust architectures to enhance security while preventing unauthorized access. Additionally, hybrid blockchain

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203032

models combining public and private chains have shown promise in balancing confidentiality and operational transparency. However, challenges such as latency, scalability, and energy consumption remain key areas for optimization. This project builds upon these existing works by developing an efficient and resilient blockchain-based communication framework tailored for decentralized army stations, ensuring real-time, secure, and interference-free military data exchange.

- Smart Contracts: Security Issues and Future Research Opportunities" by **M. S. Ali, M. Vecchio, M. Pinchetti, and A. Antonelli (2021)** [15]. 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 project, providing a basis for implementing automated security measures [11-15].
- Blockchain-Based Secure Data Sharing for IoT Devices in Smart Home Environments" by **Y. Zhang, J. Wen, D. Ma, and R. Zhang (2020)** [14]. 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) [13]. 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) [12]. 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 project's objectives.
- Blockchain Technology: Principles and Applications" by M. Pilkington (2016) [11]. 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.

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

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203032

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 [16].

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 .

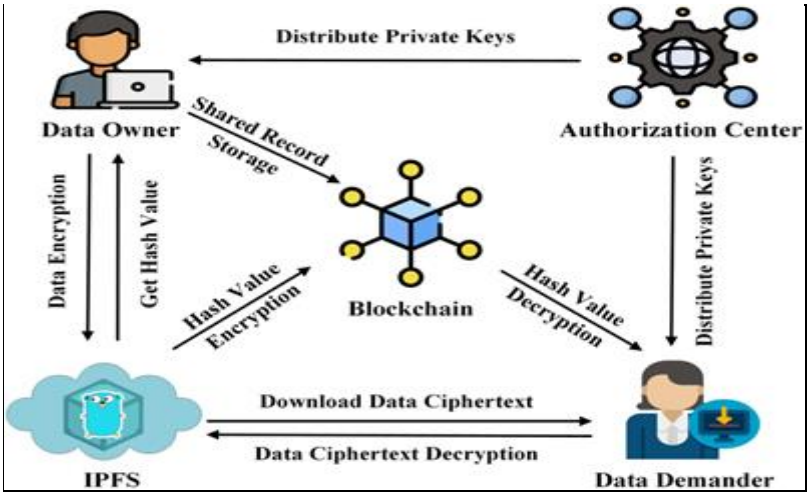


Fig.1: Proposed System Architecture

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 [17-20].

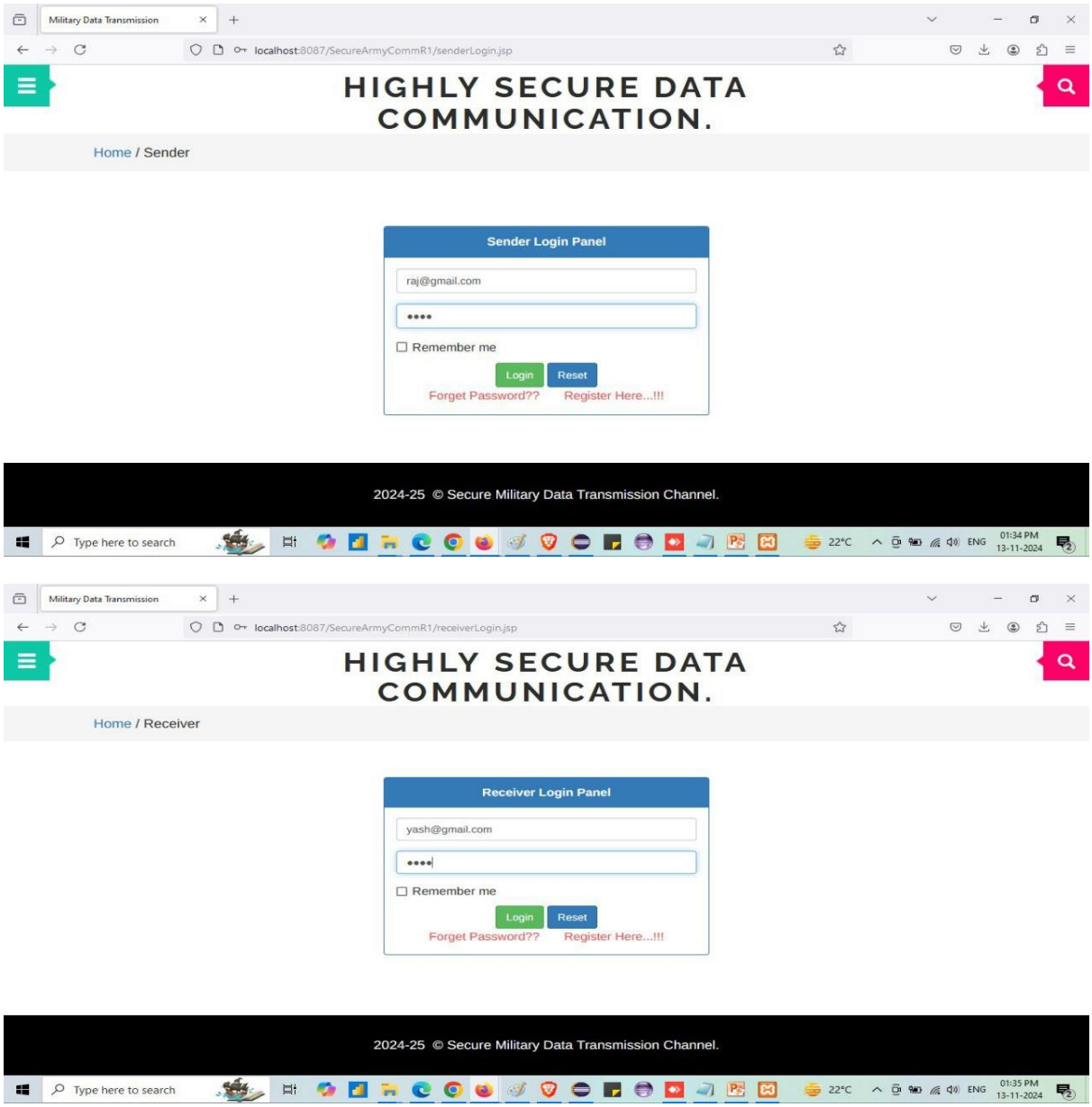
VI. RESULT ANALYSIS

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203032



VII. CONCLUSION

In conclusion, the development of a highly secure data communication system for decentralized army stations addresses critical challenges in military operations. The proposed system presents a significant advancement in military communication security. By leveraging blockchain's decentralized and immutable ledger, the system ensures that all data exchanged between army stations remains secure, tamper-proof, and reliable. This approach addresses critical vulnerabilities present in traditional centralized communication systems, providing a more resilient network that minimizes risks of unauthorized access and data breaches.

In addition to enhancing security, the blockchain-based system improves operational efficiency by ensuring continuous and reliable communication between decentralized units. The real-time data verification and decentralized nature of blockchain reduce the likelihood of disruptions and ensure accurate, trustworthy exchanges of sensitive information. Overall, the project successfully creates a robust framework for secure communication, supporting effective coordination and decision-making in military operations.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203032

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] Debashis Das, Sourav Banerjee, Pushpita Chatterjee, Uttam Ghosh (2022). "A Secure Blockchain Enabled V2V Communication System Using Smart Contract". IEEE Transactions On Intelligent Transportation Systems, Vol. 24, No. 4, April 2023.
[2] Wang, J., & Li, Y. (2022). "Resilient Communication Framework for Decentralized Military Operations." IEEE Transactions on Mobile Computing, 21(5), 2030-2042.
[3] 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.
[4] Pezeshki, S., & Sharif, M. (2021). "A Secure Communication Model for Military Wireless Networks Using Blockchain Technology." IEEE Access, 9, 99800-99810.
[5] Sharma, R., & Kumar, V. (2021). "Performance Analysis of Secure Communication Protocols in Military Applications." Journal of Information Security and Applications, 57, 102693.
[6] Mishra, A., & Kumar, A. (2020). "Challenges and Solutions in Secure Data Communication in Military Networks." International Journal of Computer Applications, 975, 8887.
[7] Panda, S., & Roy, S. (2020). "Cybersecurity for Military Communication Systems: Current Trends and Future Directions." IEEE Communications Surveys & Tutorials, 22(4), 2331-2356.
[8] Chen, T., Zhang, Y., & Xu, W. (2020). "Secure Communication Protocol for Military Wireless Networks." IEEE Transactions on Information Forensics and Security, 15, 2433-2446.
[9] Liu, J., & Wang, Y. (2019). "A Review of Encryption Techniques for Secure Military Communications." Military Communications and Information Systems Conference (MilCIS), 1-6.
[10] Seyed, M. H., & Hoshmand, A. (2019). "Decentralized Security Architecture for Military Communication Systems." Journal of Computer Networks and Communications, 2019.
[11] 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.
[12] 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 andMoney. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.
[13] L. Luu et al., "A secure sharding protocol for open blockchains," Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 17–30.
[14] Leible, S.; Schlager, S.; Schubotz, M.; Gipp, B. A review on blockchain technology and blockchain projects fostering open science. Front. Blockchain 2019, 2, 28
[15] 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.
[16] Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security. Digit. Commun. Netw. 2020, 6, 147–156.
[17] Chao, H.; Maheshwari, A.; Sudarsanan, V.; Tamaskar, S.; DeLaurentis, D.A. UAV traffic information exchange network. In Proceedings of the Aviation Technology, Integration, and Operations Conference, Atlanta, GA, USA, 25–29 June 2018
[18] Golosova, J.; Romanovs, A. The Advantages and Disadvantages of the Blockchain Technology. In Proceedings of the IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, Lithuania, 8–10 November 2018
[19] Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access 2019, 7, 117134–117151
[20] Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access 2019, 7, 22328–22370
[21] Liao, S.; Wu, J.; Li, J.; Bashir, A.K.; Yang, W. Securing collaborative environment monitoring in smart cities using blockchain enabled software-defined internet of drones. IEEE Internet Things Mag. 2021, 4, 12–18

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com