Quantum-Secured Military Communication Networks with Blockchain Integrity

1G. Beulah Rani , 2P.Neela Sundari ,3Kanta Showribabu, 4Jarugumalli Vamsi Babu, 5Lingiri Nagul Meera, 6Mandalapu Nikhil Chowdary

1,2Assistant Professor, Department of CSE, KKR & KSR Institute of Technology and Sciences, A.P, India.
3,4,5,6 B.Tech Student, Department of CSE, KKR & KSR Institute of Technology and Sciences, A.P, India.

Abstract—In the contemporary landscape of military and defence operations, ensuring the utmost security and integrity of communication channels is paramount. Conventional cryptographic methods, while robust, face evolving threats in an era of sophisticated cyber adversaries. In response, this research pioneers a groundbreaking integration of Quantum Cryptography and Blockchain technology to fortify military communication networks. The challenges faced by current military communication systems lie in the vulnerability of cryptographic keys and the potential for data tampering. To address these issues, our proposed system leverages Quantum Key Distribution (QKD) for ultra-secure key exchange. QKD harnesses the principles of quantum mechanics, providing an unbreachable shield against eavesdropping and ensuring the authenticity of communication between commandos. However, securing the communication pathway is only part of the equation. The integrity of military operation logs and communication records is equally crucial. Herein, Blockchain technology is employed to establish a decentralized and tamper-proof ledger. This ledger, distributed across military nodes, serves as an indelible record of operations, preventing unauthorized alterations and ensuring transparency. In the current landscape where cyber threats are ever-evolving, our proposed Quantum-Secured Military Communication Networks with Blockchain Integrity stand as an avant-garde solution. By amalgamating the power of quantum-resistant encryption and tamper-proof distributed ledgers, our system not only mitigates the risks faced by contemporary military communication but also outshines traditional cryptographic methods. The research validates the efficacy of our proposed model through comparative studies, pitting it against existing systems. Results consistently demonstrate the superiority of our approach in thwarting potential breaches, ensuring secure and authenticated military communication. In an era where information is a critical asset, our technology emerges as a sentinel, fortifying the foundations of military communication networks and upholding the security, integrity, and confidentiality demanded by the modern defence landscape.

Index Terms—Principle of Quantum physics, BB84 Protocol, Blockchain, Smart contracts.

INTRODUCTION

Ensuring the security of data transmission in the dynamic environment of communication networks is a challenging task and making it protected also be a main funda of our project. As we enter the digital age, the vulnerabilities of traditional encryption methods are increasing as well as cracking of algorithm by a eaves too. Primarily due to our reliance on quantum computing. Military communication plays a pivotal role in ensuring the success a0nd security of military operations. Conventional communication systems have faced many challenges related to security, reliability, availability and data tampering. Quantum computers pose a potential threat to traditional cryptographic methods. The most significant and relavant risk arises from their capability to break widely-used encryption algorithms through a process known as quantum decryption. Traditional cryptographic systems rely on the difficulty of certain mathematical problems.

In situation of military communication, a quantum computer could potentially decrypt confidential information that was considered secure using classical encryption methods. This threat extends to the compromise of classified messages, sensitive operational plans, and other critical military communications. Military communication often involves the transmission of classified and sensitive information. If intercepted by a quantum computer equipped with shor's algorithm, encrypted messages could be decrypted, it will be compromising the confidentiality of military operations. This raises an important question: how to ensure secure communications in the coming era of quantum. Conventional communication systems have reached a high level of maturity. However, it has some limitations in terms of for instance availability, bandwidth, direction (or lack of it) and security. Our proposed system

leverages quantum with blockchain integration in that quantum teleportation is an anomalous phenomenon based on the principle of quantum entanglement, providing a secure way to send quantum messages between spatially separated nodes. This represents a secure means of cryptographic exchange that cannot be eavesdropped, despite advances in quantum computing. Use python to model quantum properties such as entanglement and superposition and connect theoretical ideas with real- world applications. This simulation environment serves as a control environment for simulating quantum behaviour, allowing comprehensive evaluation of the feasibility and stability of the proposed quantum-enhanced key switch.

Two key principles of quantum mechanics, highly relevant for quantum communication, are superposition and entanglement. First, superposition is a property of states of quantum mechanical systems, like a particle. It means that although a system is definitely in one state, it can also be considered as being in several states. This is a non-classical concept since a classical system is always in a definite state specifying, e.g., the position of a particle. In contrast, quantum mechanical systems generally are complex linear combinations of these definite states. Second, two quantum mechanical systems are entangled if one system cannot be fully described without referring to the other. Such a system is described by one, non-separable state. Manipulating one of the subsystems will have an immediate consequence on the other subsystems, independent on how far these subsystems are apart. Moreover, the results of measurements of observables in an entangled system will have correlations beyond what is possible in classical mechanics.

Blockchain is a revolutionary concept transforming traditional centralized systems into decentralized and transparent networks. Unlike conventional systems governed by a central authority, blockchain operates on a distributed ledger across a network of computers, or nodes. This ledger, structured in blocks of transactions linked together through cryptographic hashes, forms an immutable and secure chain. The decentralized nature ensures equal control among participants, eliminating the need for a single governing entity. Transactions are secured using quantum cryptographic techniques, ensuring privacy and authenticity. Its consensus mechanisms, such as proof of work or proof of stake that validates transaction authenticity across the network .and added into the blockchain. Our research substantiates the effectiveness of our proposed model through comparative studies, benchmarking it against existing systems. Consistently, the results showcase the superiority of our approach in preventing potential breaches, thereby guaranteeing secure and authenticated

Military communication. In an era where information is a paramount asset, our technology stands as a sentinel, reinforcing the pillars of military communication networks and upholding the security, integrity, and confidentiality essential in the modern defence landscape. Our proposed system leverages quantum key distribution (qkd) for ultra-secure key exchange. Qkd harnesses the principles of quantum mechanics, providing an unbreachable shield against eavesdropping and ensuring the authenticity of communication between commandos. However, safeguarding the communication pathway is just one facet of the solution. The trustworthiness of military operation logs and communication records holds equal significance. To address this, blockchain technology is incorporated to create a decentralized and tamper-proof ledger. Moreover, our proposed communication system contributes to strategic advantage on the battlefield. The ability to exchange real-time information securely enhances situational awareness and decision-making capabilities, enabling commanders to adapt rapidly to changing operational dynamics.

LITERATURE SURVEY

[1] Haoming Wang; Nan Li; Haiyang Jiang (2023), proposed the research paper “Application of Quantum Technology in Military Communications” delves into the expansive realm of quantum cryptography, emphasizing its pivotal role in enhancing network security. Employing Quantum Key Distribution (QKD), Post-Quantum Cryptography, and Counterfactual Quantum Key Distribution, the study ensures a comprehensive exploration of these methodologies.

[2] According to Niels M. P. Neumann; Maran P. P. van Heesch; Frank Phillipson; Antoine A. P. Smallegange (2021), the research paper acknowledges that although the implementation of quantum communication in current operations is not yet feasible, the field of quantum hardware development is actively evolving, with substantial investments globally. It provides an in-depth exploration of different use cases and presents the current state-of-the-art technology in quantum communication.

[3] Amool Sudhan; Manisha J Nene (2017), proposed the research paper titled "Employability of Blockchain Technology in Defence Applications," presented at the International Conference on Intelligent Sustainable Systems (ICISS). It Focuses on leveraging Blockchain technology to enhance the integrity and provenance of data in military operations conducted through networks. The paper acknowledges challenges in ensuring accountability, privacy, and data validity in the distributed and diverse environment of NEMO.

[4] Guangfu Wu; Yingjun Wang (2021), Introduces the GAC- PSPR scheme, a security and privacy management solution for Electronic Medical Record (EMR) storage on the blockchain. NTRU encryption safeguards data privacy against quantum attacks, and a lattice-based ring signature solution addresses challenges associated with large signatures and key lengths in EMR data sharing. The future scope outlined in the paper emphasizes the exploration of optimization methods for the dual chain structure.

[5] Zebo Yang; Haneen Alfauri; Behrooz Farkiani; Raj Jain; Roberto Di Pietro; Aiman Erbad (2023), the goal of this paper is to examinate the both post-quantum and quantum blockchain.It Addresses the escalating threat posed by quantum computing to existing blockchain security.The merits of this research lie in its thorough examination of both post-quantum and quantum blockchains the future scope outlined in the paper emphasizes the necessity of developing quantum-resistant blockchains to safeguard decentralized systems.

[6] Mary Subaja Christo; Anigo Merjora A.; Partha Sarathy G.; Priyanka C.; Raj Kumari M. (2019), proposed the research paper titled "An Efficient Data Security in Medical Report using Blockchain Technology," presented at the International Conference on Communication and Signal Processing (ICCSP). Advancements in secure data access mechanisms for modern healthcare systems using blockchain technology. This work contributes significantly to the ongoing efforts to enhance the security and trustworthiness of healthcare information systems.

[7] Muhammad Taimour Azhar; Muhammad Burhan Khan; Asim Ur Rehman Khan (2020), the main goal of this paper, the integration of a six-state QKD protocol ensures transaction confidentiality and integrity, validated through comprehensive simulations.Explores the fusion of blockchain and Quantum Key Distribution (QKD) protocols to enhance cryptocurrency system security, and leveraging blockchain's cryptographic security.The research contributes to future implementations of key generation protocols in evolving blockchain systems, advancing the security of cryptocurrency systems.

[8] Dharani D; Soorya R; K. Anitha Kumari (2023), aims to elevate the security standard of traditional blockchain networks, ensuring resilience against potential quantum threats. Meticulously explores post-quantum cryptographic techniques, emphasizing quantum-resistant encryption methods. Addressing the susceptibility of blockchain technology to quantum attacks, the study advocates for the integration of quantum-resistant cryptographic techniques to bolster network security.

[9] Minrui Xu; Xiaoxu Ren; Dusit Niyato; Jiawen Kang; Chao Qiu; Zehui Xiong; Xiaofei Wang; Victor C. M. Leung (2023), proposed the research paper titled "When Quantum Information Technologies Meet Blockchain in Web 3.0," published in IEEE Network. The framework encompasses key components such as enabling infrastructure, quantum cryptography protocols, and quantum blockchain-based services. This strategic move aims to enhance the privacy, scalability, and security of networking systems within the next-generation decentralized digital society.

Wei Yin; Qiaoyan Wen; Wenmin Li; Hua Zhang; Zhengping Jin (2018)," introduce the research paper that offers a comprehensive security proof and analysis, emphasizing the theoretical support provided for the application of blockchain in the post-quantum age. Addresses the susceptibility of blockchain to quantum attacks, particularly focusing on the elliptic curve digital logarithm problem (ECDLP) used for transaction authentication. To tackle the challenge of fixed wallet size while ensuring manageability, the proposed approach generates public and private keys from a set of master public and private keys (Seed Key).

[10] Ivan B. Djordjevic, Fellow (2020), make research that stands at the forefront. Delving into both discrete variable (DV) and continuous variable (CV) quantum key distribution (QKD) schemes concurrently. Envisaging connected network, terrestrial QCNs are intricately woven through Low Earth Orbit (LEO) satellite quantum networks, forming a resilient heterogeneous satellite-terrestrial QCN.

[11] Zebo Yang; Tara Salman; Raj Jain; Roberto Di Pietro (2022), the goal of this paper represents to secure decentralized identity authentication by integrating quantum PKIs and blockchains. Focusing on the theoretical aspects of utilizing quantum blockchain for achieving decentralization. The finality

of a block in Bitcoin is determined by its position in the longest chain, a concept echoed in other blockchains using similar consensus methods.The decentralized perspective of quantum applications is deemed significant and likely to shape the future of secure blockchain technologies.

[12] Rubina Akter, Sanjay Bhardwaj, Jae Min Lee and Dong- Seong Kim (2019), presents a decentralized and highly secure blockchain-based system for the military industry.The analysis explores the impact of the C3I model on artificial intelligence and advocates for the integration of blockchain to ensure high security. Simulation results indicate the proposed model's potential for enhanced accessibility, throughput, and security compared to static systems.

[13] 1st Ali Ibnun Nurhadi ,2nd Nana Rachmana Syambas (2018), proposed the research paper titled "Quantum Key Distribution (QKD) Protocols: A Survey" presented at the Conference of School of Electrical Engineering and Informatics. The security of conventional cryptography relies on mathematical complexity and time inefficiency to break algorithms, but a weak key distribution procedure can render it ineffective. Quantum Key Distribution (QKD) has emerged as a potential solution, gaining significant attention due to its promise of unconditionally secure communication based on quantum mechanics laws.

[14] Wei Cui, Tong Dou, Shilu Yan (2020), proposed an article that anticipates significant developments in both blockchain and quantum computation in the coming decade, emphasizing the active research in these fields. The security risks to classical encryption methods. The solution proposed involves integrating quantum properties into blockchain for increased robustness and efficiency. Quantum key distribution (QKD) and quantum synchronization, along with detectable Byzantine agreement (DBA), are identified as mechanisms to enhance security and achieve faster consensus in blockchain systems.

Konrad Wrona∗†, Michał Jarosz† (2019), proposed high- level architecture adheres to STANAG 4774 and 4778 standards, with a technical solution based on Hyperledger Fabric. The focus is on using blockchains to store metadata from IoT devices owned by federation members, aiding information exchange in civil-military cooperation. The article presents a blockchain-based cryptographic binding of metadata to sensor data, showcasing Hyperledger Fabric's suitability for implementation.

[15] Ram S. Mohril, Bhupendra S. Solanki, Bhupesh Kumar Lad, Member, IEEE, and Makarand S. Kulkarni (2022), describes an approach for the maintenance of military equipment is integral to achieving optimal war readiness. To meet these needs, detailed maintenance data, including information on the lowest maintainable unit for each military equipment, must be meticulously recorded. The article concludes with pragmatic analytics and underscores the inherent advantages of blockchain technology in enhancing military maintenance practices.

PROPOSED SYSTEM

Ensuring the integrity of military operation logs and communication records is equally critical to a comprehensive security approach. Blockchain technology is employed for its capability to establish a decentralized and tamper-proof ledger. The blockchain ledger is distributed across various military nodes, ensuring redundancy and resilience. Quantum principles are employed to ensure secure key distribution and provide authentication in military communication systems. The immutability of the blockchain ledger plays a crucial role in preventing unauthorized alterations to military records. Quantum entanglement establishes highly secure communication channels by providing strong assurance of the authenticity of communication partners.

Securing military communication systems against ever- evolving cyber threats is paramount. By employing a decentralized and immutable ledger, blockchain technology can enhance the security and transparency of military communication systems. Quantum cryptography offers a promising solution by utilizing the principles of quantum mechanics to secure military communication. It leverages the unique properties of quantum entities and blockchain to enable highly secure encryption and decryption processes. These systems provide secure and real-time data exchange, allowing military personnel to make swift and informed decisions between commanders.

By distributing the blockchain ledger across multiple military nodes, redundancy and resilience are ensured, minimizing the risk of data loss or manipulation. Quantum principles, such as entanglement and superposition, provide an additional layer of security, guaranteeing the authenticity and confidentiality of communication channels.

The proposed system integrates Quantum Cryptography and Blockchain technology to fortify military communication networks. Quantum Cryptography ensures ultra-secure key exchange and authentication, while Blockchain technology establishes a decentralized and tamper-proof ledger for storing communication records. This fusion of Quantum and Blockchain offers unparalleled security and integrity, safeguarding sensitive military information from cyber threats and unauthorized access.

A. Registration for a new Commander:

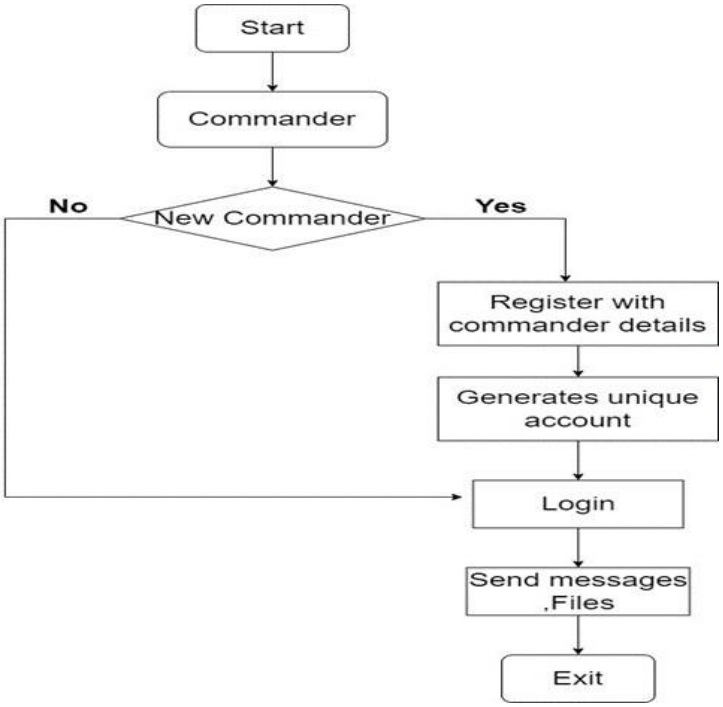

Fig 1: Registration For A New Commander

Fig. 1 shows the registration process should be done. The commander begins with a check to determine if the commander is already registered or not. According to figure1 If the commander is not found in the network, the admin is prompted to initiate the registration process. The admin then collects essential details from the commander, including their wallet address, name, and password. This information is securely stored in the system's database. Based on figure 1 Once the registration is successfully completed, the commander gains access to their account. Through the login credentials provided during registration, the commander can securely log in to the application. Once logged in, the commander can utilize the application's features to communicate with other commanders. This includes sending messages and exchanging files securely within the military network. By facilitating a streamlined registration process and providing robust security measures.

B. Authenticate the commander:

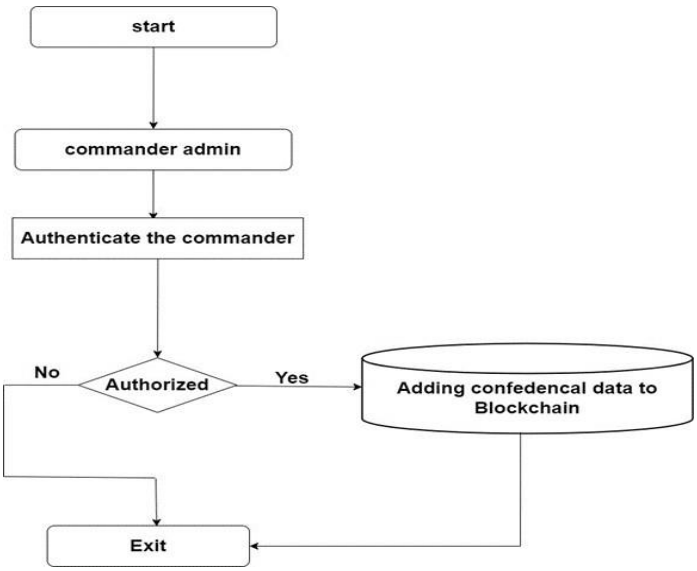

Fig 2: Authenticate The Commander

Authentication is a crucial step to ensure the security and confidentiality of communication channels. When a commander logs in to their account, they are required to provide their username (wallet address) and password. This information
is validated against the stored credentials in the network. If the provided credentials match those on record, the commander is successfully authenticated and granted access to their account.
As shown in figure 2 Once authenticated, the commander gains the ability to view received messages and files within the application. Access to these communications is restricted solely to authenticated users, ensuring that only authorized commanders can access sensitive information exchanged within the military network. This authentication mechanism helps maintain the integrity and confidentiality of communication channels, preventing unauthorized access and safeguarding critical military information.
copyright form wizard. Please complete the copyright at that time to avoid publication delays.
C. Encrypt the confidential data:

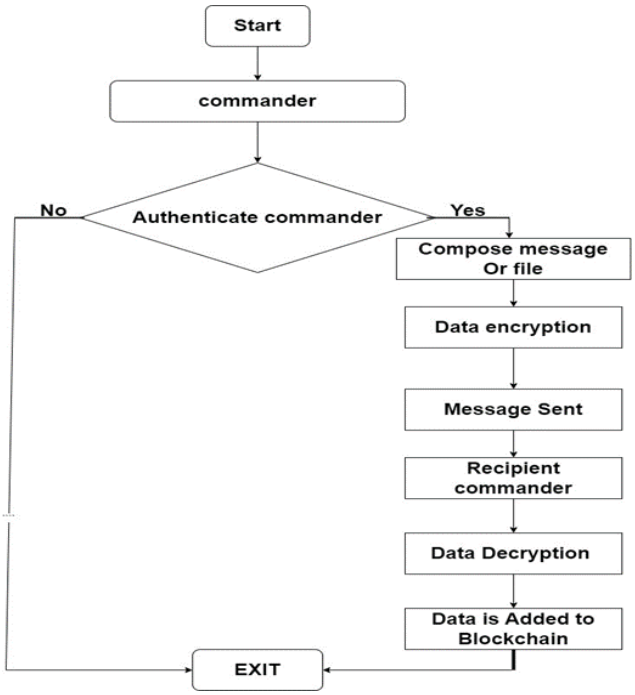

Fig 3: Communicating Confidential Data

From the figure 3 When a commander logs in using their credentials, they gain access to the functionality for sending messages and files. To send a message, the commander first composes the

message or selects the file to be sent. The data is then encrypted using advanced encryption techniques to ensure its confidentiality during transmission. Once the message is encrypted, it is sent to the recipient commander.

Upon receiving the encrypted message, the recipient commander is prompted to provide an Quantum authentication token which is created when the login into the account by the BB84 protocol. If the entered token is correct, the encrypted data is decrypted using the corresponding decryption key. This ensures that only the intended recipient can access the message content. After decryption, the recipient commander can view the message or file.

Once the recipient commander has viewed the message, the data is securely added to the blockchain. This ensures that the communication record is tamper-proof and immutable, providing a transparent and verifiable record of the interaction between the commanders. By integrating encryption, authentication, and blockchain technology, our application ensures the confidentiality, integrity, and authenticity of communication
exchanges within the military network.

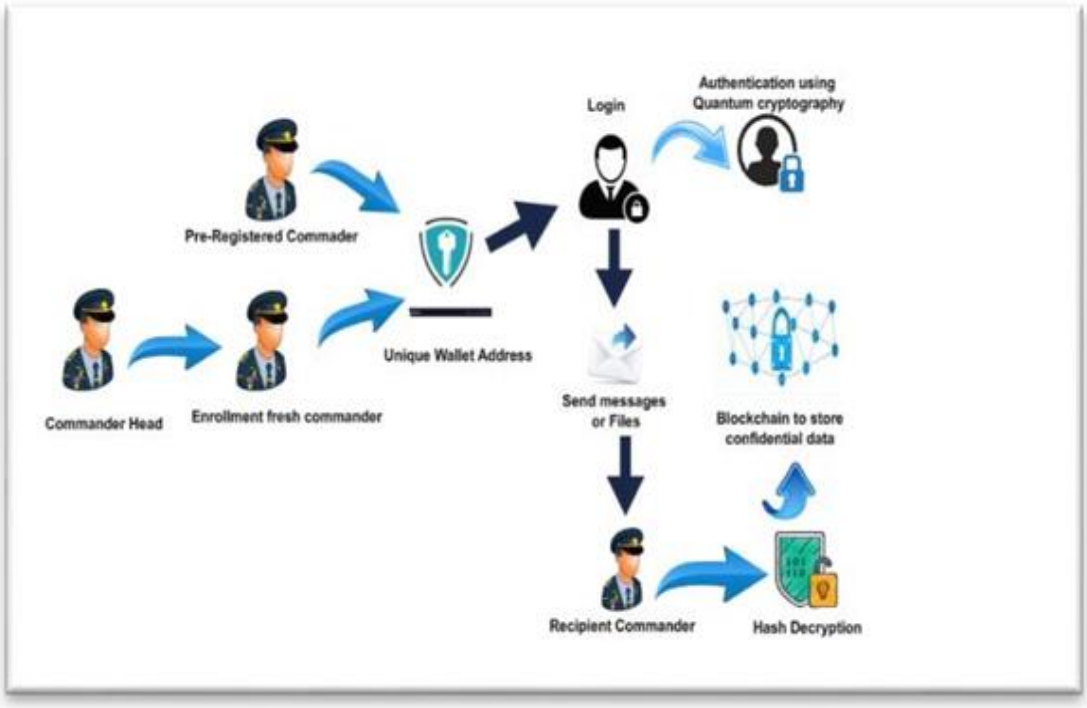

Fig 4:System Architecture-Secured Military Communication between commanders

The process commences with the commander admin initiating the registration procedure by submitting essential details such as the wallet address, username, and password. This information is pivotal for commander registration, as depicted in Figure 4. Once registered, commanders are granted access to the application by inputting their username and password into the designated login form. This step serves as a gateway to the commander's dashboard and messaging functionalities, facilitating seamless communication within the military network.

When a sender commander intends to dispatch a message, they input the recipient's wallet address and craft the message in the dedicated text field. Subsequently, the message undergoes encryption to fortify its confidentiality and security during transmission. Upon receipt of the encrypted message, BB84-based authentication can provide quantum authentication tokens. These tokens consist of quantum states encoded with information unique to each commander. By leveraging the principles of quantum mechanics. The recipient commander's application awaits an authentication token to proceed further. Upon successful authentication by entering the correct token, the encrypted message undergoes decryption and is promptly displayed within the recipient's application interface. This ensures that only authorized recipients can access and decipher the received message content.

As shown in Figure 4, our application prioritizes decentralization and integrity by storing messages in a chain format utilizing blockchain technology. This strategic approach not only enhances the security

of communication records but also fosters transparency and immutability, ensuring that the integrity of the communication data remains intact. Additionally, the application server meticulously maintains a comprehensive list of commanders authorized for communication. This ensures that only authenticated users are permitted to engage in secure messaging within the network.

RESULTS

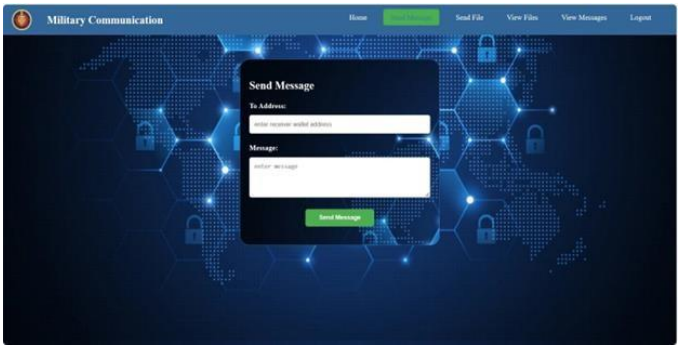

Fig 5: Commander Message Sending page where send messages to required commander

As shown in figure 5 After the commander correctly enters the login credentials, the required user interface displays, allowing for sending messages by entering the recipient wallet address and selecting the file to be sent. This ensures precise delivery to the exact receiver, facilitating secure and efficient communication within the network.

Fig 6: Commander Authenticate page to view the receive messages

deal to get login into network and site will shows sender's message or files from Sender to receiver. Upon inputting the authentication token, the receiver commander gains permission to access and view the messages sent by the sender commander. This pivotal step ensures secure and authorized communication between the two entities.

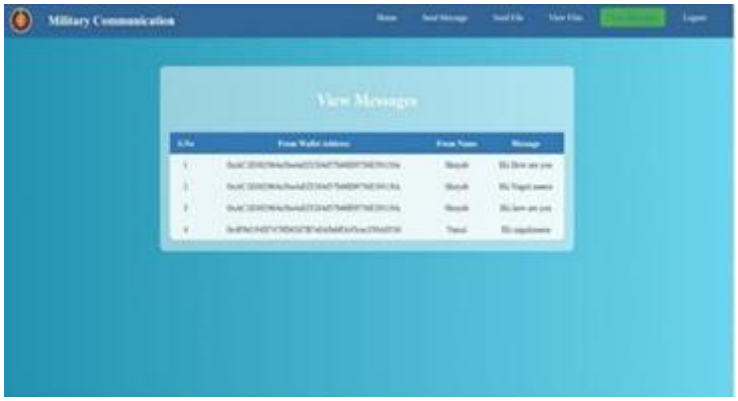

Fig 7:Received messages view page where see the received messages

Upon validation of the required authentication token, As shown in figure 8 the receiver side promptly displays the messages transmitted by the sender commander. This seamless process ensures that authorized recipients can access the intended communication securely.

CONCLUSION

By leveraging cutting-edge technologies such as quantum cryptography and blockchain, we have developed a robust platform that prioritizes security, integrity, and reliability. Through the implementation of quantum authentication, commanders can securely exchange messages and files, confident in the confidentiality and authenticity of their communications. The integration of blockchain ensures decentralization and tamper-proofing of communication records, guaranteeing transparency and immutability. Furthermore, our application streamlines the registration process and ensures that only authenticated users have access to the communication network, enhancing overall security. With its advanced features and innovative approach, our application stands as a sentinel in safeguarding sensitive military information and facilitating seamless communication among commanders.

FUTURE SCOPE

For future scope, the concept implemented in our research paper holds immense potential for expansion into various sectors of communication systems. It could help keep communications safe in government agencies, financial institutions, and healthcare organizations. Furthermore, the concept can be extended to global communication networks, enabling secure and decentralized communication on a larger scale.

REFERENCES

[1] Haoming Wang; Nan Li; Haiyang Jiang,"Application of QuantumTechnology in MilitaryCommunications",2023 International Conference on Networking, Informatics and Computing (ICNETIC),29 -31 May 2023.
[2] Niels M. P. Neumann; Maran P. P. van Heesch; Frank Phillipson; Antoine A. P. Smallegange,"Quantum Computing for Military Applications",2021 International Conference on Military Communication and Information Systems (ICMCIS),04-05 May 2021.
[3] Amool Sudhan; Manisha J Nene,"Employability of blockchain technology in defence applications", 2017 International Conference on Intelligent Sustainable Systems (ICISS),07-08 December 2017.
[4] Guangfu Wu; Yingjun Wang,"The security and privacy of blockchain- enabled EMR storage management scheme", 2020 16th International Conference on Computational Intelligence and Security (CIS),27 April 2021.
[5]Zebo Yang; Haneen Alfauri; Behrooz Farkiani; Raj Jain; Roberto Di Pietro; Aiman Erbad,"A Survey and Comparison of Post-quantum and Quantum Blockchains",IEEE Communications Surveys & Tutorials,19 October 2023.
[6]Mary Subaja Christo; Anigo Merjora A.; Partha Sarathy G.; Priyanka C.; Raj Kumari M.,"An Efficient Data Security in Medical Report using Block Chain Technology", 2019 International Conference on Communication and Signal Processing (ICCSP), 04-06 April 2019.
[7] Muhammad Taimour Azhar; Muhammad Burhan Khan; Asim Ur Rehman Khan,"Blockchain based Secure Crypto-currency system with Quantum Key Distribution Protocol", 2019 8th International Conference on Information and Communication Technologies (ICICT), 20 February 2020.
[8] Dharani D; Soorya R; K. Anitha Kumari,"Quantum Resistant Cryptographic Systems for Blockchain Network", 2023 3rd International Conference on Intelligent Technologies (CONIT),07 August 2023.
[9] Minrui Xu; Xiaoxu Ren; Dusit Niyato; Jiawen Kang; Chao Qiu; Zehui Xiong; Xiaofei Wang; Victor C. M. Leung,"When Quantum Information Technologies Meet Blockchain in Web 3.0", IEEE Network,15 May 2023.
[10]Wei Yin; Qiaoyan Wen; Wenmin Li; Hua Zhang; Zhengping Jin,"An Anti- Quantum Transaction Authentication Approach in Blockchain", IEEE Access
,01 January 2018 .
[11] Ivan B. Djordjevic, Fellow, IEEE,"Secure, Global Quantum Communications Networks",2020 22nd International Conference on Transparent Optical Networks (ICTON),19-23 July 2020.
[12] Zebo Yang; Tara Salman; Raj Jain; Roberto Di Pietro,"Decentralization Using QuantumBlockchain: A Theoretical Analysis", IEEE Transactions on Quantum Engineering,Volume: 3,15 September 2022.
[13] Rubina Akter, Sanjay Bhardwaj, Jae Min Lee and Dong-Seong Kim,"Highly Secured C3I Communication Network Based on Blockchain Technology for Military System",2019 International Conference on Information and Communication Technology Convergence (ICTC),16 -18 October 2019.
[14] 1st Ali Ibnun Nurhadi ,2nd Nana Rachmana Syambas," Quantum Key Distribution (QKD) Protocols- A Survey", 2018 4th International Conference on Wireless and Telematics (ICWT),12-13 July 2018.