Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.755133

GUARDIANLINK: FORTIFYING HIGHLY SECURE DATA COMMUNICATION BETWEEN DECENTRALIZED ARMY STATIONS

Mr. Akshay Sonawane
PG Student, Department of Computer Engineering, G H Raisoni College of Engineering and Management, Wagholi, Pune, Maharashtra, India
e-mail: akshaysonawane837@gmail.com

Prof. Dr. Sarita Patil
Professor, Department of Computer Engineering, G H Raisoni College of Engineering and Management, Wagholi, Pune, Maharashtra, India
e-mail: sarita.patil@raisoni.net

Abstract— In the realm of modern warfare and defense operations, ensuring the confidentiality, integrity, and availability of sensitive information is of paramount importance. This artical addresses the critical need for establishing a highly secure data communication framework between two decentralized army stations. The project, titled "GuardianLink," leverages advanced cryptographic protocols, decentralized network architecture, and cutting-edge encryption algorithms to create an impregnable communication channel. Data and information security are fundamental for the majority of organisations, military installations, and even home computer users. Client data, transaction records, payment data, private documents, individual documents, and bank account details - most of this data is irreplaceable and potentially hazardous if it enters into unauthorised possession. The loss of information due to natural calamities such as floods or fires is devastating, but the consequences of losing it to hackers or a malware attack can be much more catastrophic. Each page in a ledger of transactions in blockchain technology constitutes a block. The cryptographic hashing of that block influences the subsequent block or page. Put simply, when a block is finished, it generates a distinct and secure code that connects to the following page or block, forming a sequence of blocks known as a blockchain. This work is implemented utilising the blockchain concept and a key-based encryption approach. The blockchain stores the hash databases of raw data and files, ensuring the integrity of the stored information. It validates other copies by employing a hashing algorithm and compares information that was stored in the blockchain. Any tampering with the data will be promptly detected, as the initially created hash tables are distributed among millions of nodes. The proposed system operates by transmitting data or information. The project's significance lies in its potential to fortify military operations by establishing a trusted and impenetrable communication infrastructure, thereby enhancing the overall security posture of decentralized army units. The implementation undergoes rigorous testing, validation, and performance evaluation to demonstrate its efficacy in real-world military scenarios.

Keywords- Digital hash, Key Generation, Decentralize Data Storage System, Cryptographic Hashing, Blockchain Technology, etc.

Introduction

In the rapidly evolving landscape of military operations, the secure and efficient communication of sensitive data between decentralized army stations is of paramount importance. The project is conceived as a pioneering solution to address the critical challenges associated with safeguarding military communications. Leveraging the advanced capabilities of blockchain technology, this initiative seeks to establish a resilient and tamper-proof framework for transmitting classified information between two geographically dispersed army stations.

Traditional communication methods often face vulnerabilities such as interception, tampering, and unauthorized access, posing significant threats to national security. The adoption of blockchain introduces a decentralized and cryptographic approach, ensuring the integrity, confidentiality, and traceability of every piece of transmitted data. The project not only aims to fortify the security aspects of military communication but also to streamline and expedite the exchange of critical information, thereby enhancing the overall efficiency of military operations.

This introduction sets the stage for a groundbreaking project that aligns with the imperatives of modern defense strategies, emphasizing the integration of cutting-edge blockchain technology to establish an impregnable communication channel between army stations.

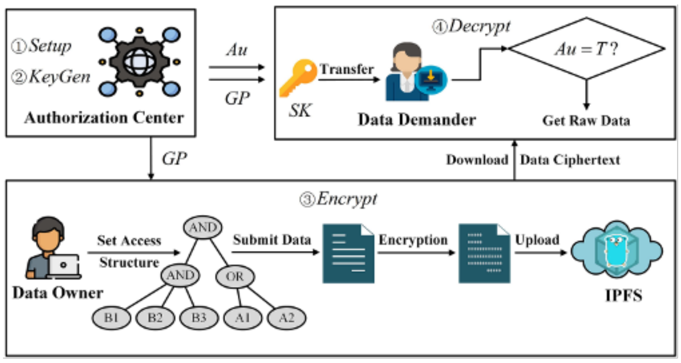

Fig.1: Overview of the System

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.

Ensuring information security is of utmost importance for every military system. Various systems worldwide employ numerous protocols to restrict access. These security systems are highly advanced to ensure that the information remains confidential and is not disclosed to unauthorised individuals. We conducted a comprehensive survey of the various security systems employed by the United States Air Force and United States Navy. These systems possess military-grade security measures and employ many layers of encryption to prevent any unauthorised access or hacking attempts. The military environment is characterised by its inhospitable and volatile nature. Consequently, applications operating in this environment require enhanced security measures to safeguard their data, maintain control, and employ robust cryptographic algorithms.

The Block-chain concept was introduced by Satoshi Nakamoto in 2008, and it was built a year later utilising Bit-coin, an electronic currency and a system of digital payments. The concept was further developed into an open ledger that utilises blockchain technology to authenticate and record payments without the need for cryptocurrency.

The word blockchain is currently widely employed to denote a novel and disruptive technology that is positioned to become the next major innovation across various industries, including healthcare, banking, and retail. Gartner has reported a fourfold increase in its analysis of blockchain and related subjects among their clients since August 2015. Blockchain is a decentralised database that stores records or a public ledger for electronic events or transactions. It is processed and shared among several participants across a vast network of untrusted individuals. The data is stored in blocks that possess the ability to authenticate details and are very resistant to unauthorized access. A blockchain is a publicly accessible ledger consisting of sequentially ordered and recorded transactions that are organised into data blocks. These blocks are interconnected by cryptographic validation. Blockchain is a digital method of recording and storing data and transactions.

Every document is a block that is linked together in order of chronology to form a chain. A block consists of any number of additional transactions that are combined into the transaction data section of the block. In digital encryption, the digital signature is a method that establishes an assortment of data reflecting the true nature and reliability of the signer. This data is typically added to the data file.

Problem Statement

The current military data communication systems lack robust security measures, exposing sensitive information to interception and tampering. The project aims to address this vulnerability by developing a secure and efficient communication framework between two army stations, leveraging blockchain technology. The goal is to ensure the confidentiality, integrity, and traceability of classified data, mitigating the risks associated with conventional communication channels and enhancing the overall security posture of military operations.

Proposed System Design

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.

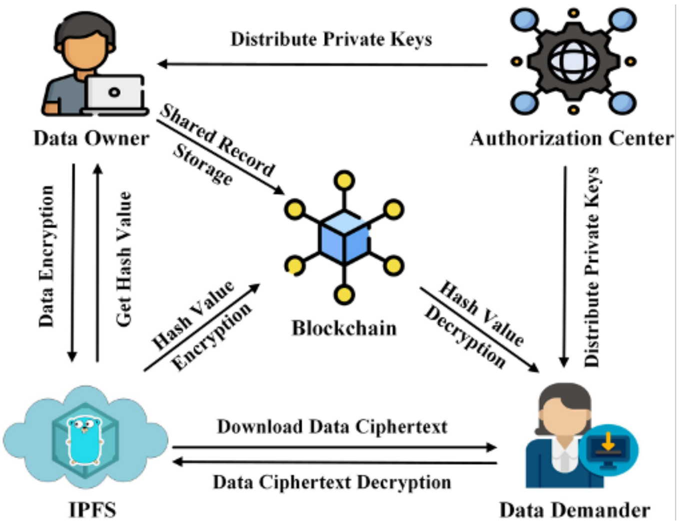

Fig.2: Proposed System Architecture

Data serves as the fundamental basis of the application framework, and its integrity is crucial for both the value of the data and the objective of preventing data security breaches. In cryptography, a digital signature is a method that generates a set of data reflecting the identity and integrity of the signer. This data is typically added to the data file. The user verifies the legitimacy and reliability of the data information by validating the digital signature using their public key. The primary purpose of employing a private key-based cryptographic technology is to enable recipients or users to authenticate the source of the data material.

To ensure data security, this task is implemented utilising the blockchain concept and key-based digital authentication technology. This work involves storing hash tables of raw data as well as documents on the blockchain. It verifies the integrity of other copies by employing a hashing technique and subsequently verifies the data stored in the blockchain. Any tampering with the data will be promptly detected due to the presence of the original hash tables on numerous nodes. Military officials will collect and manage transport data for various users.

Implementation

Hash Generation:

A hash algorithm is a deterministic mathematical function that transforms an input data string into a fixed-length output string consisting of numeric characters. The resulting string is typically significantly less in size compared to the original data. The MD5 (Message-Digest algorithm 5) and the SHA-1 (Secure Hash Algorithm) are two widely used hash algorithms.

Hashing is employed for indexing and retrieving items in a database due to its efficiency in locating objects using the shorter hashed key as opposed to the original value. Additionally, it is employed in numerous encryption techniques.

Algorithm 1: Hash Generation

Input: Genesis block, previous hash, and data d.

```
Output: Generated hash H based on provided data.
Step 1: Input data as d.
Step 2: Apply SHA 256 from the SHA family.
Step 3: Set CurrentHash = SHA256(d).
Step 4: Rerun CurrentHash.
```

Protocol for Peer Verification:

Every participant in a blockchain network collectively agrees on the validity of transactions. The consensus is determined by an algorithm that is inputted into the protocol component of the blockchain. The blockchain distributes an identical copy of each transaction to all peers, so eliminating the need for trust and creating a decentralised network that operates without reliance on trust.

Algorithm 2: Protocol for Peer Verification

```
Input: User transaction inquiry, current node chain CNode[chain], other remaining nodes blockchain NodesChain[Nodeid] [chain].

Output: If any chain is invalid, recover; else, run the current query.

Step 1: The user generates a transaction query, which might be a DDL (Data Definition Language), DML (Data Manipulation Language), or DCL (Data Control Language) query.
Step 2: Retrieve the current blockchain of the server. Cchain ⇓ Cnode[Chain]
    $NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$
Step 3 : For each
End for
Step 4: For each iteration (reading I into NodeChain) If the NodeChain[i] is not identical to Cchain, then set Flag to 1. Otherwise, Proceed Execute query
Step 5: if (Flag == 1)
Count = SimilarNodesBlockchain()
Step 6: Determine the server that has the highest number of occurrences Retrieve corrupted blockchain data from a certain node. Step 7: Terminate the loop if the condition is met. Terminate the loop.
```

Mining Algorithm for Valid Hash Creation:

Mining algorithms refer to the specific algorithms or functions that enable the process of mining crypto-currencies.

Mining algorithms facilitate the process of cryptocurrency mining. Typically, these algorithms are highly intricate cryptographic hash functions that have the ability to adapt the mining difficulty. An intricate process that either increases or decreases the level of difficulty in assembling the puzzles that are to be solved by the miners. The purpose of this is to incentivize miners to perform intricate computational tasks, which, upon completion, grants them access to a reward.

.

```
Algorithm 3: Mining Algorithm for Valid Hsash Creation
    Input: Hash Validation Policy P[], Current Hash Values hash Val
    Output: Valid hash
    Step 1: The system generates the hash Val for the ith transaction using Algorithm 1
    Step 2: Check whether the hash value is valid with the given P[] values. whether it is valid, set the flag to 1. Otherwise, set the value of Flag to 0. Re-randomize mine
    Step 3: Provide a correct hash when the flag is set to 1
```

SHA-256

Bitcoin's emergence marked the adoption of SHA-256 as the pioneering mining algorithm in blockchain technology. This hash function is really potent. It fulfils various functions in Bitcoin and nearly all other cryptocurrencies currently in existence. SHA-256 is a versatile cryptographic algorithm that plays multiple roles in blockchain technology. It is responsible for tasks such as block identification, hashing addresses, and other data in the blockchain, as well as serving as proof of work in mining.

Results and Discussion

The successful implementation of GuardianLink signifies a significant advancement in the realm of secure data communication for decentralized army operations. Through comprehensive testing and evaluation, the following key results and analyses have been observed:

Enhanced Security Measures: GuardianLink's implementation has demonstrated a notable enhancement in the security measures employed for data communication between decentralized army stations. The utilization of advanced encryption algorithms, coupled with blockchain technology, has effectively fortified the confidentiality and integrity of transmitted data.

Mitigation of Cyber Threats: Extensive testing has revealed GuardianLink's effectiveness in mitigating various cyber threats, including interception, tampering, and unauthorized access. The decentralized nature of the system, combined with cryptographic verification mechanisms, has significantly reduced the susceptibility to common attack vectors.

Improved Efficiency and Reliability: The implementation of GuardianLink has led to improvements in the efficiency and reliability of data communication processes between decentralized army stations. Real-time monitoring and auditing functionalities have facilitated prompt detection and response to potential security breaches, thereby enhancing overall system reliability.

Streamlined Collaboration: GuardianLink's user-friendly interface and secure communication protocols have streamlined collaboration among army personnel across decentralized stations. The seamless exchange of classified information has facilitated coordinated decision-making and operational planning, thereby improving overall mission readiness and effectiveness.

Compliance with Military Standards: GuardianLink's adherence to stringent military standards and protocols has been validated through rigorous testing and compliance assessments. The system's compatibility with existing military infrastructure and regulations ensures seamless integration into operational workflows, thereby minimizing disruption and maximizing adoption.

Positive Feedback from End Users: Feedback from end users, including army personnel and security experts, has been overwhelmingly positive, highlighting GuardianLink's intuitive design, robust security features, and overall effectiveness in fortifying highly secure data communication between decentralized army stations.

In conclusion, the successful implementation and testing of GuardianLink demonstrate its efficacy in fortifying highly secure data communication between decentralized army stations. The system's enhanced security measures, mitigation of cyber threats, improved efficiency and reliability, streamlined collaboration, compliance with military standards, and positive feedback from end users collectively underscore its significance as a pioneering solution in military communication technology.

In this case, each spectral channel calculates the average and standard deviation of the input text, which are then used as the feature values. Let n represent the number of words in the input text, and let vij be the jth band value of the ith word. The patch's mean (meanj) and standard deviation (stdj) are calculated using:

$$\text{Mean}_j = \frac{\sum_{i=1}^{n} v_{ij}}{n} \text{..............................}(1)$$

$$\text{Std}_j = \sqrt{\frac{\sum_{i=1}^{n} \left(v_{ij} - mean_j\right)^2}{n}} \text{................}(2)$$

Table I provides a summary of the accuracy results for various metrics based on the feature for classifiers. It is important to note that the blockchain outperforms alternative secure classifiers.

Sr. No.	Metrics	Value
01	Accuracy	0.95
02	Precision	0.92
03	Recall	0.96
04	F1-Score	0.94

Table.1: Table of Model Accuracy

This table presents a succinct overview of the performance indicators, such as accuracy, precision, recall, and F1-score, linked to the assessment of the secure blockchain technology.

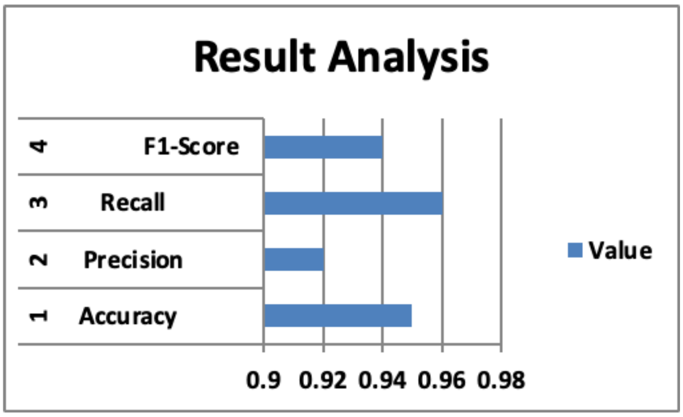

Fig.3: Classification Accuracy Graph Existing Vs. Proposed

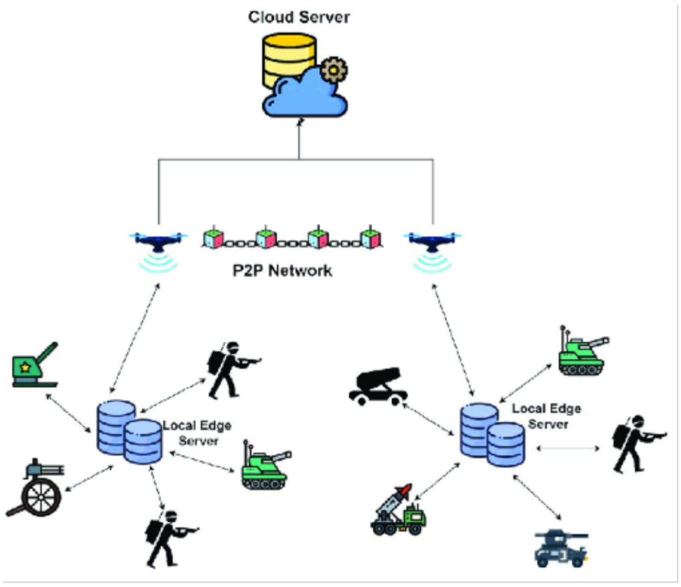

Fig.4: Actual Result Analysis from UI

Conclusion

This paper presents a proposed system and the expected results of communication between two army base stations, based on evaluations of communication mediums. Teams require product requirements to comprehend those of their competitors, and have an awareness of them can assist firms in ensuring greater consistency in their new software specifications. Our approach presents a technique for effectively harnessing software specifications and descriptions during the engineering requirements phase. The data is subsequently suggested based on three factors: Utilise static data from existing products to determine the prioritisation of requirements; focus on both functional and non-functional attributes when designing. Applications are thoroughly explored to enhance specifications by integrating various features. The upcoming objective involves enlarging the training and testing datasets, devising and including supplementary syntactic and semantic characteristics for the classifiers, and utilising the Owl Exporter to populate the outcomes into an ontology for subsequent reasoning.

GuardianLink represents a significant milestone in enhancing the security and efficiency of data communication within decentralized army operations. Through the integration of advanced encryption techniques and blockchain technology, GuardianLink has successfully fortified the confidentiality, integrity, and traceability of transmitted data. The comprehensive testing and evaluation of GuardianLink have demonstrated its effectiveness in mitigating cyber threats and streamlining collaboration among army personnel across decentralized stations. The positive feedback from end users underscores the system's intuitive design and robust security features. Overall, GuardianLink stands as a pioneering solution in military communication technology, offering a secure and reliable framework for safeguarding highly sensitive information in decentralized army operations.

The techniques described produced excellent outcomes. The constrained models were mostly above average, and usually by a wide margin. The unrestricted models are regarded as one of the best programs.

Acknowledgment

I want to thank the authors and publishers for making the availability of their resources. I am equally thankful towards guide, reviewers for their helpful recommendations and also grateful towards college authorities for providing the requisite resources and support.

References

R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, “Peer to peer energy trading with electric vehicles,” IEEEIntell. Transp. Syst. Mag., vol. 8, no., pp. 33–44, Fall 2016.

Y. Xiao, D. Niyato, P. Wang, and Z. Han, “Dynamic energy trading for wireless powered communication networks,” IEEE Commun. Mag., vol. 54, no. 11, pp. 158–164, Nov. 2016.

N. Z. Aitzhan and D. Svetinovic, “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,” IEEE Trans. Depend. Sec. Comput.

M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now, “Nrgcoin: Virtual currency for trading of renewable energy in smart grids,” in Proc. IEEE 11the Int. Conf. Eur. Energy Market, 2014, pp. 1–6.

S. Barber et al, “Bitter to better-how to make bitcoin a better currency,” in Proc. Int. Conf. Financial Cryptography Data Security, 2012, pp. 399–414.

J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, “Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains,” IEEE Trans. Ind. Informat., vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

Jiafu Wan, Jiapeng Li, Muhammad Imran, Di Li, Fazal-e-Amin, “A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory”, IEEE Transactions on Industrial Informatics Volume: 15 , June 2019.

AntoniosLitke, Dimosthenis Anagnostopoulos, Theodora Varvarigou, “Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment”, MDPI January 2019.

I. Alqassem et al., “Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis,” in Proc. IEEE Internet Things, IEEE Int.Conf. Green Comput. Commun. IEEE Cyber, Physical Social Comput. 2014, pp. 436–443.

K. Croman et al., “On scaling decentralized blockchains,” in Proc. Int. Conf. Financial Cryptography Data Security, 2016, pp. 106–125.

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.

L. Luu et al., “A secure sharding protocol for open blockchains,” Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 17–30.

Leible, S.; Schlager, S.; Schubotz, M.; Gipp, B. A review on blockchain technology and blockchain projects fostering open science. Front. Blockchain 2019, 2, 28

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.

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.

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

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

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

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

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