IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005160

# Highly Secure Data Communication between Two Decentralized Army Stations

**Mr. Akshay Sonawane, Dr. Aniruddha Rumale**

Student, Department of Computer Engineering, GHRCEM, Wagholi, Pune, Maharashtra, India

Professor, Department of Computer Engineering, GHRCEM, Wagholi, Pune, Maharashtra, India

**ABSTRACT -** Data and information security is basic for most organizations, military stations and even home computer users. Client data, transaction records, payment data, confidential documents, individual documents, financial account details - the majority of this data can be difficult to replace and conceivably dangerous on the off chance that it falls into the wrong hands. Information lost because of disasters, for example, a flood or fire is crushing, yet losing it to hackers or a malware infection can have significantly more noteworthy results. In block-chain technology, each page in a ledger of transactions forms a block. That block has an effect on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or block-chain. In proposed system data will be of healthcare data need to secure. This work is designed using block chain concept and key-based cryptographic technique. Stores the hash tables of raw data and files on the block-chain, validates other copies by running a hashing technique, and then compares the data stored in the block-chain, any interfere with the data will be quickly found, because the original hash Tables are stored on millions of nodes. Proposed system work on data / information transmission. On web more data of military security system is stored and that data need to stored securely.

**KEYWORDS**: Encryption, Decryption, Digital Hashing, Military information, Key generation.

## I. INTRODUCTION

Information Security is the highest priority for any military system. Systems across the world have multiple protocols for limited access. These security systems are sophisticated so that the information isn't leaked to any person. We surveyed multiple security systems in use by US Air force and US Navy. These systems are military grade and have multiple encryptions to stop any hacking or unknown access. Military environment is a unfriendly and a turbulent one in this way, applications running in this environment needs more security to ensure their data, get to control and their cryptographic strategies.

The world came to know about the Block-chain concept nine years back when Satoshi Nakamoto conceptualized it in 2008; but it got developed a year later, using Bit-coin, a crypto-currency and digital payment system. The concept was later discovering to distributed ledger that leverages the block-chain to verify and store transactions without crypto-currency. The term block-chain is broadly used these days to represent a new disruptive technology poised to be the next big thing across industries from healthcare to finance to retail. According to Gartner, their client analysis on block-chain and related topics has quadrupled since August 2015. Block-chain is a divided database of records or public ledger of digital events or transactions that got executed and has been shared among involving parties across a large network of un-trusted participants. It stores data in blocks that can verify information and are very difficult to hack. A block-chain is a public ledger residing of ordered and time-stamped records of transactions arranged in data blocks which will use cryptographic validation to link themselves together. Block-chain is a path of recording data and transactions digitally.

Each record is a block connected chronologically together into a chain. A block of one or more new transactions is composed into the transaction data part of a block.According to the approach of cryptography, digital signature

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005160

generates a set of data information representing the identity and data integrity of the signer, usually appended to the data file.

## II. RELATED WORK

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers.
In this section, we briefly review the related work on Military data Security.

R.Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens presented the concept between two arrangements of electric vehicles, which fundamentally diminish the effect of the charging procedure on the power framework amid business hours. This trading approach is also economically beneficial for all the users involved in the trading process. An activity-based approach is used to predict the daily agenda and trips of a synthetic population for Flanders (Belgium) [1].

Y. Xiao, D. Niyato, P. Wang, and Z. Han provide a study of the possible flow and functional factors that enable DET in communication networks. Various design issues on how to implement DET in practice are discussed. An ideal approach is created for delay-tolerant remote controlled correspondence organizes in which every remote powered device can masterminded its information transmission and energy exchanging activities as indicated by present and future vitality accessibility [2].

N. Z. Aitzhan and D. Svetinovic presents a work that address the issue of providing transaction security in decentralized smart grid energy trading without confidence on trusted third parties. We have developed a proof-of-concept for decentralized energy trading system using blockchain technology, multi-signatures, and anonymous encrypted messaging flows, enabling peers to anonymously negotiate energy prices and securely perform trading transactions. [3]

M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now presents a work that shows decentralized computerized cash, called NRG-coin. Prosumers in the smart grid framework exchange privately made sustainable power source utilizing NRG-coins, the estimation of which is indented on an open cash trade advertise. Like Bit-coins, this money proposes various favorable circumstances over fiat cash, however not at all like Bit-coins it is made by infusing vitality into the matrix, as opposed to giving vitality on computational influence. Likewise, they make a novel exchanging worldview for purchasing and offering environmentally friendly power vitality in the smart grid network. [4]

S. Barber*et al* presents a work that Bit-coin is isolated computerized cash which has pulled in a significant number of clients. They play out a top to bottom examination to comprehend what made Bit-coin so effective, while many years of research on cryptographic e-money have not prompt a vast scale appropriation. They ask additionally how Bit-coin could turn into a decent contender for seemingly perpetual stable money. [5]

J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain presents a work to accomplishes request reaction by giving motivating forces to releasing PHEVs to adjust nearby power request out of their own self-interests. Be that as it may, since exchange security and security insurance issues show genuine difficulties, they investigate a promising consortium block-chain innovation to enhance exchange security without dependence on a confided in outsider. A restricted P2P Electricity Trading framework with Consortium block- chain (PETCON) strategy is proposed to represent detailed activities of limited P2P power exchanging [6].

Jiafu Wan,Blockchain is characterized by its decentralized nature, integrity of the data stored in the chain and its openness. Due to these characteristics, another place where Blockchain can be used is to release government funds for a project. Usually when a project is allocated funds, there is no knowledge as to how these funds are being used and a

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005160

large part of it is never shown in records due to corruption. To solve this problem, a system has been proposed using Blockchain to provide the transparency.[7]

AntoniosLitke ,the author propose an innovative blockchain-based IIoT architecture to help build a more secure and reliable IIoT system. By analyzing the short-comings of the existing IIoT architecture and the advantages of the Block-chain technology. We decompose and reorganize the original IIoT architecture to form a new, multi-center, partially decentralized architecture. Thus, the proposed architecture represents a significant improvement of the original architecture, which provides a new direction for the IIoT development.[8]

I. Alqassem *et al*, presented a new information sharing scheme based on blockchain technology. Users can manage their data and understand the data being collected about them and how to use it without trusting any third party. However, the scheme did not take into account the possibility of the enterprise itself tampering with data.[9]

## III. PROBLEM STATEMENT

In Military transportation with other officers that data contain more importance and that data need to secure.

### A. Objectives

- To analyze the steps involved in the working of Block chain.
- To provide the security for important data.
- To use transportation data for secure transaction.

## IV. PROPOSED METHOD

Data forms the foundation of the application system, and its integrity is the key to the data's value and the aim of data security technology prevention. According to the approach of cryptography, digital signature generates a set of data information representing the identity and data integrity of the signer, normally appended to the data file. The user validates the digital signature through the user's public key to verify the authenticity and integrity of the data information. In general, the intension of using a private key-based cryptography technique is for recipients or users to verify the origin of the data information.

For data security, this work is designed using block chain concept and key-based digital signature technology. In this work we stores the hash tables of raw data and files on the block-chain, validates other copies by running a hashing technique, and then checks the data stored in the block-chain, any interfere with the data will be quickly found, because the original hash Tables are stored on millions of nodes. In this military officers will store transportation data for different users.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005160

**Architecture**

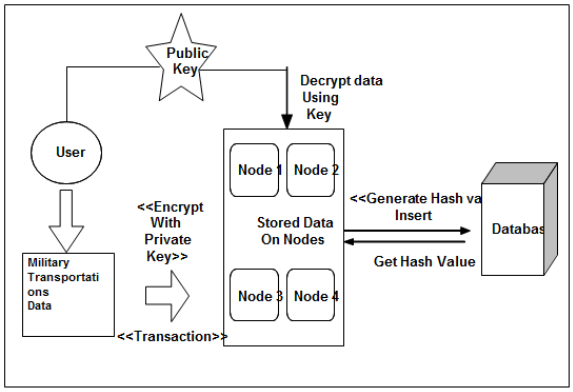


**Fig.2 System Architecture**

### A. Modules

**Module 1** - Sender (User):- Sender select the confidential file, encrypt them using encryption technique with unique private key.

**Module 2** - Receiver (User):- Receiver select file, decrypt using unique private key belong to that file and download it.

**Module 3** – Key Manager (Authority):- Key Manager have authority to give access to the user where they authorized or not. Key manager provides unique key to the users.

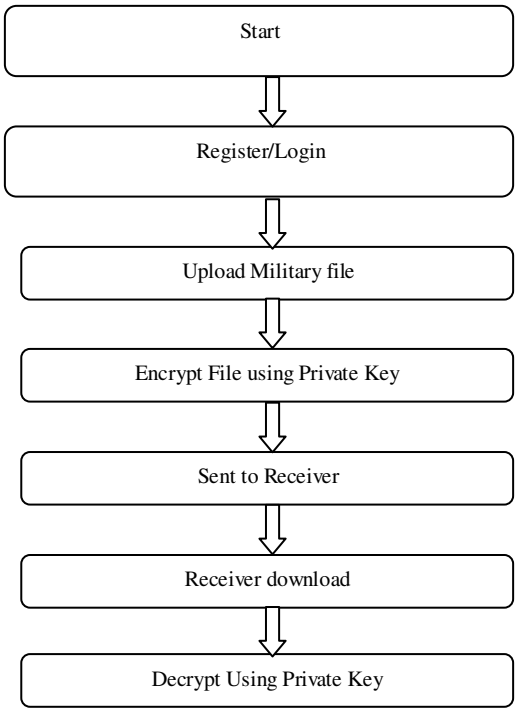


**Fig: Flow Diagram**

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005160

### B. Mathematical model

S=

INPUT:

Identify the inputs

F= f1, f2, f3 ....., FN F as set of functions to execute commands

I= i1, i2, i3I sets of inputs to the function set

O= o1, o2, o3.O Set of outputs from the function sets,

S=I,F,O

I =upload file.

O = Output i.e. file encryption.

F= Functions implemented to get the output based on given Parameter

**Space Complexity:** The space complexity depends on Presentation and visualization of discovered patterns. More the storage of data more is the space complexity.

**Time Complexity**: Check No. of patterns available in the datasets= n If (n(1)) then retrieving of information can be time consuming. So the time complexity of this algorithm is O (nn). =Failures and Success conditions.

**Failures:**

• Huge database can lead to more time consumption to get the information.

• Hardware failure.

• Software failure.

**Success:**

• Search the required information from available in Datasets.

• User gets result very fast according to their needs.

**Methodologies**

### 1. Encryption

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as cipher-text, while unencrypted data is called plaintext.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005160

**2. Decryption**

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

**3. Hashing Concept**

A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures. You can sign a hash value more efficiently than signing the larger value.

**4. Key generation**

In cryptography, a key-agreement protocol is a protocol whereby two or more parties can agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third parties from forcing a key choice on the agreeing parties.

**5. Advanced Encryption Standard**

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

**Operation of AES**

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

**6. Secure Hashing Algorithm (SHA)**

The most adopted secure algorithms associated with the blockchain technology are (SHA-1, SHA2,and SHA-256) encryption because of their unique quality of hash function that create unique outputswhen given different inputs [31,32]. The hash function here is a unique key created to identify atransaction that at the same time identifies an individual. This algorithm is efficient in verifying file and message integrity during transaction, data identification, and

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005160

password verification.

**Hashing Functions**

Hashing functions take some data as input and produce an output (called hash digest) of fixed length for that input data. This output should, however, satisfy some conditions to be useful.

- Uniform distribution: Since the length of the output hash digest is of a fixed length and the input size may vary, it is apparent that there are going to be some output values that can be obtained for different input values. Even though this is the case, the hash function should be such that for any input value, each possible output value should be equally likely. That is to say that every possible output has the same likelihood to be produced for any given input value.

  - Fixed Length: This should be quite self-explanatory. The output values should all be of a fixed length. So, for example, a hashing function could have an output size of 20 characters or 12 characters, etc. SHA-512 has an output size of 512 bits.

  - Collision resistance: Simply speaking, this means that there aren't any or rather it is not feasible to find two distinct inputs to the hash function that result in the same output (hash digest).

**Hashing Algorithm — SHA-512**

SHA-512 does its work in a few stages.

1. Input formatting
2. Hash buffer initialization
3. Message Processing
4. Output

## V. CONCLUSION

When a sender want to send confidential data or file to another person / receiver or high level authority it uses several security methods. The digital signature algorithm is the scalablecryptographic solution for the secure retrieval of confidential data.

The proposed system to be developed for this project is better than any other systems the system uses encryption algorithm to protect the classified information.

## REFERENCES

[1]. 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.

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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.

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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005160

[9]. 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.

[10]. K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2016, pp. 106–125.

[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 andMoney*. 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details