IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Resource Management System for Military Force using concepts of Blockchain Technology

Dikshita Pant
Computer Engineering
Universal College of Engineering
Mumbai, India

Anjali Singh
Computer Engineering
Universal College of Engineering
Mumbai, India

Pratik Tirodkar
Computer Engineering
Universal College of Engineering
Mumbai, India

Sridhar Iyer
Computer Engineering
Universal College of Engineering
Mumbai, India

Abstract: **Blockchain technology has gained considerable attention, with an escalating interest in a plethora of numerous applications, ranging from data management, financial services, cyber security, IoT, and food science to healthcare industry and brain research. There has been a remarkable interest witnessed in utilizing applications of blockchain for the delivery of safe and secure healthcare data management. Also, blockchain is reforming the traditional humanresource management practices to a more reliable means, in terms of effective storage and collection through safe and secure data sharing.**

Keywords—blockchain, security, data, files, encryption, confidentiality, authentication, military

I. INTRODUCTION

As blockchain technology's influence expands beyond the bounds of the cryptocurrency sector initially proposed by Nakamoto in the Bitcoin white paper, various potential use cases for the military seem apparent. For example, work is well underway to see how it might help in additive manufacturing.[1] Another clear candidate is the military intelligence system, which comprises a wide range of networked processes, many of which stand to benefit from the immutable, decentralized ledger at blockchain technology's core. Replace ledger with log, the more common synonymous term from military vernacular, and the candidate systems nominate themselves.

To secure data, most systems use a combination of techniques, including:

1. Encryption, which means they use a complex algorithm to encode information. To decode the encrypted files, a use needs an encryption key. While it's possible to crack encrypted information, most hackers don't have access to the amount of computer processing power they would need to decrypt information.

2. Authentication processes, which require creating a username and password.

3. Authorization practices -- the client lists the people who are authorized to access information stored on the cloudsystem.

Many corporations have multiple levels of authorization. Fore xample, a front-line officers might have very limited access to data stored on a cloud system, while the head of human resources might have extensive access to files. [2] Cloud storage approach poses a potential security threat to your data and moreover, only the password access to storage is not sufficient as the password can be hacked by an intruder. Also the data can be captured en-route to the storage services. But due tos maller processor speed and run time memory; these devices need an algorithm which can be used in such small computing devices. Security of stored data and data in transit may be a concern when storing sensitive data.

.

II. LITERATURE REVIEW

Blockchain's potential to facilitate better healthcare data-sharing, and to assist in various other diagnosis applications, has been previously described by several studies. [4]

For instance, using a private blockchain to monitor and store personal clinical data is one of potential examples associated with the Healthcare Data Gateway (HDG) method, introduced by Yue et al. . In this personalized healthcare method, the patients have the freedom to access, monitor, and manage their personal clinical data and healthcare summary, stored on a private blockchain (a centralized database system with restricted access control only entitled to authorized or specific users).

In another study, Griggs et al. adopted a private blockchain, based on the Ethereum protocol, to facilitate not only safe and secure use of medical sensors, and also eradicated the security risks associated with a remote patient monitoring system. Their blockchain based strategy can facilitate secure real-time remote monitoring, thus allowing practitioners to track the healthcare status of their patients from distant locations, while also maintaining a safe, secure, and up-to-date history of patients.

Recently, Wang et al. proposed a blockchain framework, based on parallel execution and artificial healthcare systems, to evaluate the healthcare status of patient diseases. The proposed method assesses the overall condition, diagnosis, and treatment process of the patient, and analyzes the associated therapeutic procedures through parallel executions and computational trials for clinical decision making. The suggested system has been tested on real, as well as artificial, healthcare systems, to evaluate the accuracy of diagnosis and effectiveness of treatment.[5]

Md Mehedi Hassan Onik, Dr Mahdi H. Miraz, Chul-Soo Kim says Application of Information Technology (IT) in the domain of Human Resource Management (HRM) systems is a sine qua non for any organization for successfully adopting and implementing Fourth Industrial Revolution (Industry 4.0). However, these systems are required to ensure non-biased, efficient, transparent and secure environment. Blockchain, a technology based on distributed digital ledgers, can help facilitate the process of successfully effectuating these specifications. A detailed literature review has been conducted to identify the current status of usage of Information Technology in the domain of Human Resource Management and how Blockchain can help achieve a smart, cost-effective, efficient, transparent and secure factory management system. A Blockchain based Recruitment Management System (BcRMS) as well as Blockchain based Human Resource Management System (BcHRMS) algorithm have been proposed.[14]

Candy So Suk Yi, Eric Yung, Christopher Fong, Shilpi Tripathi states Benefits and Use of Blockchain Technology to Human Resources Management: A Critical Review Human Resources (HR) nowadays generally faces various difficulties in the world internet era and spends a lot of time connecting, screening, and verifying the resume of applicants, conducting credentials verifications, and checking backgrounds to reduce the likelihood of poor recruitment. For example, recruiters connect the profile of candidates from different channels such as direct application, recruitment agency, and social media; and hiring resume verifications is therefore a bottleneck.[15]

Background checks on shortlisted candidates / applicants' lies are used to find increasing numbers of companies on their profiles to get job opportunities (Wood et al., 2007 cited in Brody, Richard G, 2010).[15]

III. METHODOLOGY

A. RELATED CONCEPTS ABOUT BLOCKCHAIN

The blockchain technology principally contains six key elements: Decentralized, transparent, immutable, autonomy, open source, and anonymity.

•*Decentralized*
A database system with open access control to anyone connected to the network. The data can be accessed, monitored, stored, and updated on multiple systems.

•*Transparent*
The recorded and stored data on blockchain is transparent to potential users, which can be further updated easily. The transparent nature of blockchains could certainly prevent data from being altered or stolen.

•*Immutable*
The records, once stored, become reserved forever and cannot be modified easily without having control of more than 51% of the node concurrently.

•*Autonomy*
The blockchain system is independent and autonomous, meaning that each node on the blockchain system can access, transfer, store, and update the data safely, making it trustworthy and free from any external intervention.

•*Open source*
The blockchain technology is formulated in a way that provides an open source access to everyone connected to the network. This inimitable versatility entitles anyone, not only to check the records publicly, but also develop various impending applications.

•*Anonymity*
As data transfer occurs between node to node, the identity of the individual remains anonymous, thus making it a more secure and reliable system. A person who is part of this network has to verify each new transaction made. As each transaction in a block of a blockchain is verified by all of the nodes in the network, it becomes more and more immutable. The diagram below shows the work flow of blockchain process.[6]

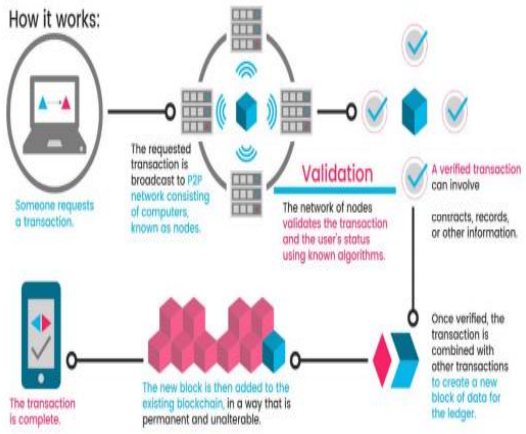

Fig 1.How It Works

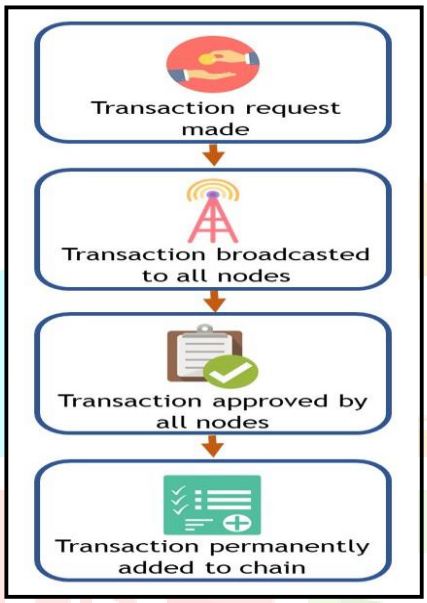

Fig 2.A generalized workflow of the blockchain process

B. Modules

Admin Module

- Admin Login
- Add User Details
- View User Details
- Upload User Files
- Share Files

User Module

- User Login
- View Record
- View Shared Data
- Download Shared Data

A blockchain system can be considered as a virtually incorruptible cryptographic database where critical information could be recorded. The system is maintained by a network of computers, that is accessible to anyone running the software.[7]

Blockchain operates as a pseudo-anonymous system that has still privacy issue since all transactions are exposed to the public, even though it is tamper-proof in the sense of data-integrity.[8]

The access control of heterogeneous military officer records across multiple military institutions and devices needed to be carefully designed. Blockchain itself is not designed as the large-scale storage system. In the context , a decentralized storage solution would greatly complement the weakness of blockchain in the perspective.[9]

C. Implementation Process Model

The waterfall model is the oldest and the most widely used paradigm. However, many projects rarely follow its sequential flow. This is due to the inherent problems associated with its rigid format. Namely:

- It only incorporates iteration indirectly, thus changes may cause considerable confusion as the project progresses.
- As The client usually only has a vague idea of exactly what is required from the software product, this IM has difficulty accommodating the natural uncertainty that exists at the beginning of the project.[10]

The customer only sees a working version of the product after it has been coded. This may result in

disaster any undetected problems are precipitated to this stage.

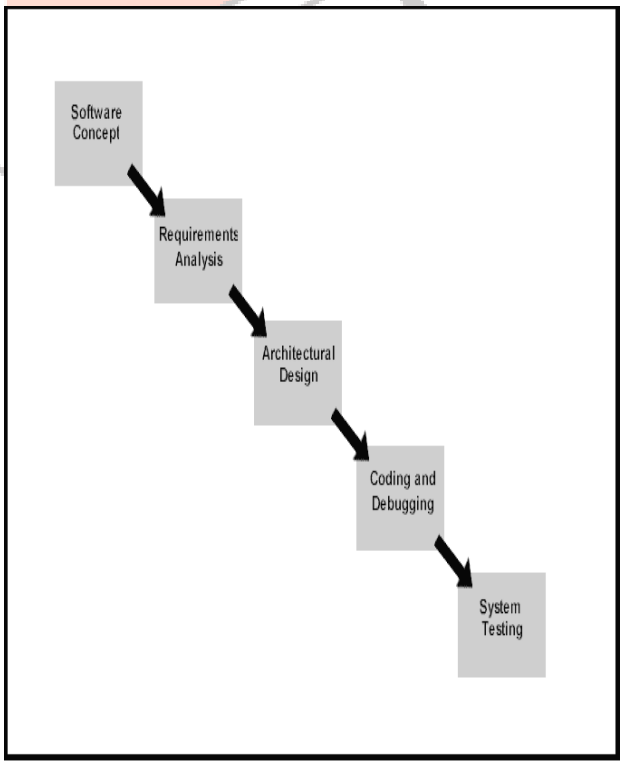

Fig 3. Waterfall Model

D. Hardware and Software requirements

HARDWARE REQUIREMENTS:

- 1 GB RAM.
- 200 GB HDD.
- Intel 1.66 GHz Processor Pentium 4

SOFTWARE REQUIREMENTS:

- Windows XP, Windows 7,8
- Visual Studio 2010
- MS SQL Server 2008
- Windows Operating System

E. Algorithm

The documents related tp the officers getting storedin the system needs to be protected and stored with prper security which leads to the use of ECC Elliptic curve cryptography. This new technique avoids the costly operation of mapping and the need to share the common lookup table between the sender and the receiver.

A problem facing military record systems throughout the world is how to share the medical data with more stakeholders for various purposes without sacrificing data privacy and integrity.Blockchain technology has the potential of securely, privately, and comprehensively manage patient health records.In this system, we discuss the latest status of blockchain technology and how it could solve the current issues in healthcare systems.[11]

Key generation:

1. A selects an integer dA. this is A's private key.
2. A then generates a public key PA=dA*B
3. B similarly selects a private key dB and computes a public key

PB= dB *B

4. A generates the security key K= dA *PB. B generates the secrete key K= dB *PA.

Encryption algorithm: Suppose A wants to send to B an encrypted message.

i. A takes plaintext message M, and encodes it onto a point, PM, from the elliptic group.

ii. A chooses another random integer, k from the interval [1, p-1]

iii. The cipher text is a pair of points

PC = [(kB), (PM + kPB)]

iv. Send ciphertext PC to cloud B.

Decryption algorithm: Cloud B will take the following steps to decrypt cipher text PC.

a. B computes the product of the first point from PC and his private key, dB

dB * (kB)

b. B then takes this product and subtracts it from the second point from PC

(PM + kPB) – [dB(kB)] = PM + k(dBB) – dB(kB) = PM

c. B cloud then decodes PM to get the message, M.

Signature Verification: For B to authenticate A's signature, B must have A's public key PA

1. Verify that r and s are integers in [1, n − 1]. If not, the signature is invalid

2. Calculate e = HASH (m), where HASH is the same function used in the signature generation

3. Calculate w = s −1 (mod n)

4. Calculate u1 = ew (mod n) and u2 = rw (mod n)

5. Calcúlate (x1, y1) = u1B + u2PA

6. The signature is valid if x1 = r(mod n), invalid otherwise.

F. Dataflow

This is the Data Flow diagram according to the system

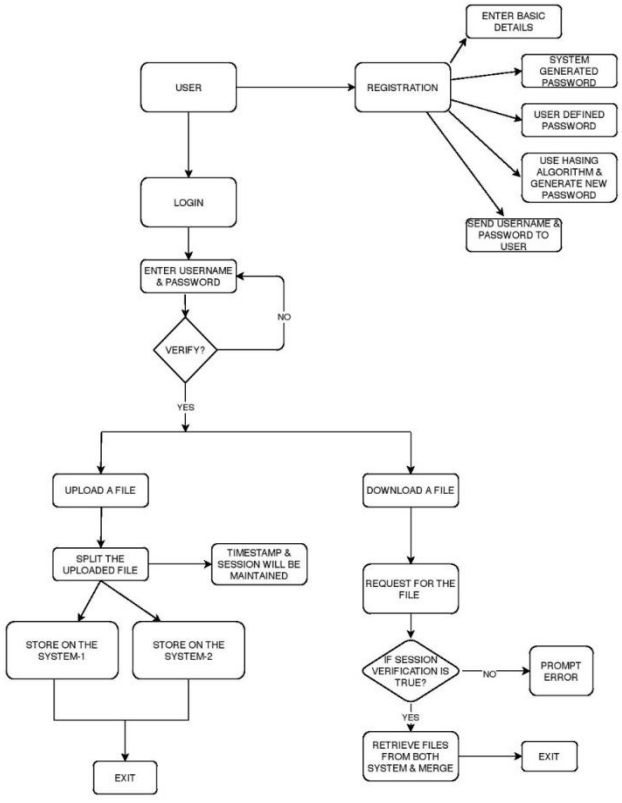

Fig 4. Dataflow

IV. RESULT AND DISCUSSION

All of the data the military department maintains is at risk of being exploited and, as more forces face data breaches, it is of utmost importance that safeguards are in place to prevent fraud and maintain security. In the face of rising cybersecurity crime, blockchain technology is being lauded as a solution.[12]

Blockchain's role as a game-changer for human resources is defined by its security capabilities. In fact, blockchain has proven itself to be so effective for risk management and software security that even aerospace and defense giant Lockheed Martin is using it.[12]

Implementing blockchain can help thwart both internal fraud and external hacks of sensitive officer records. Access to the blockchain is limited and controlled and even those with access can't arbitrarily make changes to the record. This limits both internal fraud and external hacks of sensitive officer records.[13]

The project done with the main focus that is uploading of files for the military officers in our network, securing them in BlockChain, and allowing them to download the files by keeping the confidentiality of the file.

System uses the login process to maintain the authenticity and no easy access of the files except the authorized user .[13]

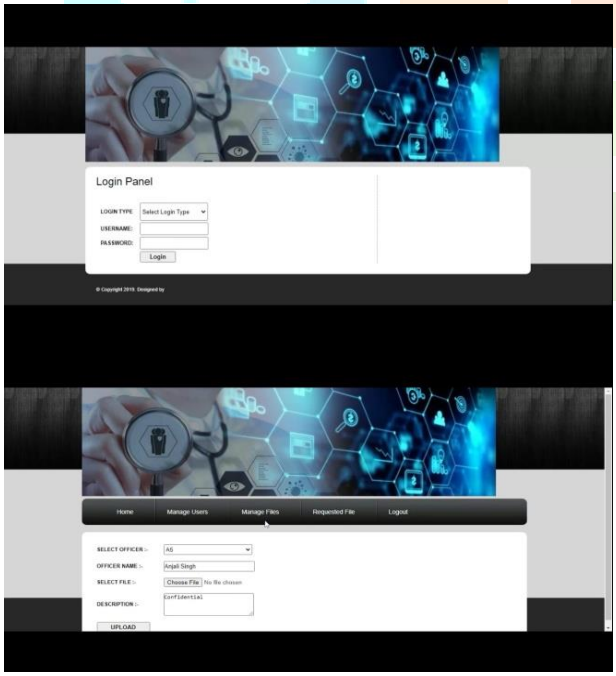

Fig 5. Proposed System

FUTURE SCOPE

We are likely expecting our application to be implemented in various sectors of Indian Administration to keep all the important data secure. BlockChain will make the system design Faster and would require less computation. Also in future more security will be added by adding layers of encryption.

ACKNOWLEDGMENT

We take this opportunity to express our deep sense of gratitude to our project guide and project coordinator, Mr Sridhar Iyer, for his continuous guidance and encouragement throughout the duration of our project work. It is because of his experience and wonderful knowledge, we can fulfil the requirement of completing the project within the stipulated time. We would also like to thank Dr. Jitendra Siturwar, head of the computer engineering department for his encouragement, whole-hearted cooperation and support. We would also like to thank our Principal Dr. J. B. Patil and the management of Universal College of Engineering, Vasai, Mumbai for providing us all the facilities and the work friendly environment. We acknowledge with thanks, the assistance provided by departmental staff, library and lab attendants.

REFERENCES

[1] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System,"2009.[Online].Available:https://bitcoin.org/bitcoin.pdf. [Accessed: Jun. 13, 2018].

[2] Mulligan, C., J. Z. Scott, S. Warren, and J. P. Rangaswami, "Blockchain Beyond the Hype: A practical framework for business leaders," white paper of the World Economic Forum, April 2018.

[3] Joint Chiefs of Staff, Joint Publication 2-0 Joint Intelligence. Washington, DC: Department of Defense, 2013.

[4] Work, B., "Remarks by Deputy Secretary Work on Third Offset Strategy," Brussels, Belgium, Address to North Atlantic Treaty Organization, 28 April 2016.

[5] Asharaf, S. and S. Adarsh, Decentralized Computing using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities, Hershey, Pennsylvania, IGI Global, 2017.

[6] D. Sravana Kumar, Ch. Suneetha and A. Chandrasekhar, Encryption of Data Using Elliptic Curve Over Finite Fields, International Journal of Distributed and Parallel Systems (IJDPS), vol. 3, no. 1, January (2012).

[7] K. Jarvinen, Helsinki and J. Skytta, On Parallelization of High-Speed Processors for Elliptic Curve Cryptography, VLSI Systems, IEEE Transaction, vol. 16, issue 9, pp. 1162–1175, August (2008).

[8] M. Amara and A. Siad, Elliptic Curve Cryptography and its Applications, 7th International Workshop on Systems, Signal Processing and their Applications, pp. 247–250, May (2011).

[9] Gopinath Ganapathy and K. Mani, Maximization of Speed in Elliptic Curve Cryptography Using Fuzzy Modular Arithmetic over a Micro-controller Environment, Proceedings of the World Congress on Engineering and Computer Science, vol. 1, (2009).

[10] Scott A. Vansfone, Elliptic Curve Cryptography-The Answer to Strong, Fast Public-Key Cryptography for Securing Constrained Environments, Information Security Technical Report, vol. 2, no. 2, pp. 78–87, (1997).

[11] O. Srinivasa Rao and S. PallamSetty, Efficient Mapping Methods for Elliptic Curve Cryptography, International Jounal of

Engineering Science and Technology, vol. 2(8), pp. 3651–3656, (2010).

[12] Williams Stallings, Cryptography and Network Security, Prentice Hall, 4th Edition, (2000).

[13] Lo'aiTawalbeh, MoadMowafi and Walid Aljoby, Use of Elliptic Curve Cryptography for Multimedia Encryption, IET Information Security, vol. 7, issue 2, pp. 67–74, (2012)

[14]https://www.researchgate.net/publication/329568625_A_Recruitment_and_Human_Resource_Management_Technique_Using_Blockchain_Technology_for_Industry_40

[15]https://www.researchgate.net/publication/341046981_Benefits_and_Use_of_Blockchain_Technology_to_Human_Resources_Management_A_Critical_Review