IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

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

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906295 |

Secure Blockchain Based Data -Sharing Model Sharing Model and Adoption among Intelligence Communit

Shete Kajal Bharat[1], Prof. Monika Rokade[2]

PG Student, Sharadchandra Pawar College of Engineering, Junnar, Pune, India[1]

Assistant Professor, Sharadchandra Pawar College of Engineering, Junnar Pune, India[2]

ABSTRACT: Data sharing among the intelligence communities is important to consolidate data analysis, which will support decision-making process to preserve the security of the nation. Data sharing within an intelligence community could be more practical if an online secure data sharing mechanism is available. However, sharing data between various parties is complicated due to the confidentiality aspect and the risk of exposure to unauthorized users and attackers. Hence, this paper proposes a secure blockchain-based data-sharing model for the intelligence community. The mechanism, rules and related policies are discussed in detail in this paper. Based on the proposed model, the intention to use this model was measured using the technology readiness and acceptance model (TRAM). This study applied four technology readiness dimensions namely optimism, innovativeness, discomfort, and insecurity to measure their relationship with the Technology Acceptance Model (TAM). The findings indicated that personality traits and feelings can influence the adoption process and intention to use blockchain-based data-sharing model for system integration within the intelligence community. This study proved that blockchain technology can be applied in a data-sharing model specifically designed for the intelligence community based on the designated.

I.INTRODUCTION

In the distribution of information in a community, digital innovation is critical. The intelligence community had switched from traditional Human Intelligence (HUMINT) to a more sophisticated and advanced form of Signal Intelligence (SIGINT) and open source intelligence as a means of acquiring data (OSINT). Intelligence community must collect reliable and precise data in order to analyse it in order to make decisions and plan for the country's security.

As a result, experts have proposed utilising blockchain as an extra technology for strengthening data security, citing the great success of various experiments. [1] and [2]. However, prior to deployment, a full research on the adoption of blockchain inside the intelligence community must be conducted to guarantee that all aspects of the technology, processes, laws, and policies are thoroughly evaluated.

This paper explores the creation of a safe data sharing model that includes the adoption of blockchain technology. Based on the requirements, norms, and regulations, this article offered a conceptual secure blockchain-based data-sharing paradigm for the intelligence community. The technological readiness and acceptance model was used to measure adoption based on the proposed model (TRAM). Based on the variables chosen, a dimension was developed. To the best of the authors' knowledge, this is the first complete research of a blockchain-based data-sharing model for the intelligence community, as well as the first to use TRAM theory to investigate blockchain-based data sharing acceptability.

II.RELATED WORK

A. Intelligence Community

The intelligence community consists of different agencies and organisations that work together and separately to conduct intelligence operations to protect national security and its interest [3]. The intelligence community often includes intelligence organisations under government bodies including the intelligence agencies under homeland security. There are also defence organisations such as the armed forces and services, namely the army, navy and air force intelligence

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906295 |

branches. However, the intelligence community is not only restricted to the government, it also encompasses corporate organisations like the financial intelligence units. The private sector also plays a crucial role in handling intelligence-related projects or systems with the intelligence agencies [4].

Data Security for the Intelligence Community

In every organization around the world, especially the intelligence community, the protection of sensitive data is one of the most significant challenges. The management of data and assets could depend on a secure and robust method of security. Data should only be handled by authorised agencies that are recognised as members of the intelligence community. Unauthorised access of data by non-intelligence agencies posits a grave effect not only to the intelligence community, but also to the national security of a country [10]. Data should exhibit confidentiality, integrity and accessibility (CIA) attributes to be trusted. However, centralised systems that manage data are exposed to exploitation [11]. Such risk to exposure is bound to happen due to a bad configuration of access control and authentication [11], [12].

Among the various ways to increase data security is to strengthen the authentication procedure using a multi-factor authentication technique [4]. However, in this pervasive usage and advancement of the Internet, a good authentication technique alone is insufficient [13], [14]. Implementing a secure access control has been suggested as a method that could increase data security. Correct configuration for access control and authentication is essential in preserving data security. Data management also plays a vital role in increasing data security. The central authority for data management faces the risk of data tampering, whereby unauthorised data editing can be done. Log of data editing could also be falsified by malicious users with a data administrator role that could be obtained by hacking into the centralised database that stores the access information.

B. Blockchain Technology

Blockchain technology is a brand-new database type. Unlike SQL or NoSQL databases, blockchain can be shared directly by a group of trusted and untrustworthy individuals [17]. A blockchain is a type of distributed database that keeps track of a list of structured documents known as blocks that grows indefinitely [17]. Each block has a timestamp and is linked to the one before it. The prior block's or parent block's hash value is used to create the link. A block can traverse the whole blockchain and find each transaction made through its parent block, as shown in Fig. 1. The genesis is the initial block, and it has no parents. Due to its two key features, blockchain differs from any current scalable database: I cryptography by design; and ii) distributed data management. Cryptography by design refers to the use of cryptography to protect user identity as well as the integrity and validity of data in a ledger. Depending on the protocol, the cryptography of each block varies. The hashing algorithm is used to ensure that blocks are well-formed in order to maintain their tamper-proof security and become essentially unbreakable.

Distributed Data Management

The ability of the blockchain to construct a new distributed and decentralised software architecture where confidential transactions or agreements may be established throughout the chain with trustworthy parties is referred to as distributed data management [2]. The fact that no human interaction is required during a transaction has led to blockchain being widely used in a variety of industries, including public services, healthcare, IoT, the financial system, and corporate governance. The use of blockchain technology has grown since it became open source software, allowing developers more flexibility in testing and proposing new applications for new techniques at minimal prices.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906295 |

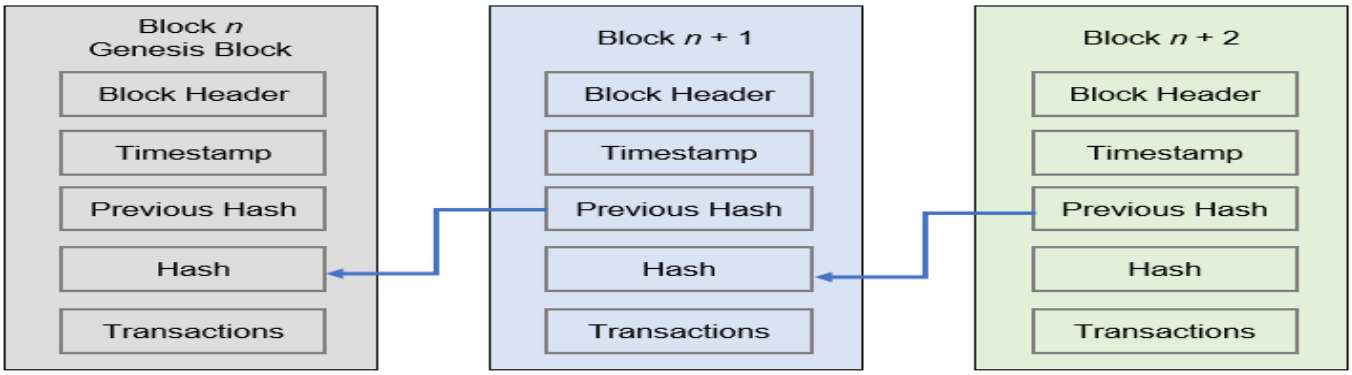

Fig. 1. Blockchain Block Architecture

Consensus mechanisms

Blockchain uses consensus procedures in a peer-to-peer network to create decentralised security structures that prevent data tampering and distribute data to all network participants. The consensus process in the blockchain system validates transactions, requests, data creation, execution, and change. Blockchains support a variety of consensus mechanisms, including Proof of Work, Proof of Stake, and Smart Contracts.

Proof of Work

The oldest and most widely used consensus algorithm in blockchain technology is Proof of Work. In order to solve the mathematical problem provided in a blockchain, it is a random procedure that requires trial and error. This feature, however, necessitates a large amount of computer power, which consumes a lot of electricity and bandwidth throughout the mining process.

Proof of Stake

Proof of Stake was designed to circumvent the limitations of Proof of Work by introducing the concept of stakeholders who have the capacity to give consensus to the block based on the stake they own. Several currency in the blockchain can be used to obtain the stake. This notion, however, has a flaw in that the owner of the earliest array of coins, or the one who possesses the most coins, will receive more incentives. As a result, demonstrating share ownership is the solution to this difficulty.

Smart Contract

The Smart Contract is another approach for reaching a consensus. End-user transactions are responded to by the Smart Contract, which implements the programming logic for interactions with ledgers in the blockchain application. This coding logic is then put into the Smart Contract, and both parties are obligated by the contract once the blockchain network participants have agreed on functional requirements.

Blockchain Application in Data Sharing

This paper suggests a private blockchain technology for the intelligence community to provide a distributed and decentralised database. This system has the potential to improve data exchange across intelligence organisations. The use of blockchain will increase the security of information communicated thanks to the cryptography design that has been developed. As a result, each transaction will have great data integrity because it will include the information about the users who requested the transaction as well as any related actions. These transactions can be followed, and the information's transparency has made blockchain an excellent candidate for use in the intelligence sector. A smart contract is an appropriate technology enabler for the consensus process.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906295 |

C. User Authentication and Identity Management

Based on authentication criteria for the intelligence community, policies specify how a user must be authenticated before access to a protected data-sharing service is authorised. This article looks into how policies could be improved by determining the dependability of an authentication system that would meet the needs of the intelligence community. Password-based authentication systems are the most popular technique of user authentication. Previous researchers have created a multi-factor authentication approach to enhance the security of a password-based authentication system due to security flaws in the password-based authentication system. However, this authentication technique is insufficient to prevent emerging attacks such as man-in-the-middle, distributed denial of service (DDos), and replay attacks [13], [14], prompting researchers to investigate dynamic authentication and dynamic authentication policy. Dynamic authentication, also known as adaptive authentication, is a multi-layered authentication solution that uses two or more authentication factors to determine risk. Dynamic authentication is dependent on the user's profile and behaviour, which includes information like the user's identifiable devices, location, regular login time, and roles. For each authentication session, user requests are assessed and a risk score is assigned. Depending on the risk score, the user may be asked to submit more credentials or allowed to use less credentials.

D. Access Control

Access control is a crucial part of secure data sharing because it allows users to restrict their access to data based on their roles and fine-grained access control to the data, which fits the need-to-know principle in intelligence sharing. The access control manager can grant or revoke user access adaptively by updating the access policy in real-time utilising fine-grained access control, and each data piece has its own personalised access control policy.

Each intelligence personnel, for example, has access to all available and acceptable intelligence data, and data owners have authority over their shared information. The following policies govern access:

1) Grant or revoke the user's access.
2) Administrative access to the system.
3) Access permissions for users (intelligence personnel).
4) Transactions can be performed by a system administrator with particular permissions.
5) Transactions can be performed by users with specified permissions.

Monika Rokade and Yogesh Patil [11] proposed a system deep learning classification using nomaly detection from network dataset. The Recurrent Neural Network (RNN) has classification algorithm has used for detection and classifying the abnormal activities. The major benefit of system it can works on structured as well as unstructured imbalance dataset.

The MLIDS A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset has proposed by Monika Rokade and Dr. Yogesh Patil in [12]. The numerous soft computing and machine learning classification algorithms have been used for detection the malicious activity from network dataset. The system depicts around 95% accuracy ok KDDCUP and NSLKDD dataset.

Monika D. Rokade and Yogesh Kumar Sharma [13] proposed a system to identification of Malicious Activity for Network Packet using Deep Learning. 6 standard dataset has sued for detection of malicious attacks with minimum three machine learning algorithms.

Sunil S. Khatal and Yogesh kumar Sharma [14] proposed a system Health Care Patient Monitoring using IoT and Machine Learning for detection of heart and chronic diseases of human body. The IoT environment has used for collection of real data while machine learning technique has used for classification those data, as it normal or abnormal.

Data Hiding In Audio-Video Using Anti Forensics Technique For Authentication has proposed by Sunil S.Khatal and Yogesh kumar Sharma [15]. This is a secure data hiding approach for hide the text data into video as well as image. Once sender hide data into specific objects while receivers does same operation for authentication. The major benefit of this system can eliminate zero day attacks in untrusted environments.

Sunil S.Khatal and Yogesh Kumar Sharma [16] proposed a system to analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. This is the analytical based system to detection and prediction of heart disease from IoT dataset. This system can able to detect the disease and predict accordingly.

III.PROPOSED SYSTEM

Based on the theoretical analyses found in the literature, this research proposed a secure blockchain-based data sharing model for the intelligence community. This model was divided into four modules as shown in Fig. 2, namely User

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906295 |

Authentication and Identity Management Module, Access Control Module, Intelligence Data Generation, Edit, and View Module as well as Intelligence Data Storage Module. The User Authentication and Identity Management Module were proposed to implement the enhanced multi factor authentication model. Meanwhile, the Access Control Module, the Intelligence Data Generation, Edit and View Module, as well as the Intelligence Data Storage Module were proposed to employ the blockchain technology.

In the proposed model, the User Authentication and Identity Management Module were used for user authentication. It was managed by the administrator of each intelligence agency connected to the Human Resource Management Systems (HRMS). Thus, details of the user will always be updated if any changes occur in the HRMS.

This study has chosen not to implement the blockchain technology in User Authentication and Identity Management Module to shorten the authentication process while simultaneously preserving the system's security. This is because implementation using updated data from HRMS would be more efficient and convenient for the management of various intelligence communities compared to user authentication using blockchain technology. A consensus mechanism is deemed unnecessary due to the nature of the operations between intelligence agencies in the intelligence community, which requires user authentication to be done and administered at each level of organisations.

After a user has successfully logged into the data system, a blockchain transaction is generated for each transaction that occurs in the system. A regulator party then regulates users' participation in the network and defines an access control policy of the users in the Access Control Module. Blocks will be created for the Intelligence Data Generation, Edit and View Module, where any accessed data will be added to the Decentralised and Distributed Storage Modul. Detailed explanation for each module is given in the following subsections

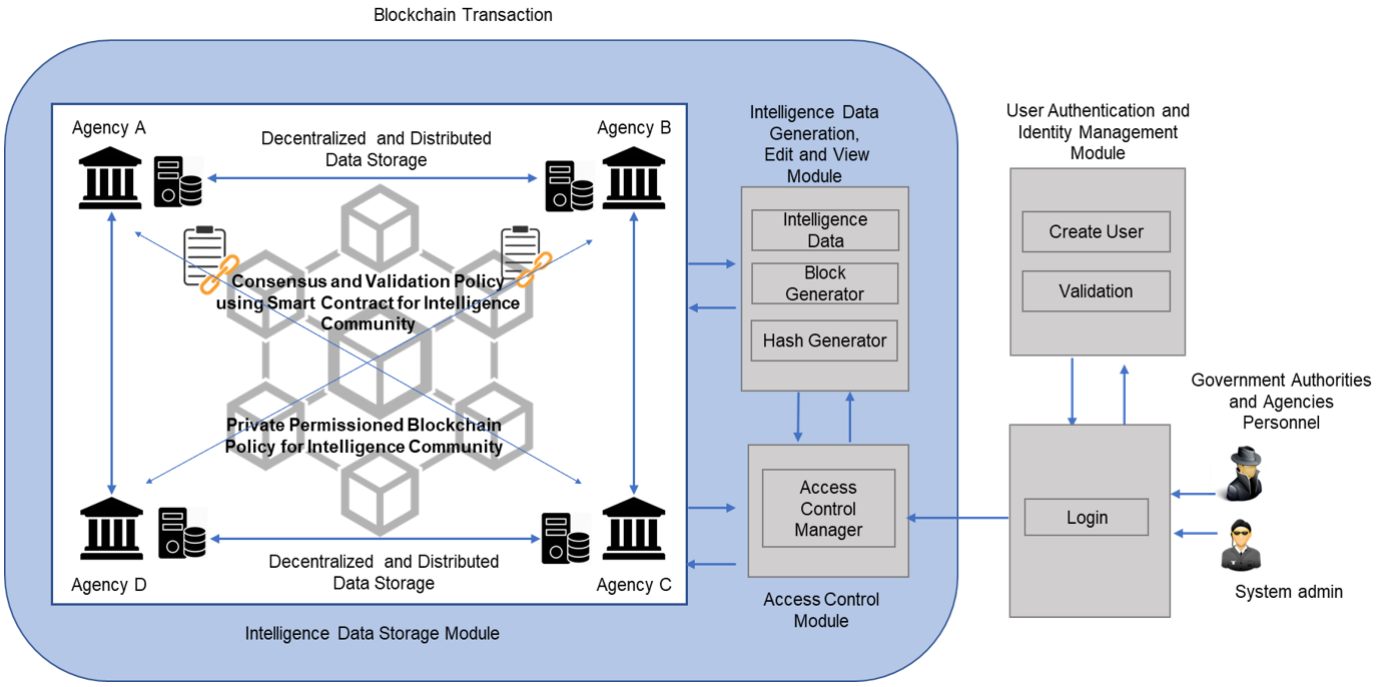

Fig. 2. Proposed system architecture

Conclusion and Future work

Based on blockchain technology, this article proposes a safe data-sharing mechanism for the intelligence community. This architecture includes numerous modules based on the intelligence community's needs. Using enhanced multi-factor authentication, a secure approach for User Authentication and Identity Management Module has been devised to increase the security of user authentication and identity management of the data-sharing system while also meeting the needs of the stakeholders. The Access Control Module was created with decentralised access control management in mind, utilising a

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906295 |

combination of role-based access control (RBAC) and fine-grained access control rules to implement consensus and validation policies using Smart Contracts. This module can help to strengthen the system's security and prevent unauthorised access.

REFERENCES

[1] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "FairAccess : a new Blockchain-based access control framework for the Internet of Things," no. February, pp. 5943–5964, 2017, doi: 10.1002/sec.1748.
[2] X. Xu *et al.*, "A Taxonomy of Blockchain-Based Systems for Architecture Design," *2017 IEEE Int. Conf. Softw. Archit.*, pp. 243–252, 2017, doi: 10.1109/ICSA.2017.33.
[3] ODNI, "Members of the IC." http://www.odni.gov/index.php/intelligence-community/members-of-the-ic (accessed May 04, 2020).
[4] W. N. Wan Muhamad *et al.*, "Enhance multi-factor authentication model for intelligence community access to critical surveillance data," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11870 LNCS, pp. 560–569, doi: 10.1007/978-3-030-34032-2_49.
[5] Daniel R. Coats, "The National Intelligence Strategy of the United States of America," 2019. doi: 10.1515/9783110212495.2.121.
[6] S. N. Q. S. Mohamed and M. Yaacob, "Understanding the Intelligence Failure and Information Sharing in Handling Terrorism among Intelligence Community," *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 9, no. 9, pp. 1201–1213, 2019, doi: 10.6007/ijarbss/v9-i9/6414.
[7] J. Schmid, "Technology and the Intelligence Community," in *Advanced Sciences and Technologies for Security Applications*, 2018, pp. 39–53.
[8] W. J. Lahneman, "Knowledge-sharing in the intelligence community after 9/11," *Int. J. Intell. CounterIntelligence*, vol. 17, no. 4, pp. 614–633, 2004, doi: 10.1080/08850600490496425.
[9] J. W. Crampton, "Collect it all: national security, Big Data and governance," *GeoJournal*, vol. 80, no. 4, pp. 519–531, 2015, doi: 10.1007/s10708-014-9598-y.
[10] S. S. De Matas and B. P. Keegan, "An exploration of research information security data affecting organizational compliance," *Data Br.*, vol. 21, pp. 1864–1871, 2018, doi: 10.1016/j.dib.2018.11.002.
[11] Monika D.Rokade ,Dr.Yogesh kumar Sharma,"Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic."IOSR Journal of Engineering (IOSR JEN),ISSN (e): 2250-3021, ISSN (p): 2278-8719
[12] Monika D.Rokade ,Dr.Yogesh kumar Sharma"MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE
[13]Monika D.Rokade, Dr. Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2324 - 2331.
[14] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Health Care Patient Monitoring using IoT and Machine Learning.", **IOSR Journal of Engineering (IOSR JEN),** ISSN (e): 2250-3021, ISSN (p): 2278-8719
[15]Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Data Hiding In Audio-Video Using Anti Forensics Technique ForAuthentication ", IJSRDV4I50349, Volume : 4, Issue : 5
[16]Sunil S.Khatal Dr. Yogesh Kumar Sharma. (2020). Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2340 - 2346.
[17] N. Abdullah and A. Håkansson, "Blockchain based Approach to Enhance Big Data Authentication in Distributed Environment," pp. 887–892, 2017.
[18] A. McAbee, M. Tummala, and J. McEachen, "Military Intelligence Applications for Blockchain Technology," *Proc. 52nd Hawaii Int. Conf. Syst. Sci.*, 2019, doi: 10.24251/hicss.2019.726.
[19] T. J. Willink, "On blockchain technology and its potential application in tactical networks," *Def. Res. Dev. Canada*, no. April, 2018.
[20] A. Sudhan and M. J. Nene, "Employability of blockchain technology in defence applications," in *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, 2017, pp. 630–637

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details