SAFELY STORING AND DELIVERING INFORMATION FROM INTERNET OF THINGS DEVICES

#1SAMEENA KOUSAR, *MCA Student,*
#2B.ANVESH KUMAR, *Assistant Professor,*
#3Dr.V.BAPUJI, *Associate Professor& HOD,*
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

Abstract: Data sharing among intelligence communities is critical for expediting data analysis and supporting decision-making in order to guarantee the security of the nation. If an internet-safe data exchange channel is available, data sharing inside an intelligence community may become more possible. However, transporting data between many parties is problematic due to the issue of confidentiality and the possibility of being exposed to unauthorized users and attackers. As a result, this study offers a blockchain-based secure data-sharing architecture for intelligence agencies. This document goes into great detail on the procedure, rules, and policies involved. To assess the intention to implement the proposed paradigm, the technology readiness and acceptance model (TRAM) was applied. The optimism, innovativeness, discomfort, and insecurity characteristics were investigated in this study to determine their link with the technical Acceptance Model (TAM). According to the study, personality traits and feelings can influence the adoption process and intention to use a blockchain-based data-sharing model for system integration inside the intelligence community. This study discovered that blockchain technology might be used in a data-sharing architecture created expressly for the intelligence community based on the established dimensions.

Index Terms: *Blockchain, secure data sharing, Technology Acceptance Model, Technology Readiness Index.*

I. INTRODUCTION

Innovations in digital technology are essential for sharing information throughout a society. The intelligence community had abandoned its reliance on HUMINT in favor of Signal Intelligence (SIGINT) and open source information (OSINT) for its investigations. In order to make choices and formulate plans for the nation's security, the intelligence agency must collect precise and accurate data.

Researchers have proposed integrating blockchain as an extra technology to increase data security after various investigations demonstrated blockchain's remarkable performance. [1], [2]. To make sure that the technology, methods, procedures, and policies associated with blockchain adoption within the intelligence community are thoroughly evaluated before implementation, a comprehensive research on the topic is required.

In this research, we investigate how blockchain technology might be applied to the formulation of secure information exchange protocols. For the intelligence community, this article proposed a conceptual secure blockchain-based data-sharing paradigm based on the requirements, norms, and rules. The technology readiness and acceptance model (TRAM) was developed with the proposed model as its basis. The proposed dimension is a direct result of the selected variables. This study is the first to our knowledge to examine the adoption of a blockchain-based data-sharing paradigm within the intelligence community, and it is also the first to do so using TRAM theory.

II. RELATED WORK

In [43], the idea of a blockchain-based, four-layer Electronic Health Record (EHR) was proposed. There were several tiers of electronic health records (EHRs), including those for user administration, record creation and display, data storage and user authorization. The basic needs of the data interchange and protection strategy were met by classifying these layers according to the module's functions. However, the research was restricted to only exploring the usage of QR codes and One-Time Password (OTP) codes as supplementary security measures for the used blockchain network. Recent studies have shown that security and privacy controls, access restrictions, data controls, and consistent standards are essential to effective data sharing and protection methods [44]. Another study has proposed an invitation-only or permission-only blockchain network wherein only node users are allowed to participate. And only people who are already part of the distributed ledger network can carry out activities or contribute to consensus [45].

Other approaches to blockchain-based data sharing include permissioned blockchain and distributed hash tables (DHT) for decentralized data storage [46] and the construction of a worldwide end-to-end Internet performance measuring project (PingER's) access architecture. In [47], the author explains how to implement a blockchain-based incentive solution for on-chain and off-chain data storage, hashing, encryption, and tracking using a discrete private key.

Permissioned Ethereum-based MultiChain access control. The authors also suggested employing smart contracts to ensure encrypted blockchain interactions [48

.User Authentication and Identity Management

A user's identity must be verified in accordance with the guidelines established by the intelligence community's authentication standards before they will be granted access to a secure data-sharing service. In this study, we look into ways in which the reliability of an authentication system might be improved to fulfill the needs of the intelligence community. Currently, password-based authentication solutions have the largest market share [49]. To address the weaknesses of password-based authentication methods, some scholars have advocated multi-factor authentication. Researchers [49], [51], and [52] investigated dynamic authentication and dynamic authentication policies because this authentication approach is insufficient to prevent newer assaults such man-in-the-middle, DDoS, and replay attacks [13, 14], [50]. Dynamic authentication, also known as adaptive authentication, is a multi-layered security system made up of two or more authentication factors based on a risk assessment. Dynamic authentication takes into account a wide variety of variables, including but not limited to user roles, login frequency, and geographic location. Based on an evaluation of the user's requests, a risk score is assigned to each authentication session [53]. More or less authentication may be necessary for a given user, depending on their risk score.

Access Control

In order to restrict users' access based on their duties and fine-grained access to the data, access control is a fundamental component of the need-to-know basis, which is central when it comes to sharing intelligence information. The access control manager can grant or revoke permission to access data on the fly by making changes to the corresponding access policy. All intelligence employees have access to view approved intelligence data that is available to the public, but data owners retain control over what information they choose to make public. Among the regulations governing admission are:

1) Give permission to use, or remove permission if necessary.

2) The IT manager must give his or her stamp of approval.

3) Authorization for end-users (intelligence analysts) is the third consideration.

4) An authorized system administrator can complete a financial transaction.

5) Financial dealings can be made only by approved users. There have lately been proposals to replace centralized access control management with a decentralized system based on blockchain technology due to its many shortcomings. In centralized access control management, the authenticity of users is certified by a single organization. The fundamental concept behind blockchain technology is the creation of a decentralized network of peers, which allows for secure and transparent information storage and transmission via blockchain transactions. This information is transmitted directly between nodes without going through a central server.

III. INTELLIGENCE COMMUNITY AND BLOCKCHAIN TECHNOLOGY

Intelligence Community

The intelligence community is made up of many entities that work together and independently to carry out intelligence activities with the purpose of safeguarding the country [3]. Government agencies, such as those devoted to homeland security intelligence, are sometimes considered part of the intelligence community. There are auxiliary defense formations beyond the army, navy, and air force, such as intelligence divisions connected to the armed forces and services. Both public and private organizations, such as financial intelligence units, are part of the intelligence community. The business sector is just as important as intelligence agencies in overseeing intelligence-related activities or systems [4].

The Central Intelligence Agency (CIA) and the Office of the Director of National Intelligence (ODNI) are two separate but equal parts of the United States' intelligence community. The National Security Agency (NSA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA), and National Reconnaissance Office (NRO) are just eight of the many components of the Department of Defense involved in intelligence gathering and analysis [5, 6]. Members of the Special Branch (SB) of the Royal Malaysian Police and the Defence Intelligence Staff Division (DISD) make up Malaysia's National Intelligence Committee. Internal security and military intelligence are two areas in which these organizations are very involved [4].

The intelligence community uses a wide variety of tools and sensors to gather intelligence. When it comes to analyzing tactical operational data [7, 8], data acquisition is of highest importance to government authorities, agencies, and fighters. Distributing information precisely and accurately is difficult [6]. As a result, the intelligence community requires a solid system for sharing knowledge and passing along facts [5, p. 22]. The political, cultural, economic, and civilian domains of a country are all vulnerable to the consequences that could result from the unauthorized publication or compromised nature of intelligence material [4, 9].’

Data Security for the Intelligence Community

Institutions around the world, and the intelligence community in particular, place a premium on keeping sensitive data safe. Data and resource management may depend on the introduction of a reliable and strong security protocol. Only verified organizations with verified membership in the intelligence community should have access to classified information. Consequences for national security and the intelligence community can be severe when unapproved parties acquire access to data, especially when those organizations are not part of the intelligence community [10]. The CIA trinity, or the confidentiality, integrity, and availability of data, is a set of characteristics necessary to create credibility. The vulnerability of centralized data management systems, however, must be recognized [11]. A configuration error in authentication and access control (11, 12) makes exposure likely.

Improving data security is possible with the use of multi-factor authentication [4]. However, in view of the Internet's widespread use and rapid development, it is not sufficient to rely just on a strong authentication technique [13], [14]. A strong access control system is presented as a means to improve data security. Data security can only be maintained through the use of a robust access control and authentication infrastructure. Improving data security is also dependent on good data management procedures being put into place. The risk of data tampering, the unauthorized modification of data, must be considered by the central authority in charge of data management. The data-altering log may be manipulated by criminals if they gained unauthorized access to the database and assumed the role of data administrator.

Experts recommend a data management architecture that is decentralized, adaptable, and scalable to deal with this problem. This is where the use of blockchain technology for managing data becomes important. The decentralized nature of blockchain technology has been proposed for use in data management because of the security it provides, especially for private and sensitive data [1, 13, 15]. As a result, it is crucial to create a new framework that can efficiently address the current security flaws.

The term "intelligence data" [16] refers to both raw intelligence data and intelligence reports. Voice and data from the target's communications, video and data from radar transmissions and satellite communication systems, picture and data from open sources and social media are all examples of raw intelligence data. It is possible for intelligence reports to include both routine and timely reports in addition to case-based reports. The intelligence community needs new technology to efficiently manage the massive amount of data because of rising data consumption and integration. This is especially crucial in a setting with stricter safety regulations. It has been discovered that blockchain technology provides a comprehensive answer to a wide variety of serious security problems [17]. Investigating security components including blockchain technology for decentralized data storage and administration, user identity, and access control is essential for efficiently handling the issues connected with promoting secure data sharing.

There is a wide variety of ways in which blockchain technology could be used to improve intelligence operations. Military intelligence can benefit from a distributed and decentralized database [18], a secure communication and data storage system [19], better data integrity in supply chain management [20], and more openness in equipment management [21]. Further, blockchain technology can help build trustworthy C3I (Command, Control, Communication, and Intelligence) networks [21].

Blockchain Technology

Blockchain technology is at the heart of a new kind of database. In contrast to traditional SQL or NoSQL databases, blockchain technology allows a network of both trusted and untrusted entities to instantly exchange information [17]. A blockchain is a distributed ledger that tracks transactions through an ever-growing chain of ledger entries called blocks [17]. Each building piece in the sequence is times tamped and connected to the one before it in a complex web of relationships. The hash value of the parent block or the block before it is used as the primary basis for making the connection. As can be seen in Figure 1, a block can travel across the whole blockchain to find all transactions related to its parent block. The first block, often called the genesis block, has no predecessors [24]. According to the cited article [25], the two main features that set blockchain apart from other scalable databases are its distributed data management and its built-in cryptography algorithms. The term "encryption by design" describes the process by which encryption methods are intentionally implemented to protect users' anonymity and the integrity of the data recorded in a distributed ledger. Each protocol has its own unique set of requirements for a block's cryptographic features [24]. The inclusion of the hashing method is intended to protect the security and privacy of blocks, making them immune to tampering and forgery [24].

Distributed Data Management

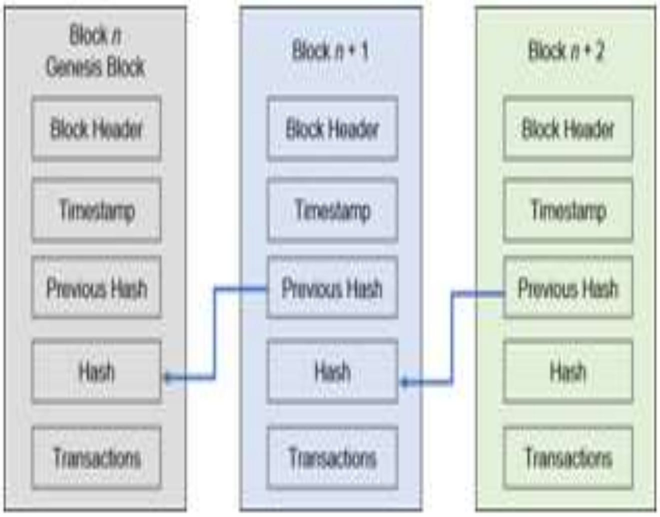

Fig. 1. Blockchain Block Architecture

Reliable transactions or agreements among trusted entities along the entire chain can be established thanks to the blockchain's ability to construct a novel distributed and decentralized software architecture [2]. Public services, healthcare, the Internet of Things, and the financial system and corporate governance are just some of the sectors where blockchain technology has seen widespread application. Developers have been able to experiment with blockchain technology and propose new applications for novel techniques because it is available as open source software, which has led to increased acceptance.

Consensus mechanisms

Decentralized security designs, made possible by blockchain technology, successfully reduce the possibility of data manipulation. This is accomplished through the use of peer-to-peer data distribution and consensus procedures in the network. Transactions, requests, and data generation, execution, and change are all guaranteed by the blockchain system's consensus mechanism. Proof-of-Work, Proof-of-Stake, and Smart Contracts are just a few of the consensus mechanisms that may be implemented with the use of a blockchain.

Proof of Work

It is often agreed that Proof of Work (PoW) is the first and most widely used consensus technique in the blockchain industry. The mathematical mystery contained in a blockchain can be solved via a stochastic technique that involves trial and error. Meanwhile, mining requires a lot of processing power, which means a lot of money spent on electricity and network bandwidth.

Proof of Stake

To overcome the shortcomings of Proof of Work, the notion of Proof of Interest was developed to provide stakeholders consensus authority based on their interest or ownership in the system. Staking is facilitated by holding numerous coins within the blockchain. The distribution of rewards under this idea is problematic since it gives an unfair advantage to people who have large quantities of coins. Therefore, the solution to this problem is to create a system of stock ownership.

Smart Contract

The Smart Contract is another way that is widely recognized in academic circles. The Smart Contract establishes the computational principles governing the interactions between the blockchain application and ledgers, as well as the corresponding responses to transactions initiated by end-users. After reaching a consensus on the functional requirements, the coding logic is incorporated into the Smart Contract within the blockchain network, thereby binding both parties to the contractual obligations.

Type of Blockchain

Blockchains can be categorized into three distinct types, namely public, private, and consortium blockchains. Participation on a public blockchain is open to all users, allowing them to function as nodes. Public blockchains are commonly regarded as decentralized systems due to their ability to reach consensus without relying on a central authority. Each local node's users will maintain a duplicate of the ledger, and a distributed consensus methodology will be employed to achieve a final conclusion or state of the ledger. The Bitcoin blockchain serves as a noteworthy illustration. In contrast, private blockchains are only accessible to a limited cohort of individuals or organizations who have mutually consented to participate in the sharing of the ledger. While a private blockchain is of a narrower scale compared to a public blockchain, empirical evidence has shown that it requires less computational resources and facilitates faster transaction processing. The presence of a central administrator serves as a deterrent against data manipulation. The consortium blockchain is formed through the integration of a public and private blockchain, wherein the consensus mechanism is supervised by a predefined quantity of nodes. The potential for blockchain technology to facilitate a decentralized, grassroots management structure raises the possibility of displacing traditional hierarchical organizations. Blockchain-based networks are purposefully engineered to exhibit a fully decentralized structure, devoid of any central authority or intermediary entity. Communication between contributors within these networks is facilitated using a decentralized architecture. Smart contracts possess the ability to oversee blockchain governance and uphold the established codes, hence automating essential tasks without human intervention.

Blockchain Application in Data Sharing

This research suggests the adoption of private blockchain technology by the intelligence community as a means to acquire entry into a distributed and decentralized database. The present technology exhibits the capacity to enhance the data exchange procedure among intelligence agencies. The implementation of cryptography is expected to enhance the security of information transmitted through the utilization of blockchain technology. The accuracy of the data is ensured due to the inclusion of information regarding the individuals who initiated each transaction, along with any related activities. The utilization of blockchain technology in the intelligence sector is highly advantageous due to its inherent ability to facilitate traceable transactions and provide transparent information dissemination. A smart contract is a technological facilitator that is deemed suitable for the consensus methodology.

IV. CONCLUSION

This study presents a novel architecture for secure data-sharing inside the intelligence community, utilizing blockchain technology. A number of architectural components were devised in accordance with requirements made by the intelligence community. In order to strengthen the security of the data-sharing system's user authentication and identity management, while also addressing the requirements of stakeholders, a secure approach for the User Authentication and Identity Management Module was devised. This involved the implementation of an improved multi-factor authentication system. The development of the Access Control Module was motivated by the need for decentralized management of access control. This was achieved by integrating two established approaches, namely role-based access control (RBAC) and fine-grained access control rules. Smart contracts were employed to establish consensus and validation protocols. This module has the potential to enhance system security and mitigate unauthorized access.

The approach employed by the Intelligence Data Generation, Edit, and View Module for the storage and retrieval of data through smart contracts has been extensively documented. Efficient and reliable data storage can be achieved through the utilization of off-chain data storage via a private cloud and distributed hash tables, as suggested by existing proposals.

The deployment of the suggested model necessitated an empirical investigation into the level of user readiness and acceptance. Therefore, the study employed the usage of TRAM. The present study has discovered a notable correlation between the level of technology readiness and the extent of user adoption in the context of the research conducted. The results of this study indicate that the Technology Readiness and Acceptance Model (TRAM) has potential applicability within the intelligence community for assessing the influence of personality factors on the adoption and desire to utilize a blockchain-based data-sharing system. The adoption of the proposed system was significantly influenced by personality qualities, specifically optimism and creativity, as motivators in Technology Readiness Index (TRI). The perceived usability and utility of this technology were found to operate as mediating variables in the desire to utilize a blockchain-based data sharing system, resulting in a significant intention to adopt it. This observation aligns with the results reported in a prior investigation. This highlights the significance of incorporating considerations of usefulness and usability into the design process of blockchain-based applications.

Based on the research findings, it is evident that innovativeness and optimism, which are considered favorable attributes linked to technological preparedness, can potentially exert a beneficial influence on the perceived usefulness and simplicity of a given entity. This observation aligns with the results of a study conducted by, which revealed that optimism and inventiveness positively influence the perceived usefulness and simplicity of blockchain technology, specifically in the domain of cryptocurrency blockchain-based data-sharing platforms. The results of the study indicate that there is a significant relationship between optimism and creativity, and the perceived usefulness and perceived usability of a certain product or service.

This study aims to expand its data gathering efforts to encompass many intelligence organizations in the future, with the objective of achieving a more comprehensive data collection approach. As per the findings of previous studies, the process of collecting data for system adoption should encompass acceptability tests conducted at various stages, including post-implementation assessments immediately after the system's initial deployment, one month subsequent to implementation, and three months following implementation. The software application mentioned

REFERENCES

1. 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. 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.
4. Daniel R. Coats, “The National Intelligence Strategy of the United States of America,” 2019. doi: 10.1515/9783110212495.2.121.
5. 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.

6. J. Schmid, "Technology and the Intelligence Community," in *Advanced Sciences and Technologies for Security Applications*, 2018, pp. 39–53.
7. 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.
8. 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.
9. 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.
10. N. Kshetri, "Big data′s impact on privacy, security and consumer welfare," *Telecomm. Policy*, vol. 38, no. 11, pp. 1134–1145, Dec. 2014, doi: 10.1016/j.telpol.2014.10.002.
11. E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," in *CEUR Workshop Proceedings*, 2017, vol. 1816, pp. 146–155.
12. Lin, D. He, X. Huang, K. R. Choo, and A. V Vasilakos, "BSeIn : A blockchain-based secure mutual authentication with fine-grained access control system for industry 4 . 0 ☆," *J. Netw. Comput. Appl.*, vol. 116, no. March, pp. 42–52, 2018, doi: 10.1016/j.jnca.2018.05.005.
13. P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things," *J. Cyber Secur. Mobil.*, vol. 1, pp. 309–348, 2013.
14. O. Alphand *et al.*, "IoTChain : A Blockchain Security Architecture for the Internet of Things," *2018 IEEE Wirel. Commun. Netw. Conf.*, pp. 1–6, 2018.
15. M. Räsänen and J. M. Nyce, "The Raw is Cooked: Data in Intelligence Practice," *Sci. Technol. Hum. Values*, vol. 38, no. 5, pp. 655–677, 2013, doi: 10.1177/0162243913480049.
16. N. Abdullah and A. Håkansson, "Blockchain based Approach to Enhance Big Data Authentication in Distributed Environment," pp. 887–892, 2017.
17. T. J. Willink, "On blockchain technology and its potential application in tactical networks," *Def. Res. Dev. Canada*, no. April, 2018.
18. 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.