International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Block Chain Based Fine Grained Data Sharing For Multiple Group

Sejal S. Dhamgaye, Supriya Sawwashere, Dr. Shrikant V. Sonekar, Mirza Moiz Baig

Department of Computer Science & Engineering, J. D. College of Engineering and Management, Nagpur, Maharashtra, India

Article Info
Volume 9, Issue 3
Page Number : 520-533
Publication Issue :
May-June-2022
Article History
Accepted : 10 June 2022
Published: 24 June 2022

ABSTRACT

It is essential for the various intelligence community to share their data in order to consolidate their data analysis, which will provide support for the decision-making process and help maintain national security. If an internet platform for secure data sharing is provided, data sharing within an intelligence community may become more viable. However, because to concerns regarding confidentiality and the possibility of the data being accessed by unauthorised users or stolen by attackers, it might be difficult to exchange data between different parties. As a result, the study suggests an encrypted data-sharing model for the intelligence community that is built on blockchain technology. This study provides a comprehensive analysis of the mechanism, rules, and policies that are associated with it. Using the technology readiness and acceptability model, we determined whether or not there was an intention to deploy this model based on the suggested model (TRAM). This research investigated the connections between the Technology Acceptance Model and the four characteristics of technological preparedness—optimism, innovativeness, discomfort, and insecurity (TAM). According to the findings, personality characteristics and feelings have the potential to impact the adoption process as well as the intention to utilise a data-sharing model that is based on blockchain technology for system integration inside the intelligence community. This study provided conclusive evidence that blockchain technology may be utilised in a data-sharing model that is tailored to the requirements of the intelligence community on the basis of the selected dimension.

Index Terms—Blockchain, Secure Data Sharing, Technology Acceptance Model, Technology Readiness Index

I. INTRODUCTION

The progression of digital technology plays an essential part in the communication of information within a community. The intelligence community had altered its method of acquiring data from the more traditional Human Intelligence (HUMINT) to the more complex and advanced method of Signal

Intelligence (SIGINT) and open source intelligence. This was done in order to better understand the world around them (OSINT). For the purpose of making decisions and making plans about the nation's security, the intelligence communities are obligated to collect facts and information that are reliable and precise.

Therefore, experts have proposed adopting blockchain as an extra technology for the purpose of strengthening data security. This is due to the fact that various studies have demonstrated the significant success of blockchain. [1], [2]. However, a comprehensive study on the implementation of blockchain within the intelligence community needs to be supplemented in order to ensure that all aspects related to the technologies, processes, rules, and policies are thoroughly considered prior to the implementation. This is necessary in order to ensure that the implementation goes as smoothly as possible.

In this work, we address the design of a model for the secure exchange of data, which incorporates the use of technology based on blockchains as a component of the model. In this work, we suggested a conceptual secure data-sharing model for the intelligence community that is built on blockchain technology. The model was based on the requirements, laws, and regulations. The measurement of adoption was carried out utilising the technological readiness and acceptability model, which was based on the model that was proposed (TRAM). The dimension was suggested on the basis of the variables that were chosen. This study is, to the best of the authors' knowledge, the first comprehensive study on blockchain-based data-sharing model for the intelligence community, and it is also the first study to study blockchain-based data sharing acceptance using TRAM theory. Both of these distinctions were achieved by conducting the study.

II. INTELLIGENCE COMMUNITY AND BLOCKCHAIN TECHNOLOGY

A. Intelligence Community

The term "intelligence community" refers to the collection of many agencies and organisations that, in conjunction with one another and on their own, carry out intelligence operations for the purpose of preserving national security and the nation's interests [3]. The term "intelligence community" typically refers to a collection of intelligence organisations that are housed within government entities, such as the intelligence agencies housed within the department of homeland security. In addition, there are defence institutions such as the armed forces and services, more specifically the intelligence sections of the army, navy, and air force. The intelligence community, on the other hand, is not limited to the government alone; it also includes private organisations such as financial intelligence units. When it comes to the management of intelligence-related projects or systems by the intelligence agencies, the private sector also plays an essential role [4].

For instance, in the United States, the intelligence community is made up of two separate agencies that go by the names of the Central Intelligence Agency and the Office of the Director of National Intelligence (CIA). They also have seven other department and agency elements in addition to the eight elements of the Department of Defense, which include the National Security Agency (NSA), the Defence Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), and the National Reconnaissance Office (NRO), as well as intelligence elements within their military services of the Army, Navy, Marine Corps, and Air Force [5, 6]. The Special Branch (SB) of the Royal Malaysian Police and the Defence Intelligence Staff Division (DISD) are both examples of organisations that are a part of Malaysia's intelligence community, which is housed under the purview of the National Intelligence Committee [4].

The information and data gathered by the intelligence community might come from a wide variety of sources, including a variety of sensors and equipment. The acquired data are essential for the government authorities, agencies, and military personnel who will be doing the tactical operational data analysis [7], [8]. Because it is difficult to correctly share accurate and exact data [5, p. 22], the community of intelligence professionals needs an effective method for sharing information and distributing data [5, p. 22]. Data from an intelligence agency that is leaked or otherwise compromised could have an effect on the sovereignty of a nation, which in turn could have a substantial impact on civilian communities in terms of politics, culture, the economy, or even life [4, 9].

Data Security for the Intelligence Community

One of the most significant issues faced by every business in the world, and particularly by the intelligence community, is maintaining the confidentiality of sensitive data. A method of security that is both secure and reliable can be necessary for the management of both data and assets. Only authorised agencies that are acknowledged as members of both the intelligence community should be permitted to handle sensitive data. Unauthorized access to data by organisations that are not part of the intelligence community poses a serious threat not just to the intelligence agencies but also to the national defense of a nation [10]. In order to be relied upon, data must possess the characteristics of confidentiality, integrity, and accessibility (CIA). On the other hand, centralised systems that manage data leave themselves open to being exploited [11]. A poor configuration of access control and authentication [11, 12] will almost certainly result in the occurrence of risks to exposure of this nature.

One of the many methods available for boosting the level of data protection is to implement a more stringent authentication process by making use of a multi-factor authentication method [4]. On the other hand, a good authentication method by itself is not sufficient in this day and age due to the widespread use and rapid development of the Internet [13], [14]. It has been suggested as a possible technique that one could strengthen data security by implementing a secure access control system. It is absolutely necessary to have a properly configured access control and authentication system in order to keep data secure. The management of data also plays an important part in the overall increase in data security. The central authority in charge of data management runs the danger of having data tampered with, which means that unauthorised changes could be made to the data. Malicious users with a data administrator role, which might be obtained by breaking into the centralised database that maintains the access information, may also falsify logs of data editing to make it appear as though legitimate changes were made.

The researchers are suggesting that in order to solve this problem, the data should be maintained by an infrastructure that is decentralised, adaptable, and scalable. The incorporation of blockchain technology into data management becomes relevant at this point in the discussion. Previous research has explored incorporating blockchain technology into the management of data, particularly sensitive and potentially dangerous data, due to its capacity to protect data through the use of a decentralised manner [1, 13], [15]. Because of this, a new model is required to address the security flaws that are present in the current implementation.

Intelligence data comprises raw intelligence data and intelligence reports [16]. Raw intelligence data can come from a variety of sources, including speech and traffic from a target's communications, films, radar transmission details, data from satellite communication systems, imagery data, open source data, and information connected to social media. Intelligence reports, however, can be categorised as either routine or timely reports, or they can be case-based intelligence reports. In an environment where higher safety requirements are required due to the increasing volume of data utilisation and integration, new technologies are required for the data management of the entire intelligence community. These new technologies must be developed. The distributed ledger technology (Blockchain) has provided a comprehensive answer to a multitude of important concerns about data security [17]. Research needs to be done on various aspects of data security, including blockchain technology for decentralised data storage and administration, user authentication, and access control, in order to fix the problems that arise while attempting to provide secure data sharing.

To provide a distributed and decentralised database for military intelligence [18], a secure communication and data storage system [19], to enhance data integrity in supply chain management and ensure transparency in equipment management [20], and to provide secure Command, Control, Communication, and Intelligent (C3I) systems [21], blockchains have the potential to be applied in a variety of intelligence operations.

B. Blockchain Technology

The technology known as blockchain is a novel implementation of a database. In contrast to SQL and NoSQL databases, blockchain technology allows for data to be directly shared among members of a community, both trusted and untrusted [17]. A blockchain is a type of distributed database that maintains a list of structured information known as blocks [17]. This list is continuously growing and cannot be altered in any way. Every block has its own individual timestamp and is connected to the one before it [22], [23]. The hash value of the block that came before it, known as the parent block, is used to determine the linkage. As shown in Figure 1, a block has the ability to traverse the entirety of the blockchain in order to locate each transaction that was executed through its parent block. The initial block is referred to as the genesis, and it does not have any parents [24]. According to [25], blockchain is distinct from any other scalable database that already exists because to its two primary characteristics, which are encryption by design and distributed data management. [Citation needed] The term "cryptography by design" refers to the application of cryptography for the purpose of safeguarding user identification, in addition to ensuring the integrity of the ledger and the authenticity of data. The cryptography used in each block is distinct from one another because it is dependent on the protocol [24]. The implementation of the hashing algorithm serves as a method to verify that blocks are well-formed in order to maintain their security of being tamper-free and to become practically unbreakable [24].

Distributed Data Management

Distributed data management is the ability of the blockchain to develop a new distributed and decentralised software architecture [2, 26], [27] that enables trusted parties to engage in confidential transactions or agreements that can be made across the chain. This ability is referred to as distributed data management. As a result of its requirement that there be no involvement from a human party during a transaction, blockchain technology has found widespread use in a variety of domains, such as public services [28–30], healthcare, internet of things, as well as in the financial system and corporate governance. Since it is now open source software, more people are using the blockchain technology. This gives developers greater leeway to test and suggest new applications for new techniques while keeping costs to a minimum

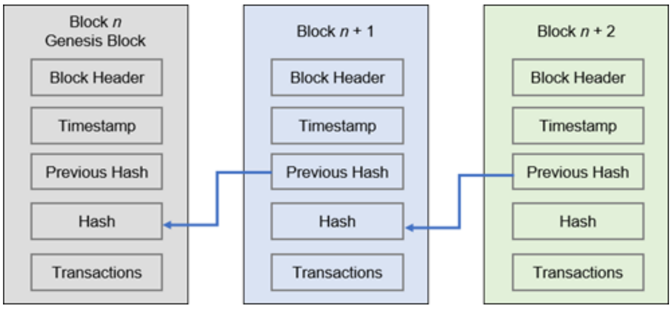

Fig. 1. Blockchain Block Architecture

Consensus mechanisms

Blockchain technology offers decentralised security designs by utilising consensus processes in the peer-to-peer network. These mechanisms help prevent data tampering and ensure that the data is sent to all of the participating nodes in the network. Transactions, requests, creation, execution, and modifications of data in the blockchain system are all subjected to the consensus mechanism for verification. There are several other methods of reaching consensus that may be used with blockchains, including Proof of Work, Proof of Stake, and Smart Contracts.

Proof of Work

Proof of Work is the consensus method that has been around the longest and is used the most frequently in blockchain technology. The method is unpredictable and requires a process of trial and error in order to solve the mathematical problem that is set up on a blockchain. However, in order to take advantage of this feature, you will need a significant amount of computational power, which will result in an increased consumption of both electricity and bandwidth throughout the mining operation.

Proof of Stake

To get around the limitations of the Proof of Work system, the Proof of Stake system was developed with the idea of stakeholders. These stakeholders have the ability to offer consensus to the block based on the amount of stake they own in the system. Those that own many coins on the blockchain will have a better chance of winning the stake. However, there is a drawback to this idea in the sense that the owner of the earliest array of coins or the one who possesses a greater number of coins will be eligible for a greater share of the awards. Consequently, the remedy to this dilemma is to demonstrate who the owner of the stake actually is.

Smart Contract

The use of smart contracts is another method that has achieved consensus. The Smart Contract reacts to the transactions that are sent from the end users and implements the coding logic for the transactions that take place with the ledgers in the blockchain application. Both parties are obligated to abide by the terms of the contract once the participants in the blockchain network have reached an agreement on the functional needs. After this, the relevant code logic is subsequently incorporated into the Smart Contract.

Type of Blockchain

There are three types of blockchains namely public, private and consortium. A public blockchain is accessible to the public whereby anyone can join as a node. Public blockchains achieve consensus without a central authority and thus, can be considered as decentralised. A copy of the ledger will be maintained by all users on each local node, and a distributed consensus mechanism will be used to achieve a decision or eventual ledger state. An example of public blockchain is the Bitcoin. Meanwhile, private blockchains are only available to a group of individuals or organisations that have agreed to share the ledger. The scale of a private blockchain is relatively small compared to apublic blockchain, but avoids data tampering by having a central administrator and proven to consume less computingpower and process faster transaction compared to publicblockchain. The combination of a public and private blockchains creates the consortium blockchain, whereby the consensus process is controlled by a nominated set of nodes. Blockchain technology would potentially replace the model of top-down hierarchical organisations with a system of distributed and bottom-up management. Instead of relying on a centralised operator or a middleman, blockchain-based networks are designed to operate in a fully distributed manner. A decentralised infrastructure is used to coordinate interactions among users who contribute to thesenetworks. Smart contract able to control the blockchaingovernance and by agreeing to the rules and principles assigned in codes, critical operations are automated without human participation.

Blockchain Application in Data Sharing

This study proposes a private blockchain technology to provide a distributed and decentralised database for the intelligence community. This technology can enhance the data-sharing process between intelligence agencies. The use of blockchain will empower the security of information shared through the implemented cryptography design. This will then produce high data integrity as each transaction includes the information of the users who requested the transaction and all related activities. These transactions can be tracked, and the transparency of information has made blockchain significantly suitable to be implemented in the intelligence community environment. As for the consensus mechanism, a smart contract is a suitable technology enabler.

Previous works

A blockchain-based four-layer paradigm for the Electronic Health Record (EHR) was proposed in. Each layer would be responsible for a different aspect of the EHR. The electronic health record (EHR) was built with several layers, the most important of which were the User Management Layer, the EHR Generation and View Layer, the EHR Storage Layer, and the EHR Access Management Layer. In order to satisfy the primary criteria of the data sharing and protection system, these layers were divided into categories according to the module and the functions it performs. The research, on the other hand, was restricted to the usage of QR pictures and One Time Password (OTP) codes as an additional layer of protection on top of the blockchain network that was being utilised. According to the findings of a previous investigation, a scheme for the sharing and protection of data ought to incorporate controls for data security and privacy, access control, data control, and unified standard. In the meantime, a different study has presented a paradigm for a private permissioned blockchain network. According to this model, only node participants who have been invited or granted permission would be able to access the network. In addition, the participants are the only ones who may carry out activities or take part in reaching a consensus across the distributed ledger network.

Other methods, such as the design of a worldwide end-to-end Internet performance measurement project (PingER's) access framework and decentralised data storage utilising Distributed Hash Tables (DHT) and permissioned blockchain, have been proposed for blockchain-based data sharing. These methods include the sharing of data between parties who have been granted permission. A framework for the exchange of data was developed in based on a blockchain-based incentive solution of on-chain and off-chain data storage, hashing, encryption, and tracking of data. This system makes use of a separate private permissioned MultiChain and Ethereum for access control. The use of hierarchical ID-based techniques of Private Key Generator (PKG) was offered as a new blockchain-based approach for the auditing of data usage. The authors also suggested implementing a secure communication system based on smart contracts that is built on the blockchain.

C. User Authentication and Identity Management

The authentication needs for the intelligence community are taken into consideration when formulating policies that outline how a user must be authorised before being permitted access to a protected data-sharing service. This research investigates the feasibility of developing more effective policies by analysing the dependability of an authentication system that is tailored to meet the requirements of the intelligence community. Password-based authentication systems are by far the most prevalent approach used to verify the identity of users. Previous researchers have developed a multi-factor authentication approach in response to the security flaws inherent in a password-based authentication system. This method aims to strengthen the system's overall security. However, this authentication method is insufficient to prevent emerging attacks such as man-in-the-middle attacks, distributed denial of service (DDoS) attacks, and replay attacks. This inadequacy is what led to the study of dynamic authentication by as well as a study on dynamic authentication policy. Both of these studies are related to the topic of dynamic authentication. A combination of two or more authentication factors that function as a multi-layered authentication strategy based on the risk that is being assessed is what is known as dynamic authentication or adaptive authentication. The user's profile and behaviour are taken into consideration during dynamic authentication. This takes into account information such as the user's identifiable devices, user location, typical login time, and user roles. A risk score is assigned to each authentication session after the user requests of each user are analysed and evaluated. Depending on the risk score, the user may be required to submit new credentials, or they may be allowed to use fewer credentials than they originally had.

D. Access Control

Access control is an important component of secure data sharing to regulate users' access based on their roles and fine-grained access control to the data, which suits the concept of the need-to-know basis in intelligence information sharing. By using the fine-grained access control, the access control manager can grant or revoke user access adaptively by updating the access policy in real-time, and each data element has its own customised access controlpolicy.

For example, each intelligence personnel have access to view available and permissible intelligence data, and data owners have control over their shared data. The access policies include:

1) Grant or revoke access of the user.
2) System administration permission.
3) User (intelligence personnel) access permission.
4) System administrator with specific permission canperform transaction.
5) Users with specific permission can perform transaction. Recently, a decentralised access control mechanism based on blockchain technology has been proposed to replaceaccess control management established on centralised architecture, whereby users' authenticity is verified by a single entity to overcome the weakness of the former mechanism. The core principle of this technology is theimplementation of a decentralised network of peers toensure that information is stored and distributed through blockchain transactions securely and transparently. Without having a central administrator, this information is directly shared across other nodes.

III. SECURE BLOCKCHAIN-BASED DATA SHARING MODEL FOR INTELLIGENCE COMMUNITY

The authentication needs for the intelligence community are taken into consideration when formulating policies that outline how a user must be authorised before being permitted access to a protected data-sharing service. This research investigates the feasibility of developing more effective policies by analysing the dependability of an authentication system that is tailored to meet the requirements of the intelligence community. Password-based authentication systems are by far the most prevalent approach used to verify the identity of users. Previous researchers have developed a multi-factor authentication approach in response to the security flaws inherent in a password-based authentication system. This method aims to strengthen the system's overall security. However, this authentication method is insufficient to prevent emerging attacks such as man-in-the-middle attacks, distributed denial of service (DDoS) attacks, and replay attacks. This inadequacy is what led to the study of dynamic authentication by as well as a study on dynamic authentication policy. Both of these studies are related to the topic of dynamic authentication. A combination of two or more authentication factors that function as a multi-layered authentication strategy based on the risk that is being assessed is what is known as dynamic authentication or adaptive authentication. The user's profile and behaviour are taken into consideration during dynamic authentication. This takes into account information such as the user's identifiable devices, user location, typical login time, and user roles. A risk score is assigned to each authentication session after the user requests of each user are analysed and evaluated. Depending on the risk score, the user may be required to submit new credentials, or they may be allowed to use fewer credentials than they originally had.

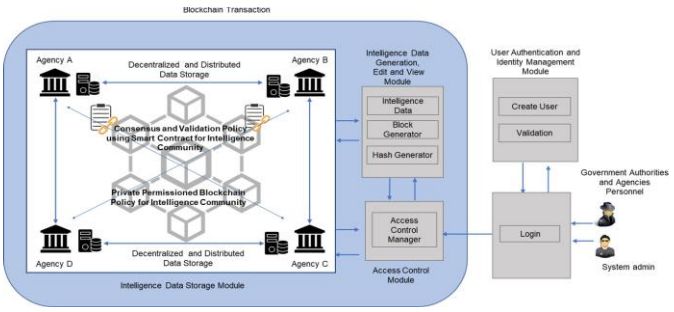
Blockchain Transaction
Agency A
Agency B
Agency C
Agency D
Decentralized and Distributed Data Storage
Decentralized and Distributed Data Storage
Consensus and Validation Policy using Smart Contract for Intelligence Community
Private Permissioned Blockchain Policy for Intelligence Community
Intelligence Data Storage Module
Intelligence Data Generation, Edit and View Module
Intelligence Data
Block Generator
Hash Generator
Access Control Manager
Access Control Module
User Authentication and Identity Management Module
Create User
Validation
Login
Government Authorities and Agencies Personnel
System admin

Fig. 2. Secured Blockchain Based Data Sharing Model for Intelligence Community

When a user has successfully logged into the data system, a blockchain transaction is generated for each and every transaction that takes place within the system. The participation of users in the network is afterwards subject to regulation by a regulator party, which also establishes an access control policy for users within the Access Control Module. The Intelligence Data Generation, Edit and View Module will have blocks constructed for it, and any data that is accessed through those blocks will be uploaded to the Decentralized and Distributed Storage Module. In the next subsections, an explanation that is further in depth for each module is provided.

User Authentication and Identity Management Moduleusing Enhanced Multi-factor Authentication Model for Intelligence Community.

Enhanced multi-factor authentication model to access critical data was proposed for this system. This model uses a combination of username and password, biometric authentication, Internet of Things (IoT) device authentication and a one-time authorisation code as shown in Fig. 3. The proposed model strengthens the authentication security of critical surveillance data access using an adaptive authentication [4].

Using a combination of both static and dynamic authentication methods, a user from the intelligence community/organisation is required to provide username and password as the first step. The next authentication is the biometric authentication, authentication using designated intelligence community devices or a one-time authorisation code that consists of six digits from a smartphone.

In steps 1 and 2 of Fig. 3, the user login process can be done on a designated workstation or mobile device, which acts as a client. Meanwhile, the authorisation process isexecuted on the authentication server owned by each intelligence agency. The characteristic of the required username and password is pre-determined to require the user to provide a secure and strong password. An effective password strength metrics is equipped within the system to estimate password's strength and security, as well as to support the password policies as proposed. Users areauthenticated by the server using the username and password provided as well as further authentication, which involves a smartcard or biometric authentication, to be decided.

In step 3 of Fig. 3, the smartcard or common access card (CAC) is specifically provided to the intelligence community. It contains a public key infrastructure (PKI)certificate and user's identity information. The smartcard reader is directly attached to the system using direct or serial port and the remote network access using the Secure Shell, as authenticated using the Kerberos authentication concept. Biometric authentication may involve the use of optical, capacitive or ultrasonic fingerprint scanner, facial recognition or retinal scanning. Pre-captured biometric is recorded and stored in the database of the authentication system. This implementation adapts the Trusted Execution Environment (TEE) and various biometric methods that can lessen the false-negative possibilities for the user to access the system.

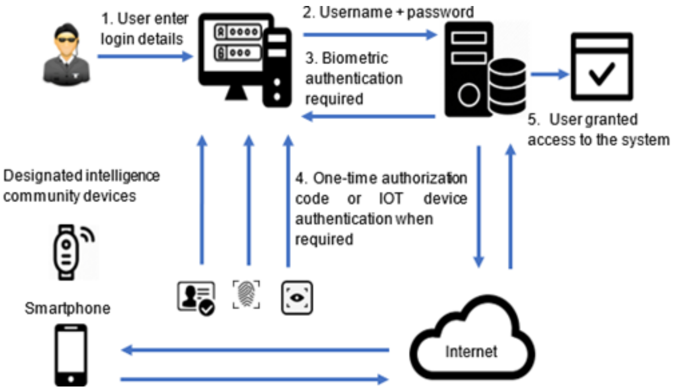
1. User enter login details
2. Username + password
3. Biometric authentication required
5. User granted access to the system
Designated intelligence community devices
4. One-time authorization code or IOT device authentication when required
Smartphone
Internet

Fig. 3. Multi-factor Authentication Model for Intelligence Community

In step 4 of Fig. 3, the user is required to provide IoT device authentication or a one-time authorisation code (OTAC) only when needed. This additional authentication step is required only for suspicious login and abnormality. A per-session short message service (SMS) representing a ciphered digital certificate will be sent to mobile phones connected to the cellular network for OTAC authentication and the user is required to provide a 6-digit code to access the system on a displayed challenge page. The server will decide whether to authenticate or deny the user based on the OTAC provided. As for the device-to-server identity authentication, a designated intelligence community IoT device is used.

To enable the authentication process using proximity-based connections such as Wi-Fi, Bluetooth or GPS, PKI digital certificates are used in the proposed IoT device. These certificates can be attached to a wearable IoT device or a compulsory traditional military identification tag. This proposed model could enhance the security of the system from possible attacks while simultaneously adapts user- friendly authentications necessary to the intelligence community. Apart from the proposed authentication mechanisms, the agencies can also implement and promote best practices and security policies to secure access to the proposed blockchain-based data-sharing system for the intelligence community.

A. Access Control Module

The access control layer is needed to control the access and sharing activities of the users in the network. In this proposed access control module, a combination of role- based access control (RBAC) and fine-grained access control was suggested. The RBAC was used to regulate user access based on their roles, while the fine-grained access control was used to manage the data, which suits the conceptof a need-to-know basis in the principle of intelligence information sharing. The users were given accesspermission based on the assigned roles. The roles of the users in this system can be as follow:

- Operator or analyst;
- Team leader;
- Director; or
- System administrator.

Due to the different geographical locations of the intelligence operators, these roles were divided into several tiers based on locations, such as tier 1 for the local operations team, tier 2 for the country operations team and tier 3 for regional or international operations teams. To further enhance the access control, a fine-grained accesscontrol method was implemented. By using the fine-grained access control, the access control manager can grant or revoke user access adaptively by updating the access policy in real-time where each data element has its own customisedaccess control policy.

For example, intelligence personnel will have access to view available intelligence data, while data owners will have control over their shared data. The access policies may include:

- Grant or revoke access of the user;
- System administration permission;
- User (intelligence personnel) access permission;
- System administrator with specific permission can perform transactions; and
- Users with specific permission can perform transactions.

This model includes a proposal for an access control module, which was accomplished by utilising the Smart Contract to construct a consensus and validation policy. A block will be generated after the user has successfully logged into the system. Decentralized access control management is implemented using this concept, which is based on the blockchain network. The utilisation of a smart contract was suggested for use in relation to file sharing under this decentralised access control management that was offered. The Smart Contract comprises of scripts that are automatically run in blockchain nodes based on user-defined rules and policies that are then translated into computer programmes. These scripts are executed in accordance with the blockchain protocol. In this particular scenario, it was presumed that a smart contract is being utilised to connect the blockchain nodes that make up the network. A participant in distributed and decentralised data storage is referred to as a "blockchain node," and this node represents the data user. The smart contract keeps a record of the data that has been shared with other users, as well as their access privileges and the actions that they have carried out.

The key component of the smart contract is known as the access control manager. The manager is responsible for determining the policies as well as controlling the access control in the data storage. Additionally, the access control manager is responsible for enforcing the policies and ensuring that the system is used for nothing but authorised business operations. The smart contract contains encoding that allows for the execution of policies whenever access is requested. The users of the access control system were separated into two groups: the owners of the intelligence data and the people who used the intelligence data.

In the context of access control management, the term "Intelligence Data Owner" refers to the individual or organisation that can legitimately claim ownership of the data because it was the source of the data in the first place. The Intelligence Data Owner is responsible for providing the data that will be distributed among the participants of the node. The term "intelligence data" can refer to a variety of resources, including "raw intelligence data" and "intelligence reports."

A individual or organisation that has permission to access and see the data is referred to as an Intelligence Data User. The Intelligence Data User is permitted to make use of the data for the purposes of conducting research and intelligence analysis. Blockchain technology makes it possible to guarantee that the data cannot be altered while also enabling the data owner to monitor who accesses the data and when.

A. Intelligence Data Generation, Edit, and View

The blockchain network's access block stores records of transactions made with data. Any requests to view or modify the data must first be validated by the other participants; this ensures the data's availability, integrity, and secrecy. This module's primary transaction consisted of a combination of the StoreData and GetAccess operations.

The steps involved in the StoreData transaction are shownin Fig. 4. The detailed steps for StoreData are as follow:

1) The Intelligence Data Owner stores the data and defines the access control policy in the Intelligence DataContract. The next process is to deploy the Smart Contract in the blockchain network.
2) The Intelligence Data Owner stores data to create

StoreData transaction.

3) The Intelligence Data Contract nodes broadcast the transaction in the blockchain network.
4) Blockchain network validates the transaction and a new block will be created or added to the verified transaction.

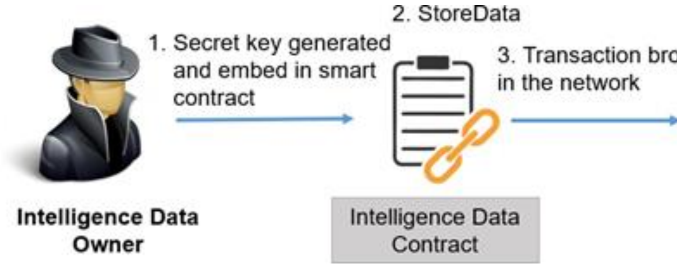
2. StoreData
1. Secret key generated and embed in smart contract
3. Transaction brc in the network
Intelligence Data Owner
Intelligence Data Contract

Fig. 4. Access Control Transaction: Owner stores data.

5) Data are successfully stored in the system.

Access Block for the users asking for access to the data include GetAccess transaction as shown in Fig. 5. Detailed steps for a user asking access to data are as follow:

1) The Intelligence Data User sends a request to access the data.
2) GetAccess transaction is created.
3) The Intelligence Data Contract nodes broadcast thetransaction in the blockchain network.
4) Blockchain network validates the transaction and a newblock will be added to verify the transaction.

Data are successfully accessed.

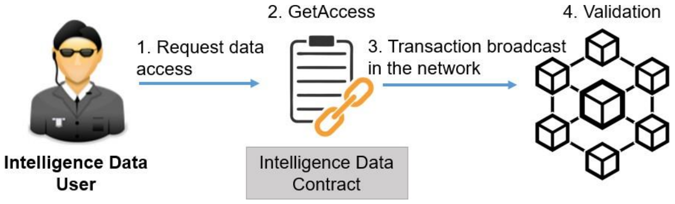

Fig. 5. Access Control Transaction: User asking for access to data.

The verified transaction of StoreData and GetAccess are arrayed and compiled into blocks. In this proposed model, each block consisted of a block header and details that include index, timestamp and hashes of Merkle Root for previous and current transaction data structure. The data structure contained User ID, verified transaction ID, content,log details, transaction type and request time. This block characteristic and details made it immutable and tamper- proof. The intelligence data block is shown in Fig. 6.

Detailed explanations for each submodule in the

Intelligence Data Generation, Edit and View module, asshown previously in Fig. 2, are as follow:

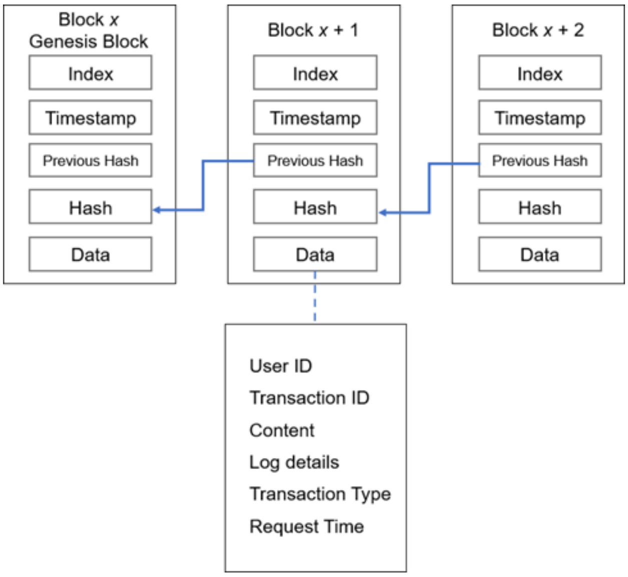

Fig. 6. Block design.

- Login

The login submodule ensures a secure login to the system. The login step is similar to the validation submodule authentication steps in the User Authentication and Identity Management Module.

- Intelligence Data

Intelligence data refers to a record of intelligence information or any related data that is useful for sharing. This data is recorded and stored by the intelligence community based on intelligence gathering using designated techniques and sources. Data can also be generated through sensors in intelligence collection methods. The stored data can be classified into events or cases according to predefined criteria and classifications.

- Hash Generator

Hash Generator generates the key for each block session in data generation. The key is generated for successful transactions and records on the blockchain block in the network.

- Block Generator

A block is generated and encodes transactions of the data generation. The accepted block becomes a part of the blockchain network, whereas a cryptographic hash will be linked to the newly generated block.

B. Intelligence Data Storage Module

The Intelligence Data Storage Layer employs the use of a distributed database in order to store intelligence data. This layer is responsible for storing both the metadata file and the data file storage. It is possible to protect both the data and the system by storing the data in a decentralised and distributed database, which offers a high level of confidentiality and is also readily available. The data that has been stored will go through a process called sharding, in which the data will be duplicated and then transformed into shards (which is a method of breaking data into smaller bits). Because the data are stored at the node, duplicated there, and then distributed across the network, a single point that is the target of an attack or that malfunctions will not have a significant impact on the system as a whole. The shard will be reassembled using an encryption key and the blockchain distributed hash table whenever an authorised user conducts a transaction to access the data (DHT). The DHT will store the data's metadata as well as a reference to it, which can then be utilised to retrieve the data from its storage location.

This study recommended the implementation of blockchain DHT coupled with an intelligence community private cloud storage, on the presumption that keeping a large amount of data in the blockchain network will result in blockchain bloating, which demands a larger block. This idea makes use of a data storage solution that is independent of the chain itself. It has the ability to overcome the problem of insufficient data storage space while also significantly improving data privacy and security.

Data from various sources and sensors, such as human intelligence (HUMINT), signals intelligence (SIGINT), technical intelligence (TECHINT), cyber intelligence (CYBINT), open-source intelligence (OSINT), geospatial intelligence (GEOINT), medical intelligence (MEDINT), and other related intelligence information, are all examples of the types of data that can be stored as intelligence. Depending on the level of access that has been provided, intelligence employees from both within an organisation and from other organisations can contribute new data, examine existing data, update existing data, or remove existing data.

IV. CONCLUSION AND FUTURE WORKS

In this piece of research, the authors recommend utilising blockchain technology to create a safe data-sharing platform for the intelligence community. This model comprised a number of modules that were organised into categories according to the needs of the intelligence community. To increase the safety of the user authentication and identity management of the data-sharing system while at the same time satisfying the requirements of the stakeholders, a secure method for User Authentication and Identity Management Module has been developed. This method makes use of enhanced multi-factor authentication. The Access Control Module was developed on the principle of decentralised access control management. This was accomplished by utilising smart contracts to implement a consensus and validation policy. At the same time, the module made use of a combination of role-based access control (RBAC) and fine-grained access control policies. This module has the potential to significantly improve the system's security and block any unauthorised users from accessing the system.

The procedure required in storing and accessing the data via a smart contract has also been detailed in depth for the Intelligence Data Generation, Edit and View Module. This module is responsible for generating, editing, and viewing intelligence data. Distributed hash tables and off-chain data storage through the use of private clouds are two solutions that have been offered for making data storage more effective and dependable.

As a result of this, the researchers behind this study intend to broaden their data collection efforts so that they encompass a greater number of intelligence organisations in the future work that they do. The data collection for the adoption of the system should include an acceptance study at several phases, such as after the initial implementation of the system, after one month of implementation, and after three months of implementation as suggested. The conduct of such a study making use of an integration of concepts derived from TAM 3 and TRI 2.0 model have to be taken into consideration for subsequent efforts.

V. 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] 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.

[12] 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.

[13] C. 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.

[14] 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.

[15] O. Alphand et al., “IoTChain : A Blockchain Security Architecture for the Internet of Things,” 2018 IEEE Wirel. Commun. Netw. Conf., pp. 1–6, 2018.

[16] 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.

[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.

[21] R. Akter, S. Bhardwaj, J. M. Lee, and D.-S. Kim, “Highly Secured C3I Communication Network Based on Blockchain Technology for Military System,” 2019 Int. Conf. Inf. Commun. Technol. Converg., pp. 780–783, 2020, doi: 10.1109/ictc46691.2019.8939813.

[22] W. Zhang et al., “Blockchain-Based Distributed Compliance in Multinational Corporations’ Cross-Border Intercompany Transactions,” in Future of Information and Communication Conference (FICC), 2019, no. July, pp. 304–320, doi: 10.1007/978-3-030-03405-4_20.

[23] C. Ngubo, M. Dohler, and P. Mcburney, “Blockchain, IoT and sidechains,” in Lecture Notes in Engineering and Computer Science, Proceedings of the International MultiConference of Engineers and Computer Scientists 2019 (IMECS 2019), 2019, vol. 2239, pp. 136–140.

[24] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, “Blockchain

– The Gateway to Trust-free Cyrptographic Transactions,” Twenty-Fourth Eur. Conf. Inf. Syst. (ECIS), İstanbul,Turkey, vol. 6, no. May, pp. 4013–4027, 2016.

[25] J. P. Es-Samaali, H., Outchakoucht, A., & Leroy, “A Blockchain- based Access Control for Big Data,” J. Comput. Networks Commun. Secur. Internet Things J., vol. 5, no. 7, p. 137, 2017, doi: 10.1109/JIOT.2018.2812239.

Cite this Article

Sejal S. Dhamgaye, Supriya Sawwashere, Dr. Shrikant V. Sonekar, Mirza Moiz Baig, "Block Chain Based Fine Grained Data Sharing For Multiple Group", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 3, pp. 520-533, May-June 2022.

Journal URL : https://ijsrset.com/IJSRSET2293182