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

Noor Afiza Mat Razali, *Member, IAENG*, Wan Nurhidayat Wan Muhamad, *Member, IAENG*,
Khairul Khalil Ishak, Nurjannatul Jannah Aqilah M. Saad, Muslihah Wook, and Suzaimah Ramli

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 unauthorised 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 dimension.**

Index Terms—**blockchain, secure data sharing, Technology Acceptance Model, Technology Readiness Index**

I. Introduction

Digital advancement plays a crucial role in the dissemination of information in a community. The intelligence community had shifted its technique of gathering data from the traditional Human Intelligence (HUMINT) to a more sophisticated and advanced method of Signal Intelligence (SIGINT) and open source intelligence (OSINT). Intelligence communities are required to gather accurate and precise data to be analysed for deciding and planning the country's security.

Thus, researchers have suggested using blockchain as an additional technology for increasing data security since several studies have shown its significant success [1], [2]. However, a comprehensive study on the implementation of blockchain within the intelligence community needs to be augmented to ensure that all aspects related to the technologies, processes, rules, and policies are thoroughly considered prior to the implementation.

This paper discusses the design of secure data sharing by including the implementation of blockchain technology as part of the model. This paper proposed a conceptual secure blockchain-based data-sharing model for the intelligence community based on the requirements, rules and regulations. Based on the proposed model, the adoption measurement was done using the technology readiness and acceptance model (TRAM). The dimension was proposed based on the selected variables. To the best of the authors' knowledge, this study is the first comprehensive study on blockchain-based data-sharing model for the intelligence community and the first to study blockchain-based data sharing acceptance using TRAM theory.

II. Intelligence Community and Blockchain Technology

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 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].

For example, in the United States, the intelligence community consists of two independent agencies known as the Office of the Director of National Intelligence and the Central Intelligence Agency (CIA). They also have eight Department of Defence elements including the National Security Agency (NSA), the Defence Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), intelligence elements within their military services of the Army, Navy, Marine Corps and Air Force, as well as seven other department and agency elements [5], [6]. In Malaysia, the

Manuscript received May 22, 2020; revised September 24th, 2020.

Noor Afiza Mat Razali is a Senior Lecturer at the National Defence University of Malaysia, Kuala Lumpur, Malaysia (e-mail: noorafiza@upnm.edu.my).

Wan Nurhidayat Wan Muhamad is a master's degree candidate at the National Defence University of Malaysia, currently working at the Ministry of Defence, Malaysia (e-mail: hidayat.muhamad@mod.gov.my).

Khairul Khalil Ishak is a Research Fellow at the Center of Cyber Security and Big Data, Management and Science University, Shah Alam, Selangor, Malaysia (e-mail: khairul_khalil@msu.edu.my)

Nurjannatul Jannah Aqilah M. Saad is a Research Assistant at the National Defence University of Malaysia, Kuala Lumpur, Malaysia (e-mail: jannatulaqilah@gmail.com).

Muslihah Wook is a Senior Lecturer at the National Defence University of Malaysia, Kuala Lumpur, Malaysia (e-mail: muslihah@upnm.edu.my).

Suzaimah Ramli is a Senior Lecturer at the National Defence University of Malaysia, Kuala Lumpur, Malaysia (e-mail: suzaimah@upnm.edu.my).

intelligence community is part of the National Intelligence Committee, which includes internal security intelligence and defence intelligence such as the Special Branch (SB) of the Royal Malaysian Police and the Defence Intelligence Staff Division (DISD) [4].

Information or data gathered by the intelligence community vary and could originate from numerous devices and sensors. The collected data are important to support tactical operational data analysis for government authorities, agencies and war fighters [7], [8]. The intelligence community needs an efficient information sharing and data distribution system [5, p. 22] as it is difficult to properly distribute accurate and precise data [6]. Leaked or breached intelligence data could affect a country's sovereignty, which could also significantly affect civilian communities in terms of politics, cultural, economy or even lives [4], [9].

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.

Researchers are proposing that data should be managed by a decentralised, flexible and scalable infrastructure to overcome this issue. This is where blockchain integration in data management comes into the picture. Prior studies have suggested integrating blockchain in handling data, especially risky and confidential data, due to its ability to protect data using the decentralised approach [1], [13], [15]. Hence, a new model is needed to solve the security vulnerabilities of current implementation.

Intelligence data include raw intelligence data and intelligence reports [16]. Raw intelligence data may vary from target's communication traffic and voice, videos, radar transmission details, data from satellite communication systems, imagery data, open source data, and social media-related data. Meanwhile, intelligence reports may include routine and timely reports as well as case-based intelligence reports. New technologies are required for the entire intelligence community data management in an environment in which more safety standards are necessary as the size of data usage and integration proliferates. Blockchain technology has offered a comprehensive solution to a variety of critical security issues [17]. To address the flaws related to providing secure data sharing, security components such as blockchain technology for decentralised data storage and management, user authentication as well as access control need to be studied.

Blockchains can be potentially applied in various intelligence operations to provide a distributed and decentralised database for military intelligence [18], secure communication and data storage system [19], enhance data integrity in supply chain management and ensure transparency in equipment management [20] as well as provide secure Command, Control, Communication, and Intelligent (C3I) systems [21].

B. *Blockchain Technology*

Blockchain technology is a new form of a database. Contradict to SQL or NoSQL databases, blockchain can be shared directly by a community of trusted and untrusted parties [17]. A blockchain is a form of a distributed database which preserves a list of structured records called blocks, that is increasing irreversibly [17]. Each block includes a timestamp and linked to the previous block [22] [23]. The linkage is based on the hash value of the previous block or the parent block. As illustrated in Fig. 1, a block can transverse through the whole blockchain and find each transaction made through its parent block. The first block is known as the genesis and has no parent [24]. According to [25], blockchain is different from any existing scalable database due to its two main features: i) cryptography by design; and ii) distributed data management. Cryptography by design refers to cryptography implementation for preserving user identity, as well as ensuring the ledger's integrity and authenticity of data. The cryptography of each block differs depending on the protocol [24]. The hashing algorithm is implemented as a way to ensure that blocks are well-formed to preserve their security of being tamper-free and become virtually unbreakable [24].

Distributed Data Management

Distributed data management refers to the ability of the blockchain to develop a new distributed and decentralised

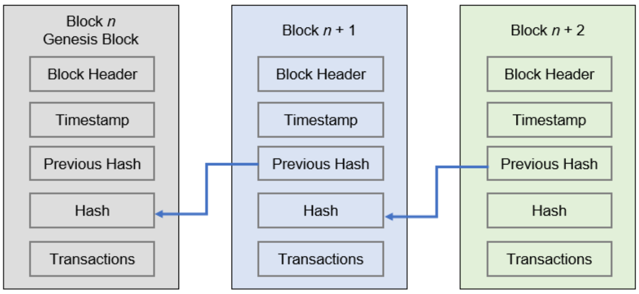

Fig. 1. Blockchain Block Architecture

software architecture where confidential transactions or agreements can be made across the chain with trusted parties [2], [26], [27]. Blockchain's criteria of having no human intervention during a transaction has made it widely applied in various fields including public services [28]–[30], healthcare [31]–[33], IoT [34], [35] and in the financial system and corporate governance [36]. Usage of the blockchain technology is increasing since it has become an open source software, which allows more flexibility for developers to test and propose new applications for new techniques at low costs [37].

Consensus mechanisms

Blockchain provides decentralised security architectures using consensus mechanisms in the peer-to-peer network, which avoid data tampering and share the data to all participating nodes in the network. The consensus mechanism validates transactions, requests, creation, execution and modification of the data in the blockchain system. Various types of consensus are available in blockchains including Proof of Work, Proof of Stake and Smart Contract.

Proof of Work

Proof of Work is the oldest and most common consensus in blockchain technology. It is a random process that requires trial and error in solving the mathematical puzzle set in a blockchain. However, this characteristic requires a lot of computing powers, which consume high amount of electricity and bandwidth during the mining process [38].

Proof of Stake

To overcome the limitation of the Proof of Work, Proof of Stake was introduced with the concept of stakeholders that have the power to give consensus to the block according to the stake they own. The stake can be obtained by owning several coins in the blockchain. However, this concept also faces an issue because the owner of the earliest array of coins or the one who owns more coins will get more rewards. Thus, the solution to this problem is by proving the ownership of the stake [39].

Smart Contract

Another consensus solution is the Smart Contract. The Smart Contract respond to the transactions sent from end-users and implements the code logic for transactions with ledgers in the blockchain application. Once the participants of the blockchain network have accepted on functional requirements, this code logic is then integrated into the Smart Contract, and both parties are bound by the contract [40].

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 a public blockchain, but avoids data tampering by having a central administrator and proven to consume less computing power and process faster transaction compared to public blockchain [41]. 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 these networks. Smart contract able to control the blockchain governance and by agreeing to the rules and principles assigned in codes, critical operations are automated without human participation [42].

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

Reference in [43] proposed a four-layer model for the Electronic Health Record (EHR) based on blockchain network. The layers used in the EHR were the User Management Layer, the EHR Generation and View Layer, the EHR Storage Layer, as well as the EHR Access Management Layer. These layers were classified based on the module and its functions to meet the essential requirement of data sharing and protection scheme. However, the study limited to use of QR images and One Time Password (OTP) code as additional layer for security on top of the blockchain network used. A previous study has suggested that data sharing and protection scheme should include security and privacy control, access control, data control and unified standard [44]. Meanwhile, another study proposed a private permissioned blockchain network model, where only node participants will have access to the network via an invitation or permission. Additionally, only the participants can execute operations or participate in consensus over the distributed ledger network [45].

Other approaches have been proposed for blockchain-based data sharing including the design of worldwide end-to-end Internet performance measurement project (PingER's) access framework and decentralized data storage using Distributed Hash Tables (DHT) and permissioned blockchain [46]. Reference in [47] proposed a data sharing framework based on blockchain-based incentive solution of on-chain and off-chain data storage, hashing, encryption, and tracking of data, which utilises a separate private permissioned MultiChain and access control using Ethereum. [48] proposed the use of hierarchical ID-based mechanisms of Private Key Generator (PKG) for a new blockchain-based solution in data usage auditing. Authors also proposed the implementation of blockchain secure communication based on Smart Contract [48].

C. *User Authentication and Identity Management*

Policies dictate how a user must be authenticated before access is granted to a protected data-sharing service based on authentication requirements for the intelligence community. This paper explores possible improvements of policies by determining the reliability of an authentication protocol that would suit the need of intelligence community. The most common method to authenticate users is by password-based authentication systems [49]. Due to security weaknesses in a password-based authentication system, previous researchers have introduced multi-factor authentication method to enhance the security. However, this authentication technique is insufficient to prevent emerging attacks including man-in-the-middle, distributed denial of service (DDos) and replay attacks [13], [14] [50], which led to the study of dynamic authentication by [49] as well as a study on dynamic authentication policy by [51] and [52]. Dynamic authentication or adaptive authentication is a combination of two or more authentication factors that act as multi-layered authentication approach based on the assessed risk [53]. Dynamic authentication is based on the user's profile and behaviour that contains details such as the identified devices, user location, normal login time and user's roles. User requests are evaluated, and a risk score is given for each authentication session [53]. The user might be requested to provide additional credentials or allowed to use fewer credentials depending on the risk score [53].

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 control policy.

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 can perform transaction.
5) Users with specific permission can perform transaction.

Recently, a decentralised access control mechanism based on blockchain technology has been proposed to replace access 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 the implementation of a decentralised network of peers to ensure 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

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 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-

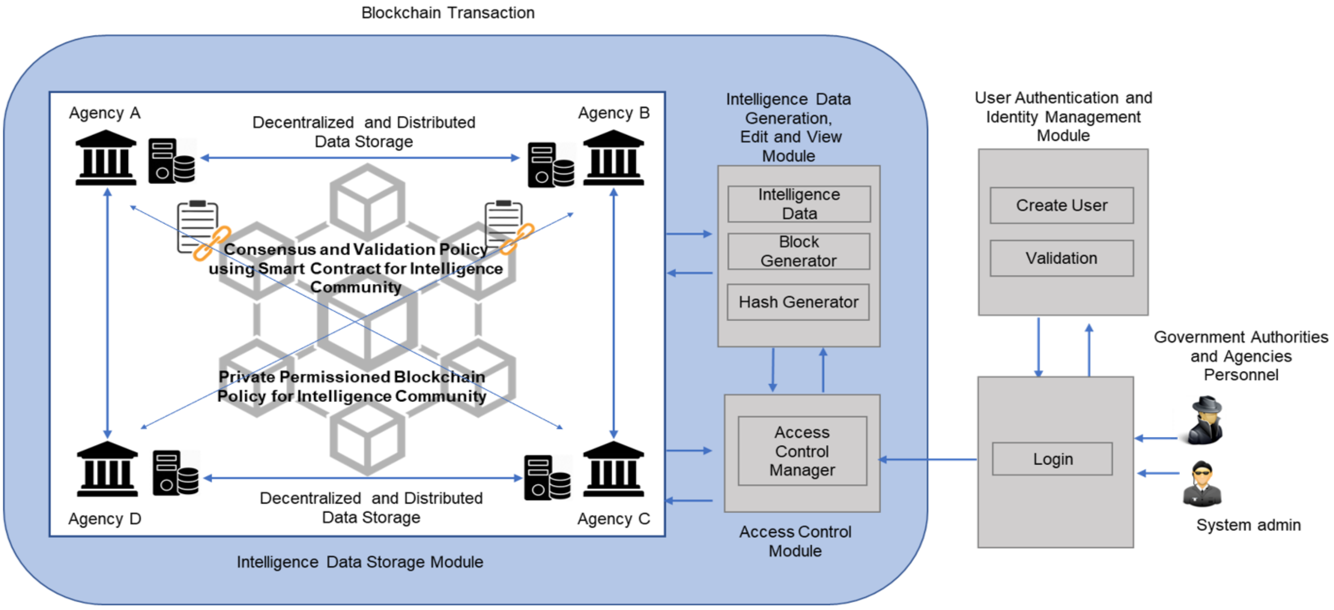
Blockchain Transaction
Agency A
Decentralized and Distributed Data Storage
Agency B
Consensus and Validation Policy using Smart Contract for Intelligence Community
Private Permissioned Blockchain Policy for Intelligence Community
Agency D
Decentralized and Distributed Data Storage
Agency C
Intelligence 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

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.

A. User Authentication and Identity Management Module using 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 is executed 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 by [54]. Users are authenticated 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.

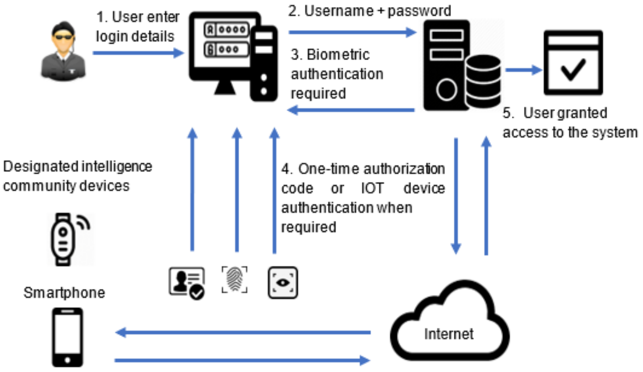
1. User enter login details
2. Username + password
3. Biometric authentication required
5. User granted access to the system
Designated intelligence community devices
4. One-time authorization code or IOT device authentication when required
Smartphone
Internet

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.

B. *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 concept of a need-to-know basis in the principle of intelligence information sharing. The users were given access permission 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 access control 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 customised access 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.

The access control module was proposed in this model by implementing consensus and validation policy using the Smart Contract. After the user has successfully logged into the system, a block will be generated. This model applies decentralised access control management based on the blockchain network. In this proposed decentralised access control management, the use of a smart contract was proposed in terms of file sharing. The Smart Contract consists of scripts that are automatically executed in blockchain nodes based on user-defined rules and policies that are translated into computer programs. In this case, it was assumed that the blockchain nodes are connected in the network using a smart contract. A blockchain node represents the data user who participates in distributed and decentralises data storage. The smart contract traces the data shared with other users, access rights and the operations executed by these users.

The access control manager is the main part of the smart contract. The manager controls the access control in the data storage and determines the policies. The access control manager also enforces the policies and ensures that only legitimate transactions are conducted in the system. Policies are encoded in the smart contract and executed upon request of access. The access control users were divided into two groups, namely the Intelligence Data Owner and the Intelligence Data User.

The Intelligence Data Owner in access control management refers to a person or organisation that owns the data in terms of generating the data. The Intelligence Data Owner contributes the data to be shared among node participants. This intelligence data may include different resources such as raw intelligence data and intelligence reports.

The Intelligence Data User is a person or organisation that can access and view the data. The Intelligence Data User can use the data for intelligence analysis and research purposes. Blockchain can ensure the data is immutable while the data owner can trace the data accessed by users.

C. *Intelligence Data Generation, Edit, and View*

Access block in the blockchain network records data transactions. Any data access and modification requests on the data must be verified by other participants, hence ensuring its confidentiality, integrity and availability. The main transaction in this module contained StoreData and GetAccess transactions.

The steps involved in the StoreData transaction are shown in 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 Data Contract. 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.

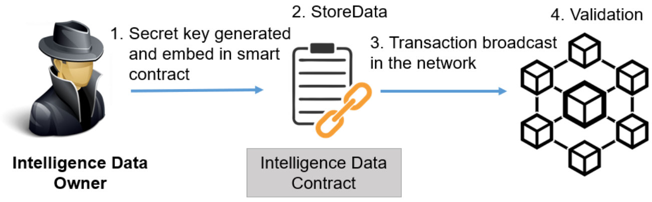
2. StoreData
4. Validation
1. Secret key generated and embed in smart contract
3. Transaction broadcast in the network
Intelligence Data Owner
Intelligence Data Contract

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 the transaction in the blockchain network.
4) Blockchain network validates the transaction and a new block will be added to verify the transaction.
5) Data are successfully accessed.

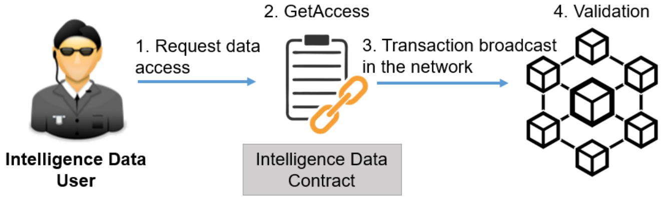

Fig. 5. Access Control Transaction: User asking for access to data.

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, as shown previously in Fig. 2, are as follow:

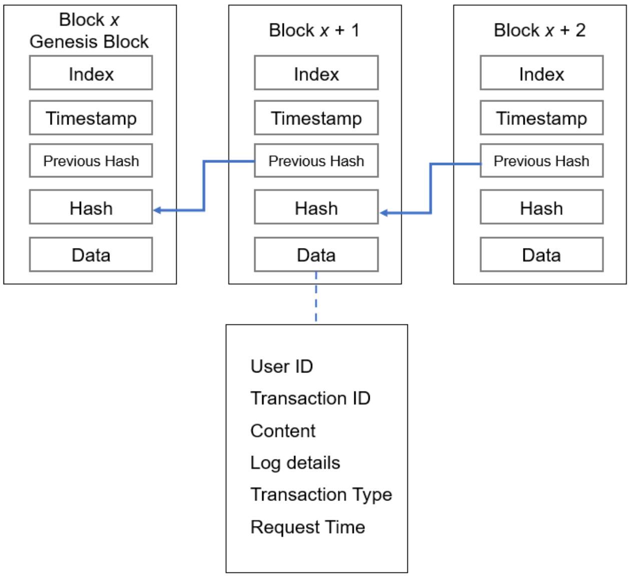

Fig. 6. Block design.

- 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.

D. Intelligence Data Storage Module

The Intelligence Data Storage Layer stores intelligence data using a distributed database. The metadata file and data file storage are stored in this layer. Storing data in the decentralised and distributed database can ensure the security of the data and system due to its high confidentiality and availability. The stored data will undergo the sharding process where data are turned into shards (a process of dividing data into smaller pieces) and duplicated. Attacks or malfunction of a single point will not seriously affect the whole system since the data are stored and duplicated in the node and distributed across the network. When an authorised user performs a transaction to access the data, the shard will be reconstructed using an encryption key and the blockchain distributed hash table (DHT). The DHT will store the metadata and reference of the data, which can be used to retrieve data from data storage.

Assuming that storing a large amount of data in the blockchain network will result in blockchain bloating that requires a larger block, this study proposed the implementation of blockchain DHT together with an intelligence community private cloud storage. This concept leverages the use of an off-chain data storage solution. It can potentially solve data storage capacity issue and effectively improve data privacy and security.

Examples of stored intelligence data include 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. Intelligence personnel within and from other organisations can add, view, edit and delete the stored data based on access granted.

IV. Understanding Blockchain-Based Data Sharing Adoption Among Intelligence Communities

In the context of this research, to understand the adoption of the proposed blockchain-based data-sharing model among the intelligence communities, an adoption study was conducted. According to [55], blockchain implementation is still in its early stage, while [56] suggested that there is a barrier in blockchain technology adoption in terms of behavioural, organisational and technological aspects. This barrier could lead to failure in technology implementation and subsequently to large financial losses [57]. Several studies have focused on adoption of certain blockchain applications in few communities and environment settings such as [56], [58], [59] and [60]. However, there is a gap in the literature for adoption studies on blockchain-based data sharing. Hence, this study was conducted in an attempt to fill this gap.

A. *Theoretical Background*

Technology Acceptance Model

The Technology Acceptance Model (TAM) was introduced by [61] to forecast technology adoption and acceptance using perceived usefulness (PU) and perceived ease of use (PEoU) as determinants. PU can be defined as the degree of a person's belief that using technology will increase their job performance. Meanwhile, PEoU is the degree of a person's belief that using a system is easy and requires minimum effort.

The original TAM has been widely recognised and revised according to the current requirements. Its revised, newer versions are known as TAM 2 and TAM 3. While TAM is mainly used to study how perceived determinants can influence usage and adoption of new technology, technology readiness index (TRI) focuses more on individual constructs since individual readiness can ensure the success or failure of technology adoption in an organisation.

Technology Readiness Index

The Technology Readiness Index (TRI) model was developed by [62] to determine the extent to which an individual is ready to adopt technology using four dimensions. Technology readiness (TR) is defined as a person's readiness to adopt new technology.

In reference [63], authors divided technology adoption into four dimensions, namely innovativeness, optimism, discomfort and insecurity. Innovativeness and optimism are classified as motivators that can positively influence technology readiness, whereas discomfort and insecurity are classified as inhibitors that can defer technology readiness [63]. The definitions of the four dimensions in TRI are as follow:

- *Optimism* - Optimistic views of a user that technology offers greater control, flexibility and efficiency in his/her daily life.
- *Innovativeness* - The trait of innovation to be the first and leader in using a new technology.
- *Discomfort* – The feeling of lack of control of technology and having a sense of being overwhelmed by it.
- *Insecurity* – Feeling sceptical or distrusting towards technology due to perceived harmful reasons and the technology's inability to work properly.

The original TRI model consisted of a 36-item scale and was specifically designed to understand employees' readiness to embrace state-of-the-art technologies to help them become confident and comfortable with the new technology and to avoid a decline in morale and productivity [63]. Thus, it is important to study the intelligence community's readiness towards technology adoption. Such study should be conducted before the implementation and further arrangement of such system are in place for making the right choice in design, implementation and management of the new technology.

Technology Readiness and Acceptance Model (TRAM)

TRAM was first introduced by [64] after reviewing TAM and construct of technology readiness. The initial study was focused on consumers' intention to use online services. In TRAM, TRI's four dimensions are associated with the two dimensions in TAM, namely perceived usefulness and perceived ease of use as mediators to the intention to use. Their research suggested that the intention to use is influenced by a user's feeling and prior experience [65].

Several studies have used TRAM to study the adoption of new technologies [66]–[69]. However, no attempt has been made to use TRAM in studying the adoption of data-sharing systems even though these systems are widely implemented by individuals as well as private and government organisations.

B. *Hypotheses Development*

This study used TRAM to predict the behavioural intention to use blockchain-based data sharing within the intelligence community. As per Fig. 7, several hypotheses were developed based on optimism and innovativeness, as well as their positive effect on the target users' perceived usefulness and perceived ease of use of this new technology. Insecurity and discomfort were expected to negatively affect the users' perceived usefulness and perceived ease of use of this new technology. It was assumed that perceived usefulness and perceived ease of use can mediate the intention to use the blockchain-based data-sharing system.

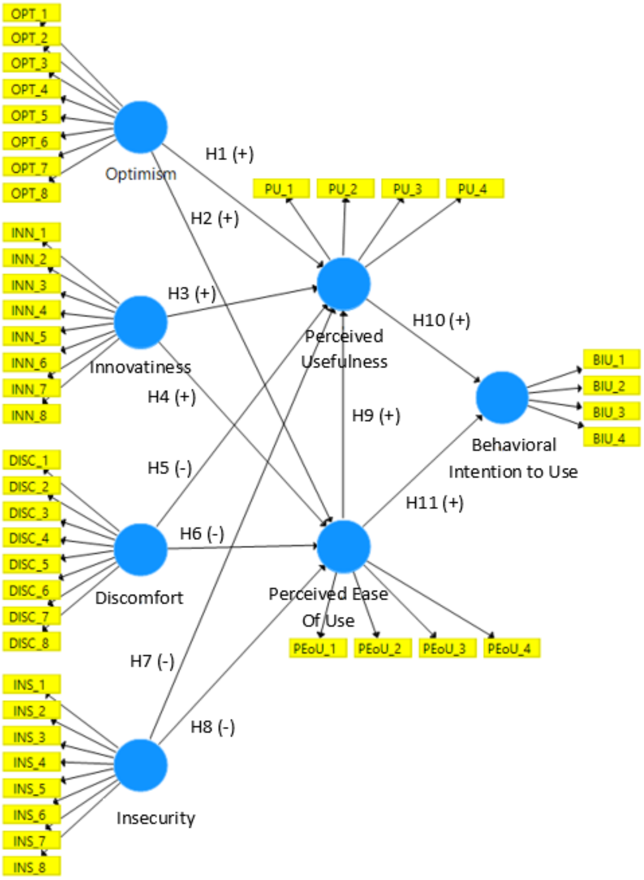

Fig. 7. Proposed Research Model.

The following hypotheses were tested in this study:

H1: Optimism positively affects the perceived usefulness of the blockchain-based data-sharing system.
H2: Optimism positively affects the perceived ease of use of the blockchain-based data-sharing system.
H3: Innovativeness positively affects the perceived usefulness of the blockchain-based data-sharing system.
H4: Innovativeness positively affects the perceived ease of use of the blockchain-based data-sharing system.
H5: Insecurity negatively affects the perceived usefulness of the blockchain-based data-sharing system.
H6: Insecurity negatively affects the perceived ease of use of the blockchain-based data-sharing system.
H7: Discomfort negatively affects the perceived usefulness of the blockchain-based data-sharing system.
H8: Discomfort negatively affects the perceived ease of use of the blockchain-based data-sharing system.
H9: Perceived ease of use positively affects the perceived usefulness of the blockchain-based data-sharing system.
H10: Perceived usefulness positively affects the behavioural intention to use the blockchain-based data-sharing system.
H11: Perceived ease of use positively affects the behavioural intention to use the blockchain-based data-sharing system.

C. Data Collection

Measurement Scales and Data Collection

The model and questionnaire in this study were adapted from previous studies by [63] and [64]. The questionnaire used 44 items as indicators in this study, which were divided into two sections namely Demographic Background as well as Technology Readiness and Acceptance Model. Demographic background included the respondent's information such as gender, age, education level, work experiences and knowledge in authentication systems and blockchain applications. This questionnaire was measured using a 7-point Likert scale, whereby 1 = Strongly Disagree and 7 = Strongly Agree. To validate the accuracy and suitability of these items, the questionnaire was validated by two experts in academics and two experts in the blockchain industry. Further validation via a pilot test was conducted with 25 respondents.

Sampling method

Data were collected from intelligence community personnel from various intelligence organisations in Malaysia. Due to their irregular working hours and difficulty in determining available intelligence personnel, convenience sampling method was used for data sampling as proposed by [70] and [71] and the survey was conducted in a controlled environment. The chosen respondents in this survey must have experience in using data-sharing systems and have been introduced to the proposed blockchain-based data-sharing system. Their knowledge on authentication system and blockchain technology was surveyed beforehand to gauge their knowledge on both matters. A total of 120 surveys were distributed and 107 survey questionnaires were returned with sufficient answers for further analysis. 100 samples were used in this study after data cleaning by removing samples with straight lining answers and negatively phrased questions were reversed code for the data analysis.

According to [72], PLS-SEM analysis is efficient for data analysis of small sample sizes. Samples for measuring a model must be 10 times higher than the largest formative indicator's number used to measure a single construct [72]. In the proposed model, perceived usefulness has the largest (five) formative indicators; hence, the minimum number of samples needed was 50.

D. Data Analysis and Results

Descriptive Statistics

A total of 100 sample data were used in this study consisting 72% males and 28% females. The majority of the respondents were 21–30 years old (76%), followed by 31–40 years old (19%), 41–50 years old (3%) and 51–60 years old (2%). Most respondents received high school education (45%) and a bachelor's degree level of education (40%), followed by diploma (10%), a master's degree (4%) and Doctor of Philosophy (1%).

In terms of working experience, 38% of respondents had 6–10 years working experience in the intelligence community, 21% of respondents had less than 3 years working experience, 26% had 3 to 5 years working experience, while 7% of the respondents possessed more than 16 years of working in the intelligence community. The number of respondents who possess knowledge on authentication systems was higher (76%), while the percentage of respondents with knowledge on blockchain applications prior to this study was lower at 21%.

Validity and Reliability Testing

Partial least squares (PLS) analysis using Smart PLS 3 (version 3.3.2) was used in this study. Referring to previous literature, this model was designed and evaluated using the reflective measurement model. According to [72], a measurement model is evaluated by assessing its internal consistency through Cronbach's alpha and composite reliability as well as convergent validity, which include indicator reliability, average variance extracted (AVE) and discriminant validity. Acceptable reliability and normality testing are required to ensure the consistency of a measuring instrument. Before significant relationships in the structural model are evaluated, the validity and reliability values must meet the satisfactory level required [73].

The Cronbach's alpha value for all constructs must be greater than 0.7 to assess the measurement model [72],[73]. In this study, all Cronbach's alpha values were higher than the acceptable level of 0.7, where insecurity and discomfort recorded the highest value (0.948) and the lowest value was displayed for the Behavioural Intention to Use (BIU) at 0.833. [72] stated that in an exploratory research, a value between 0.60 and 0.70 is acceptable for indicator reliability. Meanwhile, a value ranging from 0.70 to 0.95 is considered satisfactory to good reliability levels. In this study, one indicator (INN8) with values of lower than 0.6 was eliminated from the original 44 indicators in this study.

The composite reliability was then evaluated to determine internal consistency after unacceptable indicators have been removed from the model. The minimum level for composite reliability must be higher than 0.70 [72]. In this study, the results for composite reliability were ranged between 0.887 to 0.949, which were higher than the recommended acceptable value of 0.70, thus demonstrating the reliability of this model.

To indicate convergent validity, the recommended average variance extracted (AVE) value must be higher than 0.5 [72], [74]. The results showed that all AVE values were acceptable. Innovativeness recorded the lowest value at 0.531, while Perceived Usefulness showed the highest AVE value of 0.722. The final recommended step to test the reliability and validity of the model was the discriminant validity assessment [73]. Discriminant validity is defined as the degree of which a variable or construct is distinct from others [72], [73]. The overall result of reliability and normality test is shown in Table 1.

In the PLS-SEM analysis, discriminant validity assessment included evaluation of the heterotrait-monotrait ratio (HTMT) of the correlations. Acceptable HTMT value for each variable must be less than the threshold value of 0.85 if the path model is conceptually more distinct or must be less than 0.90 if the path model includes constructs that are conceptually similar [75]. The HTMT value in this study was lower than the threshold of 0.85, signifying discriminant validity.

TABLE 1
RELIABILITY AND NORMALITY TEST

Variable	Cronbach's Alpha	Composite Reliability	AVE
Optimism (OPT)	0.896	0.917	0.584
Innovativeness (INN)	0.863	0.887	0.531
Insecurity (INS)	0.948	0.927	0.618
Discomfort (DISC)	0.948	0.949	0.699
Perceived Usefulness (PU)	0.872	0.912	0.722
Perceived Ease of Use (PEoU)	0.836	0.891	0.671
Behavioural Intention to Use (BIU)	0.833	0.889	0.667

Structural Model Analysis

To assess the results of the structural model, relationships among constructs and predictive capabilities of the model were evaluated [72]. The evaluation was done using path coefficient analysis, while predictive capabilities of the model was evaluated using the size of the R-squared values to determine the goodness of fit of the research model [72], [76]. Path coefficients and R-squared values will show whether or not the hypothesised model can be accepted [76].

Bootstrapping function in Smart PLS was used to evaluate the significance level of the partial least square estimation in this study. The bootstrapping procedure in this study used 5,000 subsamples for a one-tailed test type with 0.05 significance level. Fig. 6 shows the path coefficients and R-squared of the structural model. In order for the hypothesised paths to be accepted, [72] recommended that the *t*-values must be significant at 2.33 (significance level = 0.01) or 1.65 (significance level = 0.05).

H1 assumes that optimism positively affects the perceived usefulness of the blockchain-based data-sharing system, while H2 assumes that optimism positively affects the perceived ease of use of the blockchain-based data-sharing system. The results indicated that optimism positively affected the perceived usefulness (path coefficients: $\gamma = 0.45$, $p < 0.05$) and the perceived ease of use (path coefficients: $\gamma = 0.31$, $p < 0.05$).

H3 assumes that innovativeness positively affects the perceived usefulness of the blockchain-based data-sharing system, while H4 assumes that innovativeness positively affects the perceived ease of use of the blockchain-based data-sharing system. However, the results indicated that H3 was insignificant (path coefficients: $\gamma = 0.052$, $p > 0.05$), whereas innovativeness can positively affect the perceived ease of use of the blockchain-based data-sharing system (path coefficients: $\gamma = 0.279$, $p < 0.05$).

H5 assumes that insecurity negatively affects the perceived usefulness of the blockchain-based data-sharing system, while H6 assumes that insecurity negatively affects the perceived ease of use of the blockchain-based data-sharing system. Both hypotheses were not significant, whereby for H5, the path coefficients were $\gamma = -0.074$ and $p > 0.05$, while for H6, the path coefficients were $\gamma = 0.149$ and $p > 0.05$.

H7 assumes that discomfort negatively affects the perceived usefulness of the blockchain-based data-sharing system, while H8 assumes that discomfort negatively affects the perceived ease of use of the blockchain-based data-sharing system. Both hypotheses were not significant, whereby for H7, the path coefficients were $\gamma = -0.045$ and $p > 0.05$, while for H8, the path coefficients were $\gamma = -0.131$ and $p > 0.05$.

H9 assumes that perceived ease of use positively affects the perceived usefulness of the blockchain-based data-sharing system. The results indicated that this hypothesis was significant (path coefficients: $\gamma = 0.334$, $p < 0.05$). H10 assumes that perceived usefulness positively affects the behavioural intention to use the blockchain-based data-sharing system, while H11 assumes that perceived ease of use positively affects the behavioural intention to use the blockchain-based data-sharing system. The results indicated that perceived usefulness positively affected the behavioural intention to use the blockchain-based data-sharing system (path coefficients: $\gamma = 0.360$, $p < 0.05$). Similarly, perceived ease of use positively affected the behavioural intention to use the blockchain-based data-sharing system (path coefficients: $\gamma = 0.285$, $p < 0.05$). Overall result of structural model testing is shown in Table 2.

Hence, hypotheses H1, H2, H4, H9, H10 and H11 were accepted, whereas hypotheses H3, H5, H6, H7 and H8 were rejected.

TABLE 2
STRUCTURAL MODEL TESTING

	Path	Path coefficient, γ	*p*-values	*t*-values	Findings
H1	OPT → PU	0.450	0.000*	4.427	**Accepted**
H2	OPT → PEoU	0.310	0.000*	3.608	**Accepted**
H3	INN → PU	0.052	0.300	0.524	Rejected
H4	INN → PEoU	0.279	0.004*	2.674	**Accepted**
H5	INS → PU	-0.074	0.254	0.662	Rejected
H6	INS → PEoU	0.149	0.198	0.848	Rejected
H7	DISC → PU	-0.045	0.336	0.423	Rejected
H8	DISC → PEoU	-0.131	0.230	0.739	Rejected
H9	PEoU → PU	0.334	0.001*	3.238	**Accepted**
H10	PU → BIU	0.360	0.005*	2.606	**Accepted**
H11	PEoU → BIU	0.285	0.005*	2.580	**Accepted**

*Significant at the 0.05 Level.

Subsequently, the R-squared values were calculated to determine the goodness of fit of the research model. The R^2 value is ranged from 0 to 1 with a lower value indicating lower predictive accuracy and vice versa [72]. The R^2 value indicates the degree of variance in endogenous constructs where the exogenous constructs may define [77]. According to [78], R^2 values at 0.75 for endogenous latent variables in the structural model are considered substantial, 0.50 as moderate, and 0.25 as weak. Fig. 8 shows that the accuracy prediction of the endogenous constructs PU was at 49.6%, which defines the dependent variables that can be explained by their associated independent variables with slightly low to moderate level, and PEoU at 26.8%, which was between the moderate and weak level. The R^2 value for BIU was at 32.4%, which was also moderate level, but considered acceptable for this study. Nevertheless, higher prediction is believed to be achieved if this study is conducted with larger sample size.

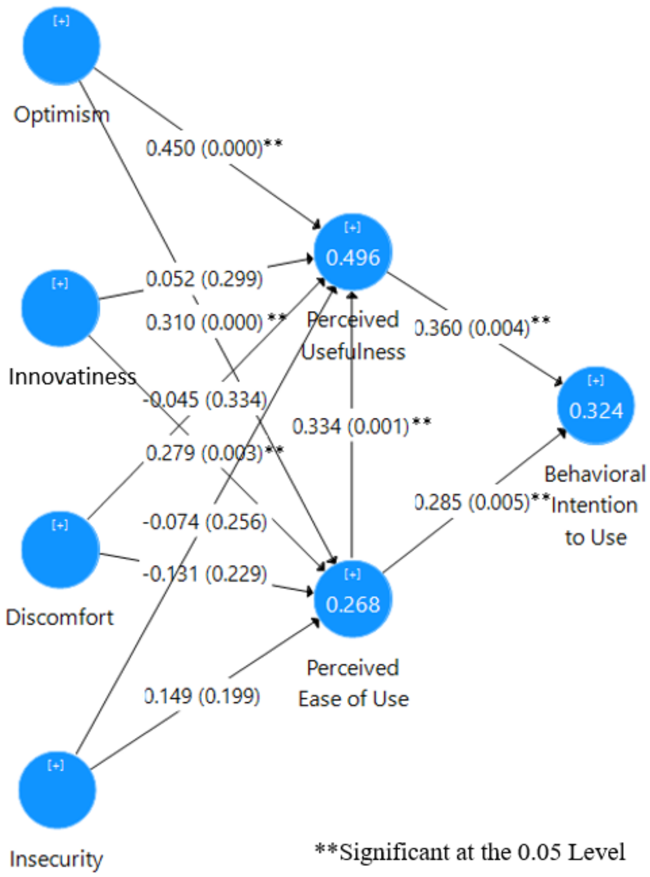

Fig. 8. Overview of results.

E. Discussion

These results showed that personality traits can influence the adoption process and intention to use the blockchain-based data-sharing system in the intelligence community by applying the Technology Readiness and Acceptance Model (TRAM). Personality characteristics particularly optimism and innovativeness as motivators construct in TRI played important roles in the adoption of the proposed system. The intention to use blockchain-based data-sharing system was found mediated by the perceived ease of use and perceived usefulness of this technology, which showed a significant intention to use blockchain-based data sharing system. This finding is similar with previous study by [69]. This indicates that usefulness and ease of use considered as among main element to be considered in development of blockchain-based application.

The results also suggest that positive technology readiness constructs, which include optimism and innovativeness, can positively influence perceived ease of use and perceived usefulness. This finding is similar to result of study by [58] which indicated optimism and innovativeness positively influence the perceived usefulness and perceived ease of use in blockchain technology particularly in cryptocurrency adoption. However, negative technology readiness constructs, which include discomfort and insecurity, were irrelevant in the adoption of the blockchain-based data-sharing system within the intelligence community. This is contradicting with study by [69] but however the finding is aligned with result concluded by [58]. The finding indicates that discomfort and insecurity is not the main significant determinant in blockchain-based data sharing acceptance as user with positive traits include optimism and innovativeness is often not anticipate discomfort and insecurity as barriers in accepting new technology.

V. Conclusion and Future Works

This paper has proposed a secure data-sharing model for the intelligence community based on the blockchain technology. This model included several modules based on the requirements of the intelligence community. A secure method for User Authentication and Identity Management Module has been designed using enhanced multi-factor authentication to increase the security of user authentication and identity management of the data-sharing system while simultaneously fulfilling the requirements of the stakeholders. The Access Control Module was designed based on decentralised access control management by implementing consensus and validation policy using Smart Contract while leveraging a combination of role-based access control (RBAC) and fine-grained access control policies. This module can further enhance the system's security and prevent unauthorised access to the system.

For the Intelligence Data Generation, Edit and View Module, the process involved in storing and accessing the data using smart contract has been also explained in detail. To achieve efficient and reliable data storage, distributed hash table and off-chain data storage using private cloud have been proposed.

However, the implementation of the proposed model required the support of an empirical study on the acceptance and readiness levels of users, which led to the study using TRAM. This study showed that technology readiness has a significant relationship with user adoption for the blockchain-based data-sharing system. The results indicated that optimism and innovativeness have significant effects on perceived usefulness and perceived ease of use.

Hence, for future work, this study plans to extend data collection efforts across several intelligence organisations to generalise a larger data collection. The data collection of system adoption shall include acceptance study in few phases including after initial implementation of system, one month after implementation and three month of implementation as suggested by [79], [80]. The implementation of such study using integration of construct from TAM 3 and TRI 2.0 model should be also considered in future works.

Acknowledgment

This research is fully supported by National Defence University of Malaysia (UPNM) under Centre of Research and Innovation Management. The authors fully acknowledged Ministry of Higher Education (MOHE) and UPNM for the approved fund, which makes this important research viable and effective.

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.

[26] M. Milutinovic, W. He, H. Wu, and M. Kanwal, “Proof of Luck: An efficient blockchain consensus protocol,” in *SysTEX 2016 - 1st Workshop on System Software for Trusted Execution, colocated with ACM/IFIP/USENIX Middleware 2016*, 2016, pp. 2–7, doi: 10.1145/3007788.3007790.

[27] T. Tuan, A. Dinh, R. Liu, M. Zhang, and G. Chen, “Untangling Blockchain : A Data Processing View of Blockchain Systems,” *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, 2018, doi: 10.1109/TKDE.2017.2781227.

[28] I. Karamitsos, M. Papadaki, and N. B. Al Barghuthi, “Design of the Blockchain Smart Contract: A Use Case for Real Estate,” *J. Inf. Secur.*, vol. 09, no. 03, pp. 177–190, 2018, doi: 10.4236/jis.2018.93013.

[29] X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao, and A. V. Vasilakos, “Designing blockchain-based applications a case study for imported product traceability,” *Futur. Gener. Comput. Syst.*, vol. 92, pp. 399–406, 2019, doi: 10.1016/j.future.2018.10.010.

[30] P. Novotny *et al.*, “Permissioned blockchain technologies for academic publishing,” *Inf. Serv. Use*, vol. 38, no. 3, pp. 159–171, 2018, doi: 10.3233/ISU-180020.

[31] X. Cheng and F. Chen, “Design of a Secure Medical Data Sharing Scheme Based on Blockchain,” *J. Med. Syst.*, vol. 44, no. 2, pp. 1–11, 2020.

[32] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare Data Gateways : Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control,” *J. Med. Syst.*, 2016, doi: 10.1007/s10916-016-0574-6.

[33] C. Service and P. Via, “MeDShare : Trust-less Medical Data Sharing Among,” *IEEE Access*, vol. 5, pp. 1–10, 2017, doi: 10.1109/ACCESS.2017.2730843.

[34] R. Xu, Y. Chen, E. Blasch, and G. Chen, “BlendCAC : A BLockchain-ENabled Decentralized Capability-based Access Control for IoTs,” *2018 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data*, pp. 1027–1034, 2018, doi: 10.1109/Cybermatics.

[35] O. Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, 2018, doi: 10.1109/JIOT.2018.2812239.

[36] D. Yermack, “Corporate governance and blockchains,” *Rev. Financ.*, vol. 21, no. 1, pp. 7–31, 2017, doi: 10.1093/rof/rfw074.

[37] K. Naerland, C. Müller-Bloch, R. Beck, and S. Palmund, “Bill of Lading on Blockchain Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments,” *Proc. Int. Conf. Inf. Syst.*, pp. 1–16, 2017.

[38] M. Vukolić, “The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication,” in *International workshop on open problems in network security*, 2015, pp. 112–125.

[39] F. Saleh, “Blockchain without waste: Proof-of-stake,” *Available SSRN 3183935*, 2019.

[40] Y. Li, W. Yang, P. He, C. Chen, and X. Wang, “Design and management of a distributed hybrid energy system through smart contract and blockchain,” *Appl. Energy*, vol. 248, pp. 390–405, 2019.

[41] S. Y. Lim *et al.*, “Blockchain technology the identity management and authentication service disruptor: A survey,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 4–2, pp. 1735–1745, 2018, doi: 10.18517/ijaseit.8.4-2.6838.

[42] M. Singh and S. Kim, “Blockchain technology for decentralized autonomous organizations,” in *Advances in Computers*, vol. 115, Elsevier, 2019, pp. 115–140.

[43] B. L. Radhakrishnan, A. Sam Joseph, and S. Sudhakar, “Securing

Blockchain based Electronic Health Record using Multilevel Authentication," in *2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019*, 2019, pp. 699–703, doi: 10.1109/ICACCS.2019.8728483.

[44] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019, doi: 10.1109/access.2019.2937685.

[45] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges," *IEEE Access*, vol. 7. pp. 164908–164940, 2019, doi: 10.1109/ACCESS.2019.2950872.

[46] S. Ali, G. Wang, B. White, and R. L. Cottrell, "A Blockchain-Based Decentralized Data Storage and Access Framework for PingER," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 1303–1308, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00179.

[47] A. K. Shrestha and J. Vassileva, "User Data Sharing Frameworks: A Blockchain-Based Incentive Solution," *2019 IEEE 10th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2019*, pp. 360–366, 2019, doi: 10.1109/IEMCON.2019.8936137.

[48] N. Kaaniche, M. Laurent, N. Kaaniche, and M. Laurent, "A blockchain-based data usage auditing architecture with enhanced privacy and availability To cite this version Availability," *Netw. Comput. Appl. (NCA), 2017 IEEE 16th Int. Symp. IEEE.*, pp. 1–5, 2018.

[49] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 629–631, 2004, doi: 10.1109/TCE.2004.1309441.

[50] W. R. Simpson and K. E. Foltz, "Secure identity for enterprises," *IAENG Int. J. Comput. Sci.*, vol. 45, no. 1, pp. 142–152, 2018.

[51] Y. P. Kim, S. Yoo, and C. Yoo, "DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things," in *2015 IEEE International Conference on Consumer Electronics, ICCE 2015*, 2015, pp. 196–197, doi: 10.1109/ICCE.2015.7066378.

[52] A. Rastogi, S. Vanikar, and N. Jeyanthi, "Background Checks in Cloud Environment," pp. 305–309, 2018.

[53] A. Yohan, N. W. Lo, and H. R. Lie, "Dynamic multi-factor authentication for smartphone," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2016, doi: 10.1109/PIMRC.2016.7794966.

[54] J. Galbally, I. Coisel, and I. Sanchez, "A New Multimodal Approach for Password Strength Estimation - Part I: Theory and Algorithms," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 12, pp. 2829–2844, 2017, doi: 10.1109/TIFS.2016.2636092.

[55] V. L. Lemieux, "Trusting records: is Blockchain technology the answer?," *Rec. Manag. J.*, vol. 26, no. 2, pp. 110–139, 2016, doi: 10.1108/RMJ-12-2015-0042.

[56] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, 2019, doi: 10.1080/00207543.2018.1533261.

[57] H. Bala and V. Venkatesh, "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decis. Sci.*, vol. 39, no. 2, pp. 273–315, 2008.

[58] S. Kamble, A. Gunasekaran, and H. Arha, "Understanding the Blockchain technology adoption in supply chains-Indian context," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2009–2033, 2019, doi: 10.1080/00207543.2018.1518610.

[59] L. Wanitcharakkhakul and S. Rotchanakitumnuai, "Blockchain technology acceptance in electronic medical record system," *Proc. Int. Conf. Electron. Bus.*, vol. 2017-Decem, pp. 53–58, 2017.

[60] G. Nuryyev *et al.*, "Blockchain technology adoption behavior and sustainability of the business in tourism and hospitality SMEs: An empirical study," *Sustain.*, vol. 12, no. 3, 2020, doi: 10.3390/su12031256.

[61] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q. Manag. Inf. Syst.*, vol. 13, no. 3, pp. 319–339, 1989, doi: 10.2307/249008.

[62] A. Parasuraman, "Technology Readiness Index (TRI): A Multipleitem Scale To Measure Readiness To Embrace New Technologies," *J. Serv. Res.*, vol. 2:307, no. May, 2000.

[63] A. Parasuraman and C. L. Colby, "An Updated and Streamlined Technology Readiness Index: TRI 2.0," *J. Serv. Res.*, vol. 18, no. 1, pp. 59–74, 2015, doi: 10.1177/1094670514539730.

[64] C. H. Lin, H. Y. Shih, P. J. Sher, and Y. L. Wang, "Consumer adoption of e-Service: Integrating technology readiness with the technology acceptance model," *Portl. Int. Conf. Manag. Eng. Technol.*, vol. 2005, pp. 483–488, 2005, doi: 10.1109/PICMET.2005.1509728.

[65] C.-H. Lin, H.-Y. Shih, and P. J. Sher, "Integrating technology readiness into technology acceptance: The TRAM model," *Psychol. Mark.*, vol. 24, no. 7, pp. 641–657, Jul. 2007, doi: 10.1002/mar.20177.

[66] R. Walczuch, J. Lemmink, and S. Streukens, "The effect of service employees' technology readiness on technology acceptance," *Inf. Manag.*, vol. 44, no. 2, pp. 206–215, 2007, doi: 10.1016/j.im.2006.12.005.

[67] C. H. Jin, "Predicting the Use of Brand Application Based on a TRAM," *Int. J. Hum. Comput. Interact.*, vol. 36, no. 2, pp. 156–171, 2020, doi: 10.1080/10447318.2019.1609227.

[68] R. Buyle, M. Van Compernolle, E. Vlassenroot, Z. Vanlishout, P. Mechant, and E. Mannens, "'Technology readiness and acceptance model' as a predictor for the use intention of data standards in smart cities," *Media Commun.*, vol. 6, no. 4Theoretical Reflections and Case Studies, pp. 127–139, 2018, doi: 10.17645/mac.v6i4.1679.

[69] O. Sohaib, W. Hussain, M. Asif, M. Ahmad, and M. Mazzara, "A PLS-SEM Neural Network Approach for Understanding Cryptocurrency Adoption," *IEEE Access*, vol. 8, no. January, pp. 13138–13150, 2020, doi: 10.1109/ACCESS.2019.2960083.

[70] I. Etikan, "Comparison of Convenience Sampling and Purposive Sampling," *Am. J. Theor. Appl. Stat.*, vol. 5, no. 1, p. 1, 2016, doi: 10.11648/j.ajtas.20160501.11.

[71] F. Farrokhi and A. Mahmoudi-Hamidabad, "Rethinking convenience sampling: Defining quality criteria," *Theory Pract. Lang. Stud.*, vol. 2, no. 4, pp. 784–792, 2012, doi: 10.4304/tpls.2.4.784-792.

[72] J. Hair, G. T. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) - Joseph F. Hair, Jr., G. Tomas M. Hult, Christian Ringle, Marko Sarstedt*. Los Angeles: SAGE Publications, Inc. Printed, 2016.

[73] A. Leguina, "A primer on partial least squares structural equation modeling (PLS-SEM)," *Int. J. Res. Method Educ.*, vol. 38, no. 2, pp. 220–221, 2015, doi: 10.1080/1743727x.2015.1005806.

[74] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *J. Mark. Res.*, vol. 18, no. 1, pp. 39–50, Jul. 1981, doi: 10.2307/3151312.

[75] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J. Acad. Mark. Sci.*, vol. 43, no. 1, pp. 115–135, 2014, doi: 10.1007/s11747-014-0403-8.

[76] W. W. Chin, *Handbook of Partial Least Squares*. 2010.

[77] M. Sarstedt, C. M. Ringle, and J. F. Hair, *Handbook of Market Research*, no. September. 2017.

[78] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a silver bullet," *J. Mark. Theory Pract.*, vol. 19, no. 2, pp. 139–152, 2011, doi: 10.2753/MTP1069-6679190202.

[79] V. Venkatesh and F. D. Davis, "Theoretical extension of the Technology Acceptance Model: Four longitudinal field studies," *Manage. Sci.*, vol. 46, no. 2, pp. 186–204, 2000, doi: 10.1287/mnsc.46.2.186.11926.

[80] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Q. Manag. Inf. Syst.*, 2003, doi: 10.2307/30036540.

Noor Afiza Mat Razali (M'16) became a member of IAENG in 2016. She holds a bachelor's degree in Computer and Information Engineering, Master of Science in Computer Science and PhD. of Science in Computer Science from Japanese Universities. Afiza is a Senior Lecturer at the Faculty of Defence Science and Technology at the National Defence University of Malaysia and appointed as Visiting Lecturer and Fellow at Management and Science University Malaysia. Afiza is also a professional technologist, a recognition given by Malaysia Board of Technologists. Her research and expertise are in the area of Cyber Security, Big Data Analytics, Artificial Intelligence & Robotics, Blockchain Technology, Disaster Management System and Human Computer Interaction.

Wan Nurhidayat Wan Muhamad (M'20) became a member of IAENG in 2020. He holds a bachelor's degree in Computer Science from the National Defence University of Malaysia. He is a master's degree candidate at the National Defence University of Malaysia and currently working at the Ministry of Defence, Malaysia. His research interest includes Blockchain

Technology, Cyber Security, Information System, and Information Warfare.

Khairul Khalil Ishak holds a bachelor’s degree in Engineering from Waseda University and master’s degree from Universiti Teknologi MARA Malaysia. He is a professional in Information Technology and Engineering fields with experience in multiple multinational companies. His research interest includes Cyber Security, Big Data Analytics, Artificial Intelligence & Robotics and Blockchain Technology.

Nurjannatul Jannah Aqilah M. Saad holds a bachelor’s and master’s degree in Computer Science from the National Defence University of Malaysia. She is a Research Assistant at the National Defence University of Malaysia, Kuala Lumpur, Malaysia. Her research interest includes Kansei Engineering, Information System and Human Computer Interaction.

Muslihah Wook received her PhD in Information Science from Universiti Kebangsaan Malaysia in 2017, Master of Computer Science from Universiti Putra Malaysia in 2004 and Bachelor of Information Technology (Hons) from Universiti Utara Malaysia in 2001. Her research interests include data mining applications in various domains particularly in education, security and defence. Currently, she is working as a senior lecturer at the Department of Computer Science, Faculty of Defence Science and Technology, National Defence University of Malaysia. She has become a member of International Association of Computer Science and Information Technology (IACSIT) and Institute of Research Engineers and Doctors (IRED) since 2011 and 2013, respectively. Recently, she has been appointed as a technical reviewer of Education and Information Technologies—Springer’s journal indexed by Scopus (Q2).

Suzaimah Ramli received her PhD in electrical, electronic and system engineering from Universiti Kebangsaan Malaysia in 2011, Master of Computer Science from Universiti Putra Malaysia in 2001 and Bachelor of Information Technology (hons) from Universiti Utara Malaysia in 1997. Her research interests include image processing and artificial intelligence applications in various domains particularly in education, security and defence. Currently, she is working as an associate professor at Department of Computer Science, Faculty of Defence Science and Technology, National Defence University of Malaysia. She is a member of Malaysia Board of Technologist and Informatics Intelligence Special Interest Group, UPNM. She has published and presented most of her research findings to various international conferences and articles in many international journals specifically in her research niche.