Multimedia Tools and Applications (2022) 81:36587–36605
https://doi.org/10.1007/s11042-021-11336-7

1219: MULTIMEDIA SECURITY BASED ON QUANTUM CRYPTOGRAPHY AND BLOCKCHAIN

Blockchain for record-keeping and data verifying: proof of concept

Razatulshima Ghazali[1] · Faizura Haneem Mohamed Ali[1] · Hussin Abu Bakar[1] · Mohammad Nazir Ahmad[2] · Nazleeni Samiha Haron[3] · Abdullah Hisam Omar[4] · Ali Ahmadian[5,6]

Received: 27 March 2021 / Revised: 5 July 2021 / Accepted: 24 July 2021 /
Published online: 11 August 2021

Abstract
The paper aims to show how blockchain, particularly Ethereum private blockchain, performs as a record keeper for Malaysian Muslim marriage records as a case study. The study also aims to demonstrate how blockchain technology conserves marriage data and improves data sharing efficiency involves accessing data from the blockchain and multiple users through proof of concept (POC). This POC also intended to seek evidence of immutability, transparency, and authenticity claims by the technology to ensure the record's security is a high priority. The study implements a smart contract on the Ethereum platform in the Government of Malaysia network environment and, the results provide significant evidence of private Ethereum blockchain principles of high availability, efficiency, immutability, transparency, and truthfulness particularly in record keeping. Future research can investigate other blockchain technology for other blockchain initiatives, such as blockchain disruptors. This paper is useful for management researchers and guides management practice for decision-making when determining whether the technology can use as a record-keeper. This paper proposes POC to design and develop record-keeping of Malaysian Muslim marriage records using Ethereum blockchain technology.

Keywords Ethereum blockchain · Proof of concept · Muslim marriage record · Record-keeper

1 Introduction

Blockchain popularity has become more hype in government agencies, although it is not a newly introduced technology in the information communication technology world. The reputations of blockchain in ensuring each transaction's security in the systems have

✉ Mohammad Nazir Ahmad
mnazir@ukm.edu.my

Extended author information available on the last page of the article

attracted the business community to invest in this technology. The technology keeps evolving and aggressively implemented in several government agencies and industries. As for government agencies, record-keeping issues always become a significant problem, security or privacy issues, and technology efficiency. Therefore, this study endeavors to seal the gap in knowledge and practice by offering a POC, one of four blockchain initiatives introduces by Gartner [11]. Four types of blockchain initiatives are i. blockchain disruptor; ii. digital asset market; iii. efficiency play; and iv. record keeper.

Blockchain is thriving as a hot trending among virtual currency traders because of the capability to generate money with guaranteed security. Blockchain characteristics such as durability, transparency, immutability, and process integrity became value added to blockchain technology's popularity [1]. However, despite the popularity of blockchain, it also has a weakness that we cannot ignore. The delivery performance through blockchain is questionable, and the data capacity constraints that can transmit through blockchain are costly [6, 24]. Furthermore, security and privacy issues are either in public or private blockchain [27]. Hence, before deciding to use this technology, especially when it comes to Government and citizen interest, we must consider all aspects [13, 20]. As for Malaysia Government, blockchain technology felt still too alien for us to implement in government agencies. However, some interesting aspects of blockchain technology should not be disregard if it can be beneficial to solve the problems faced by some agencies, such as Muslim marriage record keeping.

Scattered Muslim marriage records across states and districts are even worse because each state has its regulations and acts, especially in a Muslim marriage. Department of Islamic Development of Malaysia, known as Jabatan Kemajuan Islam (JAKIM), is one agency under Malaysia's Government currently facing data sharing issues. JAKIM wants to ensure that the records of Muslim marriages in Malaysia are accessible by agencies that require marriage information, especially the District Islamic Religious Office (PAID) and the State Islamic Religious Department (JAIN). Muslim marriage records in Malaysia are scattering among PAID and JAIN as each district and state has its acts and policies. The couples who want to get married need to register with the PAID or JAIN. JAKIM regulates both PAID, and JAIN which has built a system to keep Muslim marriage records in Malaysia called Sistem Pengurusan Perkahwinan Islam Malaysia (SPPIM). However, not all PAID and JAIN uses SPPIM as both agencies are under state regulatory authorities. If the state authorities had permitted PAID and JAIN to use SPPIM, then JAKIM can use the information. Therefore, there is no comprehensive centralized data on Muslim marriage, divorce, and referral information.

This situation makes it difficult for JAIN and PAID to not use SPPIM as their primary system to register Muslim marriage information to check the applicant's marital status while processing the marriage permit, divorce registration, and reference registration. A Muslim woman cannot have more than one husband at the same time. In comparison, Muslim men cannot have more than four wives and other conditions that JAIN or PAID need to review before the couple can be allowed to marry. As a result, there is identity fraud for polygamy, and there are several cases related to fraud recorded involving forgery of marriage documents [8]. These situations are alarming because they will lead to other Islamic law problems if the marriage does not comply with sharia.

Currently, there are two ways couples who want to get married register their marriage. A man or woman firstly needs to register through online registration using SPPIM for states that use SPPIM. Alternatively, he/she has to go to the nearest PAID or JAIN to register manually. Using the second alternative, PAID or JAIN, have to check with JAKIM, and others PAID or JAIN in other states that do not use SPPIM; thus, the application process

will take a long time. The officer should do a careful review at PAID or JAIN to ensure that the couple applying for marriage can marry without any problems. The woman is still a wife with her previous husband. The officer at PAID or JAIN demands the couples' correct identity or status, and other agencies rely on marital data to verify marital status for various services. For example, the Government Pension Division provides pension payment to the pensioner's widow or husband in the event of death to the pensioner. Confirmation is required to ensure that the widow or husband is still valid as a husband and wife to receive a pension.

Considering blockchain characteristics claim by many past studies regarding security, privacy, immutability, high availability, and efficiency, this paper demonstrates POC to understand if those JAKIM can utilize all those blockchain characteristics issues. Using private Ethereum blockchain technology setup in seven nodes to represent blockchain networks, Muslim marriage data are saved and tested to ensure all necessary characteristics essential for record-keeping. Therefore, based on a previous study by [10], we expand the investigation by developing a new POC of record-keeping and data verifying besides a thorough test of the blockchain network characteristic a potential trustful record-keeper. This POC is intended to test the claims regarding security, privacy, immutability, high availability, and efficiency of the blockchain for the Muslim marriage record-keeping process.

The paper is structured as follows; Section 2 provides an overview of the literature review that forms this paper's foundation. Section 3 discusses the research design and methods, as well as a comprehensive description of our results. Meanwhile, Section 4 discusses the POC results and limitations of the study. The last section in this study is the conclusion in Section 5.

2 Literature review

This section briefly reviews related studies of Muslim marriage laws in Sharia Law and the Ethereum blockchain used in this POC.

2.1 Sharia law

Malaysia governs by two types of laws, namely civil law and sharia laws. The civil laws apply to all Malaysians, while sharia laws are only applicable to Muslims that administer by sharia courts of the states and the federal territories. This court's jurisdiction does not cover theft, murder, robbery, rape, and other criminal offenses stipulated in Malaysia's Penal Code Laws, which fall under civil laws governed by Civil courts [15]. The Malaysian Constitution authorizes State Sharia courts the exclusive power to adjudicate their state's Islamic laws[1]. Sharia courts can adjudicate cases arising under Islamic law and personal and family law of persons professing Islam's religion, including the Islamic law relating to betrothal, marriage, divorce, dower, maintenance, adoption, legitimacy, and guardianship. The Sharia courts refer to Islamic family laws enacted by the states [19]. Although the central precepts of Islamic Family law as found to be applicable in all the states in Malaysia

[1] (Federal Territories) Act 1984, Act 303 of 1984 in Malaysia; Enakmen Undang-Undang Keluarga (Negeri Selangor) 2003 [Islamic Family Law (State of Selangor) Enactment 2003], Enactment 2 of 2003.

are almost the same. However, there are minor differences in these laws' interpretations and applications from one state to another. This situation has led some litigants to go on law-shopping by moving from one state to another when the consents required for them to tie another marriage were not forthcoming. They also move to where the interpretation given to the minimum age for marriage suits their desires because a Muslim by law is entitled to marry up to four wives provided he can treat each of them equally. In an attempt to codify and enforce uniform legislation for Muslims, the Islamic Family Law Act 303 was introduced in 1984. However, most states, given their prerogative power in a legal jurisdiction, agreed to enact a uniform code with minor differences [17]. The following sections discuss in brief of married, divorce, and rujuk (re-marry) in Islamic laws.

2.1.1 Married, divorce and rujuk

The couples who want to get married must comply with everything contained in sharia laws [9]. As stated in IFLA or Islamic Family Law [9], a marriage has solemnized by a *wali* (IFLA, Section 7) and issuance with ta'liq (IFLA, Section 26), and the couple has reached a certain age (IFLA, Section 8). Couples who want to get married must be both Muslims (IFLA, Section 10) and have no blood relationship such as siblings or parents, parents, and others enshrined in sharia law (IFLA, Section 9). married women may not marry another man (IFLA, Section 14). A man can have up to four wives or polygamy with the permission of the sharia court to ensure the life of the existing wife is guaranteed (IFLA, Section 23).

Talaq is the word divorce made by the husband to his wife. The number of *talaqs* will determine whether the husband and wife can rujuk or re-marry with the same partner. The divorce process should also be done through a sharia court to avoid any problems arising if the husband and wife want to *rujuk*. Most of the Islamic family laws provided in some states in Malaysia are clear enough on the widows' marriage, including a situation where a woman has been irrevocably divorced by three *talaqs*. In this situation, the woman will not marry her previous husband unless she has been lawfully married to another person. Such marriage shall have been completed and later legally dissolved before that marriage contract with her previous husband [17].

2.2 Private ethereum blockchain, smart contract, and metamask

Oxford dictionary defines blockchain as "A system in which a record of transactions made in bitcoin or another cryptocurrency is maintained across several computers that are linked in a peer-to-peer network." Whereby, [23] highlight the blockchain concerning consensus mechanisms as the technology that warrants unchangeable and truthful data in transacts record in the blockchain systems linked in a peer-to-peer network. [3] also define blockchain as an unchangeable ledger for recording transactions that mutually untrusting peers maintain within a distributed network. Meanwhile, [5] represent blockchain as a distributed database that maintains a growing list of blocks chain to each other. [18] emphasize that blockchain differs from traditional databases. It stores the full record of every piece of data and its modifications with redundancy features that bring protection against tampering but at a high cost of processing. [2]

[4] summarizes blockchain as a technology that allows its participants or users to retrieve only a single truth version of any information (in this case from a ledger or whatever data place in the network) without a central authority in a trustless environment

whereby its participants do not have to trust each other, and incorporates at least the following four technologies; (i) peer-to-peer networking, (ii) distributed ledger, (iii) cryptography; and (iv) mining. Additionally, [7] postulates two significant blockchain types, namely public blockchain, if all participants can participate in all processes without any central authorization body to control the network. The second type is semi-private blockchain or private blockchain. In a semi-private blockchain, the body and participants' network control is predefined with limited access to pre-selected nodes. Meanwhile, for a fully private blockchain, there is no remuneration process involved. Bitcoin is one of the most popular public blockchain besides the Ethereum blockchain, famous for public and private blockchains.

Furthermore, [2] also claims that Ethereum is a blockchain branding and defines Ethereum as a cryptographically secure transaction singleton machine with a share-state, innovating from the bitcoin network additions its network features such as smart contract usage. Ethereum smart contract could allow for more complex requests compared to more straightforward bitcoin's codes. A smart contract is a code that manages the exchange of anything of value, from property and shares to information and money between parties. Smart contracts become like autonomous agents that execute when previously specified conditions are met and can perform more instructions over the Ethereum network using a high-level object-oriented language such as Solidity. This language is similar to the JavaScript language designed to help developers write smart contract code on Ethereum [16]. However, for the smart contract to communicate with participants or users, it used a user interface called MetaMask.

MetaMask, founded in 2016, has been a browser extension that lets people to join their cryptocurrency wallets to websites that require the right of entry to the Ethereum network. It serves as a wallet that connects the users with the Ethereum node without running the node. Nowadays, MetaMask has a new mobile version that allows users to limit the information and payment methods they share with websites [12]. MetaMask requires permission to read and write and will enable users to store public and private keys. MetaMask ensures the users' control while using the blockchain to choose what to share [14]. The next section describes POC designing and methodology in detail.

2.3 Research design and method

Figure 1 illustrates the POC development process flow divides into three main components. Each component describes in detail in Section 3.1 until Section 3.3.

2.4 Concept and designing

In this phase, the planning is setting, with the requirement gathering to accommodate the system's functional and non-functional requirements. The functional requirements include user management module, marriage record keeping, data retrieval, and data validation. Meanwhile, non-functional requirements include the efficiency and high availability of record-keeping in the blockchain. Figures 2 until 5 shows the use case of activities in the functionalities.

As illustrated in Fig. 2, the system's user–data consumer or administrator registers an account to access the system using MetaMask. MetaMask is an e-wallet application to obtain private and public keys to enable transactions for blockchain execution. Using

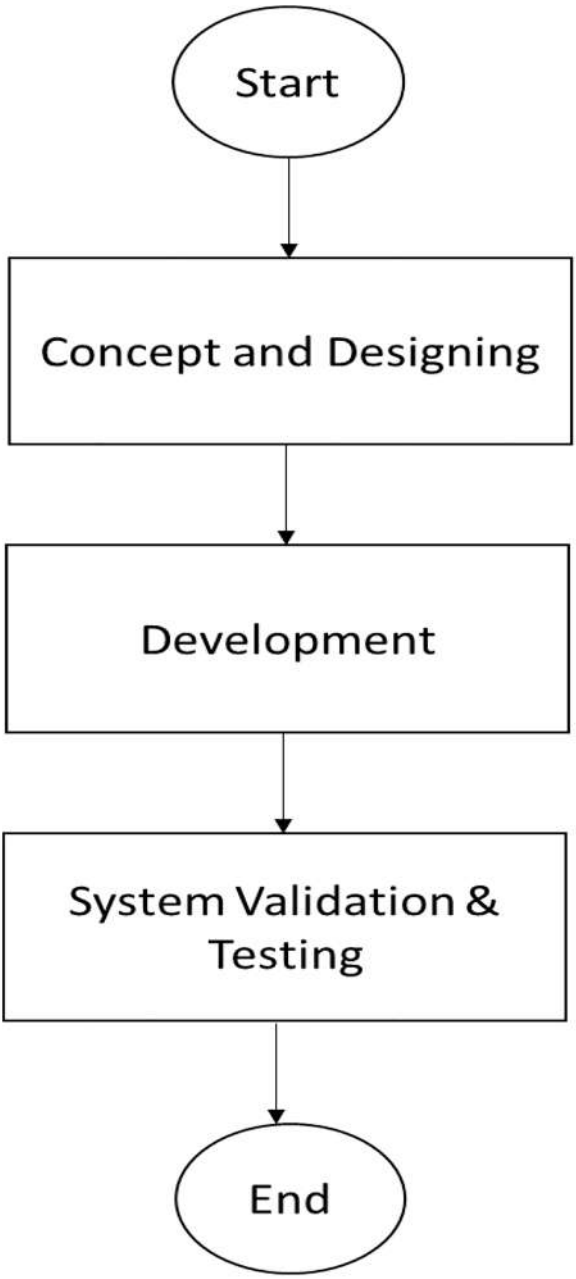

Fig. 1 POC development process flow

Ethereum compatible wallet, e.g., MetaMask, users need to log in to MetaMask to perform blockchain transactions.

After the user successfully logs in to the system and executes a transaction involving blockchain, the user at any time could log out of the system to close the session.

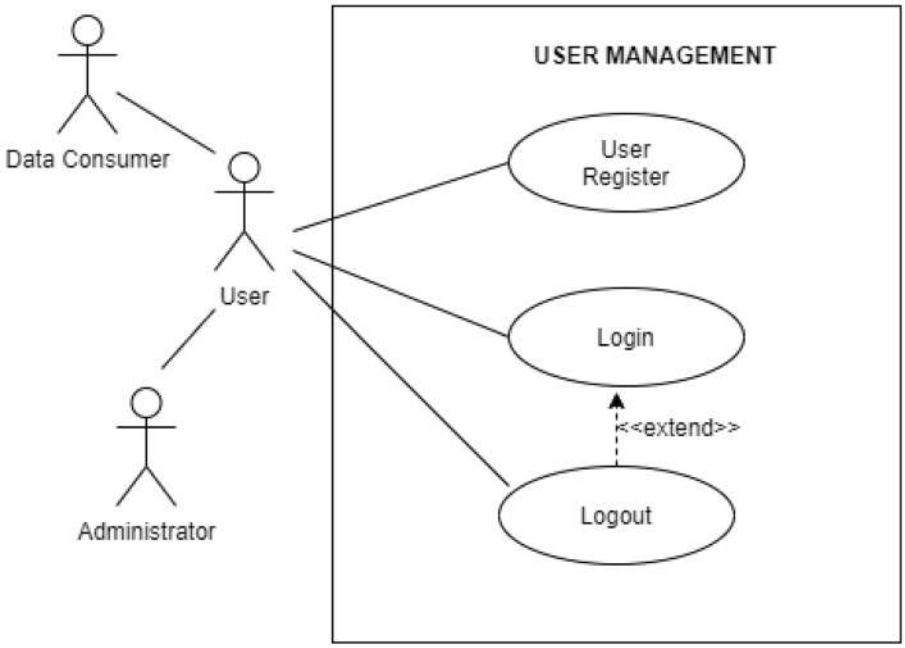

Fig. 2 Use case diagram of user management

Figure 3 shows that administrators (from JAKIM, agencies, PAID, or JAIN) can read (retrieve) marriage records from the JAKIM database of marriage records stores in the blockchain. Users could select the desired marriage record and copy it into the blockchain.

Figure 4 use case shows the function of accessing data by data consumers across agencies to the blockchain. Data consumers can do the searching based on identity card number to obtain individual marriage records.

Figure 5 illustrates the use case of the data verification function. Data consumers can verify whether the data from the Relational Database Management System (RDMS) is

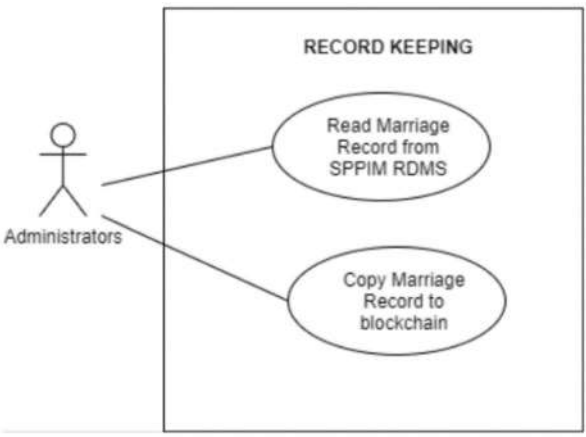

Fig. 3 Use case diagram of record keeping

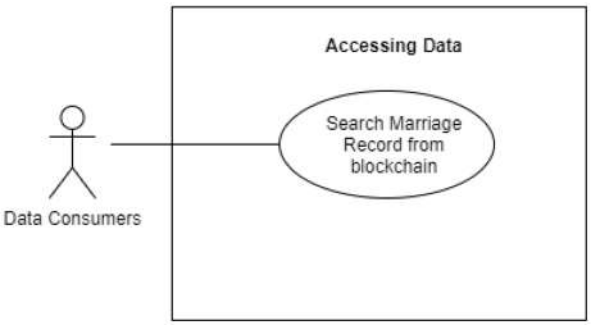

Fig. 4 Use case diagram of data consumers accessing data

valid by comparing the record with the record that has been stored in the blockchain using the identification number of the individual.

As illustrates in Fig. 6, many agencies are expected to use the blockchain network of Muslim marriage record storage for verification purposes in various daily business processes. Only the essential and relevant marriage data from SPPIM, JAIN, and PAID will be saved in the blockchain network. Meanwhile, other agencies will be referring the data through the blockchain network for verifying purposes.

2.5 Development

In the development phase, the frontend interface act as SPPIM, namely, develops for a user to key in the data into the SEMA database. The interface is creates using the bootstrap 4.0 framework and PHP programming language. The purpose of using the RDMS is to avoid delays in entering data and searching process if using the blockchain network directly. Large data storage is also more suitable for using RDMS than blockchain because blockchain networks are not ideal for large data storage as they will delay the transaction process.

As illustrated in Fig. 7, administrators from JAKIM, JAIN, or PAID will enter the data or information about the couple's marriage through the SEMA user interface, as illustrates in Fig. 8. The administrator can use all modules such as add new or update a record, save data to the blockchain, which is needed to do through the MetaMask, and verify data from the blockchain module. According to this blockchain domain, the MetaMask configuration does not require any ether because POC is setting in a private domain. Meanwhile, regular users have permission to access blockchain for verifying purposes only to avoid marriage

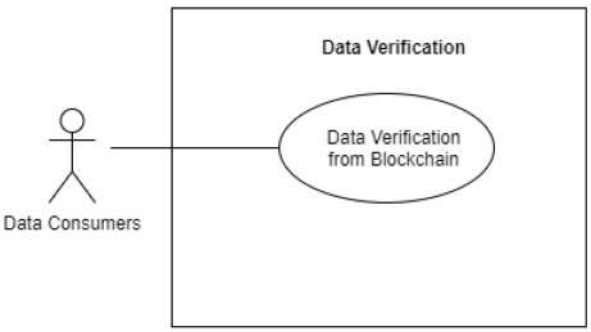

Fig. 5 Use case diagram of data verification

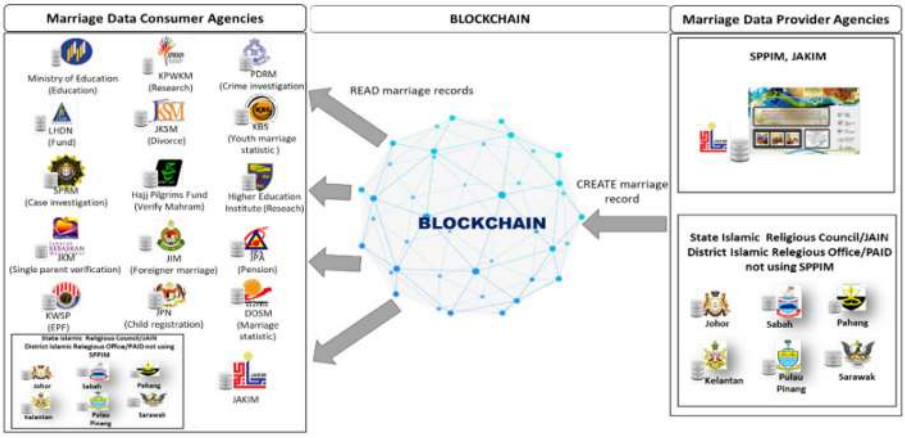

Fig. 6 Conceptual architecture of record keeping and verification marriage data

data misconduct. In our control environment, seven private Ethereum blockchain nodes are developed in Ubuntu open-source operating system on a Linux server.

The administrator will add a new record or update the existing record through *Add Records,* and the data save in the SEMA database. SEMA database store in a RDMS such as MySQL. Then, the administrator can perform the searching of RDBMS by using the identification number of individuals in the *Home* tab to check or update the information. The system will search the identification number in the SEMA RDMS database and not the blockchain. In this situation, the full record retrieves to update the information in it. The data will be copied to the blockchain using *Save to blockchain* module, as showed in Fig. 9. This interface will call selected data identifies to store in blockchain from MySQL database as listed in Table 1.

All previous records entered by the administrator are listing according to the data elements stored in the blockchain. The administrator will choose which record is copying to the blockchain by selecting the link under *Action,* as shown in Fig. 9. The selected data are copy into the blockchain node through a smart contract that is writing using

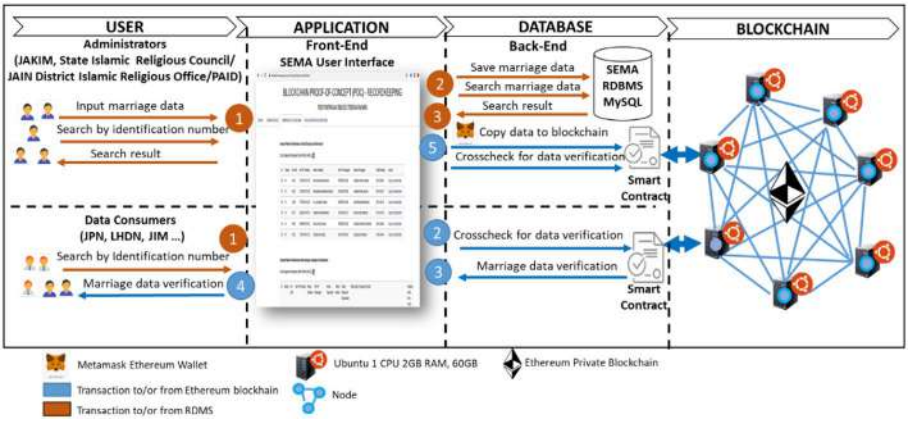

Fig. 7 The architecture of POC development

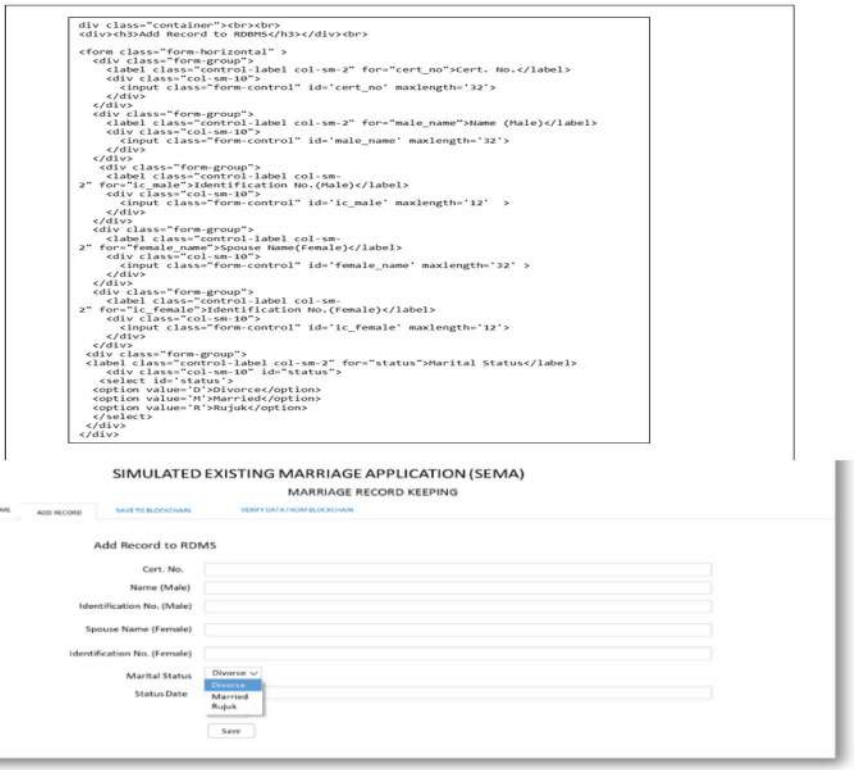

Fig. 8 Add record to RDMS code and user interface

Solidity language will appear for the administrator to write the data in the blockchain. The smart contract is developing using the Solidity development tool, namely, remix Ethereum, an open-source tool that enables the writing of Solidity Ethereum smart contract from the browser.

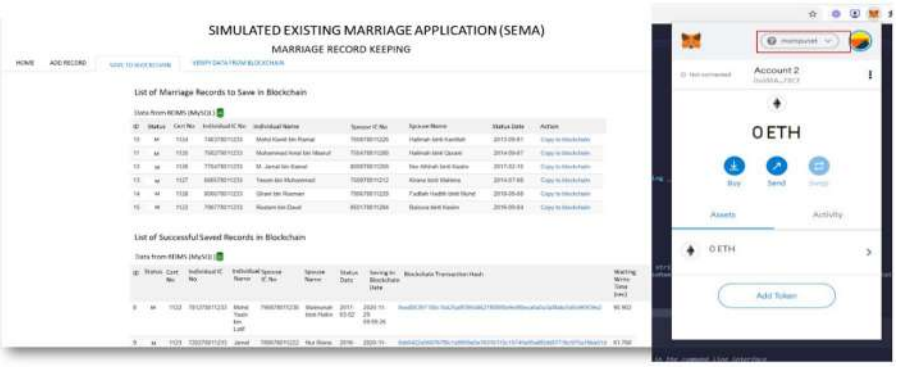

Fig. 9 Save Data to Blockchain user interface

Table 1 Data elements store in blockchain

Attribute	Data Type	Description
ID	address	administrator Ethereum id
Marriage Status	bytes32	Marriage-N Divorce-C Rujuk(re-marry)-R
Certification Number	string	certificate number for marriage, divorce or re-marry
Individual Name	string	Male individual name
Individual IC No	string	citizen: identification number non-citizen : passport number
Spouse Name	string	female name
Spouse IC No	string	citizen: identification number non-citizen: passport number
Status Date	string	Status date of marriage/ divorce/*rujuk* ' DD-MM-YYYY.'

The user has to register MetaMask to deploy a smart contract to set up a blockchain network, in this case - mampunet. Blockchain transaction hash will be automatically generated by smart contract the unique hash code once the data written in blockchain as proof. The smart contract code to generate the hash code shows in Fig. 10.

The hash code saves in RDBMS for verification purposes that only the data with allocated hash code are the valid data. The function to compare the data from RDMS and the blockchain data is developed to ensure data immutability, as shown in Fig. 11. The immutability test is done by changing the identification number one of the record (i.e., 781278011233 to 790878011238) in RDMS, and the comparison is made with the data in the Ethereum blockchain.

The users at data consumer's agencies will verify the marriage information through the blockchain by using SEMA *Verify Data from Blockchain* user interface as illustrated in Fig. 12 by using the individual's identification number.

The last step in this POC is most important as this step is to validate and test whether this POC is a success. The results of POC also are discussed in the following section.

2.6 System validation and testing

In this step, functional and non-functional are undergone thorough testing. Table 2 lists functional and non-functional requirements for this POC. Four main modules for functional testing: *User Registration*, *Save Data to Blockchain*, *Read Marriage Record from Blockchain,* and *Record Verification*. Meanwhile, for non-functional, efficiency and high availability of copying or saving data to blockchain and read data from blockchain are tested.

2.6.1 Functional test

User acceptance test (UAT) is conducted for functional test and the result as in Table 3. UAT is accomplished by several users act as administrator and user role. The test is performed by a tester that is independent of the development team to avoid bias.

```
function addMarriageInfo(id, ic,individualName,spouseIc,spouseName,status,statusDate){
  var startTime = Date.now();
   web3.eth.getAccounts().then(function (accounts)
   {
      var acc = accounts[0];
      ethereum.enable();
      //individualName must be male/man
       return contract.methods.addMarriageInfo(ic,individualName,spouseIc,spouseName,status,
       statusDate).send({ from: acc });
      /*check bc hash*/
   }).then(function (tx)
   {
      var endTime = Date.now();
      var waitingTime = endTime - startTime;
      console.log('wait = '+waitingTime);
      console.log(tx);
        transactionHash = tx.transactionHash;
       if(id!="" && transactionHash!=""){
        $.ajax({
           url: "insert_bcstatus.php",
           type: "POST",
           data: {
              id: id,
              transactionHash: transactionHash,
              waitingTime: waitingTime
           },
           cache: false,
           success: function(dataResult){
              var dataResult = JSON.parse(dataResult);
              if(dataResult.statusCode==200){
                 document.getElementById('link_desc'+id).style.display = 'none';
                 location.reload();
              }
              else if(dataResult.statusCode==201){
                alert("Error occured !");
              }
```

Fig. 10 Solidity smart contract generate hash code from blockchain

All the four main modules are passes the test performed by the user according to the roles given. Each user has their role as administrator and standard user. Each role then rotates the roles among them to ensure each module thoroughly tests.

2.6.2 Non-functional test

Efficiency for writing marriage records to the blockchain is tested by gaining time-waiting from the user interface module of *Save to Blockchain* (see Fig. 13). Figure 13 shows non-functional test results for copy marriage record efficiency to blockchain gaining from waiting-writing data time in the blockchain. The writing time also considers MetaMask user confirmation before writing or copying the data to all seven blockchain nodes.

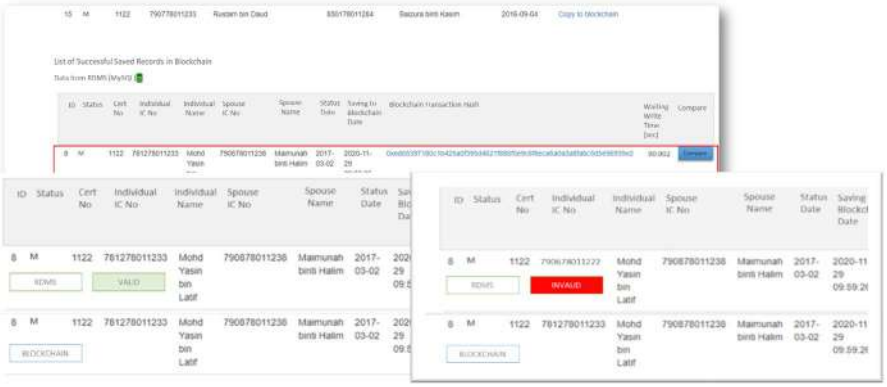

Fig. 11 Crosscheck data immutability in RDMS with Ethereum blockchain

The efficiency of reading the marriage record from blockchain is tested using the apache JMeter load testing tool (see Fig. 14). Also, high availability for both copy and read is tested by de-activating three nodes (see Fig. 15) and observe the result. The overall result of the test shows in Table 4.

Meanwhile, for non-functional test results for the efficiency of reading marriage records from blockchain, using Jmeter using 300 concurrent users accessing the SEME user interface of *Verify Data from Blockchain* module is shown in Fig. 14. In this POC, 300 simultaneous users load tests. The result indicates that Apdex is equal to 1, which means the efficiency is at the highest rate with an average response time of 24.92 milliseconds. Application Performance Index, namely Apdex, is reporting and comparing the transaction performed.

As illustrated in Fig. 15, only four nodes operated instead of seven nodes to show that the blockchain network can still perform. However, 51 percent is available, and even copying and reading data to/from the blockchain.

Fig. 12 Verify data from blockchain user interface

Table 2 Functional and non-functional testing

Functional	Four main modules
	• User registration • Save data to blockchain – RDMS system integration with smart contract • Read marriage record from blockchain • Record verification
Non-functional	Efficiency
	• save the record to the blockchain • read record from blockchain
	High-availability
	• save marriage record to the blockchain • read record from blockchain

Table 3 Functional UAT result

Function	Actor	Result
MetaMask User Registration		
Register	Administrator and User	Pass
Log In	Administrator and User	Pass
Log Out	Administrator and User	Pass
Saving Data in Blockchain		
Read marriage record from RDMS	Administrator	Pass
Copy marriage record to the blockchain	Administrator	Pass
Read Data from Blockchain		
Search data from the blockchain	User	Pass
Record Verification		
Data verification from blockchain	User	Pass

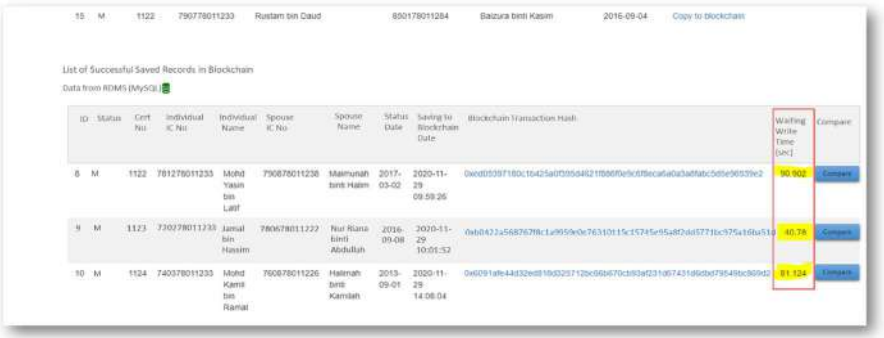

Fig. 13 Efficiency testing: write data to blockchain

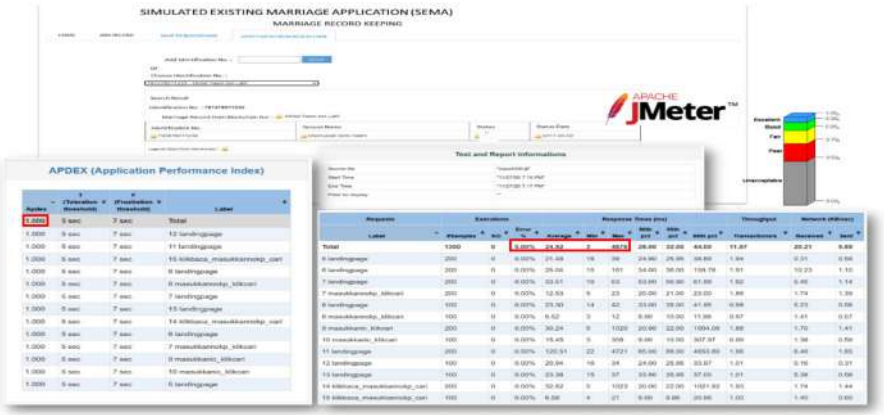

Fig. 14 Efficiency test: read marriage record from blockchain

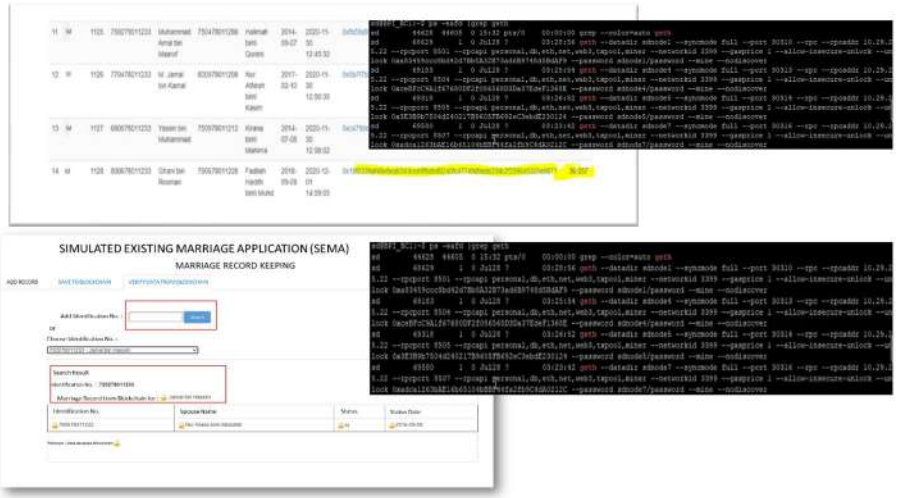

Fig. 15 High-availability test: copy/read marriage record to/from blockchain

Table 4 Non-functional result: writing and reading from blockchain

Description	Result
Efficiency	
Copy marriage record to the blockchain	40-90 seconds
Read marriage record from blockchain	Average 0.024 seconds for 300 concurrent users
High-Availability	
Copy marriage record to the blockchain	The record can be copied if at least four nodes are functioning
Read marriage record from blockchain	The record can be read if at least four nodes are functioning

3 Discussion

As proved by Kamaruzaman, Yassin [10] in their study of the data's transparency and integrity in the Ethereum blockchain network, this POC also successfully demonstrated the security, privacy, and immutability of the network. The hash code provided by the Ethereum blockchain for every transaction that involved writing to the Ethereum blockchain offers secure and private transactions as the only administrator with generated hash code has permission to save new data. The hash code then saves in the RDMS, which can be used to compare the data in RDMS with the Ethereum blockchain if any attempt is made to change the data in RDMS.

One of the distinctive blockchain features is the data stored in the chain will remain forever in the network. The data must have a high asset value and stay relevant are the right candidates to keep in the blockchain [18, 21, 22]. Therefore before deciding to store data in a blockchain network, a detailed study needs to be done to determine whether it is worthwhile to keep such data in a blockchain network. The data to be held in the blockchain network is very limited and must meet all the users' needs to ensure that the blockchain can operate efficiently as possible. Distributed blockchain architecture and encryption algorithms have their advantages and disadvantages, as acknowledged in several previous studies [6, 24]. The POC results also confirm the architectural weaknesses, whereby the result obtained for writing is long. The range of data waiting time to blockchain in 40 seconds until 90 seconds is considered quite long for a typical network to save the data to the database. However, this writing time is not a significant problem as it does not affect the efficiency of full processes. This situation occurs because the registration of users to use MetaMask also includes in the calculation. In the meantime, the blockchain speed and efficiency in the reading process can not be deniable that only takes an average response time of 24.92 milliseconds for three hundred concurrent users. This result supports some previous studies [21, 28]. Previous studies claim that blockchain is a high-availability network [25]. This POC confirms the claim when the results for data synchronization carried out are very encouraging in the situation of node failure. The results show that the nodes are still working, as the data can be stored and read even with only 51 percent of the nodes working.

This POC has demonstrated how blockchain implementation could resolve data sharing issues in managing marriage records by the government institutions. Traditional data sharing methods rely on centralized databases for data storage, which are handled in silos by related institutions, and these centralized database limitations could lead to data sharing flaws. Furthermore, because the marriage statute is under the jurisdiction of each state in the country, there is a trust and policy issue in consolidating the entire marriage record at the national level by a single institution. The blockchain implementation utilized technology itself as a connectivity center for all entities related to the marriage record management in the country. Apart from the benefits of data transparency and security in data sharing as stated by [26], Blockchain implementation also resolves trust difficulties about who is the most superior institution that may be authorized to retain the most up-to-date information on all marriage records in the country.

However, there are some limitations in this POC. There are needs to be a monitoring and auditing mechanism for data storage transaction logs (e.g., Blockchain explorer) to ensure the characteristics of security, auditability, and transparency. Blockchain development methods and terms are complex and different from conventional web application / RDMS development, requiring a high learning curve. Experienced programmers in object-oriented

have the advantage of understanding Solidity program structure and primitive data structure. Meanwhile, in a future study, the MetaMask Ethereum compatible wallet can be improved by developing its Ethereum wallet. This POC also uses private Ethereum to support the Ethereum platform regarding other platforms such as hyperledger.

4 Conclusion

This POC can provide a new perspective in the storage of Muslim marriage records in addition to conventional data storage. This technology is still relatively new for Malaysians. The Malaysian Government needs to do a more detailed and thorough study in applying a business problem using blockchain technology. Various business case selection criteria need to be considered as not all problems can be solved using blockchain technology.

Appendix

Abbreviation	Definition
POC	Proof Of Concept
JAKIM	Jabatan Kemajuan Islam
PAID	District Islamic Religious Office
JAIN	State Islamic Religious Department
SPPIM	Sistem Pengurusan Perkahwinan Islam Malaysia
IFLA	Islamic Family Law
RDMS	Relational Database Management System
SEMA	Simulated Existing Marriage Application
UAT	User Acceptance Test

Acknowledgment This work is supported by the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), ICT Consulting Division, Prime Minister Department of Malaysia, and Industrial Research Grant, Integrasi Erat Sdn. Bhd, Vot. No: ZG-2021-001. High appreciation goes to the above sponsors. The authors gratefully acknowledge ICT Consulting Division blockchain team members for their sheer dedication to this POC.

Declarations

Conflict of interest The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest

References

1. Abeyratne S, Monfared R (2016) Blockchain ready manufacturing supply chain using distributed ledger. Int J Res Eng Technol 5:1–10

2. Alghamdi TA et al (2020) Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain. IEEE Access 8:1048–1061
3. Androulaki E et al (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proc Thirteenth EuroSys Conf Porto Portugal ACM
4. Aziz AA (2020) Ethereum private network and application development lab notes. Thuleen i.o
5. Dorri A et al (2017) BlockChain: a distributed solution to automotive security and privacy. IEEE Commun Mag 55(12):119–125
6. Golosova J, Romanovs A (2018) The advantages and disadvantages of the blockchain technology. In 2018 IEEE 6th Workshop Adv Inf Electron Electr Eng (AIEEE). Lithuania:IEEE
7. Guegan D (2017) Public blockchain versus private blockchain. Université Panthéon-Sorbonne (Paris 1), Centre d'Economie de la Sorbonne
8. Ismail WAFW (2015) Forms of document falsification in Malaysia' s Syariah courts. Geografia Malays J Soc Space 11(9):32–39
9. Islamic Family Law (Federal Territory) Act 1984 IFLA (1984) In Act 303, Government of Malaysia
10. Kamaruzaman N et al (2018) Blockchain technology for islamic marriage certificate. Int J Eng Technol (UAE). 7(4):193–197
11. Kandaswamy R, Furlonger D (2018) Pay attention to these 4 types of blockchain business initiatives. Gartner
12. Leising M (2020) MetaMask's blockchain mobile app opens doors for next-level web. Bloomberg
13. Makhdoom I et al (2020) PrivySharing: a blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Comput Secur 88:101653
14. Metamask. https://metamask.io/. Accessed 15 May 2020
15. Mohamad M (2017) Contesting syariah laws in malaysia: religion, human rights and the state's response. J Polit Law 10(5):140
16. Review B (2018) Ethereum white paper made simple. pp 1-29. Report https://www.slideshare.net/antoniomanno3/ethereum-white-papermade-simple
17. Salleh AZ et al (2016) Codification of islamic family law in Malaysia: the contending legal intricacies. Sci Int (Lahore) 28(2):1753–1762
18. Sicilia M, Visvizi A (2018) Blockchain and OECD data repositories: opportunities and policy making implications. Library Hi Tech 37. https://www.emerald.com/insight/content/doi/https://doi.org/10.1108/LHT-12-2017-0276/full/html
19. Shuaib F (2012) The islamic legal system in Malaysia. Pac Rim L Policy J 21:90–91
20. Sun M, Zhang J (2020) Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. Comput Commun 149:332–342
21. Tith D et al (2020) Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. Healthcare Inf Res 26(1):3–12. https://doi.org/10.4258/hir.2020.26.1.3
22. Vazirani A et al (2020) Blockchain vehicles for efficient medical record management. NPJ Digit Med 3(1):1
23. Viriyasitavat W, Hoonsopon D (2019) Blockchain characteristics and consensus in modern business processes. J Ind Inf Integr 13:32–39. https://doi.org/10.1016/j.jii.2018.07.004
24. Wang S et al (2019) Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans Syst Man Cybernet Syst 49(11):2266–2277
25. Wang Y, Han JH, Beynon-Davies P (2018) Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. Supply Chain Manag Int J 24(1):62–84. https://doi.org/10.1108/SCM-03-2018-0148
26. Wei J et al (2019) The adoption of blockchain technologies in data sharing: a state of the art survey. In WHICEB 2019 Proc Wuhan China AIS Electron Libr (AISeL)
27. Zhao X et al (2017) The DAO attack paradoxes in propositional logic. In 2017 4th Int Conf Syst Inf (ICSAI). Hangzhou, China:IEEE
28. Zhu Y et al (2019) A new instant confirmation mechanism based on interactive incontestable signature in consortium blockchain. Front Comput Sci 13:1182–1197

Authors and Affiliations

Razatulshima Ghazali[1] · Faizura Haneem Mohamed Ali[1] · Hussin Abu Bakar[1] · Mohammad Nazir Ahmad[2] · Nazleeni Samiha Haron[3] · Abdullah Hisam Omar[4] · Ali Ahmadian[5,6]

Razatulshima Ghazali
razatulshima@mampu.gov.my

Faizura Haneem Mohamed Ali
haneem@mampu.gov.my

Hussin Abu Bakar
hussin@mampu.gov.my

Nazleeni Samiha Haron
Nazleeni@utp.edu.my

Abdullah Hisam Omar
abdullahhisham@utm.my

Ali Ahmadian
ali.ahmadian@ukm.edu.my

[1] Malaysian Administrative Modernization and Management Planning Unit (MAMPU), MKN-Embassy Techzone Building, Level 6, Block BJalan Teknokrat 2, 63000 Cyberjaya, Selangor, Malaysia

[2] Institute IR4.0, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia

[3] Centre of Research in Data Science, Universiti Teknologi PETRONAS Universiti Teknologi Petronas, 32610 Bandar Seri Iskandar, Perak, Malaysia

[4] Faculty of Built Environment and Surveying, Universiti Teknologi Malaysia, 81310 Skudai, Johor Bahru, Malaysia

[5] Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia

[6] Department of Mathematics, Near East University, Nicosia, TRNC, Mersin 10, Turkey