Enhanced Security of Iraqi National Card Based on Blockchain Technique

Montadhar Moslem Ashor, Haider M. Al-Mashhadi
Department of Computer Information System, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq.

Article Info

Article history:

Received February 13, 2023
Revised May 19, 2023
Accepted May 31, 2023

Keywords:

Blockchain
Scyther
Schnorr Digital Signature
Formal Security Analysis
Hash Function
Unlinkability

ABSTRACT

Data protection and security is one of the important issues at the present time. Because of the development of methods of data penetration and manipulation, it is necessary to find alternative ways to protect sensitive data from these violations and stored in a secure manner. A complete system has been provided for the purpose of enhanced security for storing Iraqi national cards that issues to the citizens based on the blockchain technology. This study aims to protect the sensitive data of the government from violations by using blockchain technique. The proposed method detects fraud and data alteration and protect the transmitted data between the nodes and the server by encryption the data using Schnorr Digital Signature to guarntie the confidentiality, besides detection of any alter in data stored in nodes by using hash function (SHA 256) to guarantie the integrity of data. The method is evaluation using Scyther to test the security of the traditional method and the proposed method. As a result the proposed method provide high security.

Corresponding Author:

Montadhar Moslem Ashor
Department of Computer Information System, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
Email: montadhar.moslem@gmail.com, itpg.muntadher.moslem@uobasrah.edu.iq

1. INTRODUCTION

Blockchain is a decentralized, immutable ledger that facilitates the tracking of assets and the recording of transactions inside a corporate network [1], [2]. The asset may be physical (a house, a car, money, or a piece of land) or intangible (intellectual property, patents, copyrights, trademarks) [3]. A hash function connects the blocks to one another to create an unbreakable chain [4], [5].

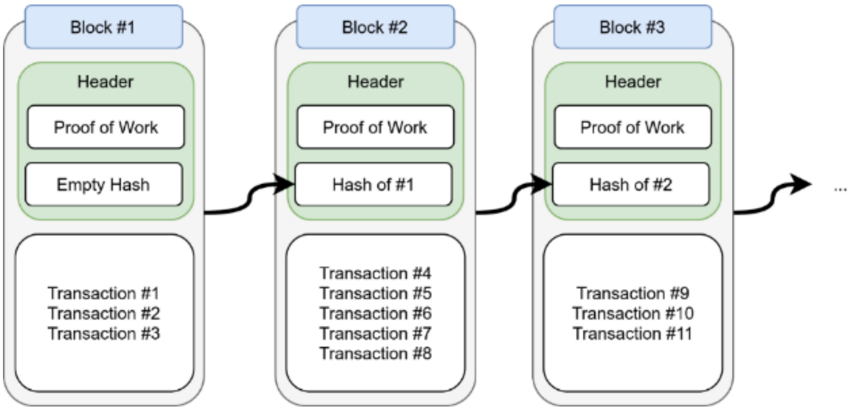


Figure 1. Blockchain general structure

A block is made up of several transactions grouped together and logically organized [6]. A transaction is a record of a specific event (for example, the case of transferring money from one account to the other) [7]–[9]. The block is made of transactions, and according to the type and architecture of the blockchain, their size varies [10]. the first block in the blockchain is called the genesis block, However, Figure (1) shows the general structure of block in the blockchain, which contains the following attributes:

A nonce is a randomly generated number. In several cryptographic operations, a nonce is used to provide replay security, encryption, and authentication. It's used in Proof-of-Work (PoW) consensus algorithms and transaction replay defense on the blockchain [11], [12].

A Merkle root is a hash of all the Merkle tree's nodes. Merkle trees are commonly used to safely and efficiently verify massive data structures [13]. Merkle trees are widely used in the blockchain environment to allow for efficient transaction verification [14].

The timestamp is the time of the block created. It is Unix Time, which means it is the event to records the time when the mining nodes began mining [15]. It’s the value is greater than the timestamp of the previous blocks [16].

A hash function is a function that compresses any length of message into a fixed-length message description. The hash operation has two properties that make it suitable for use on the blockchain [4]. First, Hash(A) = B is irreversible; however, even if B is the product of hashing, it cannot deduce the pre-hash framework A [17].

Block body that contains transactions data [18].

1.1. Traditional system

In traditional systems, data is stored in a MySQL database. As it is known, the database consists of tables, and each table contains columns and fields, and each field has a unique ID. In the case that the attacker gains access to the database in some way and manipulates the stored information, this causes confusion and Inaccuracy in the information. The ability to determine if the database has been manipulated is complicated [19].

2. RELATED WORK

Using a combination of biometric authentication and a blockchain-based strategy, the study suggests a safe national ID card system. The technology is intended to improve national ID card issuance and verification security, privacy, and openness. In addition to implementing a blockchain-based database for storing and verifying ID card data, the authors also provide a detailed description of the proposed system architecture and the technical elements involved, such as the use of facial recognition and fingerprint scanning for biometric authentication. The authors also go over the advantages of the suggested method, including a decrease in identity fraud and an increase in the effectiveness of ID card issuance and verification. The article's conclusion is that governments and organizations all over the world can adopt the suggested system, which can considerably increase the security and dependability of national ID cards [20].

A novel blockchain storage system called "Mystiko" that is based on the Apache Cassandra database was proposed by the authors in [21]. Dealing with huge data is the primary goal. According to reports, Mystiko provides important traits including fast transaction throughput, high scalability, high availability, and other text retrieval properties. Although distributed storages (like Cassendra) can store massive data on blockchain, it has been discovered that these systems require highly capable nodes in the network. Two further works that support this sort of architecture are BigchainDB, which is based on MongoDB [18], and HBasechainDB, which is based on HBase with Hadoop [22].

Recent years have seen blockchain heralded as a breakthrough in corporate technology [23]. Since its debut nine years ago, extensive research in the area has demonstrated its enormous potential in a variety of applications, including new land registries, know your customer (KYC) applications, e-commerce, insurance, supply chain, and many others. The most amazing outcomes have been achieved when blockchains have been utilized to store information, eliminate middlemen, and enable more company collaboration, for instance in regard to data standards. You may find a detailed analysis of blockchain in which covers the technology as well as potential applications and difficulties [24], [25].

presented a distributed access control paradigm for blockchain in the context of massive IoT systems with billions of devices spread out globally [11]. The blockchain-deployed smart contract that defines the access control policy. The insertion of management hub nodes (high computation nodes) and access control manager nodes (low weight nodes) into the network are crucial elements facilitating this distributed access control. Keep in mind that the model only works for private blockchain networks. Determining access control policy for the numerous internet of things (IoT) devices may be a difficult and error-prone operation because nodes can readily join the network on a worldwide scale.

Mobile environments and e-healthcare are two areas where multi-factor authentication is being utilized increasingly often. The one-time password (OTP) and security token are frequently recommended by the financial transaction attendance system [26]. Strong multi-factor authentication techniques, such as face recognition and distinctive hardware identification utilized in city and community street monitoring, have been proposed in a number of research articles. These plans centered on arming the populace with knowledge. They then use the same data to respond to some questions that are used as something you are aware of to take into account the login system [27]. Some techniques with an integrated chip and iris recognition have been proposed in the realm of automated teller machine (ATM) cards as a practical means of authenticating ATM users [28].

3. PRIMITIVE TOOLS

In this study, two tools are used, Schnorr digital signature to improve security and Scyther tool to test the algorithm.

3.1. Schnorr digital signature

Schnorr digital signatures have been presented to reduce the signature size of El-Gamal digital signatures [18], [22]. It is a small, trusted, and really helpful signature generator [17]. The Schnorr algorithm provides three functions:

Consider the following parameters:

p, q, a, x, y, s, v, r
where,
"p": any prime number
"q": factor of p-1
"a": such that a^q = 1 mod p
"s": the secret key or the private key (0<s<q).
"v": the public key = a^-s mod q.

e = H(M || X) where H() is the hash function
y = (r + s * e) mod q

KeyGen Function:

```
Begin
        Step1: select two large prime numbers $p \geq 2^{512}$ and $q \geq 2^{140}$ such that:$(p-1)\ mod\ q = 0$.
        Step2. Choose $g \in \mathbb{Z}_p$ of order $q, g \neq 1$ & $g^q = 1\ mod\ p$
        Step3. Pick $x \in \mathbb{Z}_q$ and $g^x\ mod\ p$.
        Step4. $Private\ key = x$, and $Public\ key = y = g^x\ mod\ p$.
        Step5. The public parts are $(g, p, q, y)$.
End
```

Sign (g, x, M) Function:

```
Begin
        Step6. Choose $k \in \mathbb{Z}$ and set $r = g$.
        Step7. Compute $e = H(r_{P_i} || M)$ and $s = k{+}x{*}e$.
        Step8. Send $Sign_x\ (M) = < M, s, e >$ to the verifier.
End
```

Verify (M, e, s) Function:

```
Begin
        Step9. Set $r' = g^s\ y^{-e}$.
                    $= g^{k+x*e} * g^{-x*e}$.
                    $= g^x$.
        Step10. IF $e \overset{?}{=} H(r' \| M\ )$; is true, the message is accepted; ELSE, it is rejected.
End
```

3.2. Scyther:

A tool for analyzing, falsifying, and verifying security protocols is called Scyther [29]. It is a cutting-edge, freely accessible tool that offers several unique capabilities not found in other tools. Support for multi-protocol research, unbounded verification with guaranteed termination, and an infinite number of sets of traces can be analyzed in terms of patterns are examples of novel features. A graphical user interface (GUI) is offered by the utility in addition to command-line and Python scripting interfaces. Users interested in confirming or comprehending a protocol are the target audience for the GUI. Scyther may be used for extensive protocol verification testing thanks to its scripting and command line interfaces [30].

3.3. The hash function (SHA-256)

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that generates a fixed-length, 256-bit (32-byte) hash value. A hash function is a mathematical algorithm that takes input data of random size and produces a fixed-size output, often called a hash or message digest [31]. The purpose of a hash function is to produce a unique representation of the input data that cannot be reversed or decrypted easily. Hash functions are used for many purposes, including data integrity verification, password storage, digital signatures, and key derivation [32]. SHA-256 is widely used in many security applications, including digital signatures, password storage, and blockchain technology. It has been chosen for its strength, security, and speed in generating hash values [29].

4. PROPOSED SYSTEM

In this section, the blockchain-based system will be introduced. The system consists of three components: administrator (ADM), user data entry (Ui), and online server. Figure 2.

1. Administrator: Which is the government, who is responsible for giving permission and login information to the nodes connected to the network.
2. User Data Entry: which is the node (employee) who responsible for adding new data (blocks).
3. Online Server: It is a server based on blockchain technology to store sensitive data.

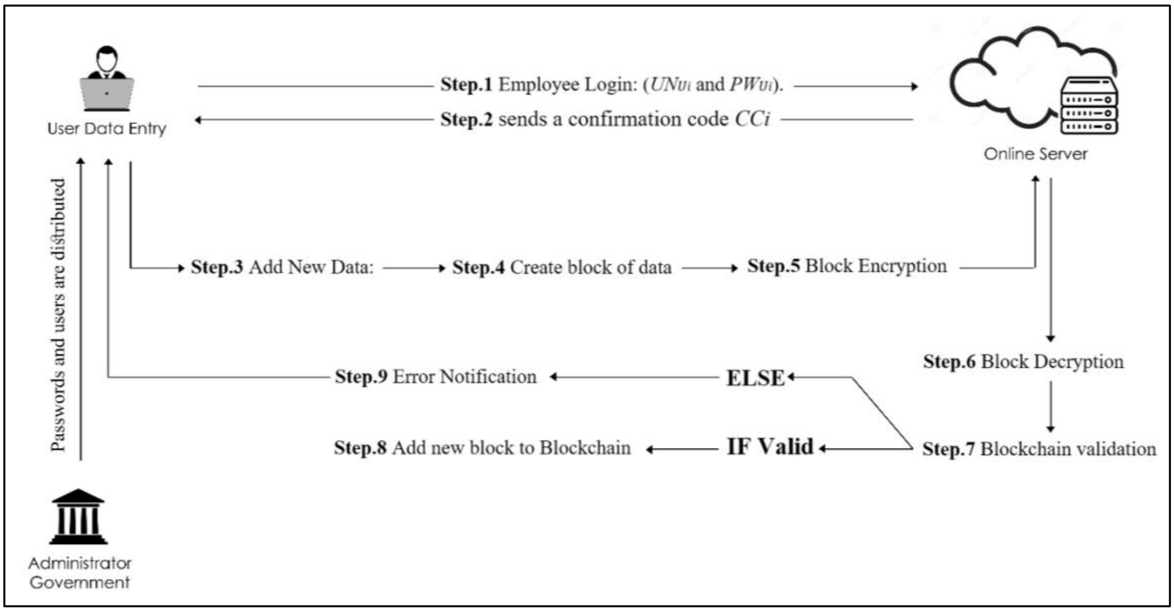

User Data Entry
Step.1 Employee Login: (UNUi and PWUi).
Step.2 sends a confirmation code CCi
Online Server
Passwords and users are distributed
Step.3 Add New Data:
Step.4 Create block of data
Step.5 Block Encryption
Step.6 Block Decryption
Step.9 Error Notification
ELSE
Step.8 Add new block to Blockchain
IF Valid
Step.7 Blockchain validation
Administrator
Government

Figure 2. Proposed system

the concept of blockchain is to distribute the blocks between nodes and initialize a decentralized network structure, this work implements the concept of blockchain on the server side only, so the blocks are stored in the main node (server) with high security because the work using a digital signature to ensure the data confidentiality and hash function to ensure the data integrity. this work is implanted to enhance the security of the traditional system used in this office branch, the next step is to implement this idea on all branches of the government organization and connect all servers with each other, and then can store the blockchain from these servers in all servers and the servers become the nodes of the blockchain network.

The system consists of five phases to perform the task: Blockchain initialization phase, register phase, login phase, user data entry phase, blocking phase. Table 1. represents the notations found in this research.

Table 1. List of notations.

Symbol	Description	Symbol	Description
PR_{Ui}	Private key	$\mathbb{Z}$	Group of positive number
PU_{Ui}	Public key	Rdm	Random number ∈ $\mathbb{Z}$
UN_{Ui}	Username	H	The hash function (SHA-256)
PW_{Ui}	Password	ID_{Ui}	Card id
$H'un$	Hash of username	FN_{Ui}	First name
$H'pw$	Hash of password	SN_{Ui}	Second name
$SDun$	Data content ($H''un$, T , Rdm)	TN_{Ui}	Third name
$SDpw$	Data content ($H''pw$, T , Rdm)	FM_{Ui}	Family name
$STun$	Username stored in the database	MN_{Ui}	Mother name
$STpw$	Password stored in the database	GN_{Ui}	Gender
CC_i	Confirmation code	BT_{Ui}	Blood type
T	Returns the current date and time		

4.1. Blockchain Initialization Phase

In this phase, the system configures the blockchain by creating a flat file type JSON. After that, a GENESIS BLOCK will be created and added to the blockchain. It contains an initial value and it does not have a previous hash. This phase is performed only once.

Then prepare and generate the public and private keys (PR$_{Ui}$, PU$_{Ui}$) by using Schnorr digital signature.

4.2. Register Phase

Passwords and users are distributed to employees by the government (administration) using protected internal methods within the government institution itself.

4.3. Login Phase

For the purpose of logging into the system you need username (UN$_{Ui}$), password (PW$_{Ui}$) and confirmation code. These login data are stored in the database in hash form, and this phase consists of six steps as shown in Figure 3.

Step1: user enters his login information (UN_{Ui} and PW_{Ui}).
Step2: the system will computes the $H'un = H(UN_{Ui})$ and $H'pw = H(PW_{Ui})$.
Step3: computes T=*NOW()* and Rdm=*RANDOM()*
Step4: computes the $H''un = H(H'un \oplus T \oplus Rdm)$ and $H''pw = H(H'pw \oplus T \oplus Rdm)$.
Step5: sends $SDun = (H''un\ ,\ T\ ,\ Rdm)$ and $SDpw = (\ H''pw\ ,\ T\ ,\ Rdm)$ to the server through the internet.
Step6: the server compares the received data with the stored data in database as following:
$H''un \stackrel{?}{=} H(STun \oplus T \oplus Rdm)$ and $H''pw \stackrel{?}{=} H(STpw \oplus T \oplus Rdm)$ if TRUE then sends a confirmation code CCi else display error msg.

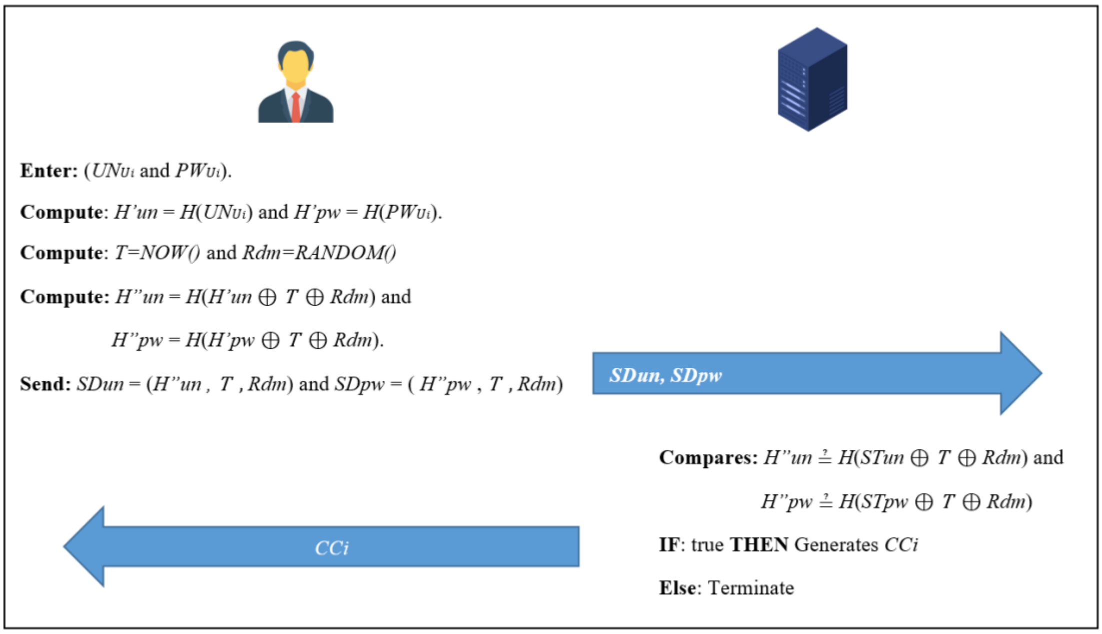

Enter: (UN_{Ui} and PW_{Ui}).
Compute: $H'un = H(UN_{Ui})$ and $H'pw = H(PW_{Ui})$.
Compute: T=NOW() and Rdm=RANDOM()
Compute: $H''un = H(H'un \oplus T \oplus Rdm)$ and
$H''pw = H(H'pw \oplus T \oplus Rdm)$.
Send: $SDun = (H''un , T , Rdm)$ and $SDpw = (H''pw , T , Rdm)$
SDun, SDpw
Compares: $H''un \overset{?}{=} H(STun \oplus T \oplus Rdm)$ and
$H''pw \overset{?}{=} H(STpw \oplus T \oplus Rdm)$
IF: true THEN Generates CCi
Else: Terminate
CCi

Figure 3. Login Phase

4.4. User data entry phase (Ui).

In order to add new data to the system, a graphical user interface exist, programed based on python language. It accepts the following input: card id (IDUi), first name (FNUi), second name (SNUi), third name (TNUi), family name (FMUi), mother name (MNUi), gender (GNUi), blood type (BTUi). There is also data that is not entered by the user, but rather that is generated from the system such as the index, timestamp, miner, proof, current hash and previous hash.

4.5. Blocking phase

After the employee entering the required information and submit it, the system will create block of data, then encrypt this block with the public key generated by server, and send it to the server through the internet. Then the server reseve the block and dycrpt it. Then the server checks the validity of the blockchain. To check if the data has been modified, whether it has been updated or part of it has been deleted. For carrying out this verification, the system makes a trace for each block of the blockchain. The hash function is executed on the information of the first block and it is compared with the "previous hash" value in the next block, and so on until we reach the last block. If all the comparison is correct, it means that the blockchain has not been tampered with and all the information in the blockchain is correct. Else if the comparison in any part of the process is wrong, this means that there is a fault and at least one or more values have been changed. After the validation of the blockchain, the block can added to the blockchain.

5. SECURITY ANALYSIS

5.1. Login in traditional system.

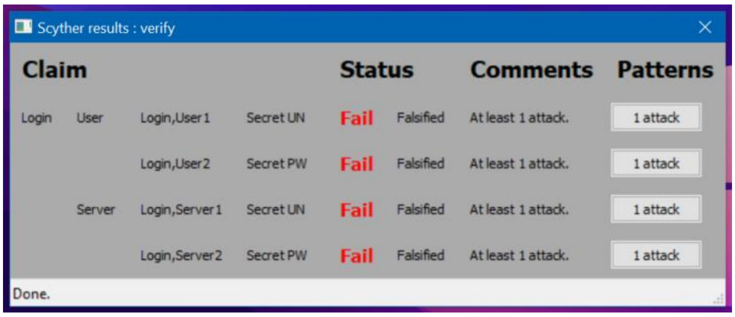
In the traditional system, the user enters a username and password and then submits the request, this data send to the server as plain text without encryption. The server in his role will take these data and compare it with the username and password stored in the database as plain text also. In this case, the attacker can claim the data or fake it and redirect it to the server. Thus, the attacker can enter the system using the obtained data, as shown in figure 4,5.

Scther program was used to test the login process in the traditional system, which sends data without encryption.

```
usertype UN,PW;
protocol Login(User,Server) {

  role User {
    send_1(User, Server, UN, PW);
    claim_User1(User, Secret, UN);
    claim_User1(User, Secret, PW);
  }
```

```
   role Server {
      recv_1(User, Server, UN, PW);
      claim_Server1(Server, Secret, UN);
      claim_Server1(Server, Secret, PW);
   }
}
```



Claim				Status		Comments	Patterns
Login	User	Login,User1	Secret UN	Fail	Falsified	At least 1 attack.	1 attack
		Login,User2	Secret PW	Fail	Falsified	At least 1 attack.	1 attack
	Server	Login,Server1	Secret UN	Fail	Falsified	At least 1 attack.	1 attack
		Login,Server2	Secret PW	Fail	Falsified	At least 1 attack.	1 attack

Done.

Figure 4: Scyther results.

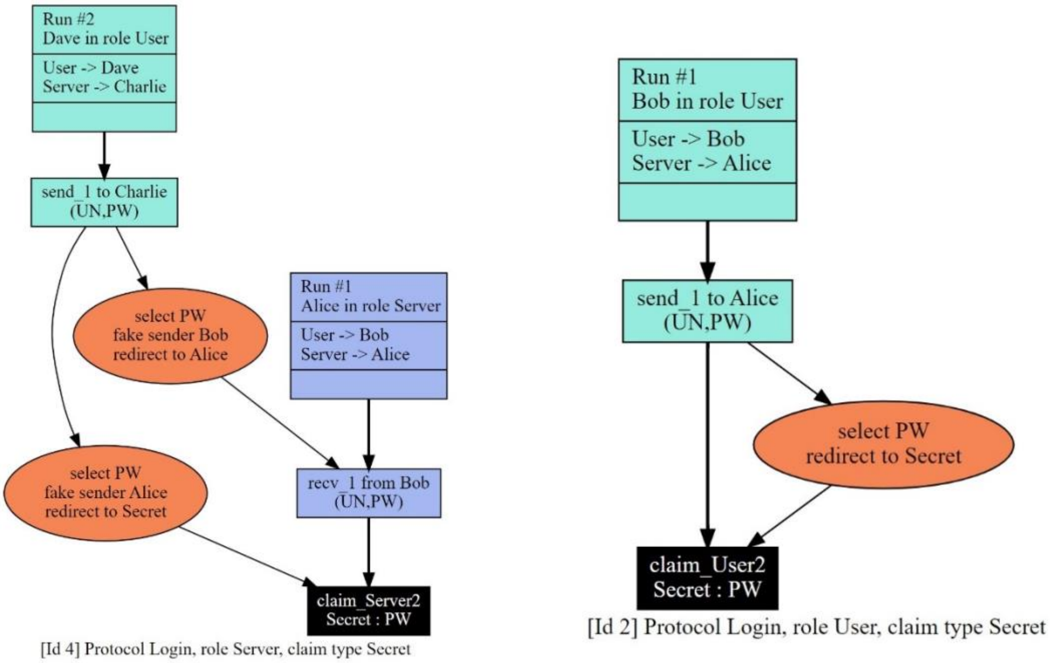
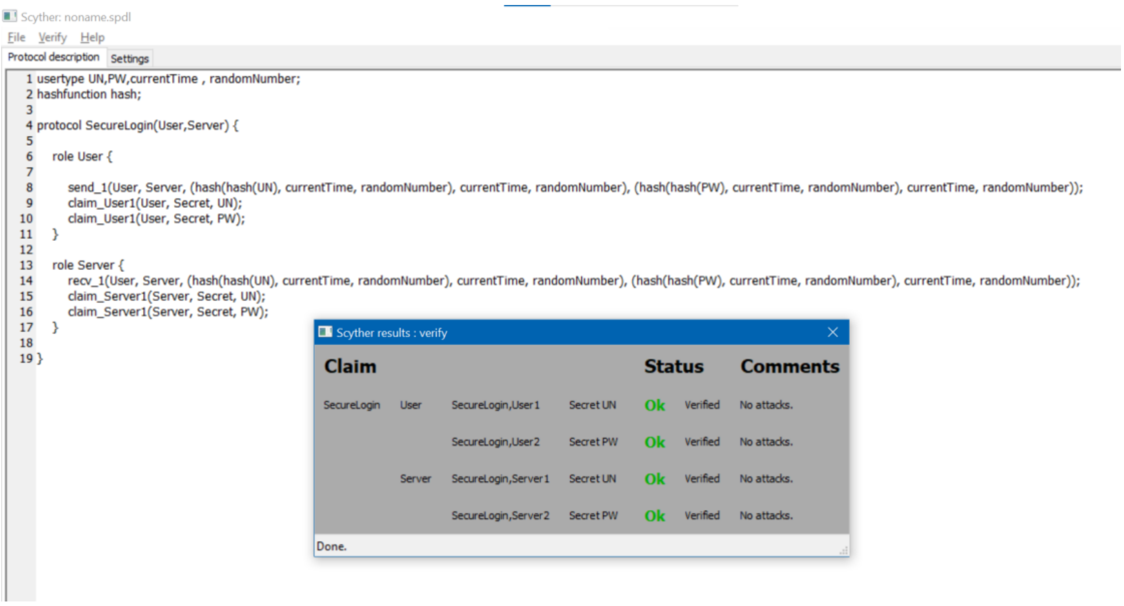


Figure 5: weakness of the traditional system

5.2. Login in the proposed system (Unlinkability).

In the proposed system, random variables, T and Rdm, were used. This feature focuses on preventing Attacker from detecting Node that has logged previously or not. We applied to feature in the proposed system by changing the values (Rdm, T) each time Node attempts to login. Consequently, Attacker cannot link different logins with the same Node, Since these variables cannot be repeated with a new login process. as shown in figure 6.

This means that every time you login to the system, a new hash will be obtained, even if the same user logged into the system.



```
usertype UN,PW,currentTime , randomNumber;
hashfunction hash;

protocol SecureLogin(User,Server) {

   role User {

      send_1(User, Server, (hash(hash(UN), currentTime, randomNumber), currentTime, randomNumber), (hash(hash(PW), currentTime, randomNumber), currentTime, randomNumber));
      claim_User1(User, Secret, UN);
      claim_User1(User, Secret, PW);
   }

   role Server {
      recv_1(User, Server, (hash(hash(UN), currentTime, randomNumber), currentTime, randomNumber), (hash(hash(PW), currentTime, randomNumber), currentTime, randomNumber));
      claim_Server1(Server, Secret, UN);
      claim_Server1(Server, Secret, PW);
   }

}
```

```
Claim                                                          Status       Comments
SecureLogin   User     SecureLogin,User1     Secret UN    Ok   Verified     No attacks.
                       SecureLogin,User2     Secret PW    Ok   Verified     No attacks.
              Server   SecureLogin,Server1   Secret UN    Ok   Verified     No attacks.
                       SecureLogin,Server2   Secret PW    Ok   Verified     No attacks.
Done.
```

Figure 6: strength in the proposed algorithm

5.3. Attack resistance

In a traditional database, each field is unique and not related to other fields in the database. In this case, it is possible to attack the database and modify some information without knowing which fields have been tampered with, because there is no way to show that.

In this proposed system, a blockchain was used, and in this case, each field present in the blockchain is associated with the field before and after it. Therefore any change that takes place in any information will be exposed through the blockchain validation process, thus illegal modifications that take place on the data will be identified. And knowing whether the data has been modified or not.

6. CONCLUSION

Security concerns is key roadblocks to large-scale government system implementations. A system based on the blockchain was proposed for the purpose of storing and protecting sensitive government data. Encryption algorithms SHA-256 and Schnorr digital signature are used to increase the security of data sent from the node to the server. The work can be developed in future works, and all the features of the blockchain are used for the purpose of increasing the security and complexity of the proposed system. After comparing the proposed system with traditional systems using the Scyther tool, we found that the data transmission process is done in a secure and encrypted way.

REFERENCES

[1] M. Banerjee, J. Lee, and K.-K. R. Choo, “A blockchain future for internet of things security: a position paper,” *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, Aug. 2018, doi: 10.1016/j.dcan.2017.10.006.

[2] S. Li, H. Xiao, H. Wang, T. Wang, J. Qiao, and S. Liu, “Blockchain Dividing Based on Node Community Clustering in Intelligent Manufacturing CPS,” in *2019 IEEE International Conference on Blockchain (Blockchain)*, IEEE, Jul. 2019, pp. 124–131. doi: 10.1109/Blockchain.2019.00025.

[3] L. Hughes, Y. K. Dwivedi, S. K. Misra, N. P. Rana, V. Raghavan, and V. Akella, “Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda,” *Int J Inf Manage*, vol. 49, pp. 114–129, Dec. 2019, doi: 10.1016/j.ijinfomgt.2019.02.005.

[4] I.-C. Lin and T.-C. Liao, “A survey of blockchain security issues and challenges,” *International Journal of Network Security*, vol. 19, pp. 653–659, Sep. 2017, doi: 10.6633/IJNS.201709.19(5).01.

[5] X. Yang, J. Liu, and X. Li, “Research and Analysis of Blockchain Data,” *J Phys Conf Ser*, vol. 1237, no. 2, p. 022084, Jun. 2019, doi: 10.1088/1742-6596/1237/2/022084.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in *2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[7] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems,” *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 6–14, Jul. 2018, doi: 10.1109/MCE.2018.2816299.

[8] S. Shahriar Hazari and Q. H. Mahmoud, “Improving Transaction Speed and Scalability of Blockchain Systems via Parallel Proof of Work,” *Future Internet*, vol. 12, no. 8, p. 125, Jul. 2020, doi: 10.3390/fi12080125.

[9] M. Majid *et al.*, “Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review,” *Sensors*, vol. 22, no. 6, p. 2087, Mar. 2022, doi: 10.3390/s22062087.

[10] A. A. Monrat, O. Schelen, and K. Andersson, “A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities,” *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

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

[12] Y. Ma, Y. Sun, Y. Lei, N. Qin, and J. Lu, “A survey of blockchain technology on security, privacy, and trust in crowdsourcing services,” *World Wide Web*, vol. 23, no. 1, pp. 393–419, Jan. 2020, doi: 10.1007/s11280-019-00735-4.

[13] M. Bartlomiejczyk, E. F. Imed, and M. Kurkowski, “Multifactor Authentication Protocol in a Mobile Environment,” *IEEE Access*, vol. 7, pp. 157185–157199, 2019, doi: 10.1109/ACCESS.2019.2948922.

[14] B. Adanur, B. Bakir-Gungor, and A. Soran, “Blockchain-based Fog Computing Applications in Healthcare,” in *2020 28th Signal Processing and Communications Applications Conference (SIU)*, IEEE, Oct. 2020, pp. 1–4. doi: 10.1109/SIU49456.2020.9302168.

[15] A. Ullah, H. Xiao, and T. Barker, “A Multi-factor Authentication Method for Security of Online Examinations,” 2019, pp. 131–138. doi: 10.1007/978-3-030-05928-6_13.

[16] N. A. K. Abiew, M. D. Jnr., and S. O. Banning, “Design and Implementation of Cost Effective Multi-factor Authentication Framework for ATM Systems,” *Asian Journal of Research in Computer Science*, pp. 7–20, Apr. 2020, doi: 10.9734/ajrcos/2020/v5i330135.

[17] C. P. Schnorr, “Efficient signature generation by smart cards,” *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, Jan. 1991, doi: 10.1007/BF00196725.

[18] M. J. Amiri, D. Agrawal, and A. El Abbadi, “SharPer: Sharding Permissioned Blockchains Over Network Clusters,” in *Proceedings of the 2021 International Conference on Management of Data*, New York, NY, USA: ACM, Jun. 2021, pp. 76–88. doi: 10.1145/3448016.3452807.

[19] A. Kayode, A. Y., A. A., and O. S., “Multi-Factor Authentication Model for Integrating Iris Recognition into an Automated Teller Machine,” *Int J Comput Appl*, vol. 181, no. 45, pp. 1–8, Mar. 2019, doi: 10.5120/ijca2019918530.

[20] P. Datta, A. Bhowmik, A. Shome, and M. Biswas, “A Secured Smart National Identity Card Management Design using Blockchain,” in *2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*, IEEE, Nov. 2020, pp. 291–296. doi: 10.1109/ICAICT51780.2020.9333487.

[21] N. M.Hamza, S. Ouf, and I. M.El-Henawy, “A Proposed Technique for Enhancing the Mining Process in Blockchain Architecture,” in *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, IEEE, Mar. 2020, pp. 7–12. doi: 10.1109/ICCMC48092.2020.ICCMC-0002.

[22] W. Hao *et al.*, “BlockP2P: Enabling Fast Blockchain Broadcast with Scalable Peer-to-Peer Network Topology,” 2019, pp. 223–237. doi: 10.1007/978-3-030-19223-5_16.

[23] S. Sahoo, A. M. Fajge, R. Halder, and A. Cortesi, “A Hierarchical and Abstraction-Based Blockchain Model,” *Applied Sciences*, vol. 9, no. 11, p. 2343, Jun. 2019, doi: 10.3390/app9112343.

[24] P. Esteva *et al.*, *A Survey of Blockchain Technologies for Open Innovation*. 2017.

[25] J. Golosova and A. Romanovs, “The Advantages and Disadvantages of the Blockchain Technology,” in *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, IEEE, Nov. 2018, pp. 1–6. doi: 10.1109/AIEEE.2018.8592253.

[26] D. Vujicic, D. Jagodic, and S. Randic, “Blockchain technology, bitcoin, and Ethereum: A brief overview,” in *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, IEEE, Mar. 2018, pp. 1–6. doi: 10.1109/INFOTEH.2018.8345547.

[27] M. F. sallal, G. Owenson, and M. Adda, “Proximity Awareness Approach to Enhance Propagation Delay on the Bitcoin Peer-to-Peer Network,” in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, IEEE, Jun. 2017, pp. 2411–2416. doi: 10.1109/ICDCS.2017.53.

[28] S. S. Hazari and Q. H. Mahmoud, “A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems,” in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2019, pp. 0916–0921. doi: 10.1109/CCWC.2019.8666535.

[29] M. Fareed and A. A. Yassin, “Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system,” *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 4, pp. 2131–2141, Aug. 2022, doi: 10.11591/eei.v11i4.3658.

[30] M. Alzuwaini and A. Yassin, “An Efficient Mechanism to Prevent the Phishing Attacks,” *Iraqi Journal for Electrical and Electronic Engineering*, vol. 17, no. 1, pp. 1–11, Jun. 2021, doi: 10.37917/ijeee.17.1.15.

[31] S. ALahmed, “Internet of Things Based Blockchain Technology for Gas Station,” *Iraqi Journal of Intelligent Computing and Informatics (IJICI)*, vol. 1, no. 2, pp. 86–96, Dec. 2022, doi: 10.52940/ijici.v1i2.17.

[32] A. J. Al-Musharaf, S. M. Al-Alak, and H. M. Al-Mashhadi, “Improving Blockchain Consensus Mechanism via Network Clusters,” in *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, IEEE, Apr. 2021, pp. 293–298. doi: 10.1109/BICITS51482.2021.9509882.