Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 01
Pages: 45-54
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.1.005

SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN

Dr. V. Suma,

Professor, Department of Information Science & Engineering,

Dayananda Sagar College of Engineering, Bangalore, India.

E-mail id: suma-ise@dayanandasagar.edu

Abstract: Block chain being a foundational technology impacting and attracting a wide range of applications has become predominant in solving the problem of privacy preserving and security in multitude sectors that is under the control of the government and the private. The paper also presents the security and the privacy mechanism using the block chain to prevent the misuse and the corruption in the sharing of huge set of data generated from the judiciary, security, legislature, commercial code registries etc. The proposed system enables reliability and the trust in the data sharing in the communication channels utilizing the block chain with the RSA digital signature. The proposed system is simulated as a java programming version to evince the enhancement in the latency in the sharing of the information's along with the privacy and the security.

Keywords: Block chain technology, security, privacy, data sharing, and latency.

1. INTRODUCTION

The latest developments in the information technology has led to a huge flow of information's and the enormous valuable data contained in it this makes them to be engrossed and prone to the cyber-attacks causing the hacking and the modification of the valuable data's [2] The constant progress in the block chain technology has made it more and more attractive among a wide range of applications such as the bank transactions, intelligent systems, internet of things based applications , government sectors, industrial sectors etc. for the prevention of the unknown attacks and the hacking of the privacy information [1]. Joshi et al present the block chaining as the "gaining traction" and one of the predominant necessity in the today's world. He also mentions that the utilization of the blockchain would warranty a "reliable and a convenient services" [3], Singh et al, say that the trustworthiness and the reliability of the blockchain technology has made it a back bone of the data sharing in the communications channels, enhancing the accuracy and the trust in it [4] most of the applications are urged to adopt to the block technology as it improves the privacy-preserving of the personal information's [5] vitalik butterin defines the block chain technology as the " the magic computer that anyone can upload program to and leave it to self –execute , where the prevailing and the previous state of the each program is openly observable and conveys a very strong crypto economically protected assurance that the databases running on the chain will continue to fulfill in exactly the way the blockchain protocol specifies”[7]. Remaining as a heart of the bit coin, and the other currencies that are virtual the block chain behaves to be open and a distributed ledger that could enable the transactions between the two people to be permanently recordable with the capability of being verified [8]. The fig.1 below shows the general block chain architecture used in the transactions.

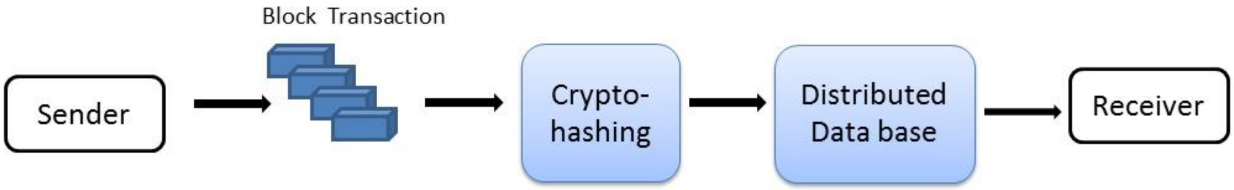


Fig .1 Processes Involved in Block Chain

So the block chain in simple can be referred as the time-stamped series of the unchangeable information managed by a group of computers that are owned by multiple entities. Every block of data are protected and made inevitable utilizing the cryptographic principles to ensure the safety of the information or the currency. The block chain initially utilized only in the amount transactions is now utilized in the communication channels to improve the reliability and the trust in the data sharing.

So the paper proposes the reliable and a trust worthy data sharing in the huge set of data generated from the judiciary, military, legislature, commercial code registries etc. utilizing the block chain and the RSA Digital signature , for securing the data transmission form the misuse and the hacks.

The paper is at the rest is organized with the related work in the section 2, proposed work in the section 3, result evaluation in the section 4 and conclusion in the section 5.

2. RELATED WORKS

Ji,et al [1] the paper presenting the comprehensive study of the issues in the protection of the private information's such as the bank transactions handled, voting systems, the IOT, systems that are intelligent and in the sharing of personal information's and summarizes the technologies bas d on the block chain for the privacy protection. Sang-Oun et al [2], the author discusses the privacy issues in the connected vehicles and the presents the review of the block chain based privacy protection. Joshi et al [3], paper details the technical aspect sand the applications of the blockchain as the comprehensive survey. Singh et al [4], discusses the block chain as the trustable and reliable technology for the sharing of data among the intelligent vehicle. Zhang et al [5] proposes a dual block chain system based on the privacy and the consortium in the sharing of the e-health information's , Casino et al [6], the systematic literature review based on the block chain applications is presented in the paper with the short coming s and the limitations of the block chain technology. Pilkington et al [7], the author elaborates the core concepts, the principles and the cutting edge applications that rely on the block chain technology for the reliability, security and privacy. Iansiti et al [8], the author proposes the truth in the block chain technology improving the economic and the social systems. Xu et al [9] presents the taxonomy of the block chain technology. Zheng et al [10], presents the challenges in the block chain in terms of the scalability and the storage Lin et al [11], the proposal explains the authentication in the block chain using the ID- based linearly Homomorphic signature strategy. Xu, et al [12] the biometric block chain for data sharing in the intelligent vehicle is proffered in the paper to build trust and the reliability in the peer to peer networks. Smys et al [13] details the cryptography based architecture for the peer-peer networks.

3. BLOCK CHAIN POTENTIALS

The block chain technology that is seated at the head of the internet is the peer –peer network .This block chain could be termed as the foundational technology, leading to the revolution of the business and the government. It is capable of developing a new foundation for the economic and the social systems. The world with the block chain could be envisioned as embedded into a digital code with transparency to all but with the security from damaging, removal and modification. The massive capability of the block chain technology has made it possible to retaining a digital record of the each movement of the each and every agreement that is made the transaction that has taken place and the every work that is done with a signature in order to identify, store, validate and share. The block chain technology ensures the communication at ease between the organizations, machines, individuals and the protocols with minute chafing eluding the mediators such as the lawyers, bankers and the brokers[8]. The reason behind the attractive ness towards the block chain is making the files hard to replicate, with damage proof and modification. The features that make them more prominent are listed as follows.

Transparency: Block chain enables to view all the data that is entered into it

Decentralization: The data and the nodes processing the data in the block chain belongs to multiple entities

Immutability: Restricts the tampering of the data using the hash functions.

3.1. RSA DIGITAL SIGNATURE

The RSA (Rivest, Shamir, and Adelman) digital signature could be utilized in constructing a digital signature strategy applying a public verification (V) key and a private signing (S) key. This could be represented using the equation (1)

$$S(mes, Key) = RSA\ (mes, Key)\ and\ V(mes, S, Key) = RSA\ (S, K) == mes \tag{1}$$

The message (mes) to be transmitted is signed applying a RSA with the private key ($Private_{key}$) and further sealed using the public key ($Public_{Key}$) and enumerates whether the results exact the message that is expected. This method could at certain times result with the lengthier keys. This problem could be solved utilizing the cryptographic hashes as shown in the equation (2)

$$S(mes, key) = RSA(hash(mes), key) and\ the\ V(mes, S, key) = RSA(S, key) = hash(mes) \tag{2}$$

The general RSA digital signature Scheme is as shown in the equation (3)

$$\begin{gathered} Encrypt(mes, key) = RSA(mes, key) \\ Decrypt(hash, key) = RSA\ (hash, key) \\ S(mes, key) = RSA(mes, key) \\ V(mes, S, key) = RSA(S, key) = m \end{gathered} \tag{3}$$

In case of the real world application, the signing does the hash function and the decryption does the post-processing, in case of the signature the hash function is applied initially followed by the RSA function, and in case of the decryption. The RSA function is initially applied followed by the post processing. The RSA signing resemble the

RSA decryption as they include RSA with the private key and the RSA verification resemble the RSA encryption as they include the RSA function with the public key.

3.2. THE BLOCK CHAIN AND THE RSA DIGITAL SIGNATURE IN DATA SHARING

The proposed method aiming to reduce the misuse and the hacks in the data sharing of the information's among a huge set of data produced from the judiciary, security, legislature, commercial code registries etc. puts forward the blockchain with the RSA digital signature to enhance the confidentiality along with the integrity and the authentication in the sharing of the information's. The block without the digital signature ensures the confidentiality of the messages but not the authentication as shown in the fig. 2 consider a person a sending a message to person b, using the block chain the data is hashed and send to the receiver sealing with the private key of the A and in the receiver side apart from B, other members such as the C and D could also view the message as all would have the public key of the A, this is represented in the fig.2

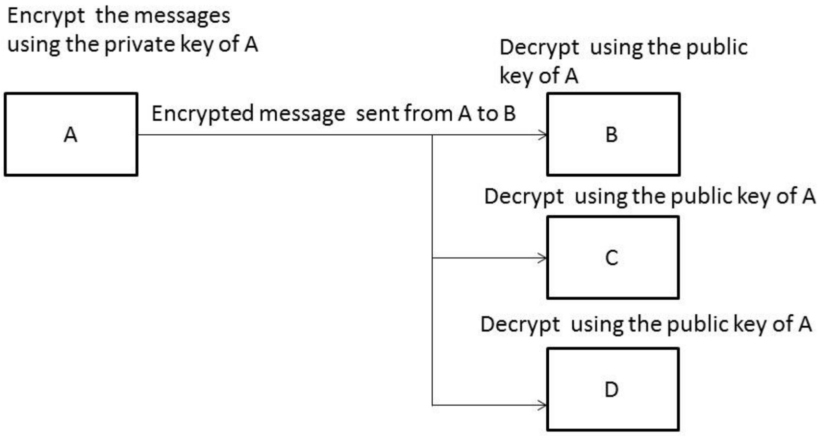

Encrypt the messages using the private key of A
A
Encrypted message sent from A to B
Decrypt using the public key of A
B
Decrypt using the public key of A
C
Decrypt using the public key of A
D

Fig.2 Block chain with Cryptography

Instead the Block Chain with the digital signature would ensure the authentication of the messages transmitted to the communication channel as the message send by the a would be encrypted initially using the private key of the A and once again encrypted utilizing the public key of the B now the information is transmitted and in the receiver side the

B decrypts the message using its private key and once again decrypts using the public key of the A. thus ensuring the confidentiality and the authentication in the message transmitted. The fig .3 below shows the Block Chain with the digital signature. The proposed method utilizing the block chain with the RSA digital signature and the cryptography hashes ensures the data sharing of the judiciary, security, and legislature, commercial code registries in a secured way preserving the confidentiality of the data and with the assurance of transmitting the data to the authorized persons. The fig.3 below shows the Bock chain with the RSA digital signature.

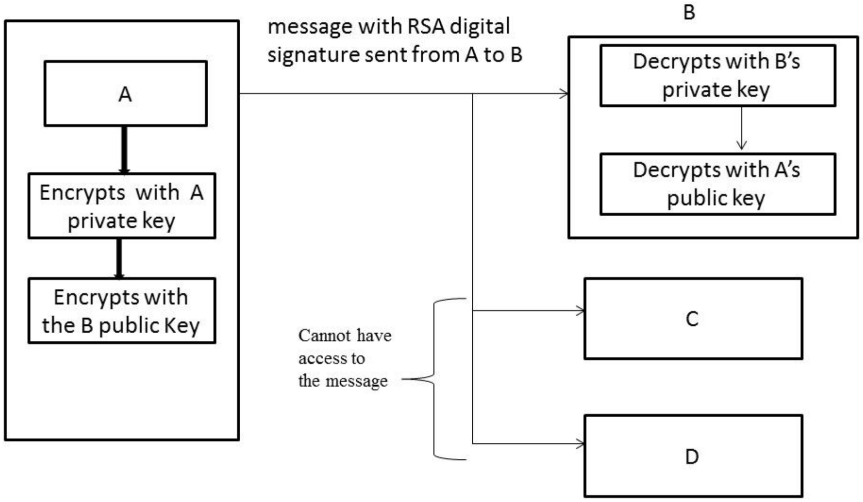
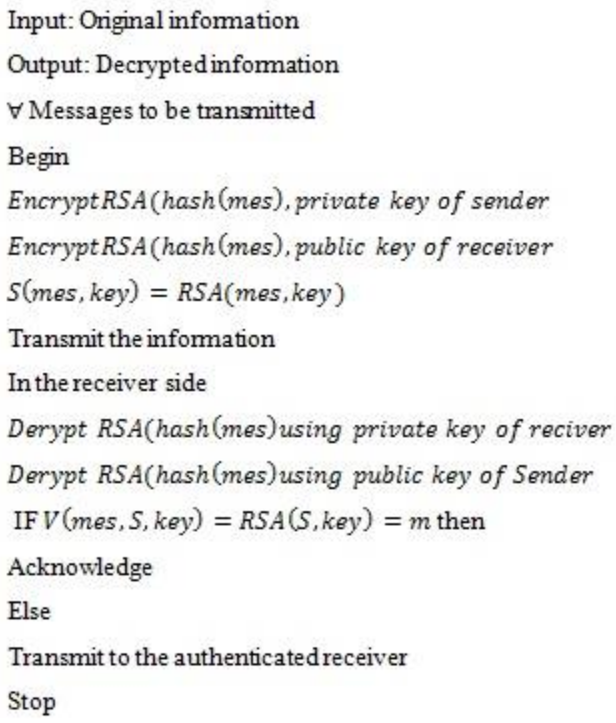

A
Encrypts with A private key
Encrypts with the B public Key
message with RSA digital signature sent from A to B
B
Decrypts with B's private key
Decrypts with A's public key
Cannot have access to the message
C
D

Fig.3 Block Chain with RSA Digital Signature

The algorithm shown below explains the steps in the proposed method of data sharing preserving the confidentiality and ensuring authentication utilizing the block chain with the RSA Digital Signature. The fig.4 below shows the algorithm of the proposed method using the Rivest, Shamir, and Adelman digital signature to ensure the message is decoded at the appropriate receiver end.



```
Input: Original information
Output: Decrypted information
∀ Messages to be transmitted
Begin
$Encrypt RSA(hash(mes), private\ key\ of\ sender$
$Encrypt RSA(hash(mes), public\ key\ of\ receiver$
$S(mes, key) = RSA(mes, key)$
Transmit the information
In the receiver side
$Derypt\ RSA(hash(mes) using\ private\ key\ of\ reciver$
$Derypt\ RSA(hash(mes) using\ public\ key\ of\ Sender$
 IF $V(mes, S, key) = RSA(S, key) = m$ then
Acknowledge
Else
Transmit to the authenticated receiver
Stop
```

Fig .4 RSA Digital Signatures for Confidential and Authenticated Data Sharing

The method describing the block chain with the RSA digital signature enables the data sharing in the judiciary, military and the legislature to be confidential and authenticated retaining the integrity of the messages. The RSA digital signature applied with the hashed cryptographies enables to have a precise size of the information to be transmitted eluding the lengthier data transmission.

4. RESULTS AND DISCUSSION

The Block Chain with the RSA digital signature is validated to evince its performance using the java programming version. The proffered method utilizing the digital signature along with the RSA enables the confidentiality and the authentication for the users. The evaluation of the proffered method done to ensure the performance enhancement in terms of the average cost, time along with security provisioning that enhances the confidentiality and the authentication in the communication channels. The table.1below shows the average time and the cost of the transmission of the messages using the proposed method for the message of varying sizes. Comparison of the results with the block chain without digital signature shown in the table ensures that the proffered method is has an enhanced performance in terms of the time and cost.

Packet size (bytes)	Average Time(ms)		Average Cost%	
	Block Chain with RSA-DS	Block Chain Without RSA-DS	Block Chain with RSA-DS	Block Chain Without RSA-DS
512	18.022	20.345	45	48
1024	18.213	21.320	52	57
5120	18.524	22.089	54	59
10240	18.552	22.554	56	62

Table.1 Comparison of Time and the Cost of Transmission

The fig.5 below shows the security provisioned by the block chain with the digital signature method, and the block chain without the digital signature, the results acquired shows that the proposed method has a highest security provisioning compared to the block chain without the digital signature.

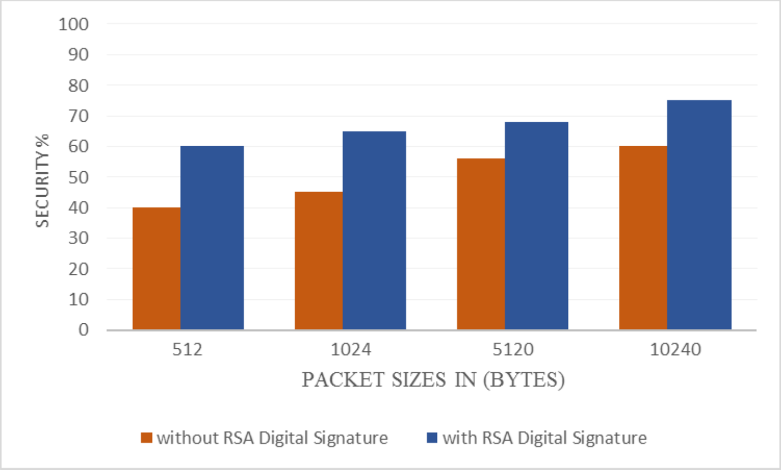


Fig. 5 Security Provision in Data Sharing

5. CONCLUSION

The proposed method utilizing the block chain with the digital signature ensures effective data transmission with confidentiality and authentication. By engaging the RSA digital signature with the block chain, a dual encryption method is followed using the private key of the sender and the public key of the receiver, thus allowing only the authorized receiver to access the information. The performance evaluation of the proffered method evinces its performance enhancements in terms of the time, cost and the security provisioning provided with better confidentiality and authentication eluding the unauthorized access causing the misuse and hacks.

References

[1] Ji, Haoyu, and He Xu. "A Review of Applying Blockchain Technology for Privacy Protection." In *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 664-674. Springer, Cham, 2019.

[2] Sang-Oun, L. E. E., J. U. N. G. Hyunseok, and Bosuk Han. "Security Assured Vehicle Data Collection Platform by Blockchain: Service Provider's Perspective." In *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 265-268. IEEE, 2019.

[3] Joshi, Archana Prashanth, Meng Han, and Yan Wang. "A survey on security and privacy issues of blockchain technology." *Mathematical Foundations of Computing* 1, no. 2 (2018): 121-147.

[4] Singh, Madhusudan, and Shiho Kim. "Blockchain based intelligent vehicle data sharing framework." *arXiv preprint arXiv:1708.09721* (2017).

[5] Zhang, Aiqing, and Xiaodong Lin. "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain." *Journal of medical systems* 42, no. 8 (2018): 140.

[6] Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: current status, classification and open issues." *Telematics and Informatics* (2018).

[7] Pilkington, Marc. "11 Blockchain technology: principles and applications." *Research handbook on digital transformations* 225 (2016).

[8] Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." *Harvard Business Review* 95, no. 1 (2017): 118-127.

[9] Xu, Xiwei, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. "A taxonomy of blockchain-based systems for architecture design." In *2017 IEEE International Conference on Software Architecture (ICSA)*, pp. 243-252. IEEE, 2017.

[10] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." *International Journal of Web and Grid Services* 14, no. 4 (2018): 352-375.

[11] Lin, Qun, Hongyang Yan, Zhengan Huang, Wenbin Chen, Jian Shen, and Yi Tang. "An ID-based linearly homomorphic signature scheme and its application in blockchain." *IEEE Access* 6 (2018): 20632-20640.

[12] Xu, Bing, Tobechukwu Agbele, Qiang Ni, and Richard Jiang. "Biometric Blockchain: A Secure Solution for Intelligent Vehicle Data Sharing." *arXiv preprint arXiv:1909.06369* (2019).

[13] Sridhar, S., and S. Smys. "Intelligent security framework for iot devices cryptography based end-to-end security architecture." In *2017 International Conference on Inventive Systems and Control (ICISC)*, pp. 1-5. IEEE, 2017