International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 7th Sept 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 10

DOI: 10.48047/IJIEMR/V11/ISSUE 10/02

Title **IMPLEMENTATION OF SECURE AUTHENTICATION PROTOCOL USING BLOCKCHAIN IN EDGE AND IOT ENVIRONMENT**

Volume 11, ISSUE 10, Pages: 9-15

Paper Authors
Mr. B. Samuel john peter, Ms. A. Sivasree, Mr. K. Durga Prasad, Mr. M. Vengal Rao, Mr. P. Poornachandra

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IMPLEMENTATION OF SECURE AUTHENTICATION PROTOCOLUSING BLOCKCHAIN IN EDGE AND IOT ENVIRONMENT

[1] Mr. B. Samuel john peter, [2]Ms. A. Sivasree, [3]Mr. K. Durga Prasad, [4]Mr. M. Vengal Rao, [5]Mr. P. Poornachandra

[1]Assistant Professor, Department of Master of Computer Applications,Narayana Engineering College,Nellore,Andhra Pradesh, INDIA.

[2,3,4,5]PG Scholar, Department of Master of Computer Apllications,Narayana Engineering College,Nellore,Andhra Pradesh, INDIA.

Abstract— Authentication is the first entrance to kinds of information systems; however, traditional centered single-side authentication is weak and fragile, which has security risk of single-side failure or breakdown caused by outside attacks or internal cheating. In this paper, we proposed a blockchain-based decentralized authentication modeling scheme (named BlockAuth) in edge and IoT environment to provide a more secure, reliable and strong fault tolerance novel solution, in which each edge device is regarded as a node to form a blockchain network. Blockchain has promise as an approach to developing systems for a number of applications within cyber security. In Blockchain-based systems, data and authority can be distributed, and transparent and reliable transaction ledgers created. Some of the key advantages of Blockchain for cyber security applications are in conflict with privacy properties, yet many of the potential applications have complex requirements for privacy. Privacy- enabling approaches for Blockchain have been introduced, such as private Blockchains, and methods for enabling parties to act pseudonymously, but it is as yet unclear which approachesare suitable in which applications.

Keywords – Block chain, cyber security, IOT.

1. INTRODUCTION

A blockchain is a growing list of records, called blocks, that are linked together usingcryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). As one of the most important entrances to kinds of information systems, authentication plays a prominent role in information system protection, which ensures the right user have access to the right system with the right identity [1-2]. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks. Blockchains are typically managed by a peer-to-peer network for use as a publicly distributed ledger, where nodes collectively adhere to a protocol to communicate and validate new blocks. Although blockchain records are not unalterable as forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. The blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. If the domain name holder loses access to these keys, or key disclosure occurs, the browser will reject the link, and the customer will not be able to access the website[10-11].The bitcoin design has inspired other applications and blockchains that are readable by the public and are widely used by cryptocurrencies. As the basic architecture of the digital certificate, Public Key Infrastructure(PKI) provides identity establishment and authentication mechanism in the network through digital certificates management, which allows users to use encryption, decryption technology and digital signature technology in various application scenarios easily[1-3,7-9]. Biometric-based identification technology has many advantages over traditional identity authentication, for example, confidentiality, convenience, good anti-counterfeiting performance, not easy to forge or steal, carry around and use anytime and anywhere. However, the collection of biometric information is difficult. If the information is not encrypted, it may cause the leakage of private information[4-10]. Since 2008, blockchain technologies[12-13] entered the public's vision with its unique characteristics of high transparency, decentralization, security and reliability. Up to now, many scholars have conducted in-depth research on the technology and security of blockchain[14-17].

2. LITERATURE SURVEY

There are many solutions to the problem of identity authentication technologies such as password-based authentication, certificate-based identity management, and finger-based access control or face-recognition-based authentications, upon which certificate transparency (CT) detects fraudulent certificates by forcing certificates issued by the certification center to be attached to the certificate transparency log. Another method is public key pinning (PKP), that is, the server sends the hash value of the public key or the public key of the certificate of the certification center to the client, and the hash value is stored by the client, which can detect whether the key has changed. Xiaofei Wang et al. proposed a FederAted Deep reinforcement learningbased cooperative Edge caching (FADE) framework.

In 2008, blockchain[12-13] came into the public's view. Blockchain is a combination of encryption algorithm, consensus mechanism, distributed data storage and point-to-point transmission. With the implementation of blockchain, scholars realized that blockchain technology can be used not only in the field of economics and currency, but also in the field of security control.Duard A et al. proposed a blockchain-based decentralized network trust and IoT authentication protocol under the public key encryption system.

3. PROPOSED WORK

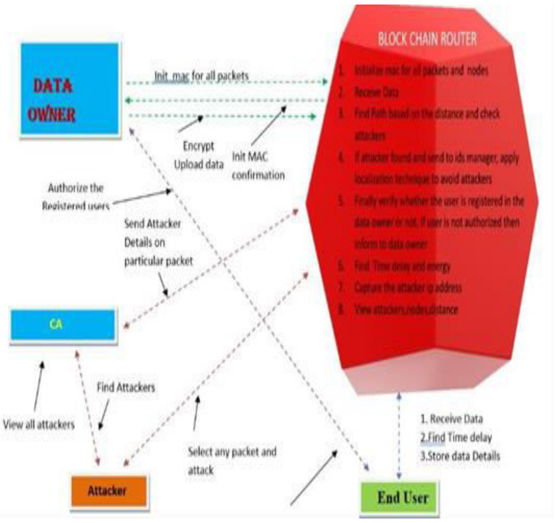
In view of the problems existing in the current identity authentication protocol, a BlockAuth Scheme is proposed. In the proposed BlockAuth Scheme, the registration protocol, consensus mechanism of security enhancement and the authentication protocol are studied in detail. In the scheme, users can access data resources, service resources, business resources and management resources through the user interface, and can send user registration or authentication requests and information to the blockchain network. The blockchain network is the core of the platform, including smart contracts, node management, consensus mechanisms, cryptographic algorithms and other functions, providing secure services for all functions of thescheme.

In the service process, user can call the interface to send the request and data to the blockchain platform. Then, in order to deal with the request and data, the blockchain platform will call the blockchain execution engine to invoke the smart contract and other functions. After verification by at least three endorser nodes, the blockchain execution engine will call the block generation module to generate a new block. Finally, the engine will write the completed transaction into the newly created block, and write the timestamp and other information additionally. When the user requests for the initialization of the authentication from the system certificate issuer, the user initiates a registration request, the user’s name and password attribute values need to be entered. The request info of user certificate includes certificate type, user’s public key and it’s validity period, then submits certificate application request and applies for registration of certificate. After receiving the user's application, the registration center verifies the validity of the user's identity information, once finished the approval of the registration center, the user identity certificate(CertU) is generated through the certificate issuing center.

During the registration stage of the BlockAuth scheme, the user signs the user's index and hash of the password attribute values to generate signature information, and then

commits the information in the blockchain by calling the smart contract of the blockchain and creates the blockchain and transaction information. The blockchain verifies the identity of the transaction initiator by verifying the transaction signature, and confirms that the certificate is issued by verifying the signature in the certificate. In details, when the authentication nodes receive the authentication request from the client user, the peers in the AuthNode authenticatethe client request.

(A) ARCHITECTURE:


BLOCK CHAIN ROUTER
1. Initialize mac for all packets and nodes
2. Receive Data
3. Find Path based on the distance and check attackers
4. If attacker found and send to ids manager, apply localization technique to avoid attackers
5. Finally verify whether the user is registered in the data owner or not. If user is not authorized then inform to data owner
6. Find Time delay and energy
7. Capture the attacker ip address
8. View attackers,nodes,distance
DATA OWNER
Init mac for all packets
Encrypt Upload data
Init MAC confirmation
Authorize the Registered users
Send Attacker Details on particular packet
CA
View all attackers
Find Attackers
Select any packet and attack
Attacker
1. Receive Data
2.Find Time delay
3.Store data Details
End User

(B) MODULE DESCRIPTION:

a) Blockchain Router:

In this module, the router shows simulation of data transmission between data owner and end users. The router assign the distances of nodes in network and also generates various reports like, view Attackers, view blockchain network nodes information, view end users details, andview time delay of nodes.

b) Data Owner:

In this module, data owner browse the file data, encrypt the file data using ECC, generate block hash and initialize the nodes in the block chain networks and the data divided into multiple blocks, and finally send the data to enduser through blockchain network.

c) End User:

In this module, end user register and login to the system. After login successful, he wait forreceiving data from network.

d) CA:

In this CA view the misbehaving node details and find their packet hash code is used forattacker.

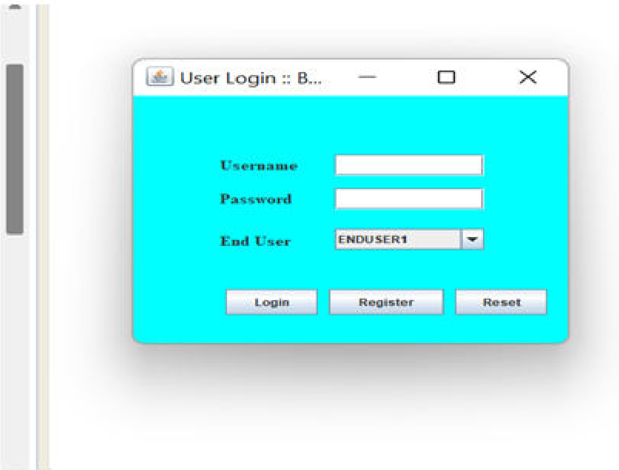
e) Attacker:

In this module, we present the attack model, in which attacker attack the node in the networkby adding malicious data to specific packet. This can be trace by the CA.

4. RESULTS

- This is user login page of which user should register with his details with user nameand password and select end user and click register .

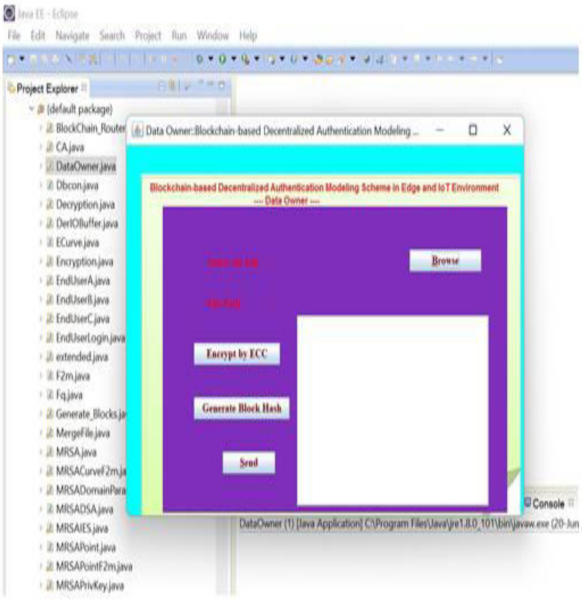
- After registration user should login with his username and password .



End User: ENDUSER1

FIG :1. USER LOGIN PAGE

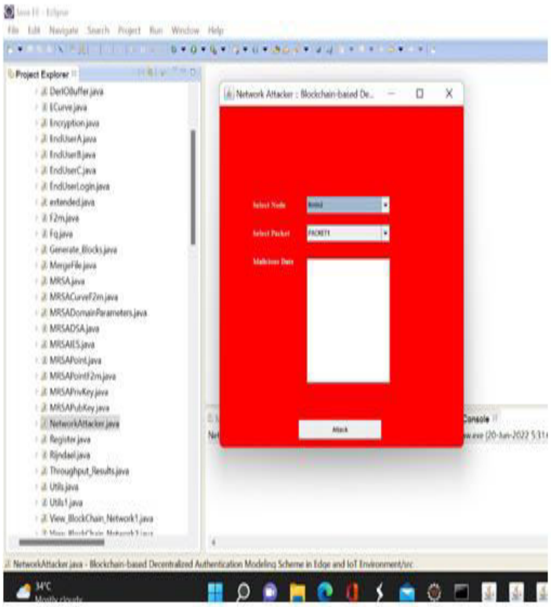
- This is a data owner page of which the user will browse the data and send to the receiver.


Java EE - Eclipse
File Edit Navigate Search Project Run Window Help
Project Explorer
Data Owner::Blockchain-based Decentralized Authentication Modeling ...
Blockchain-based Decentralized Authentication Modeling Scheme in Edge and IoT Environment
---- Data Owner ----
Browse
Encrypt by ECC
Generate Block Hash
Send
Console

DataOwner (1) [Java Application] C:\Program Files\Java\jre1.8.0_101\bin\javaw.exe (20-Jun

FIG :2. DATA OWNER PAGE

- This is a attacker page of which attacker attacks a particular node


Java EE - Eclipse
File Edit Navigate Search Project Run Window Help
Project Explorer
Network Attacker : Blockchain-based De...
Select Node
Select Packet
Malicious Data
Attack
Console

Select Packet: PACKET1

NetworkAttacker.java - Blockchain-based Decentralized Authentication Modeling Scheme in Edge and IoT Environment/src

FIG :3. NETWORK ATTACKER PAGE

- This is a receiver page of which receiver receives the data sent by the sender.

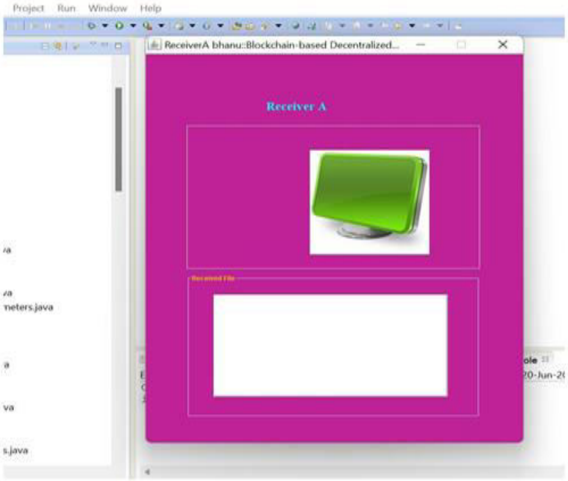
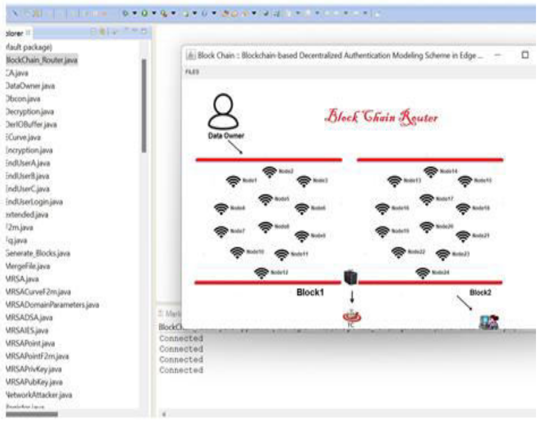


FIG :4. RECIEVER PAGE

- The router shows simulation of data transmission between data owner and end users



```
Connected
Connected
Connected
Connected
```

FIG :5. BLOCK CHAIN ROUTER

5. CONCLUSION

In order to solve the security and reliability of traditional authentication in the edge and IoT environment, we proposed a BlockAuth Scheme, which can provide a more secure, reliable and strong fault tolerance decentralized novel authentication solution with high-level security. In this scheme, each edge device is regarded as a node to form blockchain network. Specially, we designed the secure registration and authentication strategy and the blockchain-based decentralized authentication protocol, improved the blockchain consensus, developed smart contract, and finally implemented the whole blockchain-based authentication platform for the feasibility, security and performance evaluation. According to Evaluations and Comparison with the existing related scheme, our scheme enhances security and stability on the basis of sacrificing a certain degree of time complexity, and meets the high security and fault tolerance requirements of identity authentication in edge and IoT environment. Furthermore, this scheme proposed by us can meet the authentication requirements of multiple scenarios and development demand of the international standard authentication scheme.

REFERENCES

[1] Proc. Roy. Soc. A Math. Phys. Eng. Sci., vol. 426, no. 1871, pp. 233-271, 1989.

[2] M. Abadi and M. R. Tuttle, "A semantics for a logic of authentication", Proc. 10th Annu. ACM Symp. Princ. Distrib. Comput., pp. 201-216, 1991.

[3] Hung-Yu Chien. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. IEEE Transactions on Dependable and Secure Computing, vol.4, pp.227-340, 2007.

[4] Jia-Lun Tsai ; Nai-Wei Lo. A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services. IEEE Systems Journal, vol.9, pp.805-815, 2015.

[5] Muhammad Ajmal Azad; Samiran Bag; Charith Perera; Mahmoud Barhamgi; Feng Hao. Authentic Caller: Self-

Enforcing Authentication in a Next- Generation Network. IEEE Transactions on Industrial Informatics, vol.16, pp.3606-3615,2020.

[6] Libor Dostálek. Multi-Factor Authentication Modeling. 2019 9th International Conference on Advanced Computer Information Technologies (ACIT).

[7] K. M. Renuka ; Saru Kumari ; Dongning Zhao ; Li Li. Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems. IEEE Access, vol.7, pp. 51014 – 51027, 2019.

[8] T.-D. Nguyen, A. Al-Saffar and E.-N. Huh, "A dynamic id-based authentication scheme",Proc. 6th Int. Conf. Netw. Comput. Adv. Inf. Manage. (NCM), pp. 248-253, Aug. 2010.

[9] S. Chen, M. Ma and Z. Luo, "An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems", Secur. Commun. Netw., vol. 9, pp. 1146- 1157, 2016.

[10] X. Sun, S. Men, C. Zhao and Z. Zhou, "A security authentication scheme in machine-to- machine home network service", Secur. Commun. Netw., vol. 8, no. 16, pp. 2678-2686, 2015.

[11] Arno Fiedler, Christoph Thiel. Certificate Transparency. Datenschutz und Datensicherheit - DuD, 2014, Vol.38 (10), pp.679-683.

[12] Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media,Inc., 2015.

[13] Ryan Henry; Amir Herzberg; Aniket Kate, "Blockchain Access Privacy: Challenges and Directions", IEEE Security & Privacy, vol.16, no.4, pp.38-45,2018.

[14] Tomaso Aste; Paolo Tasca; Tiziana Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry", Computer, vol.50, no.9, pp.18-28,2017.

[15] Tien Tuan Anh Dinh; Rui Liu; Meihui Zhang. "Untangling Blockchain: A Data Processing View of Blockchain Systems", IEEE Transactions on Knowledge and Data Engineering, vol.30, no.7, pp.1366-1385,2018.

[16] H. G. Do, W. K. Ng, "Blockchain-based system for secure data storage with private keyword search", 2017 IEEE World Congress on Services (SERVICES), pp. 90-93, 2017.

[17] Y Zhe, Y Kan, et.al. Blockchain-based Decentralized Trust Management in Vehicular Networks，IEEE Internet of Things Journal ， Vol.6, No.2, pp.1495-1505,2019.