A Secure and Reliable Supply chain management approach integrated with IoT and Blockchain

*Humaira Ashraf
department of computer science and software engineering
International Islamic university Islamabad
Islamabad, Pakistan
humaira.ashraf@iiu.edu.pk

Maria Hanif
department of computer science and software engineering
International Islamic university Islamabad
Islamabad, Pakistan
maria.mscs1078@iiu.edu.pk

Uswa Ihsan
department of computer science and software engineering
International Islamic university Islamabad
Islamabad, Pakistan
Uswaihsan.mscs1075@iiu.edu.pk

Fatima Al-Quayed
Department of Computer Science, College of Computer and Information Sciences, Jouf University
Sakakah, Saudi Arabia;
ffalquayed@ju.edu.sa

Mamoona Humayun
department of Information Systems, College of Computer and Information Sciences, Jouf University
Sakakah, Saudi Arabia;
mahumayun@ju.edu.sa

NZ Jhanjhi
School of Computer Science and Engineering (SCE), Taylor's University, Malaysia;
NoorZaman.Jhanjhi@taylors.edu.my
Applied Science Research Center, Applied Science Private University,
Amman 11937, Jordan,
h_gaftim@asrc.asu.edu.jo

2023 International Conference on Business Analytics for Technology and Security (ICBATS) | 979-8-3503-3564-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICBATS57792.2023.10111371

***Abstract*— Nowadays, secure and reliable management of logistics is highly needed. Logistics is the delivery of goods from producers to legitimate consumers in accurate amounts and good conditions. The use of low-capable sensor nodes in smart logistics makes it vulnerable to many security threats. Smart logistics necessitated the delivery of suitable information to the authorized person at the appropriate time and place, which is only feasible with a stable infrastructure. This paper presents an authentication scheme together with blockchain technology to provide a secure supply chain management system. The presented authentication mechanism is based on standard KERBOROS scheme which is a ticket-based scheme. The scheme is evaluated by BAN logic which shows that it is an effective scheme in terms of improved response time and encryption/decryption time along with key generation time.**

Keywords— Supply chain management, IoT, Blockchain

I. INTRODUCTION

In the modern era, reliable logistics management is a significant concern. Logistics is the delivery of goods from producers to legitimate consumers in accurate amounts and good conditions. Smart logistics necessitated the delivery of suitable information to the authorized person at the appropriate time and place, which is only feasible with a stable infrastructure. A stable framework combines blockchain technology with the Internet of Things to make logistics services more reliable and convenient. The collection of logistics data management is done by the advanced technology of the Internet of things, and the integrity of this data is ensured by using Blockchain. Blockchain is an emerging technology used to store data in a distributed manner to avoid tampering. So a highly effective and reliable approach is needed for supply chain management.

Sensors and actuators are used on the Internet of Things (IoT) to link large vehicles in smart transportation and logistics. By tracking traffic, reducing congestion, and making timely decisions, these sensors help to optimize transportation. The IoT technology is used to communicate with the physical world to collect data from the physical world so that the quality of physical world activities can be improved. The integrity of data collected from IoT devices (sensors, smartphones, cameras, etc) must be ensured so that data cannot be tempered by attackers or spoofed by malicious users of the system.

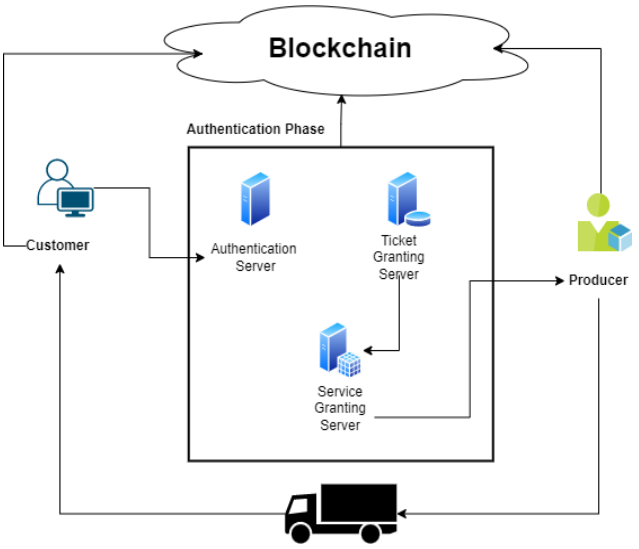

Figure 1. Supply chain management with blockchain

This paper proposes a hybrid framework of IoT systems that uses blockchain for secure and reliable data management in Smart logistics. It ensures that the data collected from devices (sensors, smartphones, smart meters) achieve high-level integrity. It detects the anomaly within data management whether sensor nodes are attacked by malicious users or information on goods is used by some intruder.

The data from IoT devices is entered into the blockchains to store the data in a distributed manner. The blockchains first verify the user who will create a block of unregistered data from IoT devices so that unauthorized access can be denied and no intruder can register anomalous data into the block. The proposed framework also speeds up the data access in the blockchain to improve the overall service quality of the system.

The critical requirements of picking the right receiver and obtaining delivery proof are achieved with Block-chain enabled IoT sensors that are being used in transportation. It also allows participants interested in getting real-time access to trustworthy identities, smart billing, formal verification, and payment details. Moreover, it displays the real-time position of items and is available to all parties involved.

The main contributions of our work are as follows:

1. An authentication scheme is presented to ensure the legitimate use of smart logistics system.
2. IoT devices integrated with blockchain ensure the data integrity of smart logistics system.
3. The presented scheme is evaluated with BAN logic in detail which proves that there is no vulnerability in presented authentication protocol.
4. The presented scheme provides high response time and less encryption/decryption time.

The section 2 presents the literature review which is followed by section 3 of methodology. The section 3 has a sub section of proofing presented authentication scheme by BAN logic. Section 4 presents results and analysis which is followed by section 5 of Conclusion. Finally, Section 6 is of References

II. LITERATURE REVIEW

Several IoT devices like cameras, smartphones, smart meters are used in the physical world to construct IoT systems. These devices produce a large amount of physical world data, which is important to facilitate the services of IoT systems. However, these devices do not provide high-level security because of low-level design and limited cost [1]. Alladi et al. presented a survey of high high-security risks of IoT devices in the physical world. An IoT device that is vulnerable to attacks can produce abnormal data of the physical world. The attacker can also build a physical attack through an IoT device in the physical world [2].

That is why it is highly needed to create a secure method to ensure the security of physical world data so that an attacker cannot tamper or spoof an IoT system through any IoT device or node. Therefore, Blockchain is used in data management to have a secure IoT system.

A blockchain is a shared data management process initially used for securing currency known as cryptocurrency (bitcoin). In the blockchain mechanism, a block acts as a unit of data structure, and several blocks are linked together as a linked list. These blocks are capable of securing physical world data. A blockchain also consists of many user terminals which calculate the hash value using a recent block's contents to create a new secure block for unregistered data. The process of creating a new block is known as 'mining'. [3] It ensures that only authorized users create the new block and protect the IoT system from attackers. The authorized user must calculate a hash value that satisfies all predefined conditions (threshold) to create a new block. Therefore, a user terminal has to do a high number of calculations to find the correct hash value.

That is why mining is the key aspect of the data integrity of blockchain because an attacker cannot create a new block for anomalous data if mining performance is the main aspect of the data integrity of blockchain. An attacker cannot create a new block for anomalous data if the performance of the attacker's created resources is not higher than the performance of other user's resources. Mining is also a heavy process that takes few seconds to a few minutes.

Acronyms	Definition	Acronyms	Definition
RS	Registration Server	CID	Customer ID
LS	Login Server	PID	Product ID
AS	Authentication Server	TID	Transaction ID
TGS	Ticket granting Server	MC	Manufacturer Company
SGS	Service granting Server	SLS	Smart Logistics System
U	User	NN	Nounce Number
PW	Password	TS	Time stamp
CID	Client ID	TGS	Ticket Granting Server
PID	Product ID	SGS:	Service Granting Server
TID	Transaction ID	K_X	X's shared key with Servers
P.Name	Product Name	$K_{X,Y}$	X's shared encrypted key with Y
C.addr	Client Address	{m}K	Message m is encrypted by key K
N.addr	Network Address	$T_{X,Y}$	Ticket that X visit Y
AS	Authentication Serve	$A_{X,}$	Authentication symbol of X and Y
CID	Client ID	P_I and P_C	Passwords which are random numbers generated by servers.

The blockchain is becoming popular in the construction of reliable IoT systems for physical world data management produced by different kinds of IoT devices [4][5]. The researchers studied blockchain to secure different IoT systems such as supply chain management, vegetable factory management, and smart home management [6][7]. Moreover, a lightweight mechanism also has been presented which accommodates IoT devices with less computation power and high speed to create new blocks on blockchain [8].

The recent researches focused only on securing data in the blockchain. They do not consider the condition of tampering and spoofing of data by intruders before it's storage on blocks. For example, the vehicle's location can be tampered and spoofed by malicious producers in the logistics management system. It can cause serious problems like food safety and destructing production areas [9] [10].

IoT is a system of highly connected devices with atomic identities. These devices are capable of transmitting data all over the network system. They can sense and gather data for transmitting it using the internet. Transportation and Logistics play a highly necessary part in the growth and development of any community. Well-managed logistics and transportation systems increase the economic aspect, which facilitates the society. IoT is becoming very popular for handling transportation and logistics systems by connecting their enormous objects. There are a lot of advantages of IoT in transportation and logistics, such as traffic controlling, condition monitoring, avoiding traffic congestion, online tracking, providing an efficient supply chain, and making a decision in time [11-13].

In smart transportation and logistics, many IoT devices are linked together intelligently. These devices are monitored and tracked in real-time. IoT system connects all these objects by using integrated sensors, actuators, and different kinds of devices to gather and transfer real-time data all over the network system.

IoT has revolutionized smart transportation and logistics, but data security and data privacy still exist, but data security, privacy, and infrastructure formation [14-16]. There is a need of powerful cryptographic techniques to ensure data security and privacy. Another issue is the 24/7 availability of services by smart devices. IoT devices have less storage space and less computational power, making them vulnerable to different attacks. Therefore, a secure infrastructure is needed to deliver correct data to the legal person in time and at the right location in smart transportation and logistics systems.

Different companies are making their transportation and logistics smart to meet people's emerging requirements. But, IoT is not enough to meet people's demands of a secure logistics system. Now-a-days, blockchain and IoT are used together to get a secure transportation and logistics system. Blockchain is a mechanism which uses blocks that are chained together and encrypted. These blocks are in sequence and used to store validated data in peer-to-peer networks**.** All clients are linked with peer-to-peer network in the blockchain framework. When a client sends a data packet, it encrypts the data packet by hashing function and broadcast it all over the network so that only an authentic person will receive the data packet and decrypt it. Such secure transaction is possible in IoT system with integration of Blockchain. As blockchain technology has blocks, it saves the complete records of all users of system and transactions and ensures the complete records of all users of system and transactions and ensures the complete records of all users of system and transactions and ensures the integrity of data.

Blockchain and IoT facilitate smart transportation and logistics with different benefits such as less cost, reliable, and high-speed transactions. It also assures the safe delivery of goods by keeping them in suitable temperatures and keeping their records [17-19]. Some main advantages of IoT with blockchain include freight track, which means a sender can track the current status of their delivery and temperature control for perishable goods for long distances. It also provides carrier and vehicle authentication. Overall, this integration provides secure and reliable smart transportation and logistics.

The IoT is becoming very popular due to cloud computing as it provides Quality of service (QoS) to IoT applications. But the data transfer is vulnerable to attack due to different network problems such as delay in data transmission. [20] These IoT applications require real-time response, which is not facilitated by cloud computing. The role of cloud service is a challenge in the development of an IoT system. Recently, Edge Cloud Computing (ECC) is secure and reliable for IoT applications. It takes cloud services back to IoT nodes in shared logistics. There are still challenges and issues in this area to be addressed.

Xu et al. presented many innovative ways to address the challenges through use of blockchain and smart contract technology [22]. Zhang et al. presented a hybrid approach of blockchain and smart contract technology named as blockchain and smart contract technology approach named Edge Chain IoT system to resolve the existing problems. This strategy uses blockchain technology and an internal payment method to link the edge cloud pool to each node's account in an IoT system [21]. The Edge Chain uses credit management in shared logistics. This approach shows that the presented approach can provide secure communication between IoT nodes on a reasonable and manageable computational cost. Blockchain ensures security, which facilitates the system by monitoring data and auctioning in shared logistics.

Huang et al. presented a Mobile-edge computing (MEC) method to enhance the computing skills of mobile devices for highly complex computational tasks which includes processing and mining of data in real-time. However, there are problems such as system takes time initially to start and sometimes delay in response occurs because mobile devices are not much capable of efficient offloading operations due to fewer coins to pay the cost [23]. Cil et al. presented an approach to solve the problem of blockchain-based MEC predictions-offloading and coin-locations so that the total cost of mobile devices can be reduced based on MEC predictions-offloading and coin-locations to reduce the total cost of mobile devices. It uses banks which facilitate mobile devices with loan services [24]. Avelar-Sosa et al. and Yu et al. designed a distributed algorithm to propose Nash mechanism which achieves Nash balance with less computational complexity [25] [26].

Cil et al. presented a deep reinforcement learning approach that uses Adaptive Genetic Algorithm (AGA) to maximize long-term offloading performance after performing data mining and processing through online offloading [24].

The authors presentedin [27-30] several security and optimization issues related to this from different perspectives.

III. METHODOLOGY

The proposed scheme includes three phases which are

1. Registration of user
2. Login
3. Authentication

All the abbreviations which are used in the proposed system are given in Table 1 of Notations.

1. Registration of user

Step 1: U ➔ RS {User ID | PW | Status}

Firstly, user sends his/her ID, password and status (Customer/Producer/Supplier) to Registration Server.

Step 2: RS ➔ U {User ID | PW | Status | TS | NN}

The registration server checks the status of user and creates timestamp value and nounce number for user. After that, the registration server saves the user ID, password and status in respective table. It sends users a registration key, including user ID, password, status, timestamp value, and nounce number.

For example, a customer wants to register into logistic system. He will send his ID, password and status to the registration server. The RS will save customer ID and password in Customers table existing in the database. It will create an encrypted registration key that includes customer ID, password, status, timestamp value, and nounce number. The customer will use this registration key at the time of login.

2. Login

If user wants to get a service, he will login to logistic system.

Step 1: LS ➔ U

Firstly, login server will ask the user to provide his ID and password. The Login server will check the user's status by verifying his ID from the database. If the ID and password do not match the database, LS asks the user to register first. If the ID and password of user match then LS will prompt user to next step.

Step 2: LS ➔ U

Secondly, the login server will ask the user to provide the encrypted registration key provided by the registration server. The LS will decrypt the key and verify the information of user. After successful verification, the LS will prompt the user to access the logistic system for services and log in to the system successfully.

3. Authentication

In this scheme, a standard KERBEROS mechanism is used to authenticate the smart logistic system's users (producers, consumers, suppliers). This scheme is based on key encryption which contains identity of users. The legitimate users are provided with encrypted key with ticket to get their services done. The framework of authentication phase is described in detail by following algorithm and Figure 2.

3.1. Authentication Protocol

Firstly, the customer will log on to the smart logistic system's server and request for service from the Authentication Server. The AS will ask the customer to enter his ID, address, and Product Name. The AS will verify the customer by checking his ID.Secondly, the AS will send a customer a ticket for TGS with an encrypted key. The encrypted key includes customer ID, transaction ID, product ID, product name, customer address and password.

Thirdly, the customer will send this ticket and encrypted key to TGS to grant ticket of service. The TGS will decrypt the key and checks all information. After that, the TGS will send a service ticket and encrypted key to customer. The encrypted key includes customer ID, transaction ID, product ID, product name, customer address, password and network address.

Authentication Protocol

1. Customer → AS (CID | Product Name | Customer address)
2. AS→ Customer (ticket | encrypted key { CID | TID | PID | Customer address | Product Name | Password})
3. Customer → TGS (ticket | encrypted key)
4. TGS: check { Customer ID | Customer Full name | Transaction ID | Product ID | Product Name | Customer Address | Password }
5. TGS→ Customer (service ticket | encrypted key {CID | TID | PID | TID | Customer address | password | network address })
6. Customer → SGS (service ticket | encrypted key)
7. SGS: check { Customer ID | Customer Full name | Transaction ID | Product ID | Product Name | Customer Address | Network address | Password }
8. SGS → Supplier (MC) order
9. MC → Transport
10. Transport → Customer

The customer will then send a service ticket and encrypted key to SGS to grant service. After successfully verifying information by decryption of key, the SGS will send the customer's order to the supplier of Manufacture Company, which furthers loads the order on transport. Finally, the transport will deliver the order to the customer.

3.2. Proof of Authentication Protocol by BAN Logic

BAN Logic proves the presented authentication protocol proves the presented authentication protocol to check the reliability and security of the protocol.

1. C ➔ AS

(Customer applying for the Ticket Granting Ticket from Authentication Server)

CID, P.Name, C.addr

2. AS ➔ C

(Authentication Server sends encrypted key and ticket to Customer)

$\{K_{AS,C}, T_{AS,C}\}K_C, T_{AS,C}\{CID, TID, PID, C.addr, P.Name, P\}K_{AS}$

3. C ➔ TGS

(Customer sends message to Ticket Granting Server)

$T_{C,TGS}, A_{C,TGS}$

$A_{C,TGS} = \{ CID, TID, PID, C.addr, P.Name, P\}$

$K_{C,TGS}$

4. TGS ➔ C

(Ticket Granting Server sends encrypted key and ticket to Customer)

$\{K_{TGS,C}, T_{TGS,C}\}K_C$

$T_{TGS,C}\{CID, TID, PID,TID, C.addr, N.addr, P.Name, P\}K_{TGS}$

5. C ➔ SGS

(Customer sends message to Service Granting Server)

$T_{C,SGS}, A_{C,SGS}$

$A_{C,SGS} = \{ CID, TID, PID,TID, C.addr, N.addr, P.Name, P\}$
$K_{C,SGS}$

7. SGS → C

(Service Granting service grants service to Customer**)**
$\{P_C +1\}K_{SGS,C}$

Some reasonable assumptions are constructed for the analysis condition of authentication protocol is as follows:

1. C believes $\overset{K_C}{\longleftrightarrow}$ AS
2. SGS believes $\overset{K_{SGS,TGS}}{\longleftrightarrow}$ TGS
1. $K_{C,Y}$ $\longleftrightarrow$
3. C believes SGS believes C TGS
4. C believes AS controls $T_{C,TGS}$
5. C believes TGS controls $T_{C,SGS}$
6. C believes TGS controls $K_{C,SGS}$
7. SGS believes TGS controls $T_{C,SGS}$
8. C believes fresh (P_1)
9. SGS believes fresh (P_C)
10. C believes fresh (P_C)

The authentication protocol proof using BAN logic is given below:

Proof: C believes C $\overset{K_C}{\longleftrightarrow}$ **AS**

Because C believes C $\overset{Kc}{\longleftrightarrow}$ AS, C sees $\{T_{C,TGS}\}K_C$.

So , according to Rule No.1, we can get a result that C believes AS said $T_{C,TGS}$.
Because C believes fresh (P_1) , So, according to Rule No.2 we can get a result that C believes AS believes $T_{C, TGS}$.
Because C believes AS controls $T_{C, TGS}$, So, according to Rule No.3 we can get a result that C believes $T_{C, TGS}$.
Then, according to Rule No.5 we can get a result that C believes $K_{C, TGS}$.
Because C sees $\{T_{C,SGS}\}K_{C,TGS}$, So, according to Rule No.1 we can get a result that C believes TGS said $T_{C,SGS}$.
Because C believes fresh ($T_{C,SGS}$) , So, according to Rule No.2 we can get a result that C believes TGS believes $T_{C,SGS}$.
Because C believes TGS controls $T_{C,SGS}$, So, according to Rule No.3 we can get a result that C believes $T_{C,SGS}$.
Finally, according to Rule No.5, we can get a result that

C believes C $\overset{K_C}{\longleftrightarrow}$ AS

Proof: SGS believes C $\overset{K_{SGS,TGS}}{\longleftrightarrow}$ **TGS**

Because SGS believes SGS $\overset{K_{SGS,TGS}}{\longleftrightarrow}$ TGS, SGS sees $\{T_{C,SGS}\}K_{SGS,TGS}$,so according to **Rule No.1** we can get a result that SGS believes TGS said $T_{C,SGS}$. Because V believes fresh ($T_{C, SGS}$), So , according to **Rule No. 2** we can get a result that SGS believes TGS believes $T_{C, SGS}$.
Because SGS believes TGS controls $T_{C, SGS,}$ So, according to **Rule No.3** we can get a result that SGS believes $T_{C, SGS}$.
Finally, according to **Rule No.5** we can get final result that

SGS believes C $\overset{KSGS, TGS}{\longleftrightarrow}$ TGS (II)

Proof: C believes SVG believes C $\overset{K_{C,Y}}{\longleftrightarrow}$ **SGS**

Because C believes fresh (P_C), so we can get a result that C believes fresh (P_C +1).
Also, we can get a result that C believes fresh ($\{NC +1\}K_{C, SGS}$).
Because C believes $K_{C, SGS}$, C sees $\{NC +1\}K_{C, SGS}$ and according to Rule No.1 we can get a result that C believes SGS said $\{NC +1\}K_{C,SGS}$.
According to Rule No.2 we can get a result that C believes SGS believes $\{NC +1\} K_{C,SGS}$.
Finally we can get result that

C believes SVG believes C $\overset{K_{C,Y}}{\longleftrightarrow}$ **SGS**
(III)

By the same process, we can also get the result

SGS believes C believes C $\overset{K_{C,Y}}{\longleftrightarrow}$ **TGS**
(IV)

From all above equations I, II, III and IV, we can draw the final conclusion that this authentication protocol achieves the key generation mechanism and real-time transmission between customer and server securely. The protocol uses ticket to improve the authentication process. The presented protocol is proved logically, and no protocol limitation can be found. This authentication protocol is reliable and secure as there is no chance of attack from outside on this protocol.

IV. RESULT AND DISCUSSION

The proposed approach is based on multiple parameters.

A. Response time

Response time describes the amount of time Authentication Servers take to send a response to the user against the Register request. Figure 3 shows the response time for the various number of authentications requests. Figure 4 shows the response time comparison with number of authentications.

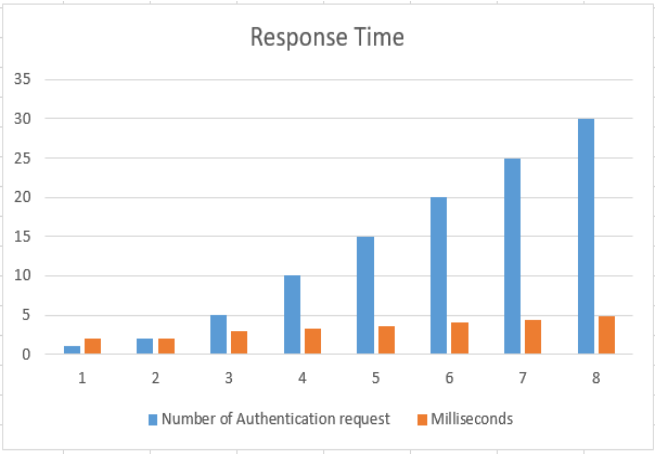

Figure 4. Response Time

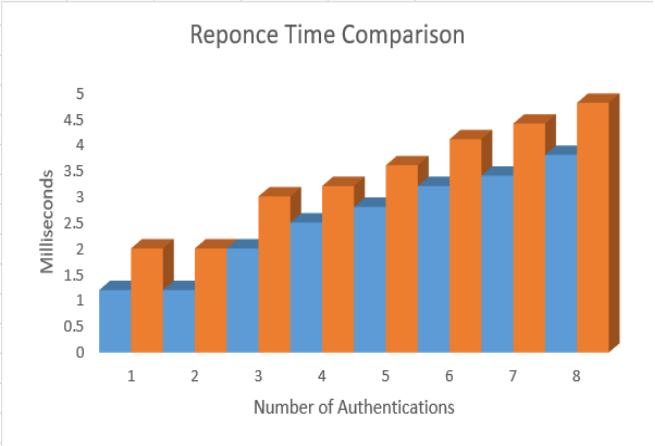

Figure 4. Response Time Comparison

B. Encryption/Decryption time

The time taken for encryption-decryption and key generation is shown in figure 5

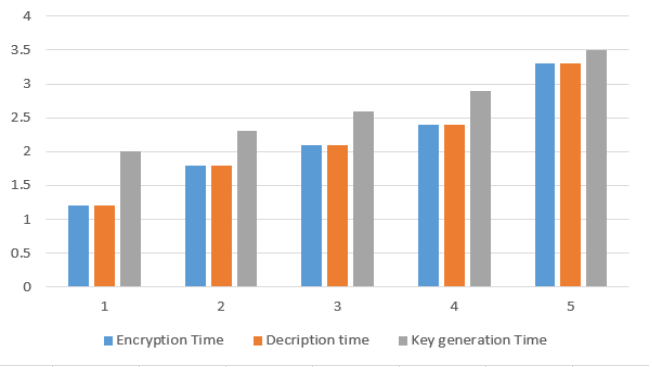

Figure 5. Encryption time comparison

CONCLUSION

As secure and reliable communication is the main concern in the supply chain system. There are many techniques that improves the security in smart logistics system in which IoT-enabled Blockchain is one of the most used technologies. The advantage of blockchain is that it improves data integrity by keeping it in secure blocks. The paper presented a -based authentication scheme for a smart logistics system with Blockchain technology. The proposed scheme works on the basis of ticket to provide customer service. The scheme has three different phases. Each phase ensures the security of communication and authentication of user in smart logistics system. The records of all transactions are saved in blockchains and the records of users are kept in a database.

REFERENCE

[1] J.-H. Lee andH. Kim, “Consumer IoT: Security vulnerability case studies and solutions,” IEEEConsum. Electron.Mag., vol. 6, no. 3, pp. 134–136, Jul. 2017.

[2] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, “Consumer IoT: Security vulnerability case studies and solutions,” IEEE Consum. Electron. Mag., vol. 9, no. 2, pp. 17–25, Mar. 2020.

[3] G. A. K. Gemeliarana and R. F. Sari, “Evaluation of proof of work (POW) blockchains security network on selfish mining,” in Proc. Int. Seminar Res. Inf. Technol. Intell. Syst., Nov. 2018, pp. 126–130.

[4] Gajendran, Natarajan. "Blockchain-Based secure framework for elearning during COVID-19." Indian journal of science and technology 13, no. 12 (2020): 1328-1341.

[5] Humayun, Mamoona, Noor Zaman Jhanjhi, Mahmood Niazi, Fathi Amsaad, and Isma Masood. "Securing drug distribution systems from tampering using blockchain." Electronics 11, no. 8 (2022): 1195.

[6] M. Conoscenti, A. Vetro, and J. C. D. Martin, “Blockchain for the internet of things: A systematic literature review,” in Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl., 29 Nov.-2 Dec. 2016, pp. 1–6.

[7] Q. Xu, Z. He, Z. Li, and M. Xiao, “Building an Ethereum-based decentralized smart home system,” in Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst., Dec. 2018, pp. 1004–1009.

[8] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE),” IEEE Consum. Electron. Mag., vol. 9, no. 2, pp. 8–16, Mar. 2020.

[9] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, “Blockchain-based soybean traceability in agricultural supply chain,” IEEE Access, vol. 7, pp. 73295–73305, May 2019.

[10] G. Baralla and A. Pinna, “Ensure traceability in European food supply chain by using a blockchain system,” in Proc. IEEE/ACM 2nd Int. Workshop Emerg. Trends Softw. Eng. Blockchain, 27–27 May 2019, pp. 40–47.

[11] G. Rathee et al., “A Secure Communicating Things Network Framework for Industrial IoT Using Blockchain Technology,” Ad Hoc Networks, 2019, p. 101933.

[12] G. Rathee et al., “A Blockchain Framework for Securing Connected and Autonomous Vehicles,” Sensors, 2019, vol. 19, no. 14, p. 3165.

[13] E. J. Schiller et al., “Scalable Transport Mechanisms for Blockchain IoT Applications,” 2019.

[14] A. Lei et al., “Blockchain-Based Dynamic Key Management for IoT-Transportation Security Protection,” Blockchain for Distributed Systems Security, 2019, p. 117.

[15] C. S. Subramaniyam et al., “A Survey on IoT Based Intelligent Road Traffic and Transport Management Systems,” 2017.

[16] Humayun, M., Jhanjhi, N. Z., Hamid, B., & Ahmed, G. (2020). Emerging smart logistics and transportation using IoT and blockchain. IEEE Internet of Things Magazine, 3(2), 58-62.

[17] A. Malak, N. Jhanjhi, and H. Mamoona, "Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review," Int'l. J. Computer Science and Network Security, 2019, vol. 19, no. 5, pp. 244–58.

[18] Humayun, M., 2020. Role of emerging IoT big data and cloud computing for real time application. International Journal of Advanced Computer Science and Applications, 11(4).

[19] A. H. F. A. Hamid et al., "Smart Vehicle Monitoring and Analysis System with IoT Technology," Int'l. J. Integrated Engineering, 2019, vol. 11, no. 4.

[20] Tan BQ, Wang F, Liu J, Kang K, Costa F (2020) A blockchain-based framework for green logistics in supply chains. Sustainability 12(11):4656

[21] Zhang Z, Hong Z, Chen W, Zheng Z, Chen X (2019) Joint computation offloading and coin loaning for blockchain-empowered mobile-edge computing. IEEE Internet Things J6:9934–9950

[22] Xu S, Niu J, Cai X (2020) Optimize logistics cost model for shared logistics platform based on time-driven activity-based costing. J Phys Conf Ser 1437(1):012115

[23] Huang L, Bi S, Zhang YJ (2019b) Deep reinforcement learning for online computation offloading in wireless powered mobile-edge computing networks. IEEE Trans Mob Comput 19:2581–2593

[24] Cil I, Demir HI, Yaman B (2020) Lean logistics in the 2020s and a cast study about logistics and supply chain management in Toyota Boshoku Turkey. In: Khan SAR (ed) Global perspectives on green business administration and sustainable supply chain management. IGI Global, Hershey, pp 276–315

[25] Avelar-Sosa L, Maldonado-Macı´as AA, Herna´ndez-Arellano JL, Estupin˜an SA (2020) A causal model to find the relationships between 3PL service providers and the performance of the logistics process in Mexican manufacturing companies. In: Garcı´a-Alcaraz JL, Jamil GL, Avelar-Sosa L, Briones Pen˜alver AJ (eds) Handbook of research on industrial applications for improved supply chain performance. IGI Global, Hershey, pp 325–352

[26] Yu Z (2020) Research on dynamic mechanism of developing green logistics in agricultural products logistics enterprises. In: Khan SAR (ed) Global perspectives on green business administration and sustainable supply chain management. IGI Global, Hershey, pp 182–191.

[27] Srinivasan, K., Garg, L., Datta, D., Alaboudi, A. A., Jhanjhi, N. Z., Agarwal, R., & Thomas, A. G. (2021). Performance comparison of deep cnn models for detecting driver's distraction. CMC-Computers, Materials & Continua, 68(3), 4109-4124.

[28] Shafiq, M., Ashraf, H., Ullah, A., Masud, M., Azeem, M., Jhanjhi, N., & Humayun, M. (2021). Robust cluster-based routing protocol for IoT-assisted smart devices in WSN. Computers, Materials & Continua, 67(3), 3505-3521.

[29] Zaman, N., Low, T. J., & Alghamdi, T. (2014, February). Energy efficient routing protocol for wireless sensor network. In 16th international conference on advanced communication technology (pp. 808-814). IEEE.

[30] Hamid, B., Jhanjhi, N. Z., Humayun, M., Khan, A., & Alsayat, A. (2019, December). Cyber security issues and challenges for smart cities: A survey. In 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS) (pp. 1-7). IEEE.

[31] Ghazal, T. M., Abbas, S., Ahmad, M., & Aftab, S. (2022, February). An IoMT based Ensemble Classification Framework to Predict Treatment Response in Hepatitis C Patients. In 2022 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-4). IEEE.

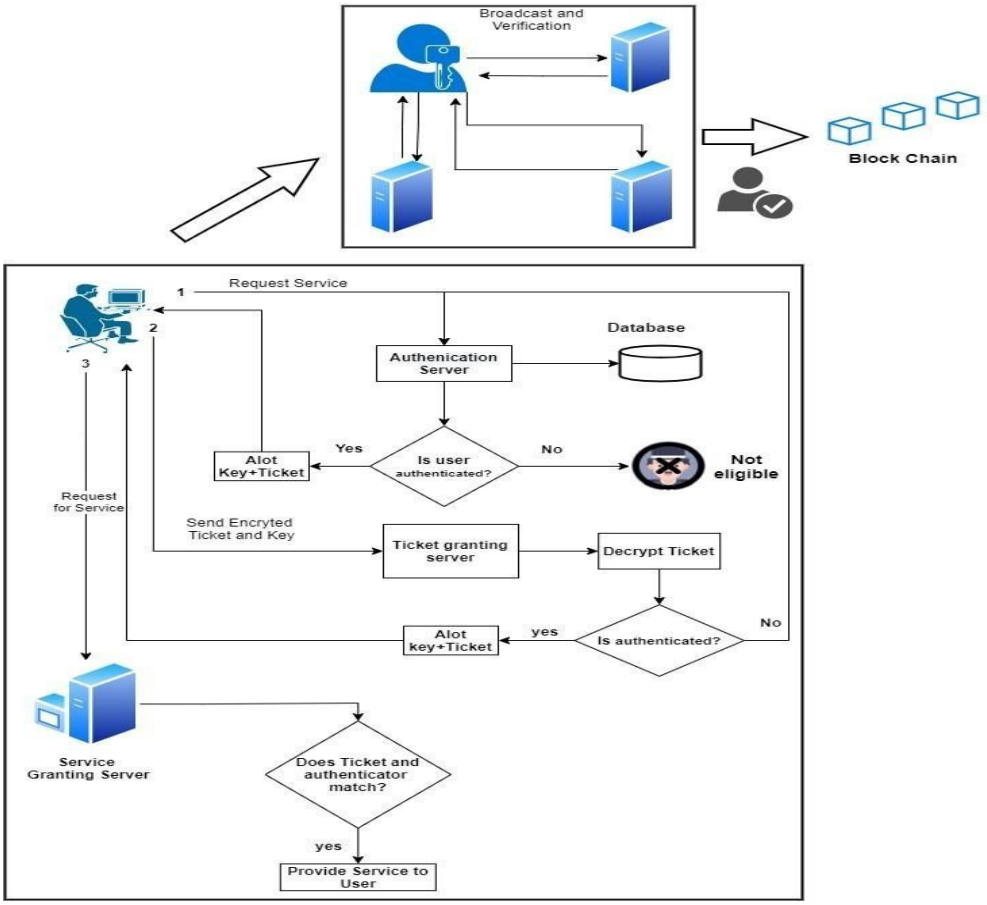

Figure 2. Flow diagram of proposed authentication system

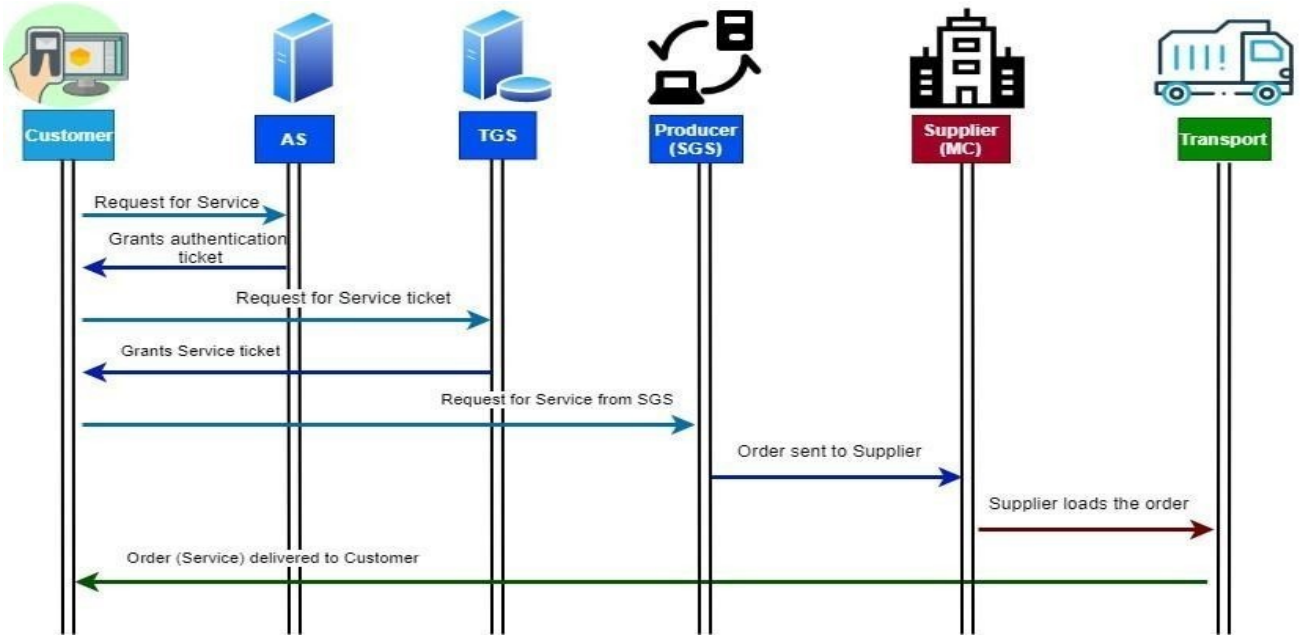

Figure 3. Framework for Authentication protocol for Supply chain management