



Blockchain-Based Secure Credit Card Storage System for E-Commerce

 Ahmet Ali Süzen¹,  Burhan Duman²

¹Corresponding Author; Isparta University of Applied Sciences, Turkey;
ahmetsuzen@isparta.edu.tr; +90 246 214 6581

²Affiliation; Isparta University of Applied Sciences, Turkey; burhanduman@isparta.edu.tr;

Received 12 March 2021; Revised 31 May 2021; Accepted 14 June 2021; Published online 31 August 2021

Abstract

Recently, serious damages have occurred in e-commerce applications due to rapidly increasing data leaks and end-user vulnerabilities. Although the source of the vulnerabilities is different, attacks result in the theft of unsafe data. In particular, the theft of credit card information reveals a financial loss. In this study, a blockchain-based secure storage model has been developed in order to prevent the theft of credit card information in e-commerce applications as a result of a possible data leak. In the sample e-commerce application developed with ASP.NET, data other than credit cards are stored. Credit card data is transmitted to the blockchain over the API with SSL protection in the e-commerce application. The blockchain model was developed using MongoDB with the BigchainDB framework. The data in each block of the blockchain is encrypted with Advanced Encryption Standard (AES) 256 bits. The data integrity of the block is provided by the SHA256 algorithm. It is aimed to protect credit card data from a possible data leak with the proposed BigchainDB-based blockchain model.

Keywords: blockchain, encryption, e-commerce, secure payment

1. Introduction

In e-commerce applications, in the payment step of the shopping made by the users; Credit cards, Money Orders / EFT, and cash on delivery options are preferred [1]. The preferred payment method is stored in application databases due to its ease of use. With increasing cyber-attacks recently, data leaks are occurring in e-commerce applications [2]. As a result of these data leaks, unauthorized transactions are made using the credit card information of the customers and material losses occur. These problems arising from the storage of customer credit cards pose a threat to both customers and e-commerce applications.

E-commerce applications are responsible for the secure storage of credit card information in the database. Although the use of SSL / TLS in client-server communication of e-commerce applications provides communication security, it does not provide database security [3]. At this point, data encryption methods are used to ensure security. The security of credit cards is tried to be determined by the Payment Card Industry-Data Security Standard (PCI-DSS) standard, recommended by Mastercard and VISA [4]. PCI-DSS is the common security standard for the use, protection, storage, and transmission of credit card data. Although the PCI-DSS standard is mandatory in e-commerce applications, potential vulnerabilities may arise due to configuration errors, developer errors, or technical errors. Possible problems encountered in e-commerce applications are listed as follows [5].

- Using weak encryption algorithms
- Encrypting data with weak or short keys
- SSL/TLS certificate authority is not preferred
- Hosting the database and the application on the same network
- Lack of updates in database and software
- Lack of vulnerability detection or non-repetition

The most difficult part of storing sensitive data is ensuring data security and integrity. For this, Data Loss Prevention (DLP), intrusion detection (IDS), or prevention systems (IPS) are widely used [6].



Current solutions are based on policy and rule-making principles. In other words, security weaknesses occur in possible wrong or incomplete configurations [7]. Recently, blockchain technology using cryptographic methods has been introduced to protect data security and integrity [8].

Blockchain technology emerged in 2008 with a study by Satoshi Nakamoto named "Bitcoin: Peer-to-Peer Electronic Cash Payment System" [9] and the structure that forms the basis of Bitcoin, which is presented as a crypto digital currency. In order to eliminate technology centralization, it stores copies of data by distributing copies of data to users on the network, using strong encryption methods, and based on consensus. Although it has been associated with the financial sector since it was first introduced with Bitcoin, the increasing and widespread studies show that the blockchain is a security-purpose database that can be used in different sectors.

End-user grievance resulting from data leaks and weaknesses in e-commerce applications is the motivation for the study. In this study, a blockchain-based model is presented for the secure storage of credit card information in e-commerce applications. SHA256 hash algorithm is used for the data integrity of the model. Since the hash is a one-way function, encrypted data cannot be restored. Therefore, the credit card information reused by the customer is encrypted with the AES symmetric algorithm. In order to test the proposed system, an e-commerce application was developed with ASP NET and the data transmitted to the blockchain with API. In the last step, 50 different credit card information was added to the blockchain and temporal performance measurements were carried out.

2. Related Work

Blockchain technology has wide use in cryptocurrency (finance), health, insurance, logistics, advertising, copyright protection, energy, and social applications [10-11]. Although it is not a very easy technique that can be applied in every field, application trials and developments continue. Although the services of the blockchain were used from the first digital currency to smart contracts, the security of this technology is based on cryptography [12].

There are problems such as fraud, commission fees, the payment between buyer and seller, and unauthorized use of personal data in E-commerce systems that have developed with digitalization. Blockchain technology has the potential to offer reliability and transparency with payments and smart contracts. [13-14]. The use of blockchain in cyberattack prevention will be able to gain gains by preventing the damage, loss, and abuse caused by security vulnerabilities. In addition, huge damages to institutions, individuals, or governments in monetary terms due to cyber-attacks can be avoided by the application of this technology [15-16].

In their studies Shaikh and Iliev presented a transaction processing system that provides secure transactions in E-commerce and a model that protects E-commerce transactions against denial of service (DoS) attack. [17]. The transaction processing system is designed using blockchain technology, zero-knowledge proof, and modified elliptic curve cryptography encryption. The Transaction processing system designed has increased the security of general E-commerce transactions by providing privacy and integrity services. With these two security solution models offered, it is easier to protect the confidentiality and integrity of E-commerce transactions.

In cross-border e-commerce and supply chain management using blockchain technology, models and methods framework have been developed in which the key recovery problem can be successfully solved, protection against clone attack, fake tag attack, and fake product attack. The framework includes a number of blockchain-based models, including a multi-chain model, data management model, and block structure model [18].

In a study investigating the resistance to cyber-attack types in distributed systems, a blockchain-based communication architecture was proposed to guarantee the integrity assurance and permanent recording of the messages exchanged between all parties, including Unmanned Aerial Vehicles and ground control stations in the military autonomous system network. The proposed architecture has been shown to protect against data integrity compromise and authentication spoofing attacks [19].

In line with the studies in the literature, security, data integrity, transparency and performance increase stand out. Most of the studies were conceptual and theoretical, and some were experimentally applied. Although blockchain technology has been emphasized in terms of providing security, there are still a variety of security problems. Research on blockchain security is mostly technical; important business, organizational and operational problems were overlooked [20-22]. Some security gaps can also be seen in the Bitcoin structure. There is a wallet structure that a person needs for blockchain-based Bitcoin, and although it is safer to use the extended public key in this structure, the wallet can still be compromised. The extended public key can reveal the chain code, which has an important role in deriving the key, and the attacker can brute force attack all chain codes using the public key together with a public chain code [23].

As the literature studies are examined, the use of cryptocurrencies in payment methods and their security are oriented due to the increasing number of cryptocurrencies with blockchain technology. Unused studies with blockchain technology focus on secure communication, not secure storage of credit card information in e-commerce applications. These studies ensure security by using different encryption algorithms in the communication of services or applications. Although it is generally advocated not to store credit card information, many applications store information. Credit card leaks, which have increased recently, prove this. In the proposed model, it appears that it provides aspects of privacy, integrity, non-repudiation, and auditability in both communication and storage of credit card information (Table 1). The study aims to securely store credit card information in e-commerce applications without the need for storage techniques belonging to a different source or institution.

Table 1. Comparison of studies on the storage of credit card information

Studies	Blockchain	Storage Location	Encryption	Privacy	Integrity	Non-repudiation	Auditability
Our Model	+	Cloud	AES 256	+	+	+	+
[24]	-	No	RSA	+	+	-	-
[25]	-	No	RSA	+	+	-	-
[26]	-	Cloud	Scale-based Secure sensitive data (SSSD)	+	-	-	+
[27]	-	No	Hybrid the El Gamal encryption scheme with RSA	+	+	+	-
[28]	-	No	Secure Online Transaction Algorithm	+	+	-	-

3. Blockchain

Blockchain is also known as a distributed ledger in which all digital transactions between the participants, called nodes, are recorded. Unlike a centralized system that needs verification by a single authority, the blockchain offers a distributed system that performs decentralized authentication in which different nodes in its network communicate with each other using the peer-to-peer protocol (Figure 1).

The blockchain consists of linked list-like block sequences that store information such as the timestamp and transaction data along with the encrypted hash value (function) of the previous block in its own network. The Hash value of the previous block is written to the next block, a connection is established between the two blocks and a chain of consecutive blocks is formed (Figure 2). This process, which is repeated in a sequence, verifies the integrity of the previous block up to the first block known as the genesis block. The hash value of each block represents a unique code that belongs to that block and is derived from the records it contains using the SHA-256 algorithm. If the information in the block is changed, the hash value of the block also changes. Accordingly, data in any block cannot be changed retrospectively without changing the hash values of all subsequent blocks.

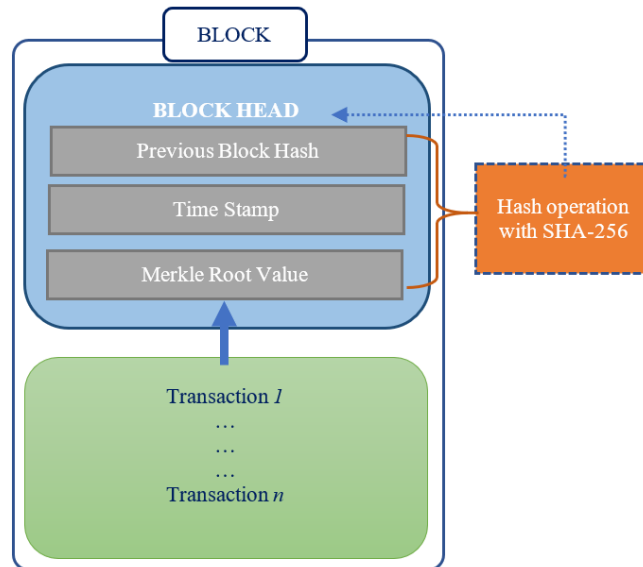


Figure 1 Block Structure

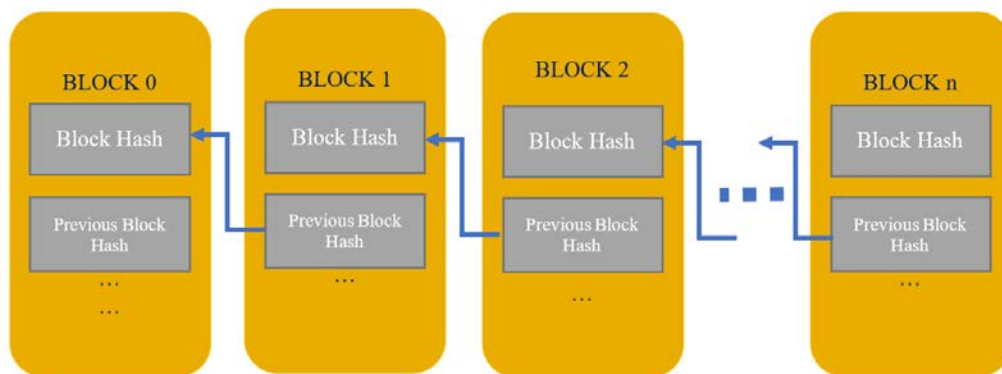


Figure 2 Basic Blockchain Representation

Commonly, Blockchain is classified into two groups as public and private. Consortium Blockchain is also encountered as a third type [29].

A public blockchain is an important structure in eliminating privacy, central authority cost, and ensuring data integrity. The private blockchain stands out in providing a central authority structure, where transactions are kept under control, data are not open to the public, and transaction speed is required. Consortium blockchain can be thought of as a semi-private blockchain. It has a structure in which fewer nodes join the network compared to the general blockchain.

In the public (distributed and open) blockchain network, data storage may be inconvenient in terms of security and privacy. Although the data is encrypted and secure in the distributed blockchain structure, there may be a possibility of leaking the information of the people with the key. In the special blockchain structure, permission must be obtained from the network structure in order to access the stored data. It can be preferred in cases where private blockchain transactions are carried out in a controlled manner, the data should not be open to the public, and the system is expected to operate quickly. Using a private blockchain structure/network in cases such as information leakage can alleviate concerns [30].

In order for a transaction to be valid and occur in the blockchain network, each block needs to look at the hash value of the previous block and have the correct hash value [31]. In case of an attack on the network and an attempt to change the information of any block, the hash value associated with the block will also change. It can be understood that there is an attack on the network since the changed hash value will not match the original. Since changing the hash value with an external intervention will break the connection between the blocks, access to other blocks will be eliminated and in this sense, data security will naturally be provided.

4. Model Architecture

In the proposed study, a local private blockchain-based database model has been developed to securely store credit card information in e-commerce applications when needed. The study consists of two parts. In the first part, an e-commerce application has been developed to collect credit card data. In the second part, data from the e-commerce application is stored in the blockchain structure. Credit card information of successful payments made in the e-commerce application is stored in a block of the block chain. As can be seen in the architecture of the model proposed in Figure 5, every β_n data coming from the application reaches the block chain server via API services. Here, the data is encrypted with AES and the previous hash data is added for data integrity to form the chain block. Encryption algorithms are divided into symmetric and asymmetric. There is a public key in symmetric encryption and a private key in asymmetric encryption. Distribution of private key in asymmetric encryption causes performance slowdown. In this study, the symmetric encryption algorithm AES was preferred. AES algorithm; It has been selected from hundreds of algorithms by the National Institute of Standards and Technology (NIST) based on many criteria such as robustness, fast working on hardware and software [32].

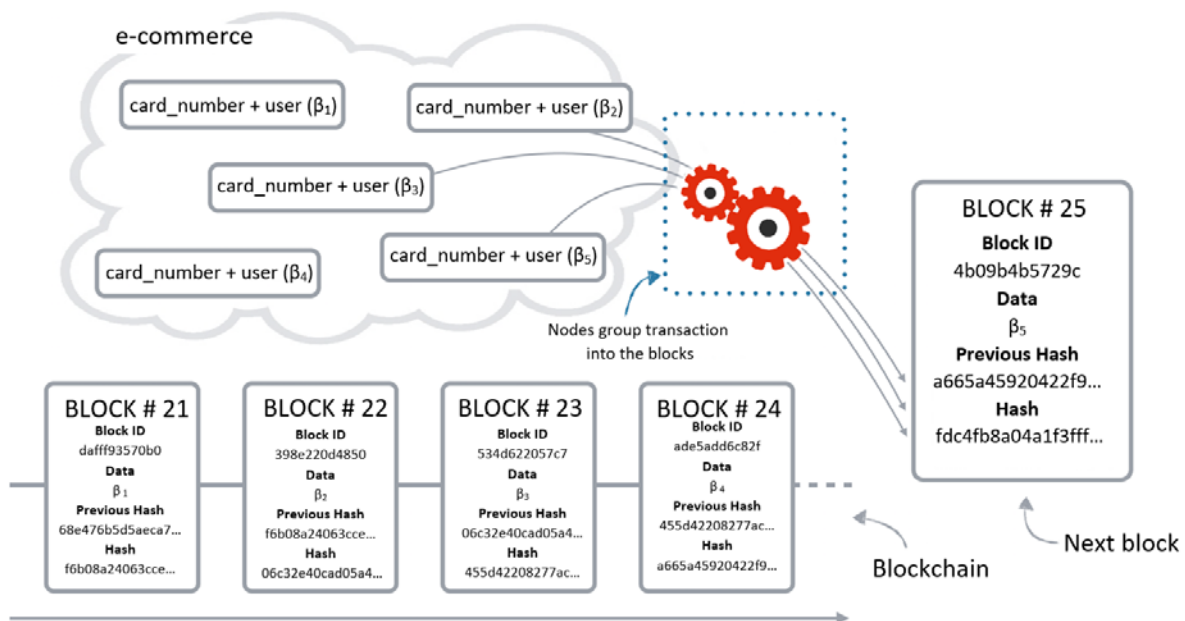


Figure 5 Working Scheme of the Proposed Blockchain Structure

4.1 Development of E-commerce Application

For testing the proposed blockchain-based security data storage system, the e-commerce application whose interface is shown in Figure 6 (a) has been developed. In the application, 3 layered architecture is used as presentation, business and data layer. In the presentation layer; A ready-made e-commerce template was placed on the ASP.NET architecture and formal (HTML + CSS) changes were made. In the data layer; The relational database shown in Figure 6 (b) has been created in the MS-SQL database. Sample computer products have been added to this database for test use. In the business layer; Database query functions are coded using the LINQ query structure.

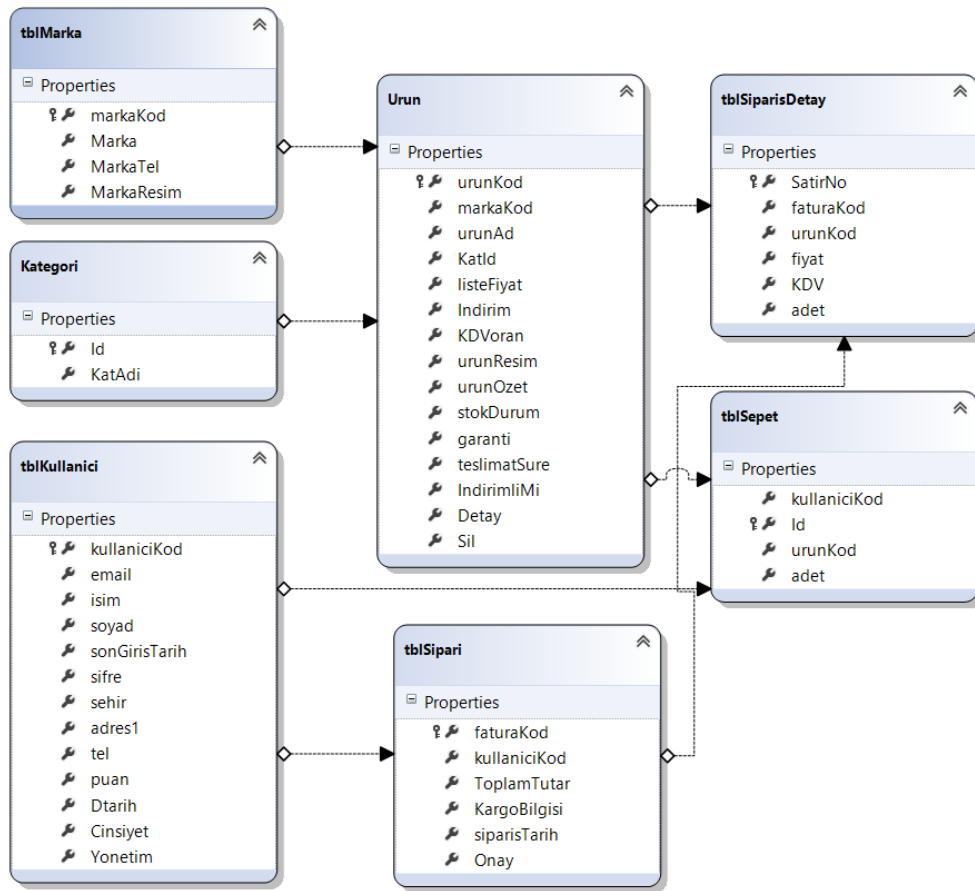
4.2 Development of Blockchain-based Secure Storage Model

A blockchain to be used for database purposes is not sufficient to process high volumes of data. In other words, a huge amount of data cannot be stored in a block. It also lacks built-in search and indexing capabilities [33]. BigchainDB was used to store credit card information in the e-commerce application in the proposed study. BigchainDB combines the main advantages of distributed DBs and blockchains with an emphasis on scale. It enables querying of data on the MongoDB structure [34]. It was used 2

servers to develop and publish the applications. The e-commerce application was used in Windows IIS that has 1 CPU, 2 GB RAM, and for BigchainDB was used UBUNTU virtual server that has 2 CPU, 4 GB RAM.



(a)



(b)

Figure 6 E-Commerce Application, a) Web Interface of the Application b) Relational Database Design

Credit card data coming from the e-commerce application will be transferred to BigchainDB Server over JSON services with HTTP API. For this, MongoDB and BigchainDB were configured on the local server with Ubuntu operating system (Ubuntu >= 16.04) (Algorithm 1). After configuration, the root url list can be accessed via BigchainDB Server localhost: 3352 /api /v1/ as shown in Algorithm 2.

Algorithm 1 BigchainDB local server configuration

```

1 $ export
2 STACK_REPO=bigchaindb/bigchaindb
3 $ export STACK_BRANCH=master
4 $ export TM_VERSION=0.22.8
5 $ export MONGO_VERSION=3.6
6 $ bash stack.sh

```

Algorithm 2 BigchainDB Server HTTP Client-Server API

```

1 HTTP/1.1 200 OK
2 Content-Type: application/json
3 {
4   "api": {
5     "v1": {
6       "assets": "/api/v1/assets/",
7       "blocks": "/api/v1/blocks/",
8       "metadata": "/api/v1/metadata/",
9       "outputs": "/api/v1/outputs/",
10      "streams":
11      "ws://localhost:3352/api/v1/streams/valid_transactions",
12      "transactions": "/api/v1/transactions/",
13      "validators": "/api/v1/validators"
14    }
15  },
16  "software": "BigchainDB",
17  "version": "2.2.1"
18 }

```

C # programming language and BigchainDB libraries are used to create the blockchain and to process incoming GET / POST requests. CREATE and TRANSFER classes are created in the block chain software and communication is carried out over these classes. The interface of block, transactions and public key requests in the blockchain software is shown in Algorithm 3.

Algorithm 3 BigchainDB Server HTTP Client-Server API

```

1 Get Blocks given block_id [C#]
2 public static async Task<Block> getBlock(int block_Id,
3 IBlockchainConfigurationBuilder builder = null)
4 Get Blocks given transaction_id [C#]
5 public static async Task<IList<int>>
6 getBlocksByTransactionIdAsync(string
7 transaction_Id, IBlockchainConfigurationBuilder builder = null)
8 Get Outputs given a public_key [C#]
9 public static async Task<List<OutputList>> getOutputsAsync(string
10 public_Key, IBlockchainConfigurationBuilder builder = null)

```

5. Testing the Application

In order to store credit card information in the blockchain structure, the user first adds the products to the basket, as shown in Figure 1, from the e-commerce application. Then he enters the credit card information (credit card information created for testing purposes) on the payment screen. After clicking the payment button, if the payment is made, the credit card information is sent to the HTTP API to be added to the block chain.


My Items In The Basket					
Product Code	Name of the product	Price	Unit price		
3511	Tablet	3	120	Update	Remove from Basket
3511	Tablet	2nd	120	Update	Remove from Basket
3506	Mobile phone	one	600	Update	Remove from Basket
3518	Iconia W510	one	1350	Update	Remove from Basket
3507	500 Gb SanDisk	one	250	Update	Remove from Basket
3516	Notebook	one	2500	Update	Remove from Basket
3516	Notebook	one	2500	Update	Remove from Basket

Subtotal:	7800.00 TRY
VAT (18%)	1404.00 TRY
Total amount :	9204.00 TRY

Credit card

Amount To Be Withdrawn From Your Card:

name on the card:

Card number: 

Security Code (CCV):

Expiration date:

Card Type:

Bank of the Card:

I Have Read, Understand and Approve the Distance Sales Agreement

Figure 7 E-Commerce application basket and payment form

Algorithm 4 Query request and transaction response into the blockchain

```

1 GET /api/v1/blocks/1 HTTP/1.1
2 Host: http://localhost:3352/
3 -----
4 HTTP/1.1 200 OK
5 Content-Type: application/json
6 {
7   "height": 12,
8   "transactions": [
9     {
10      "asset": {
11        "data": {
12          "b1": "554823589989898- h4k5sdkf67"
13        }},
14      "id":
15      "c5f40d3880b454c1ce659a90498c579f03173ccfdce038599d4a5c2440b30616",
16      "inputs": [
17        {
18          "fulfillment":
19          "pGSAIDE5i63cn4X8T8N1sZ2mGkJD51NRnBM4PZgI_zvzbr-cgUCy4BR6gKaYT-
20          tdyAGPPpknIqI4JYQQ-p2nCg3_9BfOI-15vzldhyz-j_LZVpQAlRmbTzKS-
21          Q5gs7ZIFaZCA_UD",
22          "fulfills": null,
23          "owners_before": [
24            "c2FzYWRzZGRzZmRmZGZkZ2ZnZmdoZ2hnaAsdzYcWfamZsZHNqZmIgc2R"
25          ]
26        },
27      "metadata": {
28        "sequence": 0
29      },
30      "operation": "CREATE",
31      "outputs": [
32        {
33          "data": "b1",
34          "condition": {
35            "details": {
36              "public_key":
37              "4K9sWUMFwTgaDGPfdynrbxWqWS6sWmKbZoTjxLtVUibD",
38              "type": "ed25519-sha-256"
39            },
40            "uri": "ni:///sha256;
41            PMIICXQIBAAKBgQCUENCfgan0HTeeHXSPcz851LxHpno43I29hZQ4LX8Ko0hXX4Zk"
42          },
43          "public_keys": [
44            "MIICXQIBAAKBgQCUENCfgan0HTeeHXSPcz851LxHpno43I29hZQ4LX8Ko0hXX4Zk"
45          ]
46        },
47      "version": "2.0"
48    ]}]

```


The request to add the BigchainDB API to the blockchain initiates a new create transaction and saves the incoming data in the last block of the chain. The integrity of the data is ensured by the SHA 256 hash function in the block structure. For data security, each incoming data block is encrypted with AES symmetric algorithm. The *privatekey* required for decrypting the encrypted data is stored on the local server. In Algorithm 4, the display of the record made after a payment transaction and the transaction query are given.

Within the e-commerce application, the administrator can list all the data in the blockchain database if the authorized user wants it (Algorithm 5).

Algorithm 5. JSON view of data in blockchain

```

1 GET /api/v1/assets/?search=creditcard_db HTTP/1.1
2 Host: http://localhost:3352/
3 -----
4 HTTP/1.1 200 OK
5 Content-type: application/json
6 [
7   {
8     "metadata": {"b1": "5584519788679753"},
9     "id": "
10 7dc96f776c8423e57a2785489a3f9c43fb6e756876d6ad9a9cac4aa4e72ec193"
11   },
12   {
13     "metadata": {"b2": "5109789159864971"},
14     "id": "
15 4814d92093ac8a0f4a2163ab87dee509ba306a58f5888be0edcb2fcd0712028b"
16   },
17   {
18     "metadata": {"b3": "5108451207830725"},
19     "id": "
20 76a8277347f52530e1cf979175a178980b3a180d176165c985d85f7e142f1eed"
21   }
22 ]

```

In the proposed blockchain structure, queries are carried out over all interconnected blocks (Figure 8). Therefore, it is necessary to ensure the security of the network and web application. The internal mechanism described in the modeling of the blockchain network provides its own security. Goldfinger, Finney, Spending, Feather, Vector76, Netsplit, and Eclipse attacks are used in distributed architectures. Since a special and local blockchain structure is used with BigchainDB in this study, it will not be exposed to distributed attacks. In particular, sending data to the model via APIs may cause problems in

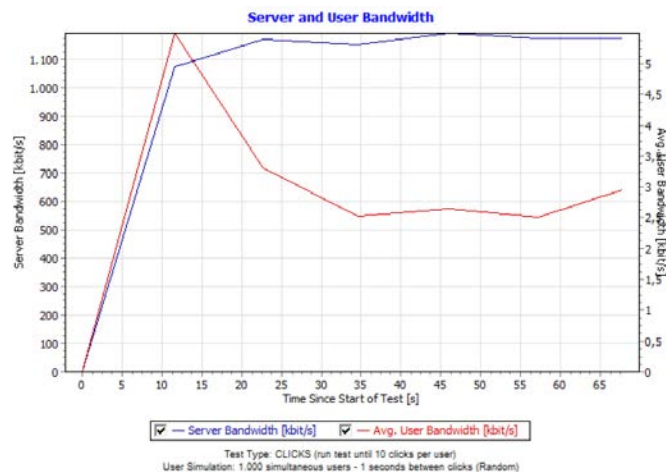


Figure 8 DDOS test attack bandwidth simulation

possible Distributed Denial of Service attacks (DDOS) attacks. Therefore, a 1000-user DDOS attack simulation was performed to see the load stress on the proposed model. According to the test results, the server can respond to what 1000 users want. Since the increase in the number of users and requests will increase the server load, there will be a delay. This problem can be overcome with application bandwidth or load balancer systems. In addition, possible attack situations can be prevented by Firewalls, IDS, or IPS systems. Although web applications do not have definitive solutions to prevent DDOS attacks, the proposed system is not considered a disadvantage.

In the second test phase, query response time was also evaluated in line with the increasing credit card data of APIs. Therefore, increasing credit card data also increases the query response time. In the BigchainDB structure, the request time account is calculated as $t_{total} = t_{in} + t_{internal} + t_{out}$ (Figure 9).

Where $t_{internal}$ is the internal software query delay and it changes depending on the number of blocks in the blockchain.

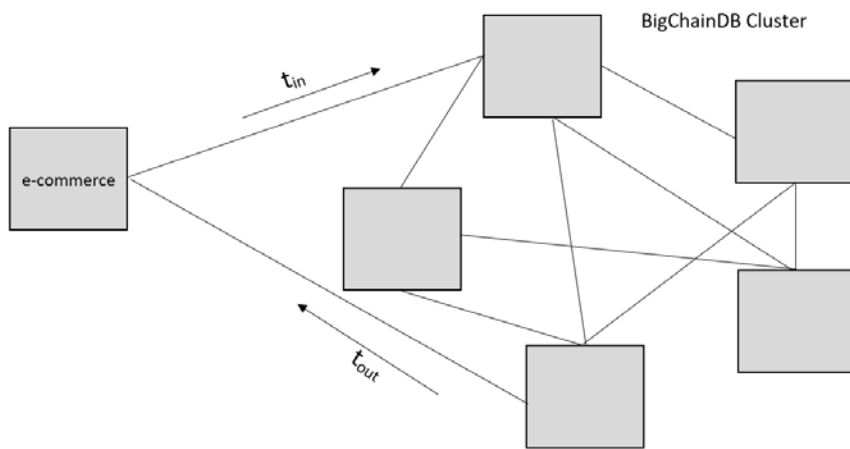


Figure 9 Query communication between BigchainDB and e-commerce application

In the e-commerce application, the total times of GET and POST requests are stored in t_{total} variable. During the test period, 50 credit card information was included in the blockchain. The times resulting from this are given in Figure 9. It is seen that the increase in the amount of data in the blockchain also increases the t_{in} and t_{out} times. In addition, the $t_{internal}$ that occurs in blockchain software creates more delay in some queries. Apache JMeter tool was used for all measurements.

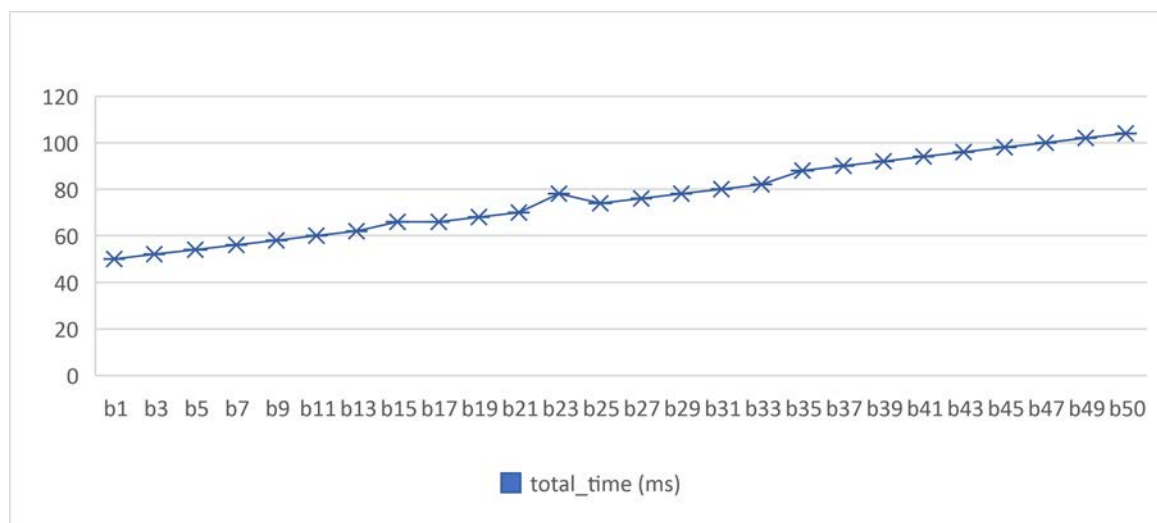


Figure 10 t_{total} Times Between BigchainDB and E-Commerce Application

6. Conclusion

E-commerce applications and the widespread use also create security weaknesses. As a result of security vulnerabilities, credit card information must be securely protected. This study, it is aimed to securely store credit card information in the blockchain-based database in an e-commerce application. An e-commerce application has been developed for the proposed model. Credit card information sent from the e-commerce application is stored in the MongoDB-based blockchain created with the BigchainDB architecture. The data in each block is encrypted with the AES asymmetric algorithm. Within the application, the authorized user can query the data with API services. When the proposed system is tested, it is seen that the blockchain structure provides data security and integrity. The increase of blocks in the blockchain structure delays the query times. This situation negatively affects the performance of the blockchain model. In future studies, it is foreseen to increase the performance by using different algorithms to encrypt and decrypt the data in the block. Also, it is aimed to develop the blockchain structure with a distributed architecture.

References

- [1] M. Halaweh, "Cash on delivery (COD) as an alternative payment method for e-commerce transactions: Analysis and implications". *International Journal of Sociotechnology and Knowledge Development (IJSKD)*, vol. 10(4), pp. 1-12, 2018.
- [2] S. Fatonah, A. Yulandari, and F. W. Wibowo, "A review of e-payment system in e-commerce". *In Journal of Physics: Conference Series*, vol. 1140, p. 012033. IOP Publishing, 2018.
- [3] K. F. Herkenhoff, and G., Raveendranathan" Who bears the welfare costs of monopoly? The case of the credit card industry" (No. w26604). National Bureau of Economic Research, 2020.
- [4] K. Kalkan, F. Kwansa, and C. Cobanoglu, "Payment Card Industry Data Security Standards (PCI DSS) Compliance in Restaurants". *Journal of Hospitality Financial Management*, vol. 16(2), 3, 2010.
- [5] A. Ukidve, D. Smantha, and M. Tadvalka, "Analysis of payment card industry data security standard [PCI DSS] compliance by confluence of COBIT 5 framework". *International Journal of Engineering Research and Applications*, vol.7(01), p. 42-48, 2017.
- [6] W. Feng, C. Liu, Z. Guo, T. Baker, B. Cheng, and J. Chen, "Data loss prevention and storage utilization improvement of the hidden volume on mobile devices", *In 2019 IEEE Symposium on Computers and Communications (ISCC)*, pp. 1-6. IEEE, 2019.
- [7] M. H. Furhad, S. Sadik, and M. Ahmed, "Chapter Nine Exploring E-Commerce In Cyber Security Context Through Blockchain Technology". *Blockchain in Data Analytics*, 2020.
- [8] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey". *IEEE Access*, vol. 8, 16440-16455, 2020.
- [9] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2018. [Online]. Available: <https://git.dhimmel.com/bitcoin-whitepaper/>. [Accessed: 21-Feb-2021].
- [10] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, "A survey of blockchain applications in different domains." *In Proceedings of the 2018 International Conference on Blockchain Technology and Application*, pp. 17-21, 2018.
- [11] M. Tekin, D. Öztürk, İ. Bahar, "Akıllı Lojistik Faaliyetlerinde Blokzincir Teknolojisi", *Kent Akademisi*, vol. 13(3), p. 570-583, 2020.
- [12] A. Ghosh, S. Gupta, A. Dua, N. Kumar, "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects" *Journal of Network and Computer Applications*, 163, 102635, 2020.
- [13] X. Zhu, D. Wang, "Research on Blockchain Application for E-Commerce, Finance and Energy" *In IOP Conference Series: Earth and Environmental Science*, vol. 252, no. 4, p. 042126, IOP Publishing, 2019.

- [14] L. Ismanto, H. S. Ar, A. N. Fajar, S. Bachtiar, "Blockchain as E-Commerce Platform in Indonesia", *In Journal of Physics: Conference Series*, vol. 1179, p. 012114. IOP Publishing, 2019.
- [15] S. Demirkan, I. Demirkan, A. McKee, "Blockchain technology in the future of business cyber security and accounting", *Journal of Management Analytics*, vol. 7(2), p. 189-208, 2020.
- [16] Ö. Aydın, S. Yükcü, "Siber Saldırı Önlemede Blokzinciri Teknolojisinin Fayda Maliyet Açısından Değerlendirilmesi". *MANAS Sosyal Araştırmalar Dergisi*, vol. 9(4), p. 2519-2530, 2020.
- [17] J. R. Shaikh, G. Iliev, "Blockchain based confidentiality and integrity preserving scheme for enhancing e-commerce security" *In 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, pp. 155-158, 2018.
- [18] Z. Liu, Z. Li, "A blockchain-based framework of cross-border e-commerce supply chain", *International Journal of Information Management*, vol. 52, 2020.
- [19] P. Angın, "Blockchain-Based Data Security in Military Autonomous Systems". *Avrupa Bilim ve Teknoloji Dergisi*, p.362-368, 2020.
- [20] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efficient mutual authentication protocol for smart grid under Blockchain". *Peer-to-Peer Networking and Applications*, p. 1-13, 2020.
- [21] M. J. Lahkani, S. Wang, M. Urbański, M. Egorova, "Sustainable B2B E-commerce and blockchain-based supply chain finance". *Sustainability*, vol. 12(10), p. 2-14, 2020.
- [22] J. Leng, M. Zhou, L. Zhao, J. Huang, Y. Y. Bian, "Blockchain security: A survey of techniques and research directions". *IEEE Transactions on Services Computing*, 2020. DOI: 10.1109/TSC.2020.3038641
- [23] E. Zaghoul, T. Li, M. W. Mutka, J., Ren, "Bitcoin and blockchain: Security and privacy". *IEEE Internet of Things Journal*, 7(10), 10288-10313, 2020.
- [24] K. Z. Oo, "Design and Implementation of Electronic Payment Gateway for Secure Online Payment System". *Int. J. Trend Sci. Res. Dev*, vol. 3, 1329-1334, 2019.
- [25] P. Dijesh, S. Babu, & Y. Vijayalakshmi, "Enhancement of e-commerce security through asymmetric key algorithm". *Computer Communications*, 153, 125-134, 2020.
- [26] M. Sumathi, & S. Sangeetha, "Scale-based secured sensitive data storage for banking services in cloud". *International Journal of Electronic Business*, vol. 14(2), 171-188, 2018.
- [27] J. P. Magsino, E. R. Arboleda, & R. R. Corpuz, "Enhancing Security Of El Gamal Encryption Scheme Using Rsa And Chaos Algorithm For E-Commerce Application". *International Journal Of Scientific & Technology Research*, vol. 8(11), 2019.
- [28] J. Gualdoni, A. Kurtz, I. Myzyri, Wheeler, M., & S. Rizvi, "Secure online transaction algorithm: securing online transaction using two-factor authentication". *Procedia computer science*, 114, 93-99, 2017.
- [29] M. Tanrıverdi, M. Uysal, M. T. Üstündağ, "Blokzinciri Teknolojisi Nedir? Ne Değildir? Alanyazın İncelemesi" *Bilişim Teknolojileri Dergisi*, vol. 12(3), p. 203-217, 2019.
- [30] Bankalar Arası Kart Merkezi, "Blockchain 101 v.2", 2015. [Online]. Available: <https://bctr.org/dokumanlar/Blockchain101v2r2.pdf>. [Accessed: 05-Feb-2021].
- [31] Parasozlugu, "Public (Genel) Blok Zincir (Blockchain) Nedir?" 2017. [Online]. Available: www.kriptoparasozlugu.com/genel-public-blok-zincir-blockchain-nedir/. [Accessed: 11-Feb-2021].
- [32] Das, D., Danial, J., Golder, A., Modak, N., Maity, S., Chatterjee, B., Sen, S EM and Power SCA-Resilient AES-256 Through > 350x Current-Domain Signature Attenuation and Local Lower Metal Routing. *IEEE Journal of Solid-State Circuits*, 56(1), 136-150, 2020.
- [33] M. Simić, G. Sladić, and B. Milosavljević, "A case study IoT and blockchain powered healthcare". *In Proc. ICET*, pp. 1-4, 2017.
- [34] BlockchainDB, "Features & Use Cases", 2018. [Online]. Available: <https://www.bigchaindb.com/features/>. [Accessed: 05-Feb-2021].