Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 6, No. 4, November 2021, Pp. 277-286

Optimization of system authentication services using blockchain technology

Imam Riadi[1], Herman[2], Aulyah Zakilah Ifani[*3]
Departement of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia[1]
Departement of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia[2,3]

Article Info
Keywords:
Authentication, Blockchain, Networkminer, NFLDC, Wireshark

Article history:
Received: August 19, 2021
Accepted: October 18, 2021
Published: November 30, 2021

Cite:
Riadi, I., Herman, & Aulyah Zakilah Ifani. (2021). Optimization of System Authentication Services using Blockchain Technology. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 6(4). https://doi.org/10.22219/kinetik.v6i4.1325

*Corresponding author
Aulyah Zakilah Ifani
E-mail address:
aulyah1908048022@webmail.uad.ac.id

Abstract
With the development of the era, one thing that must be considered for security is the Login System. In most cases, user login information is stored on the server. This gives access to sensitive informatio, many hackers easily break into data from users. Based on these problems, this research focuses on data security authentication in the form of usernames and passwords in the login system. Authentication using blockchain is used to reduce malicious access and increase security for the authentication process. One of the innovative technologies that can solve these problems is Blockchain Technology. Using blockchain technology, hackers will find it difficult to change and modify the same data on all computers at the same time because it takes a very long time to crack the encryption code on each block of data in the entire computer network. Data storage or transactions in the blockchain are stored in the form of hashes. This makes it difficult for hackers to break into it. Tests in this study using Wireshark tools and network miner. Based on the research conducted, the test was conducted as many as 5 times with two scenarios, namely authentication of the login system before using the blockchain and after using the blockchain. The results obtained. The, system built using blockchain can secure data. The test results obtained that data in the form of usernames and passwords were converted into hashes and with the immutable nature of the blockchain, data from users could not be changed or replaced by anyone.

1. Introduction

Nowadays the internet is becoming very famous, the use of the internet is not only among young people but among adults many who use the internet make it a necessity. It is this need for the internet that makes it very easy for a person to access it [1]. Services to users who need a wireless network can be accessed through smartphones, laptops, and other mobile devices [2][3]. The advantages obtained in using wireless in terms of mobility also get a big challenge in the form of securing the wireless network, many illegal attacks to get usernames and passwords from users [4]. Security systems and login processes usually use usernames and passwords as authentication methods. It is used because of the ease of implementing it [3]. Disadvantages when using authentication are usernames and passwords that are stored in a database and provide an easy effect to hack for example using Wireshark and network miner [5]. Authentication is proof of an entity's identity. For example credit cards, or machines and people [2]. Improperly secured authentication processes are vulnerable to data theft from irresponsible users. Data in the form of usernames and passwords are very easy to hack by irresponsible people, for example by using Wireshark tools, black box testing, network miner, burp suite, etc. This is the basis, data from users must be secured. The login system requires authentication to secure the identity of the user, so this study used blockchain technology to secure data from users and the framework used in supporting system development and overcoming system weaknesses i.e. Network Forensic Development Life Circle (NFDLC).

Blockchain is a decentralized and distributed technology [6][7]. Blockchain is defined as a distributed database [8]. The important thing about blockchain has three elements: replicated ledger, cryptography, peer-to-peer networking [9]. Blockchain is additional security while cryptography maintains the confidentiality and authentication of data exchange [10]. Blockchain technology makes it difficult for hackers to change and modify the same data on all computers at the same time because it takes a very long time to decode the encryption on every block of data across the computer network. There are two types of records on a blockchain system: transactions and blocks. Blockchain transactions are stored in one block together. Each block forms a network that contains cryptographic algorithms. Cryptographic algorithms are used to retrieve data from previous blocks and convert them into compact strings that can detect sabotage [11][10]. Each block has a hash value and each of those blocks gets a value from the previous hash [12]. Figure 1 shows the blockchain scheme.

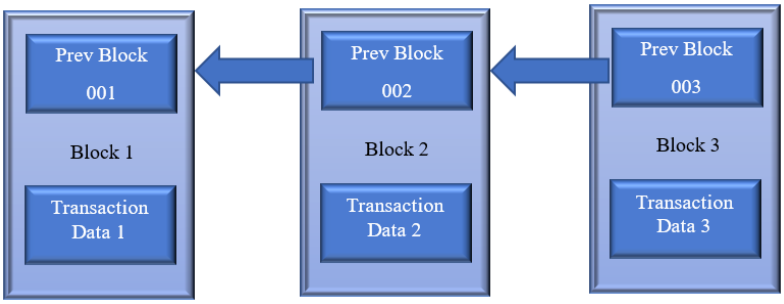

Figure 1. Blockchain Scheme

Figure 1 describes each block connected through a hash of the previous block. The first block has a connection with the previous block by entering hash and proof values. Each new block has an attribute called a hashid which is the hash (SHA256) of 4 strings i.e. hash id, index, data, and timestamp taken from the previous block. Noprevious block which is reffered by the geneses block. The, block node of the blockchain is called genesis block. Timestamp to record node time [13]. This login system uses blockchain technology, where the first block is connected to the previous block using hash and proof. Proof-of-work is a procedure that sets the cost of grouping transactions in a specific order and adding them to the blockchain [14]. Blockchain uses a peer-to-peer network for file sharing. Peer-to-peer is a collection of interconnected nodes. These nodes are individual computers that receive inputs and perform functions and provide outputs. The way each blockchain works is linked to the hash of the previous block, after validation and consensus decision. Mining process creates a new block and attached. Theoretically, the deeper position of a block in the chain the less possibility of the data in the block to be manipulated. The process of storing data or transactions on the blockchain, stored in hash form, where this hash if in the blockchain is used as a pointer or link to generate and validate new blocks**.**

Blockchain was deliberately invented to facilitate transaction between A and B without intermediaries, reduce the cost of transactions and increase security of the transaction [15][16]. Blockchain is a tamper-proof block stored in each participating node. Each block records a set of related metadata data transactions [17]. The blockchain contains transactions stored in a block of data [12]. Each block stores a hash derived from the previous block so that a blockchain is formed. The first block is called the genesis block which is the only block that does not have a hash of the previous block [18][19]. Blockchains also have cryptographic algorithms that keep strands of the blocks secured in the blockchain [20]. This algorithm will make it easier for the system to track in case of sabotage of the blockchain [6][21].

Some previous research related to blockchain technology as adjunct security is as follows. Research from Fat et al., on securitizing sensor data on IoT networks. The results of this study suggest that the Internet of Things can use blockchain for the securitization of data [22]. research from Zhang et al. researched blockchain security and privation. The result is that developing cryptographic algorithms as well as other security and privacy methods will be key to enabling the technology in the development of blockchain and its applications in the future. Blockchain provides security and cryptography as authentication [23], then research Singla et al. researched by developing a leave application using smart contracts. The system in this study was successfully developed using solidity as well as ethereum [24]. Aprialim et al., research on the application of blockchain with the integration of smart contracts on crowdfunding systems that explain crowdfunding systems operate using a centralized system, so as not to provide data security and transparency of fundraising activities in full. The functional needs of the system are proven to work according to the design of the use case for either fundraising users or funders [25]. Research from Hattab & Taha., research on blockchain cryptocurrency technology (cryptocurrency), aims to illustrate the opportunities obtained from the technology that plays a role in cryptocurrencies [8], then research Rahardja et al., This research shows that blockchain can be used as an easier, more efficient payment, and the blockchain makes the system as tracking and can synchronize the data in the blockchain to all users [26], then research from Fadlil et al., Explaining that modifying cryptocurrencies and blockchain technology can function properly on the system, it can be proven by the success of chain validation that detects the or absence of immutability data displayed invalid columns that are true or false [27]. Next about security and privacy on blockchain [23]. Research on data security for school service top-up transactions combination blockchain technology modification. The results obtained from this research are that modifying cryptography and blockchain technology can function properly on the system [27]. Various applications of blockchain technology are about health, the Internet of Things (IoT), fundraising, digital asset management, education, etc [28][29][30]. Blockchain is also used to enhance the security of e-commerce systems [31] as well as e-voting systems [32]. Blockchain can give confidence to third parties who oversee the process between sellers and buyers to confirm the authenticity of data and information [33].

Based on previous research this research aims to secure the login security system with blockchain authentication and conduct system testing. Blockchain uses the digital signature feature to make transactions so that data from users cannot be changed and modified. This is the advantage of blockchain. This blockchain-based authentication system

can be used to secure authentication processes in a decentralized and irreversible way. The login security system is modified using blockchain technology. Based on this, it can answer the formulation of problems that can be described, namely how to develop a login security system using blockchain technology, how the results of the system comparison using Wireshark and network miner, and what percentage of test results when viewed from blockchain data logs. The logs in this study can be seen in Equation 1.

$$E = 100 - \left(\frac{U_{BC}\ x\ NoS}{\sqrt{ReDB}}\right) \quad (1)$$

Where Ubc is the number of blockchain users. NoS contains the average number of blockchain logs. ReDB contains the average number of overall logs.

This research is titled optimization of system authentication services using blockchain technology. Contributions in this study use the NFLDC framework as a framework to develop systems and overcome system weaknesses. NFLDC was chosen because it has a practical and easy-to-implement research stage and has integration about the findings obtained in the forensic process. so that the most appropriate NFLDC method to achieve the objectives of this study. NFLDC is also a differentiator from previous research. The thing that distinguishes it from other research is the optimization of security using blockchain technology and to build blockhain using metamask namely crypto wallet, ganache personal Ethereum blockhain for development and testing of distrubuted application, solidity is programming languange for smart contract, nodejs is runtime environment for running the javascript, react is javascript library. As for system testing using Wireshark and network miner.

2. Research Method

The Login System is an application used as an object in this study. This application is an application or website that will be used in various other applications. The login system has a username and password that will be filled in first before logging into the system. Entering usernames and passwords becomes very vulnerable to hacking. The number of tools available makes user data threatened. This will be very dangerous if left continuously. Therefore, this research will be done optimization of login system security. Optimization of this system using blockchain is expected to be used as a security of the login system. The test was conducted using two tools, Wireshark and network miner. Wireshark analyzes network packets in as much detail as possible [34]. Wireshark uses. pcap to capture packets, pcap files, IP sources and destinations, protocols involved including protocol header data [35]. This is particularly useful for this study because it can evaluate security breach events to solve network security issues [36]. In this research, Wireshark can take all the packets that pass and select them in as much detail as possible, for example, username and password. As for network miner packet, the analyzer is used as a sniffer or tool to capture packet data that detects the operating system, hostname, session, open ports, etc. without charging a trace of traffic on the network. Network miners can parse. pcap files for offline analysis [37]. *Tested for weak usernames and passwords on the system, especially using Wireshark.* After getting the results, then the results are transferred to Network Miner. This is done to get results from Network Miner.

The research phase as a process flow of this research is guided by the Network Forensic Development Life Circle (NFDLC) framework. The NFDLC is a combination of the Information System Development Life Circle (ISDLC) and Network Forensic Readiness (NFR) methods. The concept of NFR maximizes the ability to gather credible evidence while minimizing the cost of inside response. This is a recommendation to increase the efficiency of the investigation. But there is little to discuss how to integrate NFR into a network of systems. NFR appears to investigate malicious online intruders. In this case, NFR is a case study. ISDLC is designed to incorporate security throughout the system development cycle. The ISDLC methods of each phase are analyzed and modified to include additional steps that create digital forensic embedding. Specific ISDLC modifications result in NFDLC. The NFDLC research phase contains initiation, acquisition, implementation, operations, and disposition. Figure 2 shows the system development process with the NFDLC.

Figure 2. NFDLC Methodology

The NFLDC method as Figure 2 generally describes the five main stages of performing a forensic process. The stages used include initiation, acquisition, implementation, and also operation. The NFLDC method was chosen because it has a practical and easy-to-implement research phase and has integration about the findings obtained in the forensic process.

3. Results and Discussion

The login system became an object in this study and was modified using blockchain technology. The hardware and software required in this investigation are laptop as a tester to perform scans in this study. Truffle is a development framework for daaps (decentralized applications) based on the ethereum blockchain. Ganache is part of the trufflesuite, which is used to run local ethereum servers. Solidity is used as a contract-oriented programming language for writing smart contracts. Metamask is used as a bridge that allows users to go to a web browser. Rects as a javascript library for building user interfaces.

3.1 Initiation

Case simulation of the system using the Visual Studio Code programming language. The result of the simulation stage is a system that is ready to be tested and run. The login system utilizes the Ethereum blockchain platform which implements blockchain technology and smart contracts. Web3js as an application programming interface to connect browsers with an extension called metamask as a bridge between the login system and the ethereum blockchain. This metamask acts as an ethereum wallet for information management. Meanwhile, smart contracts are built using the visual programming language studio code. In this stage of research, the user must be a member of the blockchain network, when he becomes a member then the user will have an ethereum account. An ethereum blockchain-based application must run a smart contract. So, for smart contracts will be signed first by people who already have an ethereum account to run an Ethereum-based application. The user is next if you want to log in then must have registered as a smart contract signer. Login data from users will be stored as a hash to the blockchain via smart contract. The user requests access to the website, for example, a hash derived from the user's granted credentials compared to the hash stored in the Smart Contract. So, when the user logins and the user data is suitable then the user is authorized to access the web. Conversely, if it does not fit then access is denied. Each user is required to connect with an Ethereum address that was previously done in the registration process, as this address generates the user's login hash.

3.2 Acquisition

The system that is built will be tested under two conditions, namely the system before implementation and the system after implementation using blockchain technology. System before implementation, when registering and doing the login process, users will directly enter the system without going through the authentication process. So that the process is vulnerable to break-ins. Unlike the conditions after using the blockchain, The, system will perform the authentication process first the user must be a member of the blockchain network. When the user becomes a member, the user will have an ethereum id. Simulation of blockchain using ganache. The system after using blockchain must run a smart contract. So that the smart contract will be signed by users who have ether id. The user if you want to log in must have registered as a smart contract signer. Figure 3 is the flow of the registration process before the user enters the system.

Figure 3. Registration Flow

Figure 3 shows the registration flow where commands are sent to the user and then forwarded to the browser. Metamask becomes the extension used. Then the smart contract is identified again and will appear on the web and the data can be used. Figure 4 shows the login process.

Figure 4. Login Flow

Figure 4 shows the flow of the login procedure, after the registration process is complete, then the user will be redirected to the login page in chrome. Chrome storage identifies the contract from the metamask extension storage, then on the background page contains the contract, the time stemple and the time stemple mark will be forwarded to the content script.

3.3 Implementation

The Login system in this study utilizes the use of the Ethereum blockchain platform that implements blockchain technology and smart contracts. Web3js as an application programming interface to connect browsers with an extension called metamask as a bridge between the login system and the ethereum blockchain. This metamask acts as an

ethereum wallet for information management. Meanwhile, smart contracts are built using a solidity programming language. This research user must be a member of the blockchain network. First, the user creates an account before accessing the network. Ganache becomes the place to get networked. An ethereum blockchain-based application must run a smart contract. Smart contracts will be signed first by people who already have an Ether ID to run an Ethereum-based application. Ganache already provides 10 default accounts and each account has a balance of 100 eth. The account is used for transactions on the ganache blockchain.

The user interface of ganache has 10 ethereum addresses that have 100 eth that can be used for blockchain simulation. This one ethereum network is used for one registration process if the user wants to register a new account to enter the login system then the user takes one ethereum network that is on the ganache. The user if you want to log in must have registered as a signer of the smart contract. Before the user logs into the system page, the user first connects the ganache to metamask. This metamask is a bridge for users to log into the web browser. This metamask allows users to run ethereum daaps directly in the browser. Metamask account that is already connected to the ethereum network, after which the user then performs the registration process to log in to the system. After the user registers, then the transaction details will appear to continue the transaction that has been successfully shown in Figure 5.

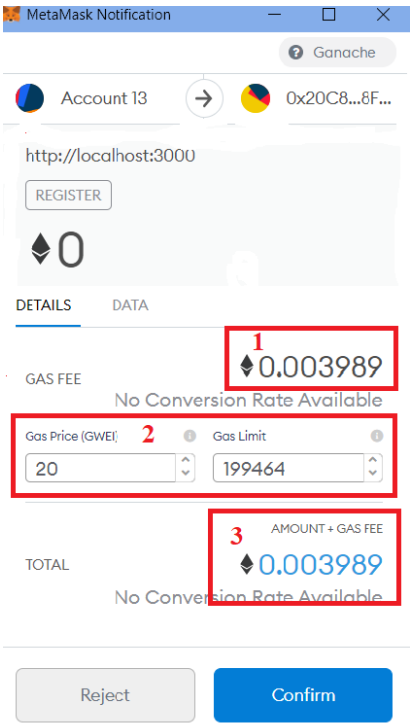

Figure 5. Transaction Details

Figure 5 shows the transaction details, where the Gas Fee (box 1) is the transaction fee paid at 0.003989. Gas Price (box 2) is paid for 20 gwei which means the transaction will be processed quite quickly. While the Gas Limit (box 2) is 199464. Amount + Gas Fee is the amount to be issued to make a transaction (box 3). When the user initiates the transaction, the request will go to the ethereum blockchain where the miner made the transaction. The price to be paid is gas limit and gas price. Once the transaction is successful it will be recorded on the blockchain and users can see the gas used. When the transaction is declared successful, the user can log in to the system using a username, password that has been registered.

3.4 Operation/Maintence

This section describes the test results using Wireshark and network miner. System testing is done with two scenarios: the login system before using the blockchain and after using the blockchain and using Wireshark tools and network miner. Users will log in by filling in a username and password. When the user logins the attacker also captures the package by using Wireshark to be able to get HTTP protocol files. Wireshark will stamp the captured packages. To get the username and password file then filter the package with the HTTP protocol file. Before using blockchain technology, users will log in by entering a username and password then the attacker will easily get data from the user. This is because the login system has not been secured. Here's Figure 6 shows user data.

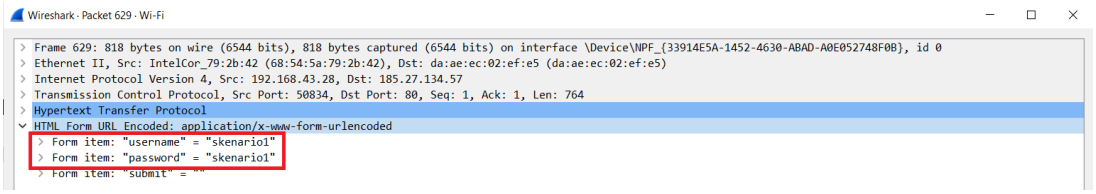

Figure 6. File Showing User Data

Figure 6 above uses a login system that has not been secured so that the security of user data transmitted over the network will be easily detected by attackers (Figure 7). So, to secure it on this research using blockchain technology that can secure data in the form of usernames and passwords from users. Testing of the login system after using the blockchain can be seen in Figure 7.

```
issuerNameHash: c72e798addff6134b3baed4742b8bbc6c0240763
issuerKeyHash: 8a747faf85cdee95cd3d9cd0e24614f371351d27
serialNumber: 0x01675c9687a505fc0a00000000f6eacb
```

Figure 7. Filter HTTP Packets After Using Blockchain

Figure 7 shows the results of HTTP packet filtering after using blockchain. Furthermore, in HTTP data there is information such as IP address 77.214.45.70 source and 192.168.1.7 destination. If the login data has been added to blockchain technology then the result of the analysis of HTTP capture packets from Wireshark is data that has been converted into a hash form so that attackers can not see the username and password sent. After testing using Wireshark, the second test will be done using a network miner. The data results are the same as those that previously used the login system before and after using blockchain technology. Files from Wireshark are stored using the format (.pcap) after which testing will be performed. Before using blockchain data in the form of usernames and passwords can be read by attackers (Figure 6). Figure 8 shows the capture before using the blockchain.

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
192.168.43.28 (Windows)	185.27.134.57 [aulyah.epizy.com]	HTTP Cookie	PHPSESSID=f04239a5190b6b201785fcc561b33593; t	N/A	Unknown	2021-08-19 15:50:31 UTC
192.168.43.28 (Windows)	185.27.134.57 [aulyah.epizy.com]	MIME/MultiPart	skenario1	skenario1	Unknown	2021-08-19 15:51:02 UTC

Figure 8. Capture Results Before Using Blockchain

Figure 8 generates data from the user in the form of a username and password. Unlike the login system that uses blockchain, data from users cannot be read by attackers. This is because the data has been converted into a hash form that makes it difficult for attackers to get usernames and passwords (Figure 7). The capture results use the network miner in Figure 9.

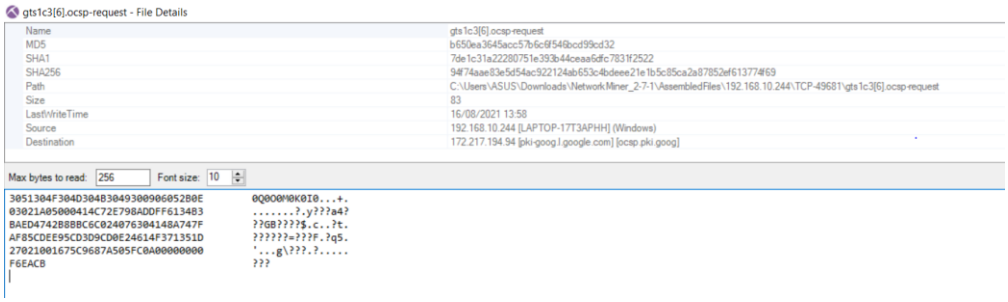

Figure 9. Capture Results After Using Blockchain

Figure 9 shows the results after using the blockchain. User data has been changed to hash form. Attackers do not get data from users.

3.5 Disposition

This section describes the data obtained in the testing process. In this case, the data in question is the testing data from the login system. One relevant form of implementation applied to support documentation is to use an external metadata pcap approach to store Wireshark files, so that data is safe for users. The disposition stage shows that blockchain technology can be applied to login authentication systems in securing user data. This is evidenced by the entire data from the user in the form of a username, a password has been encrypted or converted into a hash. The tests

showed that the overall test results of the login authentication system before and after using the blockchain using two tools namely Wireshark and network miner showed the same results. The results are obtained based on testing the login authentication system using tools, scenarios, and samples that have been determined at the initiation stage.

After implementing blockchain technology, the transmitted data becomes secure because it is converted into hash form. Table 1 shows hash transactions and gas usage data.

Table 1. Hash Transaction and Gas Usage Data

Block Number	Hash Transaction	Gas Used
1	TX 0xa0492fcd5bc4d99f475ae8f652c49f7501a7fe2c3f1819efb7adc0509584552a	147976
2	TX 0x08d46d214c66e1025ed000d81d8992d09fa547163f6e0bcb62e14f19d1f83c61	132976
3	TX 0x53420484e98de665538ce8a778a7dd3068c0c4006c78a1656fd8426e0f8fa6b732	132976
4	TX 0x22b40e6daf7c8348c27c68816ffb99d531c8877d6c62ab397d40a13ee882cb25	132976
5	TX 0x5124aed63227675ff1d4345f1a020342923c110d58395a783db86e74a00a9001	132976

Table 1 shows hash and gas usage data transactions. Hash transactions are compressed after the user registers by taking the ethreum address in the ganache. Table 2 shows the readable logs when testing.

Table 2. List of Logs Obtained Using Wireshark

No	Blockchain Log Row (NoS)	Overall Log Row (ReDB)	Information
1	15	12021	Scenario1
2	69	8234	Scenario2
3	51	2354	Skenario3
4	32	3196	Scenario4
5	31	4920	Scenario5

Table 2 presents the results of logs obtained in the blockchain process using wireshark. NoS has an average number of blockchain log lines of 39.6 logs. As for ReDB where the average overall log is 78.3 logs. Table 3 shows the comparison between the proposed scheme and the previous authentication scheme. The percentage of results from the tests carried out got results of 97.8%, where the success rate of implementing blockchain for authentication of the login system that was built was successfully carried out to secure it from hackers or irresponsible users. The 2.2% shortfall of the test results indicates that the implementation of blockchain technology still requires further improvisation and security.

Table 3. Comparison of the Security of the Proposed Scheme

Attack	System Authentication Blockchain (current research)	Shajina and Varalakhsami [35]	Yang et all [36]	Anakath et all [37]
Password Guessing Attack	Yes	No	No	Yes
Username Guessing Attack	Yes	No	No	No
Prevent replay Attack	Yes	Yes	Yes	Yes
Prevent Insider Attack	Yes	No	Yes	No
Prefer Impersonation Attack	Yes	Yes	No	Yes

Table 3 shows solutions that guarantee key security requirements. Blockchain authentication is very efficient in its operation.

4. Conclusion

Research on this login system application uses Figma in the creation of its design and system implementation using visual studio code. Blockchain technology has been successfully used to improve the security of the login system, with user login data stored as hashes to the blockchain via smart contracts. Tests were conducted that showed the condition of the system before using the blockchain and after using the blockchain. The results obtained by the system using blockchain technology managed to secure data in the form of usernames and passwords by converting the data into hashes. So, for attackers who want to get user data to have difficulty. Systems built using blockchain can secure data. This is evidenced by testing using Wireshark and network miner tools. The results of the test obtained data in the form of usernames and passwords converted into hashes and with immutable blockchain properties so that data from users cannot be changed or replaced by anyone.

References

[1] H. Lin, Z. Yan, Y. Chen, and L. Zhang, "A Survey on Network Security-Related Data Collection Technologies," *IEEE Access*, vol. 6, pp. 18345–18365, 2018. https://doi.org/10.1109/ACCESS.2018.2817921

[2] M. Rusdan and M. Sabar, "Analisis dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication," *Jt. (Journal Inf. Technol.*, vol. 02, no. 01, pp. 17–24, 2020. https://doi.org/10.47292/joint.v2i1.004

[3] A. W. P. Putra, A. Bhawiyuga, and M. Data, "Implementasi Autentikasi JSON Web Token (JWT) Sebagai Mekanisme Autentikasi Protokol MQTT Pada Perangkat NodeMCU," J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 2, pp. 584–593, 2018.

[4] Y. N. Kunang and T. Ibadi, "Celah Keamanan Sistem Autentikasi Wireless Berbasis RADIUS," Celah Keamanan Sist. Autentikasi Wirel. Berbas. Radius, vol. 34, no. 2, pp. 1907–5022, 2013, doi: 1. Yesi Novaria Kunang 2. Taqrim Ibadi 3. Suryayusra.

[5] U. Rahardja, E. P. Harahap, and D. D. Christianto, "Pengaruh Teknologi Blockchain Terhadap Tingkat Keaslian Ijazah," *Technomedia J.*, vol. 4, no. 2, pp. 211–222, 2019. https://doi.org/10.33050/tmj.v4i2.1107

[6] N. I. Fauzan, "Abstrak," vol. 4, pp. 1–15, 2018.

[7] I. Riadi, R. Umar, and I. Busthomi, "Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain," vol. 04, pp. 15–19, 2020.

[8] S. Hattab and I. F. Taha Alyaseen, "Consensus Algorithms Blockchain: A comparative study," *Int. J. Perceptive Cogn. Comput.*, vol. 5, no. 2, pp. 66–71, 2019. https://doi.org/10.31436/ijpcc.v5i2.103

[9] Y. Zheng *et al.*, "Blockchain-based privacy protection unified identity authentication," *Proc. - 2019 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2019*, pp. 42–49, 2019. https://doi.org/10.1109/CyberC.2019.00017

[10] E. P. Harahap, Q. Aini, and R. K. Anam, "Pemanfaatan Teknologi Blockchain Pada Platform Crowdfunding," *Technomedia J.*, vol. 4, no. 2, pp. 199–210, 2019. https://doi.org/10.33050/tmj.v4i2.1108

[11] W. S. Raharjo, I. D. E. K. Ratri, H. Susilo, J. Wahidin, and S. Yogyakarta, "Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login," vol. 3, no. April, pp. 127–136, 2017.

[12] S. Damai et al., "Implementasi Blockchain : Studi Kasus e-Voting," J. Infra Petra, no. 031, 2019.

[13] L. Wan, D. Eyers, and H. Zhang, "Evaluating the impact of network latency on the safety of blockchain transactions," *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 194–201, 2019. https://doi.org/10.1109/Blockchain.2019.00033

[14] N. Lasla, L. Alsahan, M. Abdallah, and M. Younis, "Green-PoW: An Energy-Efficient Blockchain Proof-of-Work Consensus Algorithm," pp. 1–11, 2020.

[15] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain, "Authentication protocol for cloud databases using blockchain mechanism," *Sensors (Switzerland)*, vol. 19, no. 20, pp. 1–13, 2019. https://doi.org/10.3390/s19204444

[16] H. F. Putra, W. Wirawan, and O. Penangsang, "Penerapan Blockchain dan Kriptografi untuk Keamanan Data pada Jaringan Smart Grid," *J. Tek. ITS*, vol. 8, no. 1, 2019. http://dx.doi.org/10.12962/j23373539.v8i1.38525

[17] S. Gupta and M. Sadoghi, "Encyclopedia of Big Data Technologies," *Encycl. Big Data Technol.*, no. May, 2020. https://doi.org/10.1007/978-3-319-63962-8

[18] O. Novo, "Scalable access management in IoT using blockchain: A performance evaluation," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4694–4701, 2019. https://doi.org/10.1109/JIOT.2018.2879679

[19] H. Baharmand, N. Saeed, T. Comes, and M. Lauras, "Developing a framework for designing humanitarian blockchain projects," *Comput. Ind.*, vol. 131, p. 103487, 2021. https://doi.org/10.1016/j.compind.2021.103487

[20] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 858–880, 2019. https://doi.org/10.1109/COMST.2018.2863956

[21] S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021. https://doi.org/10.1109/ACCESS.2021.3051602

[22] J. Fat, H. Candra, and W. Wiliam, "Sekuritisasi Data Sensor Pada Aplikasi Internet of Things (IoT) Dengan Menggunakan Blockchain Ethereum Di Jaringan Testnet," *TESLA J. Tek. Elektro*, vol. 21, no. 1, p. 79, 2019. http://dx.doi.org/10.24912/tesla.v21i1.5886

[23] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," arXiv, vol. 1, no. 1, 2019.

[24] V. Singla, I. K. Malav, J. Kaur, and S. Kalra, "Develop Leave Application using Blockchain Smart Contract," *2019 11th Int. Conf. Commun. Syst. Networks, COMSNETS 2019*, vol. 2061, pp. 547–549, 2019. https://doi.org/10.1109/COMSNETS.2019.8711422

[25] F. Aprialim, Adnan, and A. W. Paundu, "Penerapan Blockchain dengan Integrasi Smart Contract pada Sistem Crowdfunding," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 148–154, 2021. https://doi.org/10.29207/resti.v5i1.2613

[26] U. Rahardja, Q. Aini, M. Yusup, and A. Edliyanti, "Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce," *Comput. Eng. Sci. Syst. J.*, vol. 5, no. 1, pp. 28–32, 2020. https://doi.org/10.24114/cess.v5i1.14893

[27] A. Fadlil, I. Riadi, and A. Nugrahantoro, "Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 11, no. 3, p. 155, 2020. https://doi.org/10.24843/LKJITI.2020.v11.i03.p04

[28] L. Ismanto, H. S. Ar, A. N. Fajar, Sfenrianto, and S. Bachtiar, "Blockchain as E-Commerce Platform in Indonesia," *J. Phys. Conf. Ser.*, vol. 1179, no. 1, 2019. https://doi.org/10.1088/1742-6596/1179/1/012114

[29] A. Rizky, S. Kurniawan, R. D. Gumelar, V. Kurniawan, and M. B. Prakoso, "Use Of blockchain technology in implementing information system security on education," BEST (Journal Biol. Educ. Sains Technol., vol. 4, no. 1, pp. 62–70, 2021.

[30] Z. Wang, L. Yang, Q. Wang, D. Liu, Z. Xu, and S. Liu, "ArtChain: Blockchain-enabled platform for art marketplace," *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 447–454, 2019. https://doi.org/10.1109/Blockchain.2019.00068

[31] X. Zhu and D. Wang, "Research on Blockchain Application for E-Commerce, Finance and Energy," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 252, no. 4, 2019. http://dx.doi.org/10.1088/1755-1315/252/4/042126
[32] A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam, and A. Islam, "Towards Blockchain-Based E-voting System," *2018 Int. Conf. Innov. Sci. Eng. Technol. ICISET 2018*, pp. 351–354, 2018. https://doi.org/10.1109/ICISET.2018.8745613
[33] S. Shorman, M. Allaymoun, and O. Hamid, "Developing the E-Commerce Model a Consumer To Consumer Using Blockchain Network Technique," *Int. J. Manag. Inf. Technol.*, vol. 11, no. 02, pp. 55–64, 2019. http://dx.doi.org/10.5121/ijmit.2019.11204
[34] E. W. Richard Sharpe, "Wireshark User ' s Guide," Pp. 191, 2014.
[35] A. R. Shajina and P. Varalakshmi, "A novel dual authentication protocol (DAP) for multi-owners in cloud computing," *Cluster Comput.*, vol. 20, no. 1, pp. 507–523, 2017. https://doi.org/10.1007/s10586-017-0774-y
[36] X. Yang, Y. Chen, and X. Chen, "Effective scheme against 51% attack on proof-of-work blockchain with history weighted information," *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 261–265, 2019. https://doi.org/10.1109/Blockchain.2019.00041
[37] A. S. Anakath, S. Rajakumar, and S. Ambika, "Privacy preserving multi factor authentication using trust management," *Cluster Comput.*, vol. 22, pp. 10817–10823, 2019. https://doi.org/10.1007/s10586-017-1181-0