Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023
DOI : https://doi.org/10.33395/sinkron.v8i2.12381
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Securing Messages Using AES Algorithm and Blockchain Technology on Mobile Devices

Al Farissi[1)*], Arya Pradata[2)], Kanda Januar Miraswan[3)]
[1,2,3)]Universitas Sriwijaya, Indonesia
[1)]alfarissi@unsri.ac.id, [2)] aryapradata@gmail.com , [3)] kandajm@ilkom.unsri.ac.id

Submitted : April 24, 2023 | **Accepted** : May 1, 2023 | **Published** : May 4, 2023

Abstract: In recent years, there has been a rapid increase in the use of mobile devices and messaging applications for communication, leading to a growing concern about the security of text messages exchanged through these platforms. This study proposes a novel method that uses the AES algorithm and Blockchain to secure text messages in messaging applications on mobile devices. The AES algorithm is selected due to its faster encryption and decryption processes, which are superior to asymmetric cryptography algorithms. On the other hand, Blockchain is chosen for its inherent security properties that only allow data addition and cannot be altered. This study aims to achieve both speed and security to prevent cybercrime in text messages. The Avalanche Effect calculation and Processing Time measurement are used as the analysis methods to evaluate the proposed approach. The results show that the computation time of the message delivery process using Blockchain and AES algorithm has an average total process time of 33.59 milliseconds. Additionally, the testing results of the Avalanche Effect value show that the AES algorithm has a value of 50% for character lengths up to 16 characters and below 50% for character lengths greater than 16 characters. Based on these testing results, the proposed combination of the AES algorithm and Blockchain is an effective method for securing text messages in messaging applications. This method can offer a secure and efficient way of exchanging text messages on mobile devices and can adopt as a standard approach for messaging applications.

Keywords: AES Algorithm, Avalanche Effect, Blockchain, Chatting, Cryptography

INTRODUCTION

The development of information technology continues to increase, resulting in increased human needs as well. Communication is essential to facilitate daily human performance so that community productivity does not decrease and community performance is maintained. Chat Messenger is message communication that mobile smartphone users widely use, but the messages sent are not necessarily safe from cybercrime or hacker. Therefore, cryptography is critical to prevent hackers from eavesdropping on the messages sent. Cryptography is a knowledge to maintain the security of text messages (plaintext) by encrypting messages into a form that is difficult to read (ciphertext). When decrypting, a ciphertext is converted into plaintext. This encryption and decryption protect messages from unauthorized parties viewing the messages contents (Randi et al., 2020).

Cryptography has several methods, including the Advanced Encryption Standard (AES) algorithm. AES is a block cipher algorithm that uses a key when encrypting and decrypting. AES algorithm has various block sizes, such as 128-bit, 192-bit, and 256-bit. The differences between the three versions of AES affect the number of keys and their rounds (Prameshwari & Sastra, 2018).

This research uses blockchain technology as data security in the message-sending process. Blockchain technology is prevalent, especially in cryptocurrency. A security system that can only append data can only add data and cannot be changed. So the blockchain system is complex for hackers to penetrate. From these advantages, the blockchain system is developed on the Chat Messenger application and secured again with AES encryption. Blockchain is a ledger that is decentralized and not centralized. In simple words, a blockchain is a chain of blocks (chain of blocks). A block has a data structure that contains data and some attributes. Blocks can be linked to form a blockchain (Das, 2020). Based on the above considerations, research will be carried out on implementing secure chat using a Mobile-Based AES algorithm and Blockchain because of the nature of

*name of corresponding author

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023
DOI : https://doi.org/10.33395/sinkron.v8i2.12381
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Blockchain, which cannot change the data in it. In addition, the AES algorithm is also symmetric, with advantages in the encryption and decryption process being faster than the asymmetric algorithm (Basri, 2016).

LITERATURE REVIEW

Theoretical basis

1. Blockchain

A blockchain is a list of records called blocks and is interconnected and secured by cryptographic methods (Kurnia Hu et al., 2019). Blockchain is a decentralized ledger, not a central authority. In other words, the term blockchain itself is a blockchain. A block with a data structure contains data and some other attributes. Blocks can be linked with other blocks to form a blockchain. Block basic components:

1. Hash: Unique identifier of the current block with a unique value.
2. Timestamp Value: This takes the hash of each block of items to be timed and publicly publishes the hash.
3. Previous Hash: Hash of the previous block.
4. Data: Contains data based on the type of Blockchain.

A hash can be treated like a fingerprint to identify a block. Figure 1 shows a representation of a blockchain. The first block is often called the genesis block in the blockchain world and does not reference the previous block (Das, 2020).

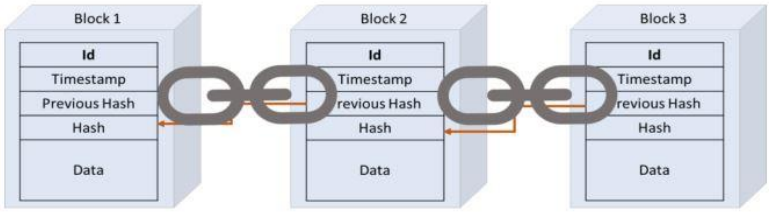

Figure 1. Representation of Blockchain (Das, 2020)

One of the mechanisms of Blockchain is the proof-of-work mechanism. With this mechanism, the node that can add data to the Blockchain is the node that solves the math puzzle first. When a node successfully solves a puzzle, the Blockchain protocol automatically issues a new puzzle for the existing nodes to solve. This mechanism is known as mining (Harahap et al., 2020).

This mechanism is useful for implementing peer-to-peer distributed server timestamps and involves scanning for values that have been hashed. For example, like SHA-256, the hash starts with a zero bit number. The average effort required is exponential to the number of zero bits required and can be verified by executing a single hash.

In this timestamp network, the proof-of-work mechanism is implemented by an incremental sequence of the nonce in the block until it gets a value that can give the hash of the block the required number of zero bits. Once the computational power is increased to meet the proof-of-work requirements, the block cannot be changed without restarting the process. When the blocks are connected afterwards, attempts to change the block require repeating the creation of the blocks after that as well (Nakamoto, 2008).

2. AES (Advanced Encryption Standard)

Advanced Encryption Standard (AES) algorithm is a block cipher algorithm with a symmetrical nature that uses a symmetric key during the encryption and decryption process. AES algorithm has various key lengths, namely 128 bits, 192 bits, and 256 bits. The difference between the three variations is the length of the key which affects the number of rounds. The following is a comparison of the processes of each variation of AES:

Table 1. AES Algorithm Data Sequence

	Key Length	Block Length	Number of Rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

AES 128-bit encryption process can be done by selecting the block size and key so that the number of processes passed can be determined. There are 4 round transformations carried out in the encryption and decryption process:

1. SubBytes: replaces the contents of the bytes using the substitution table.
2. ShiftRows: performs the process of shifting blocks per line in the state array.

*name of corresponding author

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023
DOI : https://doi.org/10.33395/sinkron.v8i2.12381
e-ISSN : 2541-2019
p-ISSN : 2541-044X

3. MixColumn: performs the randomization process of data in each state array.
4. AddRoundKey: combine state array and round key with XOR.

In the AES decryption process:
1. InvShiftRows: performs a right shift of the bits in each row block
2. InvSubBytes: maps each element to the state with an Inverse S-Box table.
3. InvMixColumn: multiply each column in the state by the AES matrix.
4. AddRoundKey: combine state array and round key with XOR.

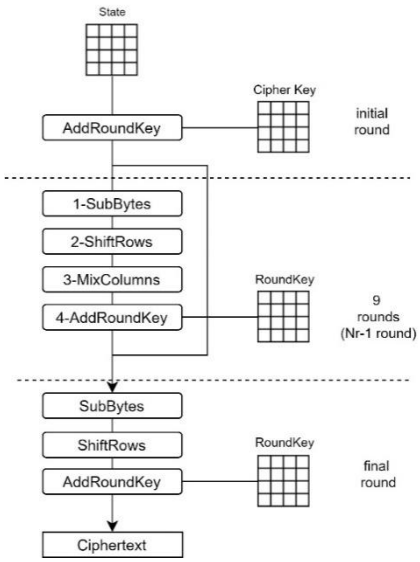

Figure 2. AES Encryption Process

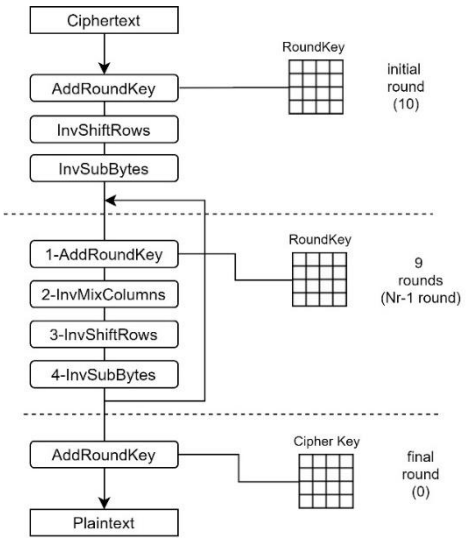

Figure 3. AES Decryption Process

Relevant Research

Research conducted by (Randi et al., 2020) concluded that the application is tested by entering a message and key. After that, the application will encrypt the message with the key that has been given and send an encrypted message so that the message cannot be known by people who do not know the key. In this study, messages stored in the firebase real-time database are in hexadecimal form because Advanced Encryption Standard algorithm requires messages and keys to be converted into hexadecimal form.

Another research by (Ilham & Widyassari, 2021) aims to design, build and implement an Android-based instant messaging application that applies the AES algorithm method and utilizes Firebase cloud services to support file storage, real-time databases, and user authentication. The conclusion obtained from this research is that the application can send and receive messages in real time. Furthermore, based on the testing results using black-box techniques, the application system developed can obtain a feasibility level of 96%.

Another research conducted by (Das, 2020) concluded that blockchain technology could solve problems related to privacy and confidentiality that exist in traditional or existing messaging systems. In this study, decentralized messaging systems performed better than centralized messaging platforms regarding scalability, throughput, processing, and uptime.

METHOD

Dataset

The data used in this study was obtained from a text data source site called https://lipsum.com/. The dataset used in this study was 1,500 characters long. The character combines Latin words and phrases with no meaning or relevance to the research question. The dataset is common in fake texts used in many applications.

Data Processing

The process of implementing the AES algorithm and Blockchain in this study is depicted in Figure 4.

*name of corresponding author

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023
DOI : https://doi.org/10.33395/sinkron.v8i2.12381
e-ISSN : 2541-2019
p-ISSN : 2541-044X

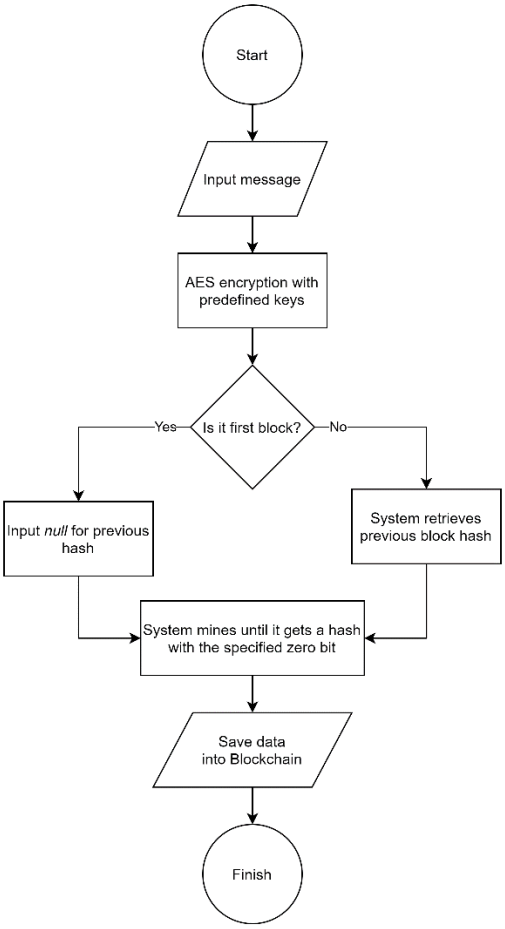

Figure 4. AES Method and Blockchain Implementation Process

RESULT

Avalanche Effect

This test is carried out by calculating the Avalanche Effect obtained from the text that has been encrypted and has a difference of one bit. This test is carried out on a dataset of 1,500 characters and then divided into blocks with a length of 8 to 44 characters in each block, after which 1-bit changes will be made in each block to produce a test of 12,609 times. The data results from the Avalanche Effect test can be seen in Figure 5.

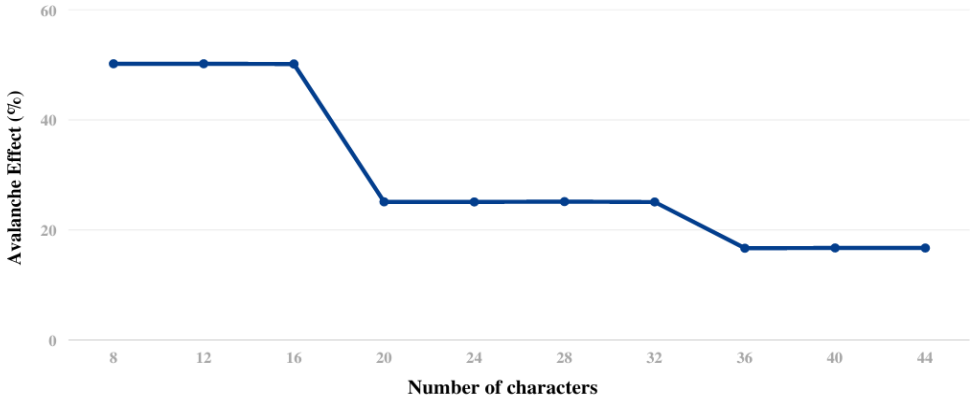

Figure 5. Line Graph of Avalanche Effect

The avalanche effect above shows that the AES algorithm method produces percentage values around 50% for 8, 12, and 16 characters. However, character lengths above 16 characters will result in a lower Avalanche Effect value because the AES-128 algorithm can only encrypt up to 128 or 16 characters, so the longer the character of a text, the result the percentage value of the Avalanche Effect will decrease.

*name of corresponding author

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023
DOI : https://doi.org/10.33395/sinkron.v8i2.12381
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Processing Time

The Processing Time calculation calculates the computational time required to secure text messages using Blockchain and the AES algorithm. The graph is summarized in the line graph below.

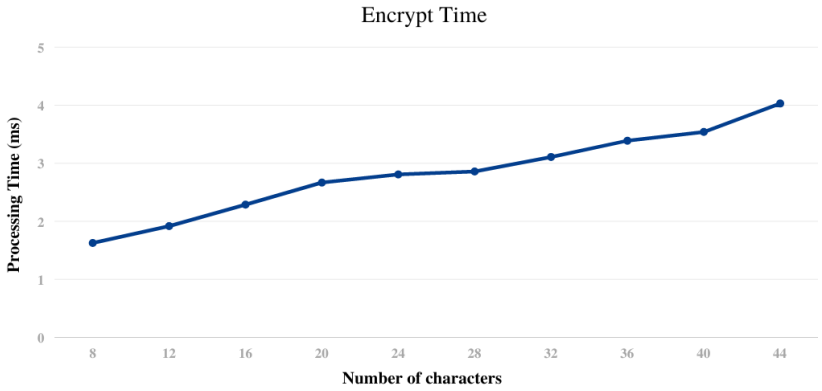

Figure 6. Encryption Process Time

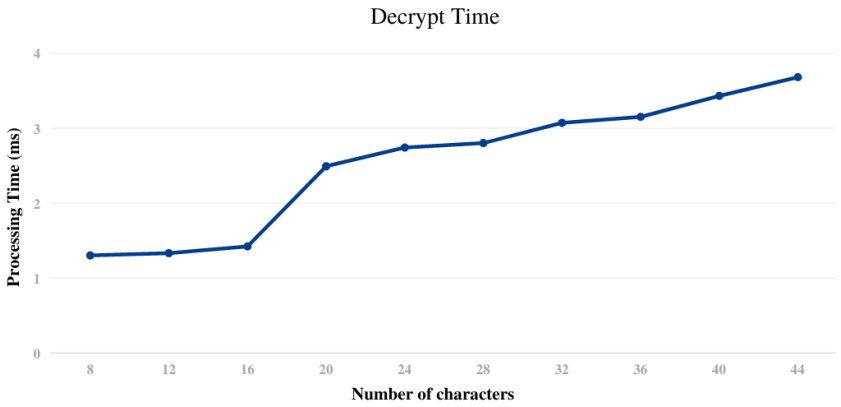

Figure 7. Decryption Process Time

It can be concluded from Figure 6 and Figure 7 that the cryptography algorithm for securing messages using Blockchain and the AES algorithm produces different times according to the length of the character. The longer the character of a text, the longer the Processing Time required. In the message encryption and decryption process, the processing time increases as the length of a text message increases, with an average encryption and decryption time of 2.83 ms and 2.54 ms.

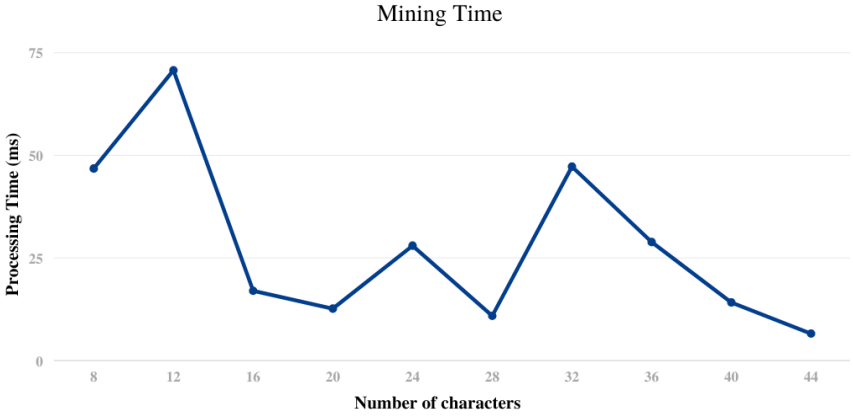

Figure 8. Mining Process Time

*name of corresponding author

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 2, April 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i2.12381 p-ISSN : 2541-044X

Whereas in Figure 8 above, the processing time experienced in the blockchain mining process is not particular. This is because, on the Blockchain, there is a proof-of-work mechanism, which is implemented with an incremental series of events (nonce) which will continue to increase until it gets a hash with the required number of zero bits so that the mining process can be faster or slower on average mining time is 28.25 ms.

CONCLUSION

Based on the results of this study, the avalanche effect test applied to measure the level of security in the implementation of the AES algorithm obtained a calculation with the avalanche effect percentage value of 50% for messages with sizes of 8, 12, and 16 characters. Based on the processing time result with the AES algorithm and Blockchain method, the message security process can maintain the security and confidentiality of the message with the time required for the encryption and decryption process, which increases every time the character length of the text message is increased. However, in contrast to the encryption and decryption time, the mining time on the Blockchain does not increase based on the size of the character length and produces an indeterminate time with the lowest time of 6.52 ms, the highest time of 70.72 ms, and the average of 28.25 ms.

REFERENCES

Alfajar, F., & Akbar, M. (2021). Implementasi Keamanan Chat Realtime Menggunakan Aes-Cbc Dan Base64. *Journal of Information System and Artificial Intelligence, 1*(2), 2-4.

Ali, A. H., & Sagheer, A. M. (2017). Design of Secure Chatting Application with End to End Encryption for Android Platform. *Iraqi Journal for Computers and Informatics (IJCI), 43*(1), 23-25. doi:http://dx.doi.org/10.25195/2017/4315

Argani, A., & Taraka, W. (2020). Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi. *ADI Bisnis Digital Interdisiplin Jurnal, 1*(1), 12-15.

Astuti, N. I., Arfani, I., & Aribowo, E. (2019). Analysis of the security level of modified CBC algorithm cryptography using avalanche effect. *IOP Conference Series: Materials Science and Engineering*, 5-6.

Basri. (2016). Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Scientific Journal of Computer Science, Faculty of Computer Science, Al Asyariah Mandar University, 2*(2), 18-20.

Das, S. K. (2020). Secure Messaging Platform Using Blockchain Technology. *International Journal of Research in Engineering and Science (IJRES), 8*(12), 27.

Harahap, A. K., Oktari, N. S., Kartini, A., Agung, A. A., & K, R. B. (2020). Perbandingan ROI Metode Konsensus Proof of Work, Proof of Stake, dan Proof of Service (Masternode). *Jurnal Teknologi Informasi dan Manajemen, 2*(2), 2-5.

Ilham, L. I., & Widyassari, A. P. (2021). Pengembangan Aplikasi Pesan Instan Terenkripsi Menggunakan Algoritma Kriptografi AES (Advanced Encryption Standard). *Jurnal Teknik Elektro Smart, 1*(1), 1-4.

Kurnia Hu, S. D., Palit, H. N., & Handojo, A. (2019). Implementasi Blockchain: Studi Kasus e-Voting. *Jurnal Infra, 7*(1), 184-185.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin*, 1-8.

Prameshwari, A., & Sastra, N. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. *EKSPLORA INFORMATIKA, 8*(1), 52-54.

Putri, A. E., Kartikadewi, A., & Rosyid, L. A. (2020). Implementasi Kriptografi Dengan Algoritma Advanced Encryption Standard (AES) 128 Bit Dan Steganografi Menggunakan Metode End Of File (EOF) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang. *Applied Information Systems and Management, 3*(2), 70-77.

Randi, A., Lazuardy, K., Chandra, S., & Dharma, A. (2020). Implementasi Algoritma Advanced Encryption Standard pada Aplikasi Chatting berbasis Android. *JIKOMSI Jurnal Ilmu Komputer dan Sistem Informasi, 3*(1), 2-4.

Takale, A. P., Vaidya, C. V., & Kolekar, S. S. (2018). Decentralized Chat Application using Blockchain Technology. *International Journal for Research in Engineering Application & Management (IJREAM)*, 92-93.

Verma, R., & Sharma, A. K. (2020). Cryptography: Avalanche effect of AES and RSA. *International Journal of Scientific and Research Publications, 10*(4), 119-122.

Yusfrizal. (2019). Rancang Bangun Aplikasi Kriptografi pada Teks Menggunakan Metode Reverse Chiper dan Rsa Berbasis Android. *Jurnal Teknik Informatika Kaputama, 3*(2), 30-33.

*name of corresponding author

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.