HASIL CEK_Block-hash of blockchain framework against man-in-the middle attacks

by Imam Riad Umar, Busthomi, Muhammad

Submission date: 23-Apr-2022 11:07AM (UTC+0700)
Submission ID: 1817899525
File name: sh_of_blockchain_framework_against_man-in-the-middle_attacks.pdf (663K)
Word count: 4588
Character count: 25064

8 (1) January 2022 1-9 ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
Register: *Jurnal Ilmiah Teknologi Sistem Informasi*

Contents lists available at www.journal.unipdu.ac.id

Register

Journal Page is available to www.journal.unipdu.ac.id/index.php/register

Research article

Block-hash of blockchain framework against man-in-the-middle attacks

Imam Riadi [a], *Rusydi Umar* [b], *Iqbal Busthomi* [c,*], *Arif Wirawan Muhammad* [d]

[a] *Department of Information Systems, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[b,c] *Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[d] *Department of Information Security and Web Technology, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia*
email: [a] imam.riadi@is.uad.ac.id, [b] rusydi@mti.uad.ac.id, [c,*] iqbal1907048011@webmail.uad.ac.id [d] HI180037@siswa.uthm.edu.my
* *Correspondence*

ARTICLE INFO

Article history:
Received 11 December 2020
Revised 17 March 2021
Accepted 19 April 2021
Available online 15 May 2021

Keywords:
authentication
Man-in-the-middle attacks
blockchain technology
block-hash
payload

Please cite this article in IEEE style as:
I. Riadi, R. Umar, I. Busthomi and A. W. Muhammad, " Block-hash of blockchain framework against man-in-the-middle attacks," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 8, no. 1, pp. 1-9, 2022.

ABSTRACT

Payload authentication is vulnerable to Man-in-the-middle (MITM) attack. Blockchain technology offers methods such as peer to peer, block hash, and proof-of-work to secure the payload of authentication process. The implementation uses block hash and proof-of-work methods on blockchain technology and testing ~~is~~ using White-box-testing and security tests distributed to system security practitioners who are competent in MITM attacks. The analyisis results before implementing Blockchain technology show that the authentication payload is still in plain text, so the data confidentiality has not minimize passive voice. After implementing Blockchain technology to the system, white-box testing using the Wireshark gives the result that the authentication payload sent has been well encrypted and safe enough. The percentage of security test results gets 95% which shows that securing the system from MITM attacks is relatively high. Although it has succeeded in securing the system from MITM attacks, it still has a vulnerability from other cyber attacks, so implementation of the Blockchain needs security improvisation.

1. Introduction

The information system is an application used in an organization that supports transaction management and makes reporting easier [1, 2]. An information system improves usability, maintainability, and security through standardization and development of best practices [3, 4]. Authentication is the main gateway in an information system to get authorization to access the account [5]. The authentication process is a user validation process in a smart card, biometric, or username-password [6, 7]. While the user enters the system, they will allow the user to access all the authorized system's services without need to enter the password [8, 9].

Information security is an important aspect that needs to be considered in building a system [10]. As the main gate of the system, has gaps and vulnerabilities, including sending and receiving the payload from the server as plain text, because it should be encrypted in sending the payload to maintain the payload's anonymity [11, 12, 13]. Security in the authentication process needs to be improved to deal with cyberattacks such as data sniffing, cross-site scripting (XSS), and man-in-the-middle attacks [14]. Man-in-the-middle (MITM) is an attack on a network with open access [14]. MTM is an attacker that inserts himself between two parties or a device in stealth mode so that all packets passing between the two legitimate parties are routed through the attacker. This attack is quite dangerous because the attacker can sniff the sent packet's information, potentially data hijacking [15]. MITM attacks are likely ball situations where two players intend to pass the ball to each other while one player between them

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (1) January 2022 1-9

tries to grab it [16]. MITM attacks focus on the information flowing between the endpoints, confidentiality, and the information's accuracy. MITM attacks are a tapping process in which in communication between two devices A and B, the attacker receives A by pretending becoming B. Whenever A wants to send a message to B and sends it to the attacker who reads the payload, then passes it to B to keep communication works. The attacker can read all communication content, including emails, pictures, and passwords [15, 17, 18]. The MITM attacks process is shown in Fig. 1 [19].

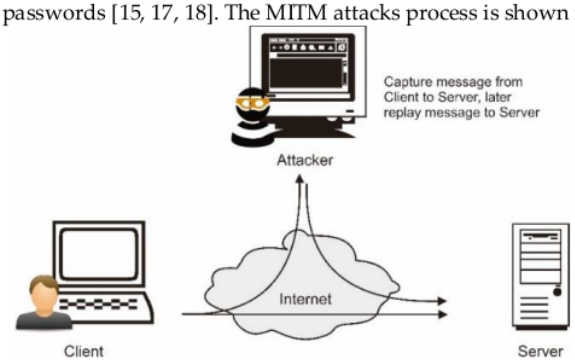

Fig. 1. MITM attacks visualization

One of the vulnerabilities of MITM attacks is that the authentication payload is sent in plain text to read the payload contents. The confidentiality of information will be leaked to allow for the hijacking of data; therefore, it is necessary to implement security mechanisms to protect the payload information. MITM attacks use the communication layer as a medium of attack. Open System Intercommunication (OSI) is the communication channel closest to a MITM attack. Although each layer takes a different approach to providing security, none of them are free from MITM attacks [18].

Blockchain technology is a collection of several security concepts that can ensure the confidentiality of information. One of the concepts used by Blockchain technology is like the concept used in a distributed database [20]. The distributed database concept of Blockchain technology is where a distributed database contains transaction records that are shared among participating members on the chain. Every transaction is confirmed by the consensus of the majority of the members, so preventing fraudulent transactions. Blockchain is a collection of blocks that make up a chain. Each block has three elements: data, the hash value of the block, and the previous hash value or a hash value of the last block. Utilizing this hash makes Blockchain more secure because if someone changes one of the blocks in the Blockchain, the hash value will change, and the next block will become invalid because it does not store the valid hash value of the previous block. This technique means that a block's changes will invalidate the entire Blockchain [21, 22]. Blockchain also has several concepts (apart from distributed databases) such as block hash and consensus protocols (proof-of-work, proof-of-stake, etc.) [23].

Blockchain technology stores data in the form of hashes, disguising the data so that the stored information in the block can be omitted [24]. This technology can also prevent changes or falsification of transactions so that it can be used to make transactions directly and safely. It distributed and transparent log recording system from this technology that can be a solution to be applied to transaction recording so that it can be an effort to minimize the level of data forgery and misuse [25].

Blockchain also has several concepts (apart from block hash), such as distributed databases and consensus protocols (proof-of-work, proof-of-stake, etc.) that can be used to make information more secure [23]. A one-way hash function, also known as a message summary or compression function, is a mathematical function that takes a variable-length input and converts it into a binary sequence of fixed length [26].

Attack tools simulations will be using Wireshark 2.9.0. Wireshark is a packet sniffer that deals with retrieving raw data at the packet level. Wireshark is used by networks or security engineers to capture payload packets sent (POST) by the system to the database. Wireshark works at the Network layer (OSI-3) to find exploits and vulnerabilities.

The system used is a vulnerability system designed to be the object of MITM attacks, which later will be implemented Blockchain technology to test its resilience against MITM attacks. Based on the identified vulnerabilities, Blockchain technology has the potential to respond to various attacks. MITM

http://doi.org/10.26594/register.v8i1.2190

3
ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (1) January 2022 1-9

attacks can be made to test Blockchain technology to protect and maintain data confidentiality from attackers.

The rest of this paper will test whether blockchain technology can secure the system from MITM attacks. Section 2 discussed the research method that was used. Section 3 presents experiment results and discussion. Finally, section 4 is for the conclusion and future work.

2. Research Method

The research method used in this research is the patching method, where the object already exist but needs some update to improve the object—the steps for the patching method show in Fig. 2.

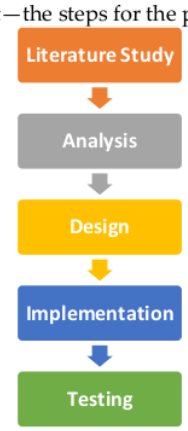

Fig. 2. Patching steps

The patching steps can be divided into five stages. The stages of literature study, analysis, design, implementation, and testing or testing are described as follows:

1. Data collection, the literature study is carried out both about the system to be used for research, an excellent theoretical basis regarding MITM attacks, Blockchain theory, to the tools that will be used in the study. The collection of literature is divided into two sources, namely from related research journals and the internet.
2. Analysis, this stage is the stage for analyzing the system's current conditions to be used in this study, both from how the system works, the system flow to the data payload, which will be the main focus of this research. Besides, the MITM attacks were also tested using the Wireshark 2.9.0 before implementing the proposed security concept. This stage aims to get all the details of the system in use today [27].
3. The design, the results of the analysis will be more precise if described with a process scheme or flow design so that at this stage, a description of the attack process and data security will be presented.
4. Implementation, this stage is an experimental implementation of the analysis results [27]. Vulnerabilities that will occur when the system is analyzed will be implemented Blockchain technology to secure information on the system.
5. Testing, this stage is the testing phase of the implementation of Blockchain technology that has been done. White Box Testing is a test case method that is entirely controlled by the developer [19]. White Box Testing dramatically improves the overall effectiveness of testing. It can more easily detect bugs that are difficult to find by testing Black Box Testing or other testing methods. Therefore, a White Box Tester should know programming structures [28]. The test that will be carried out is a direct attack experiment using a MITM attack.

Apart from using white box testing, this test also uses security testing. Security testing is a testing method to ensure that the system used is safe from attacks, including MITM attacks [29]. The survey used a quota sampling method. The questionnaire will be filled out by examiners who are competent against MITM attacks.

3. Results and Discussion

The system used in this study is a system prototype equipped with an authentication process, which is then called the Login System. The login system is a prototype that will be implemented as the main gate

http://doi.org/10.26594/register.v8i1.2190

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (1) January 2022 1-9

in an information system. Therefore, it is necessary to implement adequate security to ensure that the information stored and managed is safe from cyber-attacks.

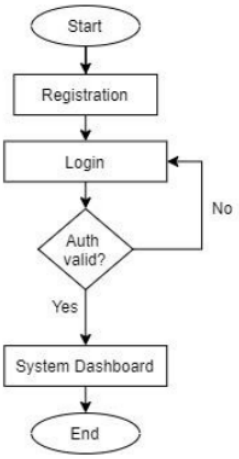

Fig. 3. Authentication flowchart

Fig. 3 is a flowchart of the authentication process in the Login System. Before logging in, users need to register for an account. After having a user account, you will be asked to enter a username and password, and the authentication process will be successful when the username and password entered are correct. After successful authentication, users can access the permitted information system page following their access rights. The authentication process has not implemented security so that the payload information sent for the authentication process is still vulnerable to attacks.

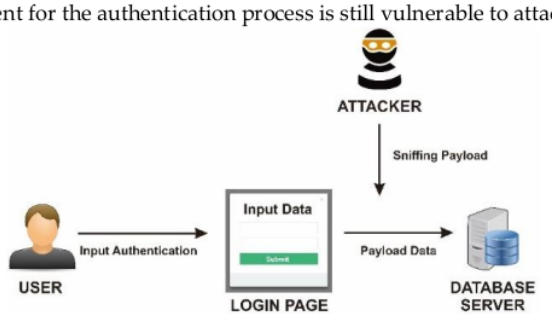

Fig. 4. MITM attacks visualization

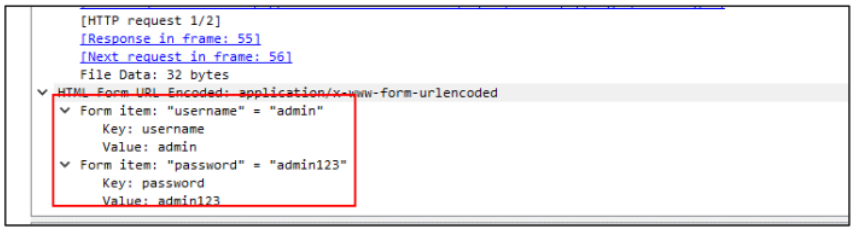

Fig. 5. Capture the authentication process using Wireshark

Before the authentication process, the user must first register to create an account and get a username and password stored in the database—authentication process by entering a username and password validated. The MITM attack scenario to analyze system vulnerabilities, as seen in Fig. 4, is a conceptual flowchart of the authentication, sniffing, and validation process workflow from the database server.

As in the previous explanation, users must first authenticate to access the system dashboard. The required authentication is to enter the username and password from the registered account. The current condition is as described in Fig. 4 that the system, when doing POST data for authentication (sending

http://doi.org/10.26594/register.v8i1.2190

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (1) January 2022 1-9

payload), is still in plaintext. When sniffing is carried out in the process, the input username and password will be obtained. Attack simulation will be carried out using Wireshark 2.9.0 tools to capture the system's payload (POST) to the database. Wireshark has tools to capture, view, and analyze data packets. Wireshark has advanced wireless protocol analysis support to help administrators troubleshoot wireless network problems. With proper driver support, Wireshark can capture traffic and decode it into a format that allows administrators with issues causing poor performance, intermittent connectivity, and other common problems [30].

Vulnerabilities in the login system can be seen in Fig. 5 when authenticating the payload sent can be seen when captured using Wireshark tools. In the picture, it can be seen that the username and password used for authentication are still plain text that is easy for attackers to take to use for account hijacking.

The Login System's current condition is that there is no authentication payload security so that it is still in plaintext. Therefore the hash block mechanism of Blockchain technology provides an opportunity to make sending authentication payloads safer. This study implements two Blockchain methods, including the block hash method and the proof-of-work method. The hash block will be created during the account registration process and stored in a hash block that can be used for user authentication. Encryption process on the system's front-end, using javaScript to convert the payload to be sent into ciphertext. This algorithm can be seen in Fig. 6.

```
function register() {
    console.log(sha256(''))
    var username = $('#username').val()
    var password = $('#password').val()

    var auth = sha256(sha256(username) + sha256(password))
```

Fig. 6. Hash Block Making Algorithm (Phase 1)

Fig. 6 explains that the username and password variables, which the values are then taken to be used as an authentication tool. The 5th line of code creates a hash block by combining each hash of the username and password, then carrying out a second hash before being saved into the database.

The encryption process, before stored in the database, is on stage 2. The previously created hash block will be added with a key in the form of a random number and then reset again to increase the data's security. This algorithm can be seen in Fig. 7.

```
function aksi_register()
{

    $auth = $this->input->post('auth');
    $calculate_hash = hash('sha256', $auth . strval(rand(1, 1000)));
    $this->m_register->register($calculate_hash);
}
```

Fig. 7. Hash Block Making Algorithm (Phase 2)

Fig. 7 explains that the hash block from the previous stage will be stored in $auth and entered in the "auth" table that was previously created. The second line adds a randomly generated key in the range of 1 to 1000 in the hash block. Then the block is encrypted back to be stored in the database.

Login is the process of matching the hash (payload) sent by the hash stored in the database. Before being reached, the hash will be calculated first because the payload sent will be different from the one stored in the database. This calculation process uses the proof-of-work method by looping values 1 to 1000 to find the correct number so that the hash sent is the same as the one stored in the database. The algorithm used can be seen in Fig. 8.

The hash block sent as an authentication payload and stored in the database will be in the form of a ciphertext. It will be safer from tapping and is resistant to Man in the Middle attacks because besides being unreadable, the payload is also hard to decrypt.

The testing method uses the White Box Testing method, in which the developer carries out a security test by testing attacks on the system developed after implementing the patch. The results of the capture of the authentication process using the Wireshark shown in Fig. 9. Based on the capture results, it is known that the payload sent for authentication is in the form of ciphertext or has been adequately encrypted because the contents of the payload are not readable.

http://doi.org/10.26594/register.v8i1.2190

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (1) January 2022 1-9

```php
function aksi_login()
{
    $auth = $this->input->post('auth');
    $i = 1;
    while ($i <= 1000) {
        $calculate_hash = hash('sha256', $auth . $i);
        $where = array(
            'auth' => $calculate_hash,
        );
        $cek = $this->m_login->cek_login('auth', $where)->num_rows();
        if ($cek > 0) {
            $data_session = array(
                'status' => "login"
            );

            $this->session->set_userdata($data_session);

            // redirect("admin");
            echo json_encode(['status' => 'berhasil']);
            break;
        }
        $i++;
    }
    if ($i > 1000) {
        echo json_encode(['status' => 'gagal1']);
    }
}
```

Fig. 8. Proof-of-Work Algorithm for hash calculation process

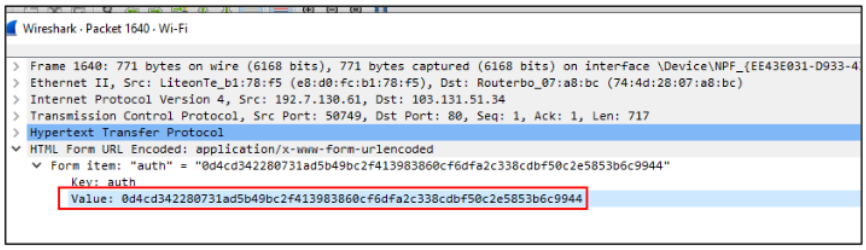

Fig. 9. Capture authentication process using Wireshark after implementation

In addition to using the White Box Testing method, a questionnaire was also tested by four respondents who could try the MITM attack. The results obtained from the questionnaire test can be seen in Table 1.

Table 1. Test results by respondents

No.	Parameter	Yes	No
1.	Is the payload being sent adequately secured?	4	0
2.	Is the system safe from Man in the Middle attacks?	3	1
3.	Is the hash safe?	4	0
4.	Is the payload that is sent not easily decrypted?	4	0
5.	Can the payload sent be readable?	0	4

Based on the answers given to the four respondents, the points obtained from each question can be calculated as a test point, for the "Yes" option has a value of 10 and for the option "No" has a value of 0, except for point number 5 is worth the opposite, as in Table 2.

Table 2. Total questionnaire points results

No.	Parameter	Yes	No	Accumulation
1.	Is the payload being sent adequately secured?	40	-	40
2.	Is the system safe from Man in the Middle attacks?	30	-	30
3.	Is the hash safe?	40	-	40
4.	Is the payload that is sent not easily decrypted?	40	-	40
5.	Can the payload sent be readable?	-	40	40

Based on the points obtained, the percentage of the test results can be calculated. The formula used to calculate the percentage of test response results is shown on Eq. 1, Eq. 2, and Eq. 3.

$$\sum Test\ Score = \sum Maximum\ Weight\ of\ Answers \times \sum Respondents \quad (1)$$

$$Percentage = \left(\frac{\sum Score}{\sum Test\ Score}\right) \times 100\% \quad (2)$$

$$Accumulated\ total\ percentage\ (\%) = \frac{\sum Percentage}{\sum Question\ Points} \quad (3)$$

http://doi.org/10.26594/register.v8i1.2190

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (1) January 2022 1-9

The greater the number of percentages, the application before implementing Blockchain Technology has a vulnerability so that patching is needed on the system. The implemented patch results can run well so that it can better secure data from MITM attacks. From the questionnaire results in Table 2, the calculation is obtained using Eq. 1 and Eq. 2.

$$\sum Test\ Score = 10 \times 4 = 40$$

$$Percentage\ of\ Points\ 1 = \frac{40}{40} \times 100\% = 100\%$$

$$Percentage\ of\ Points\ 2 = \frac{30}{40} \times 100\% = 75\%$$

$$Percentage\ of\ Points\ 3 = \frac{40}{40} \times 100\% = 100\%$$

$$Percentage\ of\ Points\ 4 = \frac{40}{40} \times 100\% = 100\%$$

$$Percentage\ of\ Points\ 5 = \frac{40}{40} \times 100\% = 100\%$$

$$Accumulated\ total\ percentage\ (\%) = \frac{475}{5} = 95\%$$

The percentage gained shows that the system has been secured using methods on Blockchain technology. The block hash method converts the sent payload into a block and then encrypted using SHA256. The proof-of-work method is implemented to make the payload block more difficult to decrypt. The comparison of the results can be seen in Table 3. For example, you are using the username "admin" and the password "admin".

Table 3. The comparison of result before and after proof-of-work

SHA256	8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
Block hash	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Proof-of-work	0d4cd342280731ad5b49bc2f413983860cf6dfa2c338cdbf50c2e5853b6c9944

The tests that have been carried out show the conditions before and after Blockchain technology is implemented. Before implementation, the system displays an indication of the vulnerability of the MITM attack. After implementing Blockchain technology, the payload that is sent is more secure from MITM attacks tested using the Wireshark tool. The percentage of security testing distributed to security practitioners got 95%. The success rate of implementing Blockchain technology on the system was successfully carried out to secure MITM attacks. The lack of 5% of the accumulated percentage is showing that the proposed method still needs some security improvisation.

The block hash mechanism of the proposed Blockchain is proven to amplify the complexity of the hash. Adding a proof-of-work method that performs repeated encryption of the resulting block hash can make it more difficult to decode the stored payload. This proposed method works to secure the authentication process against MITM attacks.

4. Conclusion

Authentication is the main gateway in an information system, so vulnerabilities in an authentication process must be secured. MITM attack is one of the attacks that can open vulnerabilities in the authentication process. Blockchain technology has a block hash mechanism that can be used to close vulnerabilities in the authentication process, including MITM attacks. The hash block mechanism converts the authentication payload data in plaintext into ciphertext data by converting it into a block hash. Based on the results obtained, Blockchain technology's implementation has succeeded in securing the authentication payload data in an information system from the MITM attack. The final total percentage of security testing shows that 95% of testers agree that the system can guarantee the authentication payload security from MITM attacks. The proposed method works to secure the authentication process against MITM attacks. In the future, it needs some improvisation closer to 5% of accumulation lacks and also needs to be tested again with other attacks to guarantee its reliability.

Author Contributions

Imam Riadi: Writing - Review & editing. Rusydi Umar: Methodology. Iqbal Busthomi: Software and Writing - Original Draft. Arif Wirawan Muhammad: Validating.

Declaration of Competing Interest

http://doi.org/10.26594/register.v8i1.2190

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (1) January 2022 1-9

We declare that we have no conflict of interest.

References

[1] I. Riadi, I. T. R. Yanto and E. Handoyo, "Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI," *IOP Conf. Series: Materials Science and Engineering*, vol. 821, 2020.

[2] A. D. Kozlov and N. L. Noga, "Risk Management for Information Security of Corporate Information Systems Using Cloud Technology," in *2018 Eleventh International Conference "Management of large-scale system development" (MLSD)*, Moscow, Russia, 2018.

[3] M. Trnka, T. Cerny and N. Stickney, "Survey of Authentication and Authorization for the Internet of Things," *Security and Communication Networks*, 2018.

[4] I. Riadi, R. Umar and A. Sugandi, "Web Forensic on Kubernetes Cluster Services Using Grr Rapid Response Framework," *International Journal of Scientific & Technology Research*, vol. 9, no. 1, pp. 3484-3488, 2020.

[5] Y. Zhao, S. Li and L. Jiang, "Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment," *Security and Communication Networks*, 2018.

[6] Y. Park, K. Park and Y. Park, "Secure user authentication scheme with novel servermutual verification for multiserver environments," *International Journal of Communication Systems*, vol. 32, 2019.

[7] O. A. Simon, U. I. Bature, K. I. Jahun and N. M. Tahir, "Electronic doorbell system using keypad and GSM," *International Journal of Informatics and Communication Technology*, vol. 9, no. 3, pp. 212-220, 2020.

[8] A. O. Christiana, A. N. Oluwatobi, G. A. Victory and O. R. Oluwaseun, "A Secured One Time Password Authentication Technique using (3, 3) Visual Cryptography Scheme," *IOP Conf. Series: Journal of Physics: Conf. Series*, vol. 1299, 2019.

[9] A. Bánáti, E. Kail, K. Karóczkai and M. Kozlovszky, "Authentication and authorization orchestrator for microservice-based software architectures," *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018, pp. 1180-1184.

[10] I. Riadi, R. Umar and A. Sugandi, "Web Forensic on Container Services Using GRR Rapid Response Framework," *Scientific Journal of Informatics*, vol. 7, no. 1, 2020.

[11] P. Chandrakar and H. Om, "RSA Based Two-factor Remote User Authentication Scheme with User Anonymity," *Procedia Computer Science*, vol. 70, pp. 318-324, 2015.

[12] R. A. Megantara, F. A. Rafrastara and S. N. Mahendra, "A combination of Hill CIPHER-LSB inRGB image encryption," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, vol. 4, no. 3, 2019.

[13] S. Zhu, C. Zhu, W. Wang, "A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256," *Entropy*, vol. 20, no. 9, pp. 716, 2018.

[14] A. R. Chordiya, S. Majumder and A. Y. Javaid, "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools," *2018 IEEE International Conference on Electro/Information Technology (EIT)*, 2018, pp. 0438-0443.

[15] R. A. S. K. B. Ofori-Amanfo, G. A. Mills and K. M. Koumadi, "Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications*, 2019.

[16] A. Mallik, A. Ahsan, M. M. Z. Shahadat and J. C. Tsou, "Understanding Man-in-the-middle-attack through Survey of Literature," *Indonesian Journal of Computing, Engineering, and Design*, vol. 1, no. 1, pp. 44-56, 2019.

[17] P. Radhika., G. Ramya., K. Sadhana and R. Salini., "Defending Man In The Middle Attacks," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 3, 2017.

http://doi.org/10.26594/register.v8i1.2190

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
8 (1) January 2022 1-9

[18] A. Mallik, "Man-in-the-Middle-Attack: Understanding in Simple Words," *Cyberspace: Jurnal Pendidikan Teknologi Informasi,* vol. 2, no. 2, pp. 109-134, 2018.

[19] W. Stallings, Cryptography and Network Security, 4th ed., Prentice-Hall, 2005.

[20] C. Harris, "The History of Bitcoin," Crypto Currency News, 21 2 2018. [Online]. Available: https://cryptocurrencynews.com/the-history-of-bitcoin/.

[21] R. C. Noorsanti, H. Yulianton and K. Hadiono, "Blockchain-Teknologi Mata Uang Kripto (Crypto Currency)," in *Proceeding SENDI_U*, 2018.

[22] D. Efanov and P. Roschin, "The All-Pervasiveness of the Blockchain Technology," *Procedia Computer Science,* vol. 123, pp. 116-121, 2018.

[23] K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," *IEEE Access,* vol. 7, pp. 10127-10149, 2019.

[24] R. Zhang, R. Xue and L. Liu, "Security and Privacy on Blockchain," *ACM Computing Surveys,* vol. 52, no. 3, 2019.

[25] W. Pourmajidi and A. Miranskyy, "Logchain: Blockchain-Assisted Log Storage," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018.

[26] S. Barjtya, A. Sharma and U. Rani, "A detailed study of Software Development Life Cycle (SDLC) Models," *International Journal Of Engineering And Computer Science,* vol. 6, pp. 22097-22100, 2017.

[27] M. M. Syaikhuddin, C. Anam, A. R. Rinaldi and M. E. B. Conoras, "Conventional Software Testing Using White Box Method," *KINETIK,* vol. 3, no. 1, pp. 65-72, 2018.

[28] P. X. Mai, F. Pastore, A. Goknil and L. Briand, "Metamorphic Security Testing for Web Systems," in *2020 IEEE 13th International Conference on Software Testing, Validation and Verification (ICST)*, 2020.

[29] L. Zhou, C. Su, Y. Wen, W. Li, and Z. Gong, "Towards practical white-box lightweight block cipher implementations for IoTs," *Future Generation Computer Systems*, vol. 86, pp. 507-514, 2018..

[30] P. Navabud and C. Chen, "Analyzing the Web Mail Using Wireshark," *2018 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, 2018, pp. 1237-1239.

 http://doi.org/10.26594/register.v8i1.2190

HASIL CEK_Block-hash of blockchain framework against man-in-the□middle attacks

ORIGINALITY REPORT

9%	6%	8%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

6%

★ I'tishom Al Khoiry, Rahmat Gernowo, Bayu Surarso. "Fuzzy-AHP MOORA approach for vendor selection applications", Register: Jurnal Ilmiah Teknologi Sistem Informasi, 2021

Publication

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		