APTISI Transactions on Management (ATM)
Vol. 7, No. 3, 2023, pp. 184~193
E-ISSN: 2622-6804 P-ISSN: 2622-6812, DOI: 10.33050

Blockchain Based Certificate Verification System Management

Qurotul Aini[1], Eka Purnama Harahap[2], Nuke Puji Lestari Santoso[3], Siti Nurindah Sari[4], Po Abas Sunarya[5]
[1,2,3]Master of Information Technology, University of Raharja, Indonesia
[4]Department of Information System, University of Raharja, Indonesia
[5]Master of Information Technology, University of Pasundan, Indonesia
[1]aini@raharja.info, [2]ekapurnamaharahap@raharja.info, [3]nuke@raharja.info, [4]siti.nurindah@raharja.info, [5]abas@raharja.info

Article Info

Article history:

Received 09-13-2022
Revised 11-23-2022
Accepted 11-25-2022

Keywords:

Authentication
Blockchain
Certificate



ABSTRACT

One of the key responsibilities of the Public Key Infrastructure (PKI) is revocation management. Additionally, the security of any Public Key Infrastructure (PKI) depends on it. Today's revocation methods are susceptible to a single point of failure when network traffic rises due to the growth in the quantity and size of networks as well as the adoption of new paradigms like the Internet of Things and the use of the web. The author uses the strength and resiliency of blockchain to overcome these issues and present a productive decentralized certificate revocation management and status verification system. The author adds a field that specifies which distribution point the certificate will belong to in the event that it is revoked using the certificate structure extension field. Then, the author carries out a thorough assessment of our plan using performance indicators like execution time and data consumption to show that it can fulfill the demands with high effectiveness and little expense. Additionally, the author contrasts the effectiveness of our strategy with two of the most widely-used revocation approaches, namely the Certificate Revocation List and the Online Certificate Status Protocol. The data collected demonstrate that our suggested strategy works better than the existing scheme.

This is an open access article under the CC BY-SA license.



Corresponding Author:

Siti Nurindah Sari
Department of Information System, University of Raharja, Indonesia
Email: siti.nurindah@raharja.info

1. INTRODUCTION

The way people live, connect, and do business has altered since the invention of the Internet. The World Wide Web is now a crucial component of our everyday activities and surroundings, and it facilitates the daily transit of massive amounts of data. For user privacy, the majority of the data sent must be safe- guarded since it is sensitive. Additionally, in order to be received or accessed, many desired messages and services demand authentication[1]. The most popular method for addressing these security criteria is public key infrastructure, while various approaches are put forth. In fact, the Secure Sockets Layer (SSL) and Trans-port Layer Security (TLS) protocols, along with the Public Key Infrastructure, offer private communications through encryption and certificate chains for authentication.

The set of authorities, rules, and practices necessary to control the public key mechanism is known as the public key infrastructure. It is a collection of rules and procedures that link the identification of each entity to its public key[2]. The registration procedure and the issue of a certificate serve as the binding mechanisms.

As a result, PKI issues, maintains, uses, saves, and revokes the aforementioned certificates.

In order to cancel a certificate before it expires for different reasons, such as the theft of the certificate's private key or the certificate owner's dishonesty, it must be possible to revoke a previously granted certificate. For methods that employ certificates for authentication and authorisation, certificate revocation is crucial, and its absence from the authentication cycle might have serious repercussions. For instance, within a week of the Heart bleed SSL/TLS vulnerability announcement, more than 80,000 SSL certificates were canceled [3]. Remote attackers can steal private keys from vulnerable servers thanks to the Heartbleed flaw. It's doubtful that most web server access logs will include proof of such a hack. If the susceptible certificate has not been revoked, the secure site may still be insecure even after it has been replaced. Indeed, until their natural expiration date, which may be years away, compromised certificates will continue to be usable by attackers. The old certificate can be used by a well-positioned attacker to pretend to be the target site if they have access to the old certificate's private key and can intercept the victim's Internet traffic (e.g. using phishing techniques). Another instance of a security event involving certificate revocation checks making news is given [4]. It was discovered that a trustworthy website runs a malicious Java program that infects users' PCs with malware. It was discovered that the website's certificate had actually been revoked when it was utilized in the attack, despite the fact that the infected victim had not checked its status.

The Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP), Certificate Revocation Tree (CRT), and other systems and techniques for revocation are only a few examples. However, each of the current methods has a number of drawbacks, including limited support for scaling, higher costs for both computing and money, vulnerability to user privacy, and so on.

Like many researchers, blockchain represents a very promising technology for the development of decentralized and robust security solutions. The author summarize the main contributions of this work as follows:

1. Relying on the advantages of blockchain strength and resilience, the author proposes an efficient decentralized certificate revocation management and status verification system.
2. The author adds a field that specifies which distribution point the certificate will belong to if it is revoked using the X509 certificate structure extension field. Each distribution point is represented by a Bloom filter that contains certificates that have been revoked. In the public blockchain, revocation details and bloom filters are kept.
3. In comparison to prior work, the authors significantly reduce the time needed to get revocation information by employing a bloom filter.
4. The author suggests a method that is entirely compliant with current web standards. To use this strategy in a web context, no modifications are necessary.
5. The system can fulfill the necessary security and performance criteria, according to the findings of the rigorous study the authors did of our proposed revocation system (using performance indicators like time and data consumption).

The remaining portions of the document are organized as follows: The methods and procedures now in use for certificate revocation are described in Part II. Then, Section III discusses our method for revoking access and verifying status[5]. Following that, Section IV provides a description of our execution as well as an assessment of how well our suggested strategy worked and the outcomes. The work is concluded in Section V, which also makes a suggestion for future research directions.

2. RELATED WORK

There are several plans and ideas to control and enhance certificate revocation methods. The author discusses a few of the most well-known, utilized by genuine systems and standards, in this part.

2.1. Principal Process for Revoking Certificates

Revocation of Certificates List The Certificate Revocation List is a list of expired certificates that is updated on a regular basis and is dated and signed by a Certification Authority (CA). The publication server that hosts the associated CRL must be contacted in order to verify the validity of a certificate[6]. The request must include the identifier of the CA that issued the certificate as one of its arguments. After receiving the most

recent CRL produced by the CA, the verifier must verify the CRL's signature and validity before searching for the certificate in the CRL.

The benefits of CRL include its ease of use, depth of knowledge, and minimal danger. The CRL's size, however, is its primary disadvantage because it drastically restricts its expansion due to the high bandwidth needed for update and verification.

The CRL includes the date of the subsequent update to guarantee freshness (from the CRL). Users that want updated revocation information will thus wish to obtain updated CRLs all at once. The server that distributes CRL's may experience a point of failure as a result of the surge of CRL requests that might result from this.

The list of all certificates that haven't expired but have been revoked after the last CRL was issued is represented by the Delta-CRL schema. The scalability issue with downloading CRLs is addressed by Delta-CRL [6]. The client doesn't need to download the complete CRL each time, in fact. The revocation data, however, is only useful upon the linkage of the Delta-CRL with the primary CRL. CRL as a whole is much smaller than Delta-CRL. Therefore, the length and difficulty of revocation verification grow along with the amount of the CRL.

This approach does have a significant flaw, though, and that is the uneven development of the pieces. More specifically, it is decided where a certificate will remain if it is revoked when it is generated. Due to (1) some distribution points being uprooted more frequently than others and (2) some CRL segments being requested more frequently than others, it encounters an imbalanced strain on the distribution points[7]. Additionally, CRL segmentation is permanently fixed for the duration of the certificate in question when the CRL-DP approach is utilized. As a result, before issuing certificates, CAs must declare static fragmentation, which adds to the challenge.

2.2. Comparative Analysis of Certificate Revocation Processes

Table 1 presents a comparison of the different revocation schemes. Comparisons are based on five metrics:

1. Scalability: outlines how the method responds as the user base or revocation rate grows. The author distinguishes three tiers. Low level signifies that the approach is (or soon will be) unable to satisfy the needs of the current system; mid-level signifies that the approach can satisfy the needs of the current system, but that it is unable to handle system evolution, particularly in light of IoT requirements; and high level signifies that the approach can satisfy both the needs of the current system and those of the future.
2. Connectedness: This term refers to the level of connectivity (online or offline) that the party depending on the information must adopt to assure reliability.
3. List type, which can be either a blacklist, a whitelist, or both, indicates the kind of list that is being utilized.
4. Real-time Services: This term describes the approach's ability to give end users access to real-time information.
5. Indicates if the stated strategy requires more computing cycles than the CRL approach, which depends on associated work and outcomes. For purposes of comparison, the author decided to specify the CRL approach as it is the most widely used and well-known method.
6. Privacy exposure: identifies if the method makes use of a responder that may determine whose certificate the end user is verifying and, consequently, monitor the websites the user is visiting.

The authors remark from Table 1 that the majority of the currently used approaches have added expenses and do not offer real-time information. Additionally, all current approaches—with the exception of the Dynamic CRL Distribution Point approach—cannot satisfy future scaling needs. Additionally, the majority of the approaches function both offline and online. The author may infer from this comparison that neither of these strategies can fully satisfy all the requirements for a reliable retraction mechanism [8].

As a result, it's essential to provide a decentralized revocation process that promotes network scalability and prevents a single point of failure. It must also include real-time revocation information. It should also respect user privacy and address problems with privacy exposure.

Table 1. Summary of revocation solutions for X509 certificates

Approach	Scalability	Connectivity	List Type	Additiona Cost	Real-time Service	Privacy Expo-sure
CRL	Low	offline, on-line	Blacklist	/	No	No
Delta-CRL	Low	offline, on-line	Blacklist	No	No	No
CRL distribution points	Medium	online	Blacklist, Whitelist	No	No	No
Dynamic CRL distri-bution points	Hight	offline, on-line	Blacklist	Yes	No	Yes
CRS	Low	offline, on-line	Blacklist	No	No	Yes

2.3. Blockchain Based Revocation Proposal

Blockchain technology is a desired solution for PKI design and implementation because of its distributed, event recording, and non-reproducible properties. Indeed, the key issues with conventional PKI infrastructure are addressed by blockchain features: (1) There is no single point of failure for blockchain-based PKI solutions since they are distributed. (2) No third party is trusted and no prior system trust is necessary since confidence is established based on the majority vote of miners. And (3) there are a number of open source blockchain implementations that support the development of solutions that are reasonably priced. The author next goes through a few PKI methods based on blockchain. The author concentrates on managing their revocation.

A fully decentralized PKI called Certcoin uses the Namecoin blockchain's consistency to give a solid assurance of identity retention. Registration, renewal, search, verification, and revocation are the five functions that Certcoin employees. The user creates his own secret and public keys locally upon registration. The transaction's public key and signature are then sent to the blockchain [9]. The blockchain network authenticates the transaction signature and determines whether or not this ownership has already been registered in the system. The tuple (ID, public key) is discarded if the verification fails; otherwise, it is added to the blockchain.

Certcoin defines a PKI scheme that addresses some of the issues discussed earlier. However, it still suffers from many drawbacks such as high costs in mining and public key lookup and verification. Moreover, there is no real verification of the linkage of the ID to the registered public key. Finally, because the authors are interested in the revocation technique in this work, at Certcoin, the identity ID owner can revoke his public key simply by posting the transaction to the blockchain. Thus, the revocation process is completely handled by the owner himself which can lead to various drawbacks such as: (1) It can be a difficult task for the user to handle the revocation by himself as it requires knowledge of how to proceed [10]. Also, the user cannot tell if the key has been compromised. (2) A malicious user will not revoke his key because he is acting maliciously. (3) In order to verify the certificate status, the mechanism must first ensure that the certificate is not revoked by verifying the revoked certificate published on the blockchain, which means exploring the blockchain. However, it is well known that searching on the blockchain can be very expensive in terms of time.

New revocation information structure: Revocation records that are normally stored in the CRL will be stored in the bloom filter. Each filter represents a distribution point.

3. METHOD

The planned cancellation of fresh certificates and a status verification system are the key goals of our strategy. Our method depends on a public blockchain to store and distribute information about revoked certificates. More particular, our solution follows the same guidelines as CRL distribution locations in order to allow scalability. The author adds a field that specifies which distribution point the certificate will belong to in the event that it is revoked using the X509 certificate structure extension field. A Bloom filter presenting revoked certificates at each distribution point (See Figure 1). The blockchain stores data on revocation and bloom filters. When a CA revokes a certificate, it updates the relevant Bloom filter and generates a fresh

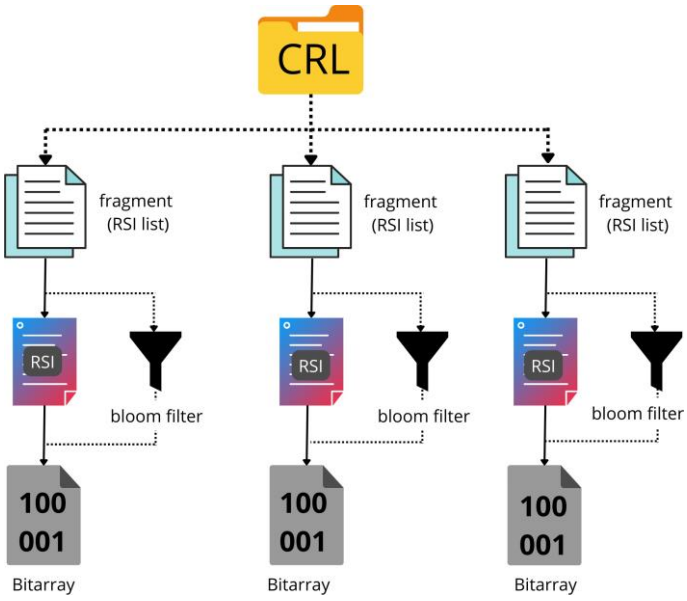


Figure 1. New Revocation Information Structure Blockchain Transaction to Store the New Certificate.

3.1. Background

Our strategy principally depends on bloom filters and blockchain. The author gives a succinct overview of these ideas in this section. Blockchain: A distributed database (ledger) that keeps an unalterable, permanent record of transactional data is known as a blockchain. Blockchain relies on a peer-to-peer network to be completely decentralized. To avoid a single point of failure, each network node keeps a copy of the ledger instead. All copies are concurrently updated and confirmed.

The double spending issue with cryptocurrencies is a problem that blockchain technology was designed to address. The use of blockchain applications as a safe method to build and administer distributed databases and keep track of all manner of digital transactions, however, is now the focus of several studies [11].

The blockchain ledger is made up of many blocks, each of which has two sections. The former contains transactions or facts, which the database must keep and can be of any kind, including financial transactions, health information, system logs, traffic statistics, and so on [12]. The second is referred to as a header and provides details about the block as well as the hash of the preceding block (such as a date, transaction hash, etc.). As a result, the already existing block sets create a chain of linked and organized blocks. The tougher it is to fabricate, the longer the chain. In fact, because their hashes are connected, if a rogue user wishes to alter or swap transactions in a block, they must also alter all of the blocks that follow. Then, it has to change the version of the blockchain stored by each participating node.

3.2. System Operation

This section contains a thorough explanation of how our system functions. The author achieves this by describing how each sub-system works.

1. CA - Blockchain: The CA determines how frequently it updates and propagates its revocation information. For instance, hourly updates all newly issued certificates that have been canceled via network connection. This period of time is known as Tu (update time) [13]. When it's time for renewal, the CA creates a data structure called Revocation Status Information (RSI) for each revoked certificate and

```
public function uploadfile() {
      header('Content-type: application/json');
      $user = Auth::user();
      $actionTakenBy = escape($user->fname.' '.$user->lname);
      $random = Str::random(61);
      /*
       * Check, whether IP address register is allowed in .env
       * If yes, then capture the user's IP address
       */
      if (env('REGISTER_IP_ADDRESS_IN_HISTORY') == 'Enabled') {
         $actionTakenBy .= ' ['.getUserIpAddr().']';
      }
      $data = array(
                  "company" => $user->company,
                  "uploaded_by" => $user->id,
                  "name" => input("name"),
                  "folder" => input("folder"),
                  "file" => $_FILES['file'],
                  "is_template" => "No",
                  "source" => "form",
                  "document_key" => "ABC".$random,
    "activity" => 'File uploaded by <span class="text-primary">'.
$actionTakenBy.'</span>.'
                );
      $upload = Signer::upload($data);
      if ($upload['status'] == "success") {
         exit(json_encode(responder("success", "",
"","documentsCallback()", false)));
      }else{
         exit(json_encode(responder("error", "Oops!",
$upload['message'])));
      }
   }
```

Figure 2. New Revocation Information Structure

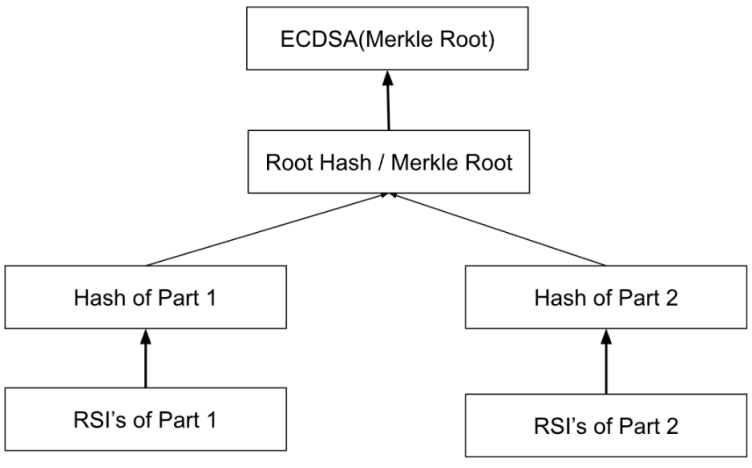


Figure 3. New Revocation Information Structure

executes blockchain operations to disseminate each RSI. More specifically, the CA creates a Bloom filter and propagates it through blockchain transactions such that it contains both previously and recently revoked certificates (RSI corresponds to the equivalent CRL distribution point).

2. There are two different kinds of blockchains: public and private. A feature of public blockchains is the usage of an infinite number of anonymous nodes. On the blockchain, transactions may be read, written, and verified by any actor. Private blockchains, on the other hand, impose restrictions on consensus contributors. Transaction validation rights are only granted to a small group of trustworthy parties. Since every node in the globe may view blockchain data and traffic without needing to be a part of the network, public blockchains have been employed due to their openness. The sole services performed on a block are integrity protection and immutability, and blocks and transactions transparently travel without any encryption. Furthermore, a robust community often oversees the management of public blockchains, ensuring their dependability [14].

In our approach, the server should keep checking for new transactions provided by its CA. In other words, the server must download every transaction associated with its distribution point. It therefore downloads the RSI which includes the new Bloom filter from its distribution point. Additionally, for each RSI downloaded, the server must create a structure called Lightweight Revocation Status Information (LRSI) [15]. The LRSI hasthe same structure and data fields as the RSI, except that it doesn't include a Bloom filter. Indeed, the server just removes the Bloom filter field and keeps everything else. The LRSI structure will be used in case of further investigation from the client side to detect false positives [16].

4. IMPLEMENTATION

The author employ the Namecoin blockchain to put our strategy into practice. A fork of Bitcoin called Namecoin seeks to offer decentralized DNS. The Internet Corporation for Assigned Names and Numbers (ICANN) is not involved in the implementation of the.bit top-level domain2. A Proof of Work (PoW) consensus algorithm is used. The primary attributes of Namecoin are listed in Table V [17]. All public blockchains may be utilized to implement our method because they all provide data storage (e.g., Bitcoin3, Litecoin4, dash5 or others) [18]. A blockchain that uses smart contracts is not necessary to accomplish our concept. It is possible to employ such blockchains, such as Ethereum6, Cosmos7, Tezos8, Metahash9, or others. Each blockchain has unique benefits and drawbacks compared to our strategy. However, the majority of contractless blockchains only provide a small amount of storage capacity for transaction-based data. When it comes to contract-based blockchains, our method becomes unnecessarily complex because contract creation is needed to read and write into the blockchain [19]. Contracts also have additional delay while being executed. Therefore, author choose Namecoin for the three reasons listed below:

1. Allows key/value pairs to be used as data storage, which is a good option for our strategy. The key and its value, which is 520 bytes, can be stored by the user.

2. Because of the daily transaction volume's minimal size, searching for data on the blockchain is simple.

As previously stated, author employ a similar strategy to distribution points to promote scalability. Different RSIs are used to symbolize each distribution point [19]. Using the RSI structure previously mentioned, the field needs 170 bytes of storage (without taking into account the Bloom filter field). Our Bloom filter will be 350 bytes in size since the Namecoin value is only allowed to be 520 bytes (2800 bits) [19].

The Bloom filter in our implementation should be able to maintain a fair rate of false positives while representing the greatest number of revoked certificates possible. Therefore, author also need to take into account how many revoked certificates (n) will be represented by a single Bloom filter when calculating the ideal number of hash functions (k). Author varied k and n while accounting for the filter size $m = 2800$ to get the false positive probability of the filter response as specified by Equation 1. The outcomes are shown in Figure 8. It should be noticed that the false positive rate is usually quite low whether $n = 100$ *or* $n = 250$. The amount of certifications that have been revoked that author must reflect, meanwhile, is similarly minimal [20]. The publishing/revoke ecosystem may suffer as a result of using numerous Bloom filters when taking this value of n into account. Additionally, the risk of a false positive is always higher than 26% for $n = 1000$, which is a large probability, especially given that the system would regularly check for certificate revocation using the

LRSI method in this scenario, adding time and increasing computing costs. Author contend that the optimal compromise may be reached by taking the parameters $k = 3$ with $n = 500$ *or* $n = 750$ into account. In fact, Pfp is 7% when $n = 500$ and 18% when $n = 750$. So, depending on the use case, any of these values can be chosen.

5. CONCLUSION

Certificate revocation management is still a problem that keeps coming up and becoming worse, especially given how open and evolving today's networks are and how quickly new paradigms like the Internet of Things and cloud computing are being adopted. Existing revocation management strategies have a number of problems, [21] including: (1) centralization creating a single point of failure; (2) increased costs; (3) exposure to user privacy; and many others. The difficulty of present ways to assure adequate revocation management would result from this vulnerability given the growth of the network and the openness/connection of the many use cases.

Some of these issues are resolved by blockchain-based strategies. The suggested method, however, is incompatible with the present X509 standard, and its implementation necessitates the development of a completely new web infrastructure [22].

In this regard, author provide a brand-new revocation management and status verification system that satisfies all criteria and delivers excellent performance outcomes. Our strategy depends on blockchain, making it extremely durable and completely decentralized to accommodate network development and scalability. Furthermore, it does not require any modifications to be implemented and is entirely compliant with current web standards, which, as far as author are aware, no other solution has presented [23]. Furthermore, the previously suggested blockchain-based revocation method has significant time delays as a result of the time required for blockchain tracing to locate the necessary transactions. The author provide a strategy that significantly reduces the amount of time needed to convey retraction information and depends on a bloom filter. Our plan, specifically, follows the CRL distribution point's basic tenets. Each distribution point is shown with a Bloom filter that has been filled with certificates that have been revoked [24]. Then, utilizing the public blockchain, Bloom filters and revocation information are shared and distributed.

On a genuine testbed, author implement and assess our strategy. This study amply proves our revocation system's capabilities to surpass current methods while meeting the necessary security and performance criteria (OCSP and CRL based systems) [25]. Future research will concentrate on the worst-case situation of our method, in which the filter reacts favorably. In fact, author are striving to provide a substitute for downloading every LRSI from the server.

ACKNOWLEDGMENT

This work is supported by Research Funding and Higher Education PKM for Fiscal Year 2022 Referring to Letter Number 0357/E5/AK.04/2022 from the Ministry of Education, Culture, Research, and Technology.

REFERENCES

[1] N. Lutfiani, U. Rahardja, and K. T. Khasanah, "The Development Viewboard As an Information Media at Official Site Asosiation," APTISI Trans. Manag., vol. 6, no. 1, pp. 10–18, 2022.

[2] P. Hendriyati, F. Agustin, U. Rahardja, and T. Ramadhan, "Management Information Systems on Integrated Student and Lecturer Data," Aptisi Trans. Manag., vol. 6, no. 1, pp. 1–9, 2022.

[3] U. Rahardja, P. A. Sunarya, N. Lutfiani, M. Hardini, and S. N. Sari, "Transformation of Green Economic Recovery Based on Photovoltaic Solar Canopy," International Journal of Marine Engineering Innovation and Research, vol. 7, no. 2, Jun. 2022, doi: 10.12962/j25481479.v7i2.12495.

[4] U. Rahardja, N. Lutfiani, A. Yolandari, J. Sistem Informasi, and S. Raharja, "Penerapan Viewboard Informatif Pada Asosiasi Perguruan Tinggi Swasta Indonesia Dalam Era Industri 4.0," Technomedia Journal, vol. 3, no. 2 Februari, pp. 224–234, Feb. 2019, doi: 10.33050/TMJ.V3I2.738.

[5] Jerry Heikal, Vitto Rialialie, D. Rivelino, and Ign Agus Supriyono, "Hybrid Model Of Structural Equation Modeling Pls And Rfm (Recency, Frequency And Monetary) Model To Improve Bank Average Balance," Aptisi Transactions on Technopreneurship (ATT), vol. 4, no. 1, pp. 1–8, Dec. 2021, doi: 10.34306/ATT.V4I1.221.

[6] A. Pambudi, R. Widayanti, and P. Edastama, Trust and Acceptance of E-Banking Technology Effect of Mediation on Customer Relationship Management Performance, ADI Journal on Recent Innovation (AJRI), vol. 3, no. 1, pp. 87–96, Sep. 2021, doi: 10.34306/AJRI.V3I1.538.

[7] A. Bagus Setiawan, W. Rachmawati, A. Taufiq Arrahman, N. Natasyah, and F. N. S. Fadil, "Aplikasi Monitoring Stok Barang Berbasis Web Pada PT. Intermetal Indo Mekanika," ADI Bisnis Digital Interdisiplin Jurnal, vol. 2, no. 2, pp. 1–6, Sep. 2021, doi: 10.34306/ABDI.V2I2.254.

[8] M. Nurchaerani, Haryati, and F. Nursyamsi, "Upaya Meningkatkan Minat Belajar Di Masa Pandemi Melalui Pelatihan Bahasa Inggris Secara Daring," ADI Pengabdian Kepada Masyarakat, vol. 2, no. 1, pp. 1–7, Oct. 2021, doi: 10.34306/adimas.v2i1.451.

[9] M. R. Anwar and S. Purnama, "Boarding House Search Information System Database Design," International Journal of Cyber and IT Service Management, vol. 2, no. 1, pp. 70–81, Mar. 2022, doi: 10.34306/ijcitsm.v2i1.89.

[10] A. Dudhat and T. Mariyanti, "Indoor Wireless Network Coverage Area Optimization," International Journal of Cyber and IT Service Management, vol. 2, no. 1, pp. 55–69, Mar. 2022, doi: 10.34306/ijcitsm.v2i1.86.

[11] E. Dolan and R. Widayanti, "Implementation Of Authentication Systems On Hotspot Network Users To Improve Computer Network Security," International Journal of Cyber and IT Service Management, vol. 2, no. 1, pp. 88–94, Mar. 2022, doi: 10.34306/ijcitsm.v2i1.93.

[12] U. Rahardja, A. N. Hidayanto, P. O. H. Putra, and M. Hardini, "Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol," Journal of Applied Research and Technology, vol. 19, no. 4, pp. 308–321, Aug. 2021, doi: 10.22201/icat.24486736e.2021.19.4.1046.

[13] N. Lutfiani, D. Apriani, E. A. Nabila, and H. L. Juniar, "Academic Certificate Fraud Detection System Framework Using Blockchain Technology," Blockchain Frontier Technology, vol. 1, no. 2, pp. 67–76, Jan. 2022, doi: 10.34306/BFRONT.V1I2.55.

[14] U. Rahardja, A. N. Hidayanto, P. Oktavia, H. Putra, and M. Hardini, "Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol," jart.icat.unam.mx, vol. 19, no. 4, p. 309, 2021, doi: 10.1016/j.jart.2017.02.005.

[15] S. Kosasi, U. Rahardja, N. Lutfiani, E. P. Harahap, and S. N. Sari, "Blockchain Technology - Emerging Research Themes Opportunities in Higher Education," Feb. 2022. Accessed: Aug. 22, 2022. [Online]. Available: http://dx.doi.org/10.1109/icostech54296.2022.9829053

[16] R. Donny M. Iskandar, T. Maryanti, Acep R. Jayaprawira, and S. N. Sari, "Indonesian Islamic Banking Fintech Model Strategy: ANP Method," Aptisi Transactions on Technopreneurship (ATT), vol. 4, no. 2, pp. 142–152, Jul. 2022, doi: 10.34306/att.v4i2.257.

[17] U. Rahardja, I. Handayani, N. Lutfiani, and F. P. Oganda, "An Interactive Content Media on Information System iLearning+," IJCCS (Indonesian Journal of Computing and Cybernetics Systems), vol. 14, no. 1, pp. 57–68, Jan. 2020, doi: 10.22146/IJCCS.51157.

[18] U. Rahardja, N. Lutfiani, A. Setiani Rafika, and E. Purnama Harahap, "Determinants of Lecturer Performance to Enhance Accreditation in Higher Education," Oct. 2020. Accessed: Aug. 22, 2022. [Online]. Available: http://dx.doi.org/10.1109/citsm50537.2020.9268871

[19] S. A. Yakan, "Analysis of Development of Artificial Intelligence in the Game Industry," International Journal of Cyber and IT Service Management, vol. 2, no. 2, pp. 111–116, May 2022, doi: 10.34306/ijcitsm.v2i2.100.

[20] U. Rahardja, Q. Aini, F. Budiarty, M. Yusup, and A. Alwiyah, "Socio-economic impact of Blockchain utilization on Digital Certificates," APTISI Transactions on Management (ATM), vol. 5, no. 2, pp. 106–111, Mar. 2021, doi: 10.33050/ATM.V5I2.1508.

[21] Q. Aini, N. Lutfiani, N. P. L. Santoso, S. Sulistiawati, and E. Astriyani, "Blockchain For Education Purpose: Essential Topology", ATM, vol. 5, no. 2, pp. 112–120, May 2021.

[22] F. Agustin, Q. Aini, A. Khoirunisa, and E. A. Nabila, "Utilization of Blockchain Technology for Manage- ment E-Certificate Open Journal System", ATM, vol. 4, no. 2, pp. 133–138, Apr. 2020.

[23] I. A. Kurniawan, D. Yusman, and I. O. Aprilia, "Utilization of Blockchain Technology Revolution in Electronic ID Card Data Integrity", ATM, vol. 5, no. 2, pp. 137–142, Apr. 2021.

[24] K. B. . Rii, "Digital Ilearning Chain Scheme in Education Blockchain Based", att, vol. 4, no. 2, pp. 174–183, Jul. 2022.

[25] Q. . Aini, "Security Level Significance in DApps Blockchain-Based Document Authentication", att, vol. 4, no. 3, pp. 292–305, Oct. 2022.