ICAITI 2021
ICAITI2021
The 4th International Conference on
Applied Information Technology and Innovation

ICAITI 2021

The 4th International Conference on Applied Information Technology and Information

LETTER OF ACCEPTANCE

Dear Respected Authors,
It is a pleasure to inform you that your submission (detail below) is accepted at the 4th ICAITI 2021 that will be held on March 15-17, 2022 in Lombok, Indonesia.

Author(s)	:	Ahmad Zafrullah Mardiansyah, Ario Yudo Husodo, Cahyo Mustiko Okta Muvianto, Ryan Adhitya Nugraha and Iqbal Santosa
Title	:	Design of A Secured Electronic Voting System by Using Cross-Hash Validation Mechanism
Paper ID	:	147
Review result	:	*refer to easychair attachment*

INFORMATION FOR AUTHOR(S)-Please read very carefully.

1. *Be sure that the final paper is prepared as per the reviewer (s) comments.*
2. *Please submit your camera-ready paper no later than 3rd March 2022, or your submission will not be published in our journal.*
3. *Be sure that the submitted camera-ready paper is in the prescribed format (.docx).*
4. *For any questions, please contact us at iqbals@telkomuniversity.ac.id*

On behalf of the Organizing Committee of the 4th ICAITI, we would like to congratulate you on the acceptance of your paper and for participating in the 4th ICAITI. Other arrangements regarding the conference will be informed through the website and your registered email.

Sincerely,
Bandung, 23 February 2022

ICAITI 2021
ICAITI2021
The 4th International Conference on
Applied Information Technology and Innovation

Rd. Rohmat Saedudin, Ph.D.
General Chair of ICAITI 2021

Design of A Secured Electronic Voting System by Using Cross-Hash Validation Mechanism

Ahmad Zafrullah Mardiansyah[a*], Ario Yudo Husodo[a],
Cahyo Mustiko Okta Muvianto[a], Ryan Adhitya Nugraha[b]

[a] Department of Informatics Engineering, University of Mataram,
Jl. Majapahit No. 62, Mataram, 83125, Indonesia
[b] Department of Information Systems, Telkom University,
Jl. Telekomunikasi Terusan Buah Batu No. 1, Bandung, 40257, Indonesia
**Corresponding author: zaf@unram.ac.id*

***Abstract*—One of the most critical aspects of the Electronic Voting (E-Voting) system is its confidentiality. A sound E-Voting system should be able to keep voters' votes secret. It means that the E-Voting system could not allow any person to analyze the vote of any specific voter. In this paper, we design a secure E-Voting system that systematically encrypts voters' ballots in the database that makes any person, including the E-Voting admin, unable to interpret the votes recorded in the database. We develop a cross-hash validation approach as our basis. In our approach, the votes from two different voters, even both voters who vote for the same candidate, will be recorded in two different values. We combine a voter's data with their vote, adding extra parameters and keys, then hashing it with some specific algorithm. We also use timestamp information for our hashing parameter. By doing so, any voter will never have the same hashing output value. This approach makes recorded votes data unique and impossible to be decoded. We developed a cross-validation algorithm to count the election results to interpret the votes data because the hashed vote value cannot be decrypted to its original value. With this approach, the system can only retrieve the summary of E-Voting without analyzing the vote from any specific voter. Our method has been tested in a real-case scenario. We test our approach on the election of the Engineering Faculty Senate of the University of Mataram. In the experiment, we conclude that our system is practically secure and can be developed for a larger scale of E-Voting.**

***Keywords* - Confidentiality system design, cross-hash validation, electronic voting, unique vote record, vote data security.**

I. Introduction

The social representative election process has become an inseparable part of human life. As the increased necessity of society to establish a social organization, the need to conduct an effective and efficient election process has also immensely increased. In a conventional election process, representative candidates or leaders are usually done by using a voting system. All the members of the organization vote for their candidates, then the candidates with the highest votes typically win the election.

The voting system has become a well-accepted approach for society to choose their representatives or leader for any organization or governance leaders. For example, district head election, governor election, or even presidential election is conducted using a voting system. In general, we can say that the election process has become a central administrative work in society, where it is usually conducted using a voting system.

Currently, there are two main approaches to running the voting system. First, by using a manual voting system, and second, electronic voting (E-Voting) system. In a manual voting system, voters commonly vote their candidates on a ballot, and then the official election committee will manually calculate the votes. This approach, although practically proved to be effective, is time-consuming. Meanwhile, in the second voting system, E-Voting, the voters use an electronic device as their ballot. Usually, it is implemented in both online process and offline processes. In this approach, the calculation of voters' choices can be done automatically, and the result of the election can be summarized in a very short time.

As described earlier, we can observe that the E-Voting system is a more efficient way to conduct the voting process. Although this approach is promising, the main concern in the E-Voting system implementation is its security and privacy aspect. In the E-Voting system, voters' privacy has become the system's main concern. A sound E-Voting system should fall to these main requirements: each voter can only have one voting account, each voter can only vote for a one-time election process, and no one can know an individual voter's vote.

In today's growing E-voting mechanism, guaranteeing that a voter can only have one account and can only vote for one time is relatively well established. The most critical aspect that is still debatable in the E-Voting system is the privacy of voters' votes. Because each vote is recorded in an electronic system, where the source (voters' identity) can be easily retrieved when the vote is recorded in the system, it is doubtful that their votes are kept private and secure E-Voting database. Currently, many societies are skeptical about it. Many people argue that voters' privacy is not well secured in an E-Voting system. Thus, if voters choose a candidate, they worry that their votes can be crosschecked and known by any irresponsible party. If this happens, of course, the privacy aspect of the voting system is broken.

As we can analyze from the previous passages, we can conclude that one of the most important aspects to be developed in a good E-Voting system is its privacy. Because today's society needs an E-Voting system, but today's E-Voting system still has one potential threat, we are concerned about developing a secured E-Voting system that minimizes the threat to voters' privacy data break. In this paper, we manage to establish a well-developed E-Voting system tested in one of Indonesia’s government institutions. To guarantee that there is no data break-in voters vote data, we develop a cross-hash validation approach to secure voters' vote data. No one can analyze any specific voters’ vote data in our system, including the E-Voting system administrator. Our approach is practically secured and well tested in a real-life scenario that involves hundreds of voters. According to our experiment, we can deduce that our proposed method to secure voters' vote privacy is practically safe and can be implemented to secure a bigger scale of a social election, like national presidential E-Voting.

II. Related Works

The electronic voting (E-Voting) scheme was first proposed in 1981 [1]. In E-voting gradual development, there have been many approaches proposed to establish a secured E-Voting system. For example, [2] proposed a secure data transfer in cloud technology-based E-Voting. Meanwhile, [3] proposed homomorphic elliptical curve cryptography to secure a cloud E-Voting system. The blockchain approach has also been considered a method to secure an E-Voting system. Researchers in [4-6] have developed a blockchain-based approach to reducing voter fraud, preventing ballot content attacks, and establishing universal ballot verification.

A good E-Voting system should be capable of securing its voters' ballot privacy. Some aspects must be handled carefully to establish a secure E-Voting system. Some researchers have developed distinctive approaches to achieving a sound E-Voting system, especially data encryption techniques. In [7-10], the researchers use a mix-net method to encrypt E-Voting data. Meanwhile, a blind signature is used by [11-17] to ensure voters' data integrity. Researchers in [18-22] use homomorphic encryption, while researchers in [23-25] use a secret sharing approach to secure E-Voting system data.

To establish a secure and feasible E-Voting result, one of the most popular methods used is homomorphic encryption in conjunction with other encryption methods like zero-knowledge proof [26] or partial knowledge proof [27]. Although these approaches have good results, they require a high computation resource. To overcome that drawback, [28] propose a decentralized E-Voting system in cloud computing. Some methods have also been developed to ensure that voters are allowed to prove nothing about their ballot's content to others. It is usually done by using the coercion resistance approach [29-33].

In the E-Voting system, there are usually 5 elements involved. First is Voter (V), second is Candidate (C), third is trusted Authority Center (AC), fourth is Voting System (VS), and fifth is Bulletin Board (BB). A voter (V) is a user in the E-Voting system that can choose any candidate as their favorite. A trusted Authority Center usually arranges the list of eligible voters, for example, a country's government. A Candidate is an applicant for a position. In the E-Voting system, candidates are users elected/chosen by voters to win an election. Authority Center in the E-Voting system acts to authorize any legal voters, such as giving them a digital certificate to cast an E-Voting ballot. A voting system is a system that is used to run the election. It generates credentials for voters and even shares for candidates. VS should never leak any intention of the voter. Meanwhile, the Bulletin Board is used to publish information about the voting process.

VS's technical aspect is the most crucial factor in developing a secured E-Voting system from all essential elements involved in the E-Voting system. Thus, most researchers focus on developing security mechanisms for this VS aspect. The design goal of a good E-Voting system should follow these requirements:

i. Coercion resistance: no voter can prove to others which candidate they choose.
ii. The integrity of ballots: the voters' votes must be counted validly.
iii. Privacy of ballots: no one can leak voting information recorded by the system.
iv. Multiple-voting avoidance: the system can only allow a legal voter to cast a ballot once.
v. Fairness: no candidate can gather information about their ballot in advance.

Technically speaking, many approaches have been established to secure the E-Voting system. In this research, we design a security workflow of the E-Voting system that ensures voters' vote privacy data. Although our proposed technical approach can be used in any E-Voting system, we focus on our e-voting system for the election mechanism adopted in Indonesia. We do this because the security policy of an E-Voting system depends on the social administration election process of a country, as also stated by [34]. According to the analysis of [35, 36], it is indicated that Indonesia is theoretically ready for an E-Voting system. Thus, as we propose in this paper, developing a security mechanism for voters' vote privacy data brings a promising benefit for Indonesian society.

Although Indonesia is theoretically ready for the E-Voting system, [37] argues that the implementation of the E-Voting system has one main drawback from its underlying technology, which is the internet. So, designing an E-Voting system should be conducted carefully. According to [38], there are many holes in the system that allow attackers to make the E-Voting system becomes highly vulnerable. As argued by [39], research on E-Voting, especially in Indonesia, should be observed from a development research perspective.

The E-Voting system has a different philosophy from e-commerce, e-banking, or any other recent e-procurement system. The E-Voting system applies different sets of rules. As stated by [38], E-voting is categorized as a Safety-Critical System. Thus, designing a secure E-Voting system is a complex task. Many social and technical aspects are involved in providing a secure and convenient E-Voting system in Indonesia. When publishing a research article, most researchers on the E-Voting system focus their discussion on some narrow but deep specific aspects. In this paper, we will also follow that approach.

This article focuses our discussion on the voters' vote data privacy aspect of the E-Voting system. We develop an algorithm to secure the confidentiality of votes data. In our system, no one, including the E-Voting administrator, can analyze the ballot content of any particular voter. It means that no one can know which candidate is chosen by any specific voter. Our proposed algorithm works as an optimization algorithm, just like the optimization algorithm provided by [40-41]. We try to improve current E-Voting data security, especially on data privacy. We analyze that this aspect is very critical for the E-Voting system. Thus, we enhance the state-of-the-art E-Voting system by developing our algorithm, especially for the Indonesia E-Voting system.

III. Proposed Method

The design of our E-Voting hash algorithm consists of several components, including voter basic information, tokens, validator, cross-hashing (CH), and cross-validation (CV).

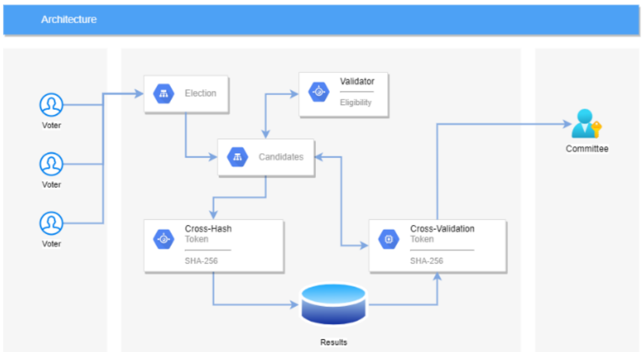


Fig. 1 E-Voting Architecture

As an initial stage in Figure 1, the system requires basic voter information as a foundation to form a combination of hashing algorithms. As in the general election system, the system will ensure that the user has access or voting rights as the voter.

The second component is a token, which is a unique character set from the server where the system is running. This unique character is taken from the build version of the operating system and the server hardware serial number which is then hashed.

The validator is an additional component to support E-Voting security from the user's side, including Two Factor Authentication (TFA) methods [42]. TFA helps voters to improve access security from their e-voting accounts. TFA is optional and users can activate or deactivate the TFA feature right inside the system.

The online election process is very sensitive thus making user validation become the most important aspect. When a user account is hacked, its credentials like username and password will be exposed, so then the system difficult to validate these users. One additional option to assist the system in ensuring that the user who is authenticating is the valid user is to use an additional code that is sent to the user via the mobile device.

The core components in this architecture are CH and CV. CH is used to hash the election results data (voters choose candidates) combined with voter data and tokens generated by the server, where next this hash data will be stored in the database.

CV has an improved way of working from CH. CV performs hashing of the combination of voter data with a combination of each existing candidate. Furthermore, CV validates each of the results of the combination into the election results database. Each matched result will count as the gain of the respective candidate.

From the data flow aspect, in Figure 2 the e-voting design has several groups, namely voters, elections, candidates, and results. In the results section, the basic data of voters used as a combination to perform hashing are ID, username, and password. The ID and username in the e-voting design are static and do not change. Unlike the password that can be changed, the password cannot be used as a combination for hashing.

The second group is in terms of election data, where the basic voter data will then be compared with an election which will produce a conclusion whether voters have access to vote or not.

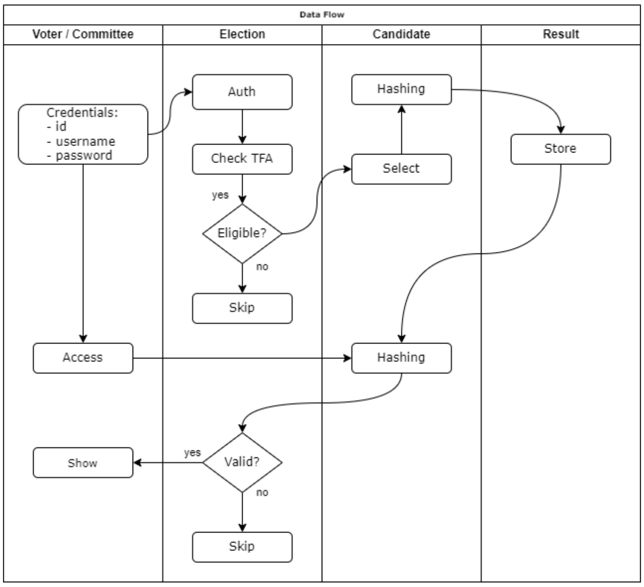


Fig. 2 Data Flow

In the design of the e-voting system, this system can accommodate many elections at once. Academics can register to be users in the e-voting system, but users can only vote when the user is entered into an active election.

The election group has an additional data flow, namely checking the status of TFA whether it is active or not. If the voter activates TFA, the system will perform a series of validations to check the validity of voter access via a token sent via a mobile device as described previously.

The third group is from the candidate side. Candidate data will always be used as a hashing combination to form the result data. The combination formed is that only voters and candidates are selected. As previously explained, to make the combination unique, the combination is added with a token that comes from the server. The token is used to ensure the integrity of the data source. So if there is an attempt to move data in the hope of being opened, the system can protect the data using the token.

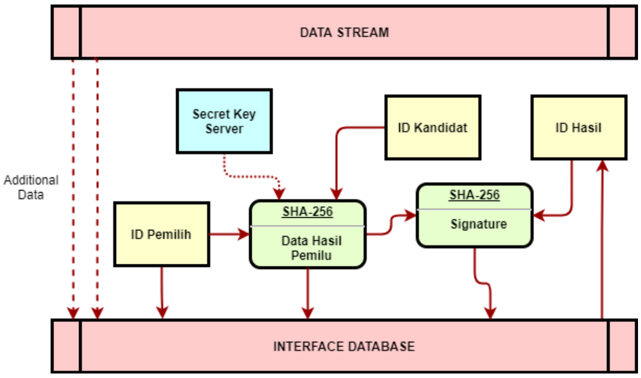


Fig. 3 Data Entry

Figure 3 describes the flow of the data entry process and its parts. The data entry process starts from the data stream that comes from the application and also from data entry in the specified system to the final storage place of the hashed data into the database.

Hashing is done using the SHA-256 algorithm with 256 bits of length. More about the SHA-256 algorithm is not explained in this study. An ID field of the voter, a secret key from the server, an ID of the candidate are stored into an array and then hashed with a specified hashing algorithm.

The voter' ID and the hash result will be directly inserted into the database. Each hashed data will generate a separate ID. To increase the security of the data contained on the server, in the e-voting design, an additional entry is added which is called a signature.

The signature ensures the integrity of each entry into the hash combination. In principle, each hash result will be re-validated based on the resulting signature compared to the signature entries that have been stored in the database from the previous process.

In the e-voting design, the signature is formed using a combination of the hashed result and the hashed ID in the database. The process of forming a signature is also done by hashing using the SHA-256 algorithm too.

In the end, the final data that will be stored in the database is the voter ID, the hash of the chosen candidates, and the hash signature. In addition to the three data combinations, there are also some supporting data required by the system. In this condition, it is sufficient for the architecture to secure data from illegal access. Illegal access either by the system administrator, or illegal access from other applications if in certain scenarios a data leak occurs. In this condition, the architecture can guarantee an important aspect of the e-voting itself, namely that the chosen candidate's data cannot be accessed or read by anyone.

From Figure 3 we can explain that the data stored in the database is quite safe, both from reading manually and by the system. When the data security system has been designed properly then the challenge is how to read it. In the e-voting design to read CH, the CV scenario is used. CV uses a similar path to CH with some additional functionality for validation. Figure 4 describes the flow of the data validation process of the e-voting system.

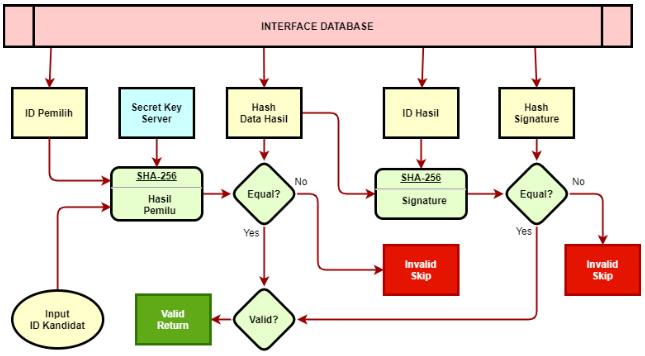


Fig. 4 Data Validation

In the recapitulation scenario of election results, each candidate must count the votes obtained. In the e-voting design, the election result data stored in the database is in the form of hashed results. Technically, hashing is a form of data security where data that has been hashed cannot be returned to its original form. The only way to make sure these results are valid is to create a new hash and then compare the new hash with the hash already stored in the database.

In the e-voting design, to get the votes from candidate A, the system must generate a hashed version of candidate A for the voter ID that is in each row of the data in the results table. If the result of the new hash matches the hash value in the same result column, it can be temporarily flagged that the data row is the result for candidate A.

The same process is done for other candidates. Furthermore, to ensure the integrity of the data row, the signature column in each data row is compared with the new hash result obtained from the result row ID with the value in the hash column.

If it turns out that the new hash results obtained are different from the hash values in the signature column, it can be ascertained that the values in the hash column have been illegally altered. For hashes that are not the same when validated, they can be skipped and not included as a result of the vote recapitulation for all candidates, and the data is excluded from the final total of the vote results.

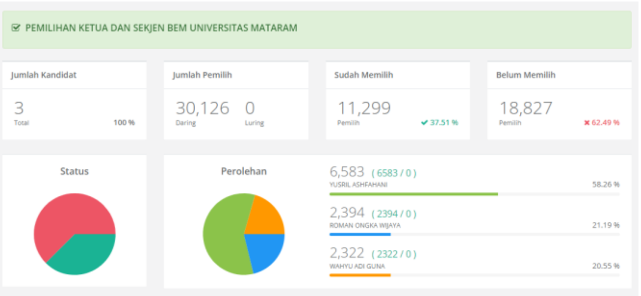
IV. Experiment Result and Analysis

To test the validity and performance of this e-voting system design, e-vote is used in the election opportunity at Mataram University. Tests were carried out for several types of voter levels, ranging from students, staff, to lecturers. The voters were also made from several different scopes, ranging from the scope of universities, faculties, departments, to the level of student associations.

TABLE I
Successful Election Held

Year	Name	Type	Voter(s)
2020	Election of Chairman and Secretary	Student Executive Board (BEM)	30,126
2020	Election of Chairman and Secretary	Student Representative Council (DPM)	29,212
2021	Election of Members from Engineering Faculty	Senate	133
2022	Election of Rector	Rector	60

The election with the most participants was made during the election of the Student Executive Board (as known as BEM) of Mataram University in 2020. The number of voters from the student level reached 30,126 people.



☑ PEMILIHAN KETUA DAN SEKJEN BEM UNIVERSITAS MATARAM

Jumlah Kandidat
3
Total 100 %

Jumlah Pemilih
30,126 0
Daring Luring

Sudah Memilih
11,299
Pemilih ✓ 37.51 %

Belum Memilih
18,827
Pemilih ✗ 62.49 %

Status

Perolehan

6,583 (6583 / 0)
YUSRIL ASHFAHANI 58.26 %

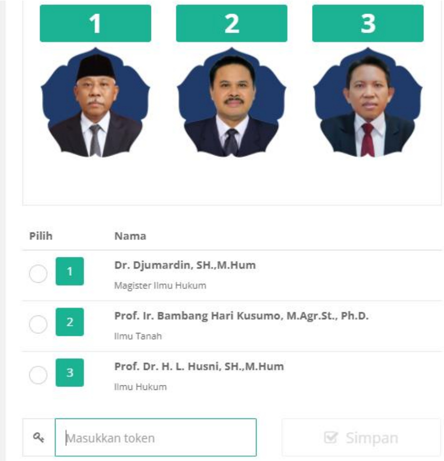
2,394 (2394 / 0)
ROMAN ONGKA WIJAYA 21.19 %

2,322 (2322 / 0)
WAHYU ADI GUNA 20.55 %

Fig. 5 BEM Election in 2020

Figure 5 shows the total gains of each candidate. The system can validate the hash value of the total voters described previously.

In terms of volume, the highest participation was when the system was used during the election of the BEM at Mataram University. Furthermore, in terms of confidence (confidentiality), the e-voting system was used in the election of the chancellor and the election of the senate members of Mataram University.

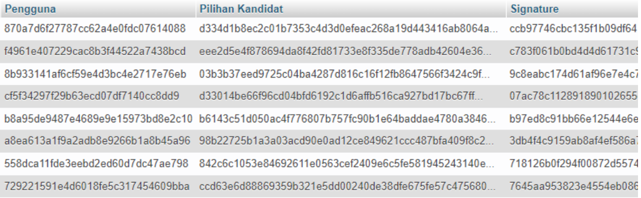


Pilih	Nama
○ 1	**Dr. Djumardin, SH.,M.Hum** Magister Ilmu Hukum
○ 2	**Prof. Ir. Bambang Hari Kusumo, M.Agr.St., Ph.D.** Ilmu Tanah
○ 3	**Prof. Dr. H. L. Husni, SH.,M.Hum** Ilmu Hukum

Masukkan token

Fig. 6 Rector Election 2022

Figure 6 shows the e-voting system used in the election of the rector of Mataram University. In the system architecture, the validator component also provides facilities for generating and distributing tokens to voters. Voting tokens are a further addition to the increased security in voting after TFA.



Pengguna	Pilihan Kandidat	Signature
870a7d6f27787cc62a4e0fdc07614088	d334d1b8ec2c01b7353c4d3d0efeac268a19d443416ab8064a...	ccb97746cbc135f1b09df64
f4961e407229cac8b3f44522a7438bcd	eee2d5e4f878694da8f42fd81733e8f335de778adb42604e36...	c783f061b0bd4d4d61731c
8b933141af6cf59e4d3bc4e2717e76eb	03b3b37eed9725c04ba4287d816c16f12fb8647566f3424c9f...	9c8eabc174d61af96e7e4c
cf5f34297f29b63ecd07df7140cc8dd9	d33014be66f96cd04bfd6192c1d6affb516ca927bd17bc67ff...	07ac78c112891890102655
b8a95de9487e4689e9e15973bd8e2c10	b6143c51d050ac4f776807b757fc90b1e64baddae4780a3846...	b97ed8c91bb66e12544e6e
a8ea613a1f9a2adb8e9266b1a8b45a96	98b22725b1a3a03acd90e0ad12ce849621ccc487bfa409f8c2...	3db4f4c9159ab8af4ef586a
558dca11fde3eebd2ed60d7dc47ae798	842c6c1053e84692611e0563cef2409e6c5fe581945243140e...	718126b0f294f00872d5574
729221591e4d6018fe5c317454609bba	ccd63e6d88869359b321e5dd00240de38dfe675fe57c475680...	7645aa953823e4554eb08

Fig. 7 Hashed data in Database

Figure 7 shows the form of the data when it is stored in the database. The core data is stored in hash form and some other data is stored in plain text to help the system and is not related to the election result data. In a data format, as shown in Figure 7, it is difficult to read data directly into the database.

Conclusion

This study shows that the implementation of the hashing algorithm is able to block direct access to the chosen candidate data in the database. The value of the result in each row of data is unique, it cannot be classified easily. On the other hand, the implementation of this algorithm does not interfere with the final recapitulation results.

References

[1] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[2] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, "Privacy preserving E-voting cloud system based on ID based encryption," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2399–2409, 2021.

[3] V. S. Anjima and N. N. Hari, "Secure cloud e-voting system using fully homomorphic elliptical curve cryptography," in *Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, pp. 858–864, Secunderabad, India, June 2019.

[4] N. Kshetri and J. Voas, "Blockchain-Enabled E-voting," *IEEE Software*, vol. 35, no. 4, pp. 95–99, 2018.

[5] S. Panja and B. Roy, "A secure end-to-end verifiable e-voting system using blockchain and cloud server," *Journal of Information Security and Applications*, vol. 59, Article ID 102815, 2021.

[6] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: blockchainenabled large-scale e-voting system with robustness and universal verifiability," *International Journal of Information Security*, vol. 19, no. 3, pp. 323–341, 2020.

[7] C. A. Neff, "A verifiable secret shuffle and its application to E-voting," in *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pp. 116–125, Association for Computing Machinery, Philadelphia, PA, USA, November 2001.

[8] X. Boyen, T. Haines, and J. M¨uller, "A verifiable and practical lattice-based decryption mix net with external auditing," in *Computer Security – ESORICS 2020*, L. Chen, N. Li, K. Liang, 10 Security and Communication Networks and S. Schneider, Eds., Springer International Publishing, New York, NY, USA, pp. 336–356, 2020.

[9] N. Islam, K. M. R. Alam, S. Tamura, and Y. Morimoto, "A new e-voting scheme based on revised simplified verifiable reencryption mixnet," in *Proceedings of the 2017 International Conference on Networking, Systems and Security (NSysS)*, pp. 12–20, Dhaka, Bangladesh, December 2017.

[10] C. Culnane, A. Essex, S. J. Lewis, O. Pereira, and V. Teague, "Knights and knaves run elections: internet voting and undetectable electoral fraud," *IEEE Security & Privacy*, vol. 17, no. 4, pp. 62–70, 2019.

[11] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds., pp. 199–203, Springer, Boston, MA, USA, 1983.

[12] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," in *Advances in Cryptology — AUSCRYPT '92*, J. Seberry and Y. Zheng, Eds., Springer Berlin Heidelberg, Berlin, Germany, pp. 244–251, 1993.

[13] X. Chen, Q. Wu, F. Zhang et al., "New receipt-free voting scheme using double-trapdoor commitment," *Information Sciences*, vol. 181, no. 8, pp. 1493–1502, 2011.

[14] M. Kumar, S. Chand, and C. P. Katti, "A secure end-to-end verifiable internet-voting system using identity-based blind signature," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2032–2041, 2020.

[15] M. Kumar, C. P. Katti, and P. C. Saxena, "A secure anonymous E-voting system using identity-based blind signature scheme," in *Information Systems Security*, R. K. Shyamasundar, V. Singh, and J. Vaidya, Eds., Springer International Publishing, New York, NY, USA, pp. 29–49, 2017.

[16] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for IIoT devices," *IEEE Transactions on Industrial Informatics*, vol. 14, p. 1, 2021.

[17] W. Wang, H. Huang, L. Zhang, Z. Han, C. Qiu, and C. Su, "BlockSLAP: blockchain-based secure and lightweight Authentication protocol for smart grid," in *Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and

Communications (TrustCom), pp. 1332–1338, Guangzhou, China, December 2021.

[18] R. L. Rivest, L. M. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found.* Secure Compuation.vol. 4, pp. 169–180, 1978.

[19] K. Peng, R. Aditya, C. Boyd, E. Dawson, and B. Lee, "Multiplicative homomorphic E-voting," in *Progress in Cryptology - INDOCRYPT 2004*, A. Canteaut and K. Viswanathan, Eds., pp. 61–72, Springer Berlin Heidelberg, Berlin, Germany, 2005.

[20] J. Dossogne and F. Lafitte, "Blinded additively homomorphic encryption schemes for self-tallying voting," *Journal of Information Security and Applications*, vol. 22, pp. 40–53, 2015.

[21] S. M. Toapanta Toapanta, L. J. Chavez Chal' en, J. G. Ortiz' Rojas, and L. E. Mafla Gallegos, "A homomorphic encryption approach in a voting system in a distributed architecture," in *Proceedings of the 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, pp. 206–210, Shenyang, China, July 2020.

[22] X. Fan, T. Wu, Q. Zheng, Y. Chen, and X. Xiao, "DHS-voting: a distributed homomorphic signcryption E-voting," in *Dependability in Sensor, Cloud, and Big Data Systems and Applications*, G. Wang, M. Z. A. Bhuiyan, S. De Capitani di Vimercati, and Y. Ren, Eds., pp. 40–53, Springer Singapore, Singapore, Asia, 2019.

[23] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed., Springer Berlin Heidelberg, Berlin, Germany, pp. 148–164, 1999.

[24] L. Yuan, M. Li, C. Guo, W. Hu, and X. Tan, "A verifiable E-voting scheme with secret sharing," in *Proceedings of the 2015 IEEE 16th International Conference on Communication Technology (ICCT)*, pp. 304–308, Hangzhou, China, October 2015.

[25] R. Tso, Z.-Y. Liu, and J.-H. Hsiao, "Distributed E-voting and E-bidding systems based on smart contract," *Electronics*, vol. 8, no. 4, p. 422, 2019.

[26] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "A secure verifiable ranked choice online voting system based on homomorphic encryption," *IEEE Access*, vol. 6, pp. 20506–20519, 2018.

[27] X. Fan, T. Wu, Q. Zheng, Y. Chen, M. Alam, and X. Xiao, "HSE-Voting: a secure high-efficiency electronic voting scheme based on homomorphic signcryption," *Future Generation Computer Systems*, vol. 111, pp. 754–762, 2020.

[28] J. Li, X. Wang, Z. Huang, L. Wang, and Y. Xiang, "Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing," *Journal of Parallel and Distributed Computing*, vol. 130, pp. 91–97, 2019.

[29] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Towards Trustworthy Elections: New Directions in Electronic Voting*, D. Chaum, M. Jakobsson, R. L. Rivest et al., Eds., Springer Berlin Heidelberg, Berlin, Germany, 2010.

[30] O. Spycher, R. Koenig, R. Haenni, and M. Schl¨apfer, "A new approach towards coercion-resistant remote E-voting in linear time," in *Financial Cryptography and Data Security*, G. Danezis, Ed., pp. 182–189, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[31] P. Grontas, A. Pagourtzis, A. Zacharakis, and B. Zhang, "Towards everlasting privacy and efficient coercion resistance in remote electronic voting," in *Financial Cryptography and Data Security*, A. Zohar, I. Eyal, V. Teague et al., Eds., pp. 210–231, Springer Berlin Heidelberg, Berlin, Germany, 2019.

[32] P. Grontas, A. Pagourtzis, and A. Zacharakis, "Coercion resistance in a practical secret voting scheme for large scale elections," in *Proceedings of the 2017 14th International Symposium on Pervasive Systems, Algorithms and Networks & 2017 11th International Conference on Frontier of Computer Science and Technology & 2017 Third International Symposium of Creative Computing (ISPAN-FCST-ISCC)*, pp. 514– 519, Exeter, United Kingdom, June 2017.

[33] Yuanjing Hao, Zhixin Zeng, Liang Chang, "An Improved Coercion-Resistant E-Voting Scheme", *Security and Communication Networks*, vol. 2021, Article ID 5448370, 11 pages, 2021.

[34] R. Suganya, Rajendran Anandha Jothi, Vellaiyan Palanisamy, "A survey on security methodologies in E-voting system", *International Journal of Pure and Applied Mathematics*, vol. 118, no. 8, pp. 511-514. 2018.

[35] M. Hapsara, "Imposing Transparency in Indonesia's E-Voting System through Security by Design," in *E-Indonesia Initiative*, Bandung, Indonesia, 2011.

[36] M. Hapsara, "E-Voting Indonesia: A safety-critical-systems model towards standard and framework for Indonesia's presidential election," in *International Conference on Information Technology*, Bali, Indonesia, 2013, pp. 81-86.

[37] R. Mercuri, "A better ballot box?," in *IEEE Spectrum*, vol. 39, no. 10, pp. 46-50, Oct. 2002.

[38] Margaret McGaley and J. Paul Gibson, "Electronic Voting: A Safety Critical System," *Final Year Project – B.Sc. Computer Science and Software Engineering, National University of Ireland*. 2003.

[39] M. Hapsara, "E-voting Indonesia: Framing the research," *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1-6, 2014.

[40] A. Y. Husodo, G. Jati, A. Octavian and W. Jatmiko, "Enhanced Social Spider Optimization Algorithm for Increasing Performance of Multiple Pursuer Drones in Neutralizing Attacks From Multiple Evader Drones," in *IEEE Access*, vol. 8, pp. 22145-22161, 2020.

[41] A. Y. Husodo, G. Jati, A. Octavian and W. Jatmiko, "Switching target communication strategy for optimizing multiple pursuer drones performance in immobilizing Kamikaze multiple evader drones," in *ICT Express*, vol. 6, issue 2, pp. 76-82, 2020.

[42] Mardiansyah, A. Z., Ariyan Zubaidi, I Gde Putu Wirarama Wedaswhara W, & Andy Hidayat Jatmika. (2021). “Two Factor Authentication Berbasis SMS pada Layanan Single Sign-On Universitas Mataram”. *Journal of Computer Science and Informatics Engineering (J-Cosine)*, 5(2), 167–174. https://doi.org/10.29303/jcosine.v5i2.424