Journal of Systemics, Cybernetics and Informatics (2023) 21(2), 39-46
https://doi.org/10.54808/JSCI.21.02.39

Improving the Integrity of a Voting Process with Biometric Authentication and Data Encryption

Walter M. MOLINA
Faculty of Engineering, Universidad Peruana de Ciencias Aplicadas
Lima, Perú

Lino R. MAC KAY
Faculty of Engineering, Universidad Peruana de Ciencias Aplicadas
Lima, Perú

Daniel SUBAUSTE
Faculty of Engineering, Universidad Peruana de Ciencias Aplicadas[i]
Lima, Perú

ABSTRACT

Throughout the years, the voting process has under-gone a digital transformation, aiming to achieve greater control and optimize time while ensuring the integrity of each vote. While previous solutions have introduced changes in architecture and security processes, there hasn't been a defined secure model for voting. The applications developed in this study employed biometrics and a fingerprint reader for authentication security, along with cryptography algorithms to safeguard the flow of voting data. Experts and individuals involved in the Peruvian electoral process evaluated the web and mobile applications to determine their viability in a real-world context and their potential to enhance the electoral process in Peru. This evaluation was conducted through a case study involving 50 participants and satisfaction surveys, which qualitatively assessed the usability and effectiveness of the applications. The results indicated that the developed applications were well-received, perceived as intuitive, and provided an interactive experience.

Keywords: Mobile Application, Web Application, Voting Process, Data Encryption, Bio-metric Authentication

1. INTRODUCTION

In contemporary society, the act of voting holds significant importance as it represents the aspirations of individual citizens to seek improvement within their communities, primarily through the selection of their authorities [25]. However, during the recent electoral process in Peru, concerns regarding the integrity of the process emerged among the citizens, evident from Datum's findings that less than 50% of Peruvian citizens perceive the authorities responsible for the electoral process as impartial [24].

Despite efforts to address these issues through the implementation of an electronic voting system, challenges pertaining to vote veracity continue to persist, including instances of identity theft and vote duplication [13]. In response, various methods have been employed to ensure data integrity, including the utilization of encryption algorithms and blockchain technology.

Based on our research, we have determined that the implementation of AES and RSA algorithms represents the most effective approaches for addressing these challenges [3], [27], [28], [29]. The proposed solution in this study tackles a significant portion of the aforementioned issues by employing not only the RSA algorithm to ensure data integrity but also by incorporating biometric authentication to prevent user impersonation. Furthermore, efficient resource management is achieved by avoiding the use of blockchain as a method and implementing backup instances to mitigate potential cloud service interruptions.

This document is structured as follows: In Section 2, we will delve into related work and previous studies in the field. Section 3 will introduce the pertinent concepts and outline the defined problem statement. Subsequently, in Section 4, we will present our proposed solution. Finally, Section 5 will provide an analysis of the results obtained and present the concluding remarks.

[i] I'm deeply grateful to Professor Alfredo Barrientos for his meticulous document editing and invaluable guidance during our research process.

2. BACKGROUND AND METHODOLOGY

Rivest–Shamir–Adleman algorithm

"According to Quisquater and Couvreur, RSA (Rivest, Shamir, and Adleman) is a cryptosystem that utilizes both public and private keys for encryption and decryption purposes" [32]. The RSA encryption method will be implemented in our system as it addresses security concerns related to key configuration. The recommended key size is 2048 bits, which is considered a global standard. The process of encryption can be defined as follows [27].

To generate the keys, we need to calculate two prime numbers, which are chosen using a primality test.

$$n = p \times q \quad (1)$$

After calculating n, we use Carmichael's totient function to find the least common multiple.

$$\lambda(n) = \text{lcm}\,(p - 1, q - 1) \quad (2)$$

To encrypt the data, we will use the public key.

$$c = m^e \pmod n$$

where:
m = sensible data
n = value obtained from the result of the equation. Eq. (2)
e = public key (3)

To decrypt the data, we will use the private key.

$$m = c^d \pmod n$$

where:
c = data encrypted from the result of the equation. Eq. (3)
n = value obtained from the result of the equation. Eq. (2)
d = private key (4)

Biometric authentication

There are two types of biometrics: physical biometrics, which is based on biological traits and behavioral biometrics, which analyzes user actions [33]. In our implementation, we focused on the physical biometrics and specifically processed and verified the authenticity of each user's fingerprint information.

For fingerprints capture, we utilized the Zkteco SLK20R model. This device is certified by the FBI with PIV Single Finger Capture Device and PIV Mobile ID FAP20 certifications, which validate its capability to detect fake fingerprints [31]. Figure 1 depicts the captured image.

Figure 1: The image captured by the Zkteco sensor

Algorithm for fingerprint comparison

We will employ the Source Afis algorithm for fingerprint comparison. This algorithm is composed of three key steps. Firstly, it extracts termination points at the bifurcations of the fingerprint. Secondly, it abstracts the lines connecting these points along with their respective angles, as shown in Figure 2. Lastly, it searches for similarities between the edges and points of the fingerprints using the nearest neighbor algorithm, and based on this analysis, it determines whether a match is coincidental or not [30]. This process is demonstrated in Figure 3.

Figure 2: Reference image of Source AFIS algorithm

Figure 3: Reference image of Source AFIS algorithm

3. CONTRIBUTION

Architecture design

The designed architecture was based on the utilization of microservices due to their ability to provide high availability and fault tolerance [40]. This architecture enabled us to divide the business model into three separate scenarios to distribute the data load. These microservices are built on Java Spring Boot, utilizing RESTful services.

Additionally, for the database, MongoDB was employed as it offers a reactive driver for asynchronous stream processing, which helps prevent request blocking [34]. Lastly, through the developed interfaces, requests are made by sending and receiving messages in JSON (JavaScript Object Notation) format. All of these aspects are depicted in Figure 4.

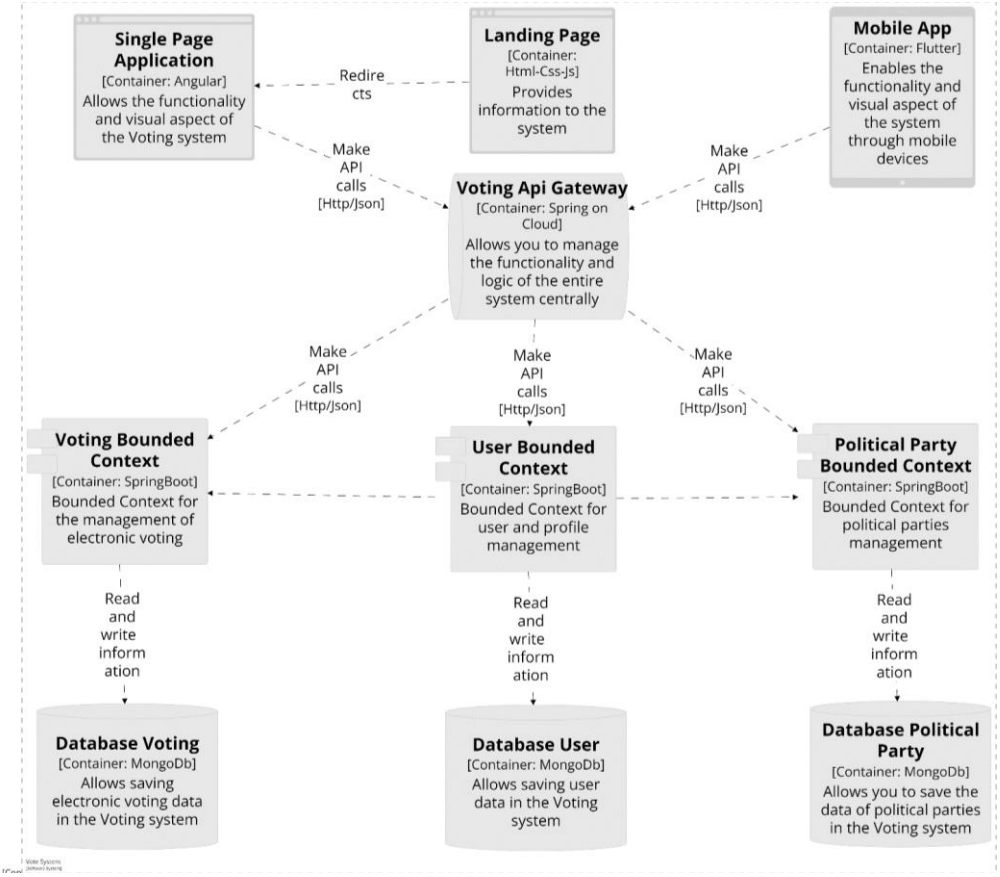


Figure 4: Container

Development

For the backend development of the application, the Spring Boot framework was chosen due to its open-source nature, which provides access to pre-developed libraries. Maven was used for dependency management, Spring Data Mongo Reactive for data access, Spring Webflux for creating reactive applications, Spring Security for request authorization and security management, and Source Afis algorithm for fingerprint comparison. Additionally, two Single Page Applications (SPAs) were developed using the Angular framework, along with a hybrid mobile application built with Flutter.

These applications facilitated interaction from various users on different devices, including web and mobile, over the internet. One of the Single-Page Application (SPA) served as a dashboard focused primarily on system management and the voting flow, while the other SPA and mobile application provided users with the voting process flow.

Deployment

For the application deployment, a cloud infrastructure on Amazon Web Services (AWS) was adopted. A virtual computing environment, known as an instance, was utilized on Amazon EC2 (Amazon Elastic Compute Cloud) to deploy the backend services of the application [37]. Additionally, ports 80 and 443 were configured to allow the server to handle incoming requests. Moreover, the HTTPS protocol was enabled using Amazon Route 53, where domain registration and configuration were managed, and a connection to an application load balancer was established. The load balancer contacts the necessary instances to distribute traffic and also enables the HTTPS protocol through SSL certificates [35].

Furthermore, Amazon S3 (Amazon Simple Storage Service) was employed for image management, providing a scalable and secure object storage solution with audit policies and security measures in place [36].

Finally, the web application was deployed, making it accessible from any device, as both a web interface and a mobile interface were developed. The entire Cloud architecture can be observed in Figure 5.

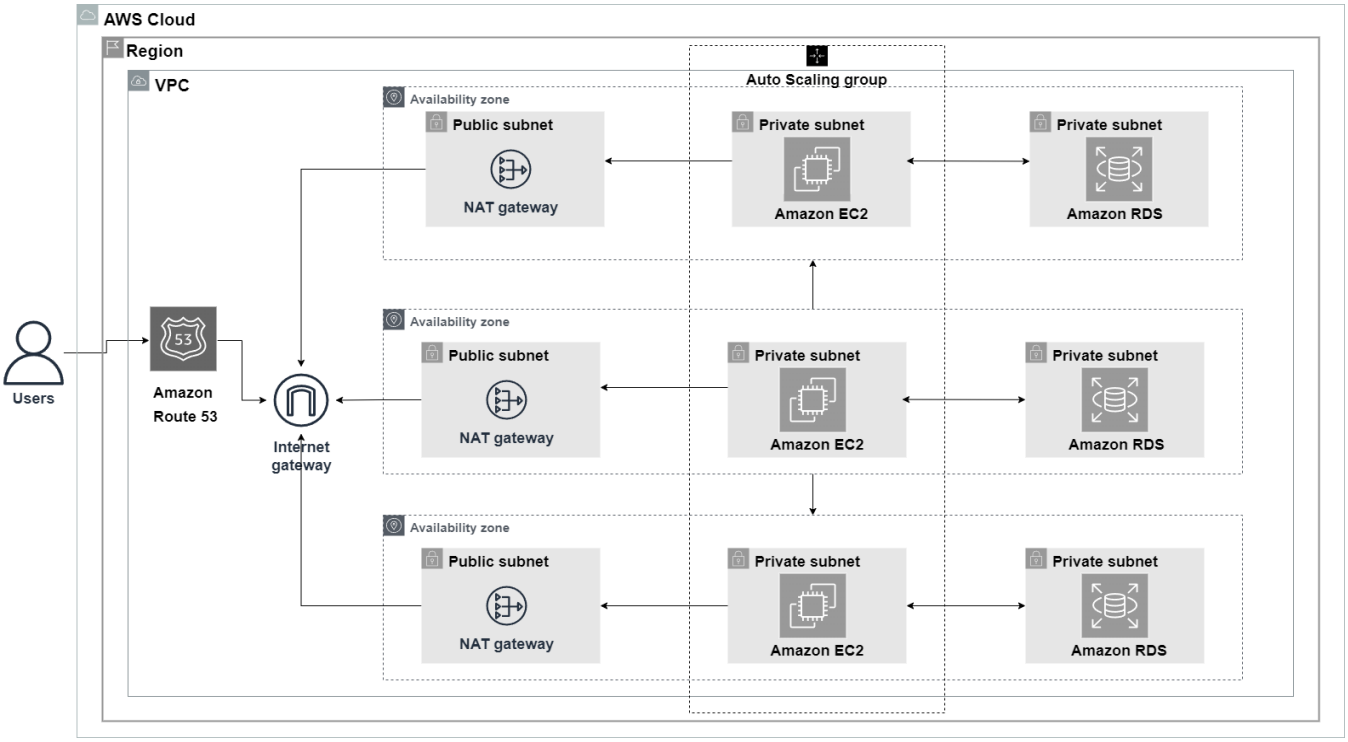


Figure 5: Deployment

4. PREVIOUS WORK

Problem

"According to C.H. Roh and I. Y. Lee, the problem they aim to solve is the interdependence of administrators in such systems" [11]. "On the other hand, A.M. Larriba, J.M. Sempere et al. focus on improving the efficiency of existing electronic voting systems through their research" [8]. "Additionally, the investigation conducted by F.D. Giraldo, B. Milton et al. takes a more generic

approach by aiming to enhance the security of voting systems in general and increase the trust and reliability placed in these systems" [6].

The latter approach is primarily adopted due to the previous dismissal of solutions involving complex architectures that would incur high costs and be less feasible to develop on a large scale in the Peruvian context. When referring to solutions with complex architectures, we primarily refer to the different proposed systems that utilize blockchain networks as their main architectural method [06], [11], [13], [15], [16], [22].

Biometric authentication

A decision was made to adopt a less complex architecture, such as blockchain, and instead utilize multiple security methods that ensure complete transparency and security of the developed system.

Therefore, we opted for the method of biometric authentication, specifically focusing solely on fingerprint recognition. This choice is supported by the consistent use of fingerprint recognition in various previously developed systems [1], [2], [3], [4], [20], [39].

The use of biometric authentication allows voters to be authenticated based on their physiological data, thereby mitigating potential cases of duplication and fraud and ensuring the integrity of the voter.

Encryption

Furthermore, we consider it necessary that information remains non-visible in its original form. That is why we decided to utilize the RSA encryption method.
The selection of this algorithm was based on various comparisons that involved different encryption methods [5], [7], [18], [38]. Through our analysis, we concluded that this algorithm is the optimal choice for achieving the objectives of the project.

5. RESULTS

For the experimentation, four Amazon EC2 instances (Amazon Elastic Compute Cloud) were configured, which hosted various backup services to implement the microservices pattern and ensure fault tolerance. Amplify was also utilized to visualize the web application, and a mobile version in APK format was developed.

The source code for all the mentioned services can be found at the following URLs: https://github.com/Voting-System-App and https://github.com/VotingSystemThesis.

Lastly, performance tests were conducted on the deployed backend using the load testing tool called JMeter. The results of these tests can be observed in Figure 6.

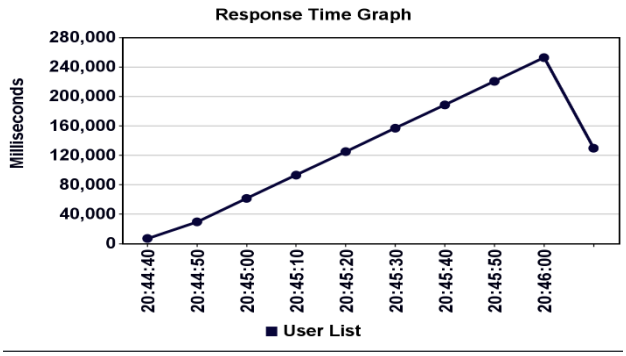


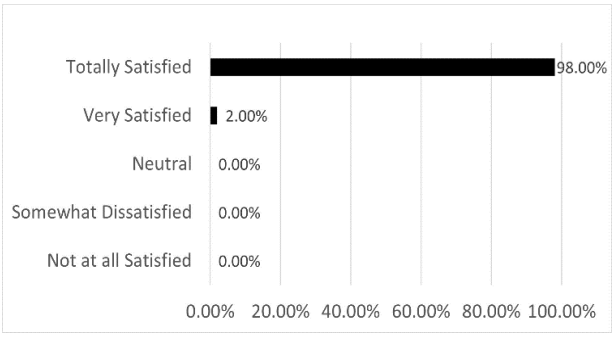
Figure 6: Performance diagram in milliseconds (10,000 requests per second)

The Likert scale questions administered to 50 individuals yielded the following results: Firstly, 98% of the respondents were completely satisfied with the speed of the voting process, while 2% were very satisfied. Secondly, 88% of the respondents were completely satisfied with the ease of the voting process, while 10% where very satisfied and 2% expressed a neutral opinion.

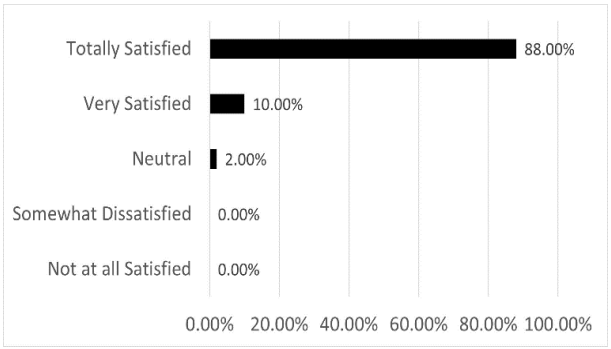
Furthermore, 84% of the respondents were completely satisfied with the ease of the authentication process, while 12% were very satisfied, and 4% had a neutral opinion.

Lastly, 80% of the respondents were completely satisfied with the speed of the authentication process, while 12% were very satisfied, 6% had a neutral opinion, and 2% were slightly dissatisfied.

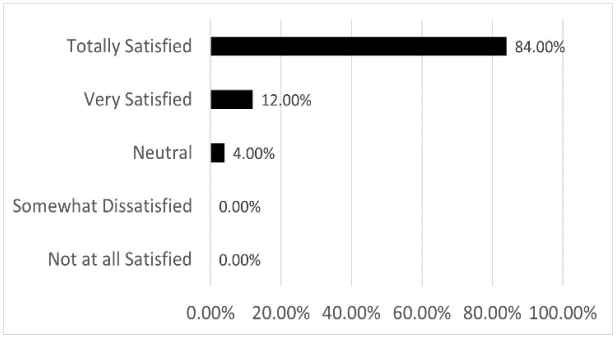
The agree/disagree questions yielded the following results: Firstly, 96% of the respondents considered the proposed virtual voting to be viable, while 4% disagreed. Secondly, 96% of the respondents would recommend the use of the proposed voting system, while 4% would not. Finally, 92% of the respondents believed that the application did not require any changes, while 8% provided suggestions for improvement. All the survey results can be seen in Figure 7.



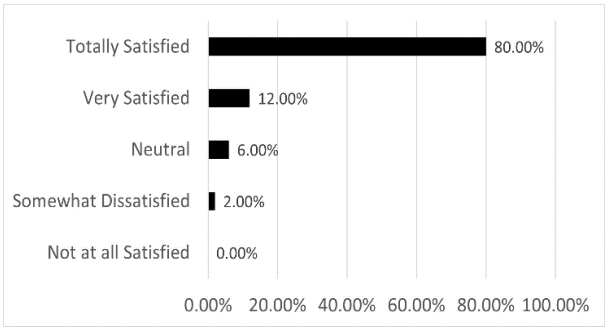
(a) Survey on the speed of the voting flow



(b) Survey on the usability of voting



(c) Survey on the usability of authentication



(d) Survey on the speed of authentication

Figure 7: App surveys

6. CONCLUSIONS

As part of the conclusions, we were able to validate that the proposed authentication method provides high precision in mitigating possible fraud cases. By using a physiological attribute of users, duplications are not possible, ensuring the integrity of the authentication process and preventing fraud cases.

Furthermore, the implemented auditing service allowed for persistent information about system activities. This enabled an auditable security flow in case of error reports and facilitated the validation of the existence and correct creation of cast votes.

Moreover, we concluded that the RSA encryption algorithm ensured end-to-end security of shared data, preventing interception in its original state. The implementation of this algorithm also ensured complete anonymity in the voting process, as even we were unable to view the vote information. Finally, based on the different results, we can conclude that the proposed solution has high feasibility for implementation in a real-world context. Although many users expressed their willingness to use a product like ours in the near future, we need a bigger amount of people to truly validate If the app will affect on a big scale.

Users also reported that the flow was simple and fast, indicating a good user experience and reduced completion times for the entire voting and authentication process. Additionally, we confirmed that using a microservices architecture allows the system to exhibit high resilience and fault tolerance, ensuring high availability and optimal server response times.

7. ACKNOWLEDGMENT

We express our gratitude to Daniel Subauste and Alfredo Barrientos for their valuable review and corrections, as well as to our collaborators and funding sources for their support in completing this document. Their contributions were instrumental in the success of this work. Furthermore, we would like to thank Professor Jorge Delgado Vite for his support in the research development; he provided us with the knowledge and guidance necessary to achieve the product discussed in this document.

8. REFERENCES

[1] J. Zhao Et Al., “A Secure Biometrics and Pufs-Based Authentication Scheme with Key Agreement for Multi-Server Environments,” Ieee Access, Vol. 8, Pp. 45292–45303, 2020, Doi: 10.1109/Access.2020.2975615.

[2] M. Ahmad Et Al., “Security, Usability, and Biometric Authentication Scheme for Electronic Voting Using Multiple Keys,” Int J Distrib Sens Netw, Vol. 16, No. 7, P. 155014772094402, Jul. 2020, Doi: 10.1177/1550147720944025.

[3] S. Ajish and K. S. Anilkumar, “Secure Mobile Internet Voting System Using Biometric Authentication and Wavelet Based Aes,” Journal of Information Security and Applications, Vol. 61, P. 102908, Sep. 2021, Doi: 10.1016/J.Jisa.2021.102908.

[4] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, “Edge-Centric Multimodal Authentication System Using Encrypted Biometric Templates,” Future Generation Computer Systems, Vol. 85, Pp. 76–87, Aug. 2018, Doi: 10.1016/J.Future.2018.02.040.

[5] W. Gao and L. Yang, “Quantum Election Protocol Based on Quantum Public Key Cryptosystem,” Security and Communication Networks, Vol. 2021, 2021, Doi: 10.1155/2021/5551249.

[6] F. D. Giraldo, B. Milton C., and C. E. Gamboa, “Electronic Voting Using Blockchain and Smart Contracts: Proof of Concept,” Ieee Latin America Transactions, Vol. 18, No. 10, Pp. 1743–1751, Oct. 2020, Doi: 10.1109/Tla.2020.9387645.

[7] M. U. Hassan, M. H. Rehmani, and J. Chen, “Privacy Preservation in Blockchain Based Iot Systems: Integration Issues, Prospects, Challenges, and Future Research Directions,” Future Generation Computer Systems, Vol. 97, Pp. 512–529, Aug. 2019, Doi: 10.1016/J.Future.2019.02.060.

[8] A. M. Larriba, J. M. Sempere, and D. López, “A Two Authorities Electronic Vote Scheme,” Computers & Security, Vol. 97, P. 101940, Oct. 2020, Doi: 10.1016/J.Cose.2020.101940.

[9] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure Attribute-Based Data Sharing for Resource-Limited Users in Cloud Computing," Computers & Security, Vol. 72, Pp. 1–12, Jan. 2018, Doi: 10.1016/J.Cose.2017.08.007.

[10] W. Qu, L. Wu, W. Wang, Z. Liu, and H. Wang, "A Electronic Voting Protocol Based On Blockchain and Homomorphic Signcryption," Concurrency and Computation, P. E5817, 2020, Doi: 10.1002/Cpe.5817.

[11] C. H. Roh and I. Y. Lee, "A Study on Electronic Voting System Using Private Blockchain," Journal of Information Processing Systems, Vol. 16, No. 2, Pp. 421–434, Apr. 2020, Doi: 10.3745/Jips.03.0135.

[12] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Continuous User Authentication Using Multi-Modal Biometrics," Computers & Security, Vol. 53, Pp. 234–246, Sep. 2015, Doi: 10.1016/J.Cose.2015.06.001.

[13] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," Ieee Access, Vol. 7, Pp. 24477–24488, 2019, Doi: 10.1109/Access.2019.2895670.

[14] N. M. Shakiba, M. A. Doostari, and M. Mohammadpourfard, "Esiv: An End-To-End Secure Internet Voting System," Electronic Commerce Research, Vol. 17, No. 3, Pp. 463–494, Sep. 2017, Doi: 10.1007/S10660-016-9230-Y.

[15] 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 2020 14:4, Vol. 14, No. 4, Pp. 2399–2409, Aug. 2020, Doi: 10.1007/S12083-020-00977-4.

[16] J. G. Song, S. J. Moon, and J. W. Jang, "A Scalable Implementation of Anonymous Voting Over Ethereum Blockchain," Sensors (Basel), Vol. 21, No. 12, Jun. 2021, Doi: 10.3390/S21123958.

[17] R. Tas¸ and O. O. Tanriover, ¨ "A Manipulation Prevention Model for Blockchain-Based E-Voting Systems," Security and Communication Networks, Vol. 2021, 2021, Doi: 10.1155/2021/6673691.

[18] M. Tejedor-Romero, D. Orden, I. Marsa-Maestre, J. Junquera-Sanchez, and J. M. Gimenez-Guzman, "Distributed Remote E-Voting System Based on Shamir's Secret Sharing Scheme," Electronics (Basel), Vol. 10, No. 24, P. 3075, Dec. 2021, Doi: 10.3390/Electronics10243075.

[19] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and Enhancements of Image Encryption Using Combination of the 1d Chaotic Map," Signal Processing, Vol. 144, Pp. 444–452, Mar. 2018, Doi: 10.1016/J.Sigpro.2017.11.005.

[20] M. Yaman, A. Subasi, and F. Rattay, "Comparison of Random Subspace and Voting Ensemble Machine Learning Methods for Face Recognition," Symmetry (Basel), Vol. 10, No. 11, P. 651, Nov. 2018, Doi: 10.3390/Sym10110651.

[21] X. Yang, X. Yi, A. Kelarev, F. Han, and J. Luo, "A Distributed Networked System for Secure Publicly Verifiable Self-Tallying Online Voting," Inf Sci (N Y), Vol. 543, Pp. 125–142, Jan. 2021, Doi: 10.1016/J.Ins.2020.07.023.

[22] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "Blockchain Voting: Publicly Verifiable Online Voting Protocol Without Trusted Tallying Authorities," Future Generation Computer Systems, Vol. 112, Pp. 859–874, Nov. 2020, Doi: 10.1016/J.Future.2020.06.051.

[23] M. Hammad, Y. Liu, and K. Wang, "Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of Ecg and Fingerprint," Ieee Access, Vol. 7, Pp. 26527–26542, 2019, Doi: 10.1109/Access.2018.2886573.

[24] "Estudio De Opinion Publica A Nivel Nacional" Accessed: Sep 12, 2022. [Online]. Available: Https://Www.Datum.Com.Pe/New_Web_Files/Files/Pdf/Jun%202021%20coyuntura_210621084954.Pdf

[25] "Defensoría Del Pueblo Peru" https://www.defensoria.gob.pe/el-voto-ciudadano-fortalece-la-democracia/ (Acessed Sep 27, 2022).

[26] B. Ahn, "Implementation and Early Adoption of An Ethereum-Based Electronic Voting System for The Prevention Of Fraudulent Voting," Sustainability, Vol. 14, No. 5, P. 2917, Mar. 2022, Doi: 10.3390/Su14052917.

[27] P. Pranav, S. Dutta, and S. Chakraborty, "Empirical and Statistical Comparison of Intermediate Steps of Aes-128 and Rsa in Terms of Time Consumption," Soft Computing, Vol. 25, No. 21, Pp. 13127–13145, Nov. 2021, Doi: 10.1007/S00500-021-06085-6.

[28] Y. A. Liu Et Al., "A Dynamic Aes Cryptosystem Based on Memristive Neural Network," Sci Rep, Vol. 12, No. 1, P. 12983, Dec. 2022, Doi: 10.1038/S41598-022-13286-Y.

[29] S. Mohammad Safi, A. Movaghar, and M. Ghorbani, "Privacy Protection Scheme for Mobile Social Network," Journal of King Saud University - Computer and Information Sciences, Vol. 34, No. 7, Pp. 4062–4074, Jul. 2022, Doi: 10.1016/J.Jksuci.2022.05.011.

[30] "How Sourceafis Algorithm Works - Sourceafis." https://sourceafis. machinezoo.com/algorithm (Accessed Sep. 29, 2022).

[31] " Slk20r." https://www.zkteco.com.pe/slk20r (Accessed Sep. 29, 2022).

[32] J. J. Quisquater and C. Couvreur, "Fast Decipherment Algorithm For Rsa Public-Key Cryptosystem," Electron Lett, Vol. 18, No. 21, 1982, Doi: 10.1049/El:19820617

[33] M. Al Rousan and B. Intrigila, "A Comparative Analysis of Biometrics Types: Literature Review," Journal Of Computer Science, Vol. 16, No. 12, Pp. 1778–1788, Dec. 2020, Doi: 10.3844/Jcssp.2020.1778.1788
[34] "Web On Reactive Stack." https://docs.spring.io/spring-framework/docs/current/reference/html/web-reactive.html (Accessed Oct. 27, 2022).
[35] "Servicio Web Dns En La Nube — Amazon Route53." https://aws. amazon.com/es/route53/ (Accessed Oct. 28, 2022).
[36] "Aws — Almacenamiento De Datos Seguro En La Nube (S3)." https: //aws.amazon.com/es/s3/ (Accessed Oct. 28, 2022).
[37] " Aws — Elastic Compute Cloud (Ec2) De Capacidad Modificable En La Nube." Https://Aws.Amazon.Com/Es/Ec2/ (Accessed Oct. 28, 2022).
[38] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy Preservation in Blockchain Based Iot Systems: Integration Issues, Prospects, Challenges, and Future Research Directions," Future Generation Computer Systems, Vol. 97, Pp. 512–529, Aug. 2019, Doi: 10.1016/J.Future.2019.02.060
[39] A. Bedari, S. Wang, and W. Yang, "A Secure Online Fingerprint Authentication System for Industrial Iot Devices Over 5g Networks," Sensors, Vol. 22, No. 19, P. 7609, Oct. 2022, Doi: 10.3390/S22197609
[40] "¿Que´ Son Y Para Qué Sirven Los Microservicios?" https://www.redhat.com/es/topics/microservices(Accessed Nov. 10, 2022).