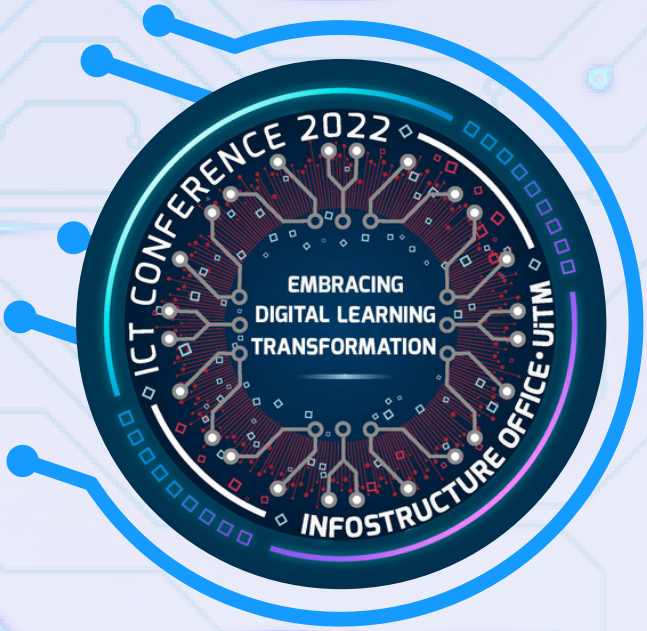
UNIVERSITI TEKNOLOGI MARA

E-Proceeding of the 1st ICT Conference 2022

ICT CONFERENCE 2022

"Embracing Digital Learning Transformation"

22 - 23 November 2022



JABATAN INFOSTRUKTUR
PEJABAT PEMBANGUNAN INFRASTRUKTUR & INFOSTRUKTUR UNIVERSITI TEKNOLOGI MARA, MALAYSIA

PRESERVING ANONYMITY IN E-VOTING USING AUTHENTICATION TECHNIQUES: A REVIEW

Nurain Nabilah Salehuddin[1], Siti Rahayu Abdul Aziz[2], Shahadan Saad[3]
[1,2,3]*Faculty of Computer and Mathematical Sciences,*
Universiti Teknologi MARA Cawangan Melaka Kampus Jasin,
Melaka, 77300, Malaysia.
2021102003@student.uitm.edu.my, rahayu748@uitm.edu.my,
shahadan@uitm.edu.my

ABSTRACT: The use of an electronic voting system allows voters to cast ballots over a computer network. As a result, voters will be able to participate in elections without having to travel to polling stations, which is more convenient and efficient. The confidentiality of voter information is one of the criteria that is considered essential and desirable. Electronic voting protocols must ensure voter anonymity as a fundamental requirement in order to provide adequate protection for voters' privacy. This ensures that a specific vote cannot be traced back to any voter. To put it another way, it is not possible to disclose or demonstrate a connection between voters and their votes. The requirement for voters' anonymity is what differentiates electronic voting from other types of electronic applications. It's possible that voters won't reveal their true preferences if their anonymity is threatened. As a result, the primary concentration of this article will be on the problem of maintaining voters' anonymity within electronic voting systems. A few concerns revolve around the design of the system, and two of those concerns are the voters' anonymity in the database records and the authenticity of the vote that is cast to the system. It is planned to implement a hashing algorithm on the data stored in the database to protect the anonymity of the voters. The method of authentication that will be used will be Multifactor Authentication (MFA), which will use user identification and a One-Time Password (OTP). It is anticipated that the project will contribute toward satisfying the demand for a secure and reliable electronic voting system.

Keywords**:** e-voting, one-time password (OTP), hashing algorithm, anonymity, 2FA authentication.

INTRODUCTION

Democracy is the healthiest and most participative form of government in the world. It encourages collaboration and coordination between public and private sectors, as well as citizens and the government. It allows residents to elect their representatives and participate in the workings of government, allowing them to exercise power and political influence through voting (Raut et al., 2021). In general, voting is a method used by a community of people to reach a collective decision or express an opinion. Not far behind, the concept of election is very tightly knitted with the concept of voting. Elections or voting is commonly used in many situations, whether it is in much higher stakes such as democracies to elect high-level officials or to even vote for something less of significance, such as the winner of Miss Universe.

As time goes by, the world becomes more advanced with the assistance of technology. Nowadays, the traditional paper-based elections are still valid and are quite frequently used. Alongside, there is also a local, electronic system for the voting process where they replaced the physical paper ballot system with a digital version of it using voting machines. Nevertheless, with the rapid growth of the internet and technologies in general, the existence of electronic facilities such as e-applications is inevitable. With that, the project is inspired by three main problem statements, which are: the inconvenience of the traditional voting process, the issue of the anonymity of the voters, and the need of an online e-voting system.

LITERATURE REVIEW

A. TRADITIONAL VOTING PROCESS

The traditional voting process or procedure refers to the standard way of voting. Most standard elections require physical participation from their voters. It is a requirement and is a part of the major procedure of the voting process itself. The voters will be set into a specific place, day, and time where they will need to attend the election and cast their vote. The most popular and well-known type of voting process would be the paper-based election or ballot vote. Like its name, the voters cast their votes through a paper ballot on the voting site they were co-opted with prior. In recent years, with the evolution of technology, there has been the existence of a local, electronic system as a substitute for the paper-based voting system (Djanali et al., 2018). However, as it is a local system and not an online system, the voters will still need to attend the designated place and time, much like the traditional paper-based election.

Therefore, naturally, whenever an election happens, whether it is with a higher purpose or lesser, a voter will need to attend the election site on a specific date. The voters will go through much stricter rules and steps during the voting process based on the type of election itself. The more significant the election is, the stricter the rules revolve around it. Although physical participation in a voting process is crucial and beneficial to the authenticity of the voting ballot, it might also pose a problem. With the troubles of the COVID-19 pandemic striking the world without warning and the social distancing protocols implemented in our daily lives, it is the lack of an online or remote voting system that has become a problem as it increases the difficulty in the traditional voting procedure (Fernandez-Navia et al., 2021).

B. ISSUE OF THE ANONYMITY OF THE VOTERS

When it comes to voting, and depending on the election's priority or policy, the anonymity of the voting or ballot is critical. Indeed, whether using a traditional paper-based system or an online voting system, voter anonymity is a must, particularly for high-level elections. It is critical to keep the relationship between the voter's identity and the cast vote private and anonymous. This is because it is a part of a protection measure or a political privacy to forestall the aims of influencing the voters' choices through intimidation, extortion or even potentially buying the votes.

According to (Jonker & Pieters, 2010), anonymity means it is impossible to determine who sent which message to whom. Depending on the context, different formalizations of anonymity appear to be required. In conjunction with that, anonymity is also crucial in electronic voting – voters should be able to vote without anyone knowing which option they chose. Instead of anonymity, the property expressed precisely is usually referred to as "privacy" in the electronic voting community. On the other hand, enabling privacy in voting is insufficient because it does not prevent vote-buying. The elections must be conducted in private to prevent vote-buying; No voter should be able to persuade anyone else of how a person voted and vice versa.

The problem statements for Universiti Melaka and Universiti Teknologi MARA (Melaka) in Malaysia are the foundation for the issue of voting anonymity in this paper. The votes cast at the institutions cannot indeed be considered anonymous because the voting area is open to the public (meaning there is no secure and private booth) and is closely monitored by the actual person in charge who lingers around the voting area. Furthermore, because they have a login system in order to vote, and the credentials are dependent on the students' identification, it is possible that the voter's identity is stored in the database.

C. THE NEED FOR AN ONLINE E-VOTING SYSTEM

The very first online voting was initially used in Estonia's national elections in 2005. Because of the growth of e-technology and direct democracy, voting machines and postal voting have emerged as models for developing online voting.

Low voter turnout increases the influence of a split opposition. Remote voting over online platform is thought to make distance to a polling site and other issues obsolete. The Barisan Nasional (BN)'s victory in the recent Johor state election (2022) was due to several issues, the most important of which is that low voter turnout increases the influence of a split opposition. The voter turnout was barely 55 percent, but BN received 43 percent of the ballots, giving them more than two-thirds of the seats with less than a quarter of the vote, which leads the way to the path victor, “If more people had shown up, the outcome could have been different"

Take UNIMEL (Universiti Melaka) and Universiti Teknologi MARA (Melaka) in Malaysia as an example. For every semester, they hold an election day to vote for their high-level committee. Due to the COVID-19 pandemic, all educational institutions were required to put a halt in terms of the normal face-to-face and physical classes. As a result, online e-voting has emerged as the most important method to implement.

Many researchers have proposed schemes to enhance the security of e-voting systems and put them into practice. According to Kho et al. (2022), the conventional approaches for e-voting systems can be categorized into mix-net-based and blockchain-based e-Voting, as well as latest developments in the field of post-quantum e- voting and hybrid e-voting. The use of different e-voting approaches may vary depending on the application to which they are applied. A hybrid scheme refers to the scheme that is constructed by integrating two or more approaches. Hybrid schemes are more practical and efficient than other approaches, according to an analysis of Table 1.

Table 1: The Advantages and disadvantages of various e-voting approaches

Approach	Advantages	Disadvantages
Mix-net-Based e-Voting	● Provides unlinkability between voters and their votes ● The computation cost is lower than the homomorphic tallying e-voting scheme ● Supports write-in ballots	● Difficult to implement on large-scale elections due to its complexity ● Large amount of computation power is required for the mix server to prove the correctness of mixing ● Vulnerable to DDOS attack
Homomorphic e-Voting	● Suitable for small-scale elections, efficient in the open phase ● Do not require decrypting of the encrypted votes to tally the election result. Thus, voter privacy is achieved	● Requires intensive zero knowledge proof to prove the validity of votes (high communication cost) ● High computation cost for the vote verification ● This is not suitable for multi-candidate elections because the ballot must contain proof of a possible choice in the election; therefore, the encryption cost is high when there is a large range of preference

Table 1: *Cont.*

Approach	Advantages	Disadvantages
Blind Signature-Based e-Voting	● Simple, flexible, universally verifiable, ● and efficient ● Intensive zero knowledge proof is not required ● Guarantees anonymity ● Supports write-in ballots ● Most efficient in the tallying phase ● Does not require high communication cost for the intensive phase	● Requires an anonymous channel where it suffers from complex computation and might be impractical to implement in the real world ● Blind factor can serve as a voting receipt ● Receipt-free blind signature e-voting requires physical assumption, e.g., an untappable channel that is impractical to implement over internet ● Most of the proposed schemes required certificate authority to distribute key pairs to the voter and it is costly to maintain
Blockchain-Based e-Voting	● The votes stored in the blockchain are immutable ● Allows the election results to be generated instantly ● Offers transparency while guaranteeing Privacy ● Able to withstand a DOS attack	● Facing scalability as an issue due to the technology is new ● Inadequate testing tools
Post-Quantum e-Voting	● Sustainable against quantum attacks ● Does not require intensive zero knowledge proof	● Larger key size than public key algorithms, thus requires more storage space ● Large sizes of data for signature and key establishment to be transmitted over communication channels, thus limits the speed of transmission and vulnerable to unforeseen quantum attacks

Note. From **"**A Review of Cryptographic Electronic Voting" by Kho et al. (2022) *Symmetry*, *14*(5), 858. https://doi.org/10.3390/sym14050858

D. HASHING TECHNIQUES

Hashing algorithms or hash functions is a process of converting input strings into output strings of a specific length. The output data, known as hash code, is usually smaller than the original. Hash functions are widely used in data integrity and security, both important for data transfer and authentication (Velioglu et al., 2019).

According to Stevens (2018), hashing is frequently used to manage and protect our digital life in various ways. For instance, whenever users input their password on a website, the server will most likely take action to save a hashed version of it instead of the plain text inputted by the users. The content of the hash code assures that the input string has not been modified. Since passwords are used in various computing applications, storing data in clear text is deemed unsafe and difficult. Choosing a model that cannot be used to recreate the original data is the most secure way to store a password, and the saved value, on the other hand, should be used for verification.

Generally, hash functions can be divided into two distinct type which are the cryptographic hash algorithms and the non-cryptographic hashing algorithms. Since the use of the hashing algorithm is simply to generate an ID or some sort of 'signature' for the voters, this particular project suggested the use of the non-cryptographic hashing algorithms. Although there are diverse types of the hashing algorithms, ranging

from 8 bits in size to an output size of 224 bits, this particular project targets the shorter sizes of hashing functions to encrypt the data stored in the database. Some hashing functions that are considered to be implemented in this project are CRC32, ADLER32, JOAAT128 and FNV132. Table 2 shows the comparison between the hashing algorithms.

Table 2: Comparison between CRC32, ADLER32, JOAAT128 and FNV132

	CRC32	ADLER32	JOAAT PHP	FNV132
Type	Originally a checksum algorithm that is occasionally used as hash functions	Originally a checksum algorithm that is occasionally used as hash functions	The Jenkins hash functions. The PHP's version.	Fowler–Noll–Vo hash function.
Length (Bits)	32	32	32	32
Output Size (Letters)	8	8	8	8
Example (Plain text à hashed)	hello = 3d653119	hello = 084b021f	hello = c8fd181b	hello = b6fa7167
Speed (GB/s)	13.19	2.00	0.80	1.00

E. ONE-TIME PASSWORD

A dynamic password is sometimes known as a one-time password. It's a random sequence of numbers created by a certain algorithm. It is the most basic form of one-time-password, therefore the passwords generated usually does not have validation termination. The simplicity of the is also include in terms of the implementation and maintenance within a system. And because a single password that only works once, it's a good technique to prevent account theft (Nayaka K et al., 2019). The name One Time Password implies that it is only valid for a single interaction, session, transaction, or authentication. These are more secure than the static password created by the user (Chowhan & Tanwar, 2019).

Nowadays, although its use in its purest form has yet to find commercial use, it is a component of many multi-factor authentication systems. An OTP is produced for the user when they log in, and they must return it correctly. For sending a one-time password, an alternative channel is usually employed, such as SMS, e-mail notification, a specific mobile application, or a hardware token (Landyshev et al., 2020).

Even with the various selection of multifactor methodologies that can be used, ranging from biometric verification, security question, one-time passwords, etc. This project, however, is planning to use the one-time password (OTP) as its method of authentication which in the choices between the basic One-Time-Password, Time-Based One-Time Password (TOTP), and HMAC-based One-time Password algorithm (HOTP). Table 3 shows the comparison between the three types of OTPs (One Time Password).

Table 3: Comparison between OTP, TOTP and HOTP
(Source: Chowhan & Tanwar (2019)*)*

Type	OTP (One-Time Password)	TOTP (Time-Based One Time Password)	HOTP (HMAC Based One Time Password)
Algorithm-base	None	Time-based	Event-based
Timeout	No	Yes	No
Security	Medium	High	Medium
Implementation Complexity	Low	High	High
Maintenance	Low	Low	High
Cost	Low	High	High

Note. From **"**Password-Less Authentication" by Chowhan & Tanwar (2019)*,* IGI Global bookstore*, p. 190–212 (https://doi.org/10.4018/978-1-5225-8100-0.ch008)*

F. RELATED WORK

As the need of online e-voting system increases by the year, it is inevitable that there are already plenty of attempts to develop the system with several types of technologies. However, the goal of the pass studies and this particular project is quite similar.

In research done by Oke et al. (2017), the electronic voting system is designed with a combination of the proposed improved Feistel block cipher which guarantees the confidentiality of the recorded data stored on the smart card and the enhanced voter's fingerprint model using first moment extraction algorithm for verifying the authenticity of valid real-time voters.

Another prime example is the system developed by Hasta et al. (2019), where they created a client/server web application software architecture for e-voting that uses biometrics of the voters' fingerprints for authentication and the SHA-1 hashing algorithm for data security. Although the system captures the key functional aspects of a voting system, it also addresses several important non-functional needs such as the requirements for fidelity, robustness, coherence, consistency, safety, and security are critical.

And recently, the technology of blockchain is also introduced in the e-voting systems. As created by K & K (2022), the e-voting system uses biometrics identification for the authentication and implemented the blockchain algorithm to the security at the storage level. As a result, the proposed method will help to increase overall voting system trust and transparency while also making voting more environmentally friendly, time-saving, and efficient. Table 4 shows the comparison between the three research.

Table 4: Comparison between the research prior.

Author (Year)	Oke et al. (2017)	Hasta et al. (2019)	K & K (2022)
Title	Developing Multifactor Authentication Technique for Secure Electronic Voting System	Fingerprint Based Secured Voting	Blockvoting: An Online Voting System Using Block Chain
Main feature	Multifactor Authentication	Biometrics-based	Blockchain technology
Authentication method	Smart card and biometric (fingerprint)	Biometric (fingerprint)	Biometric (fingerprint)
System's target area	Authentication	Authentication, Data security	Data security, Transparency

G. EXPECTED RESULTS

To simplify the understanding of the project, flowcharts are used as guidance for further comprehension. In this project, there are several modules that are considered crucial that for the user will need to go through, which are the Login module, Voting module, Vote Verification module and the Check Vote Status module. Below, however, is the basic overview of the application's function. Figure 3.4 illustrates the overview flowchart of the application.

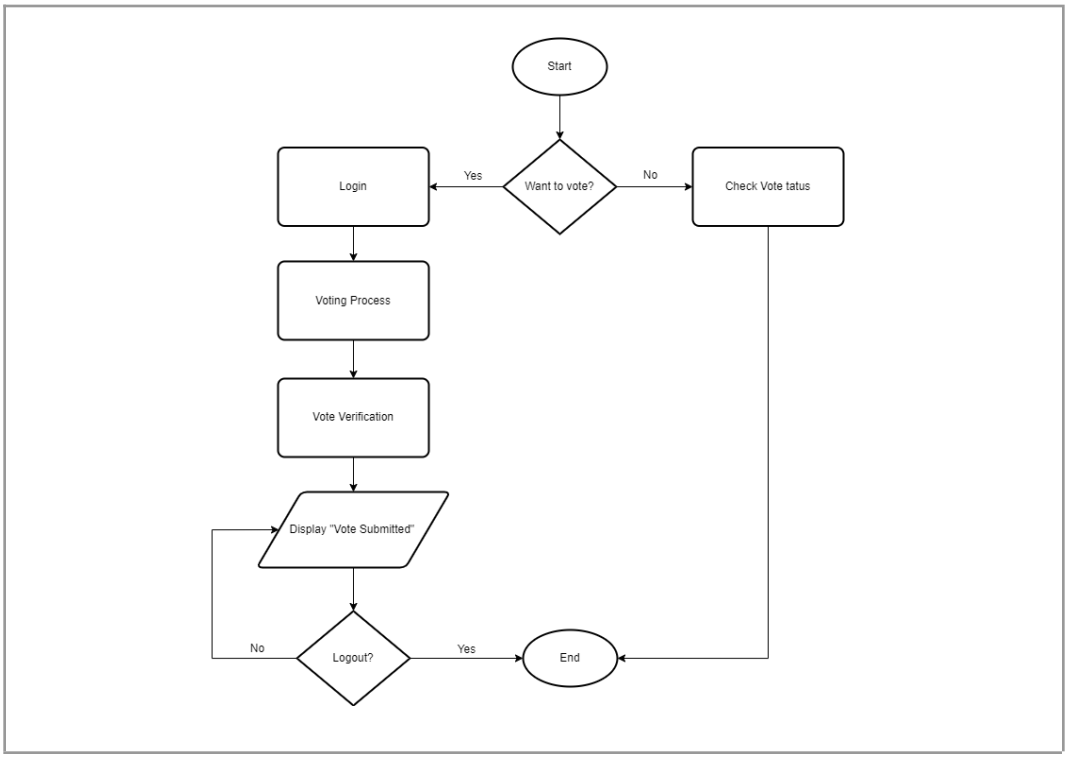


Figure 1: Basic overview flowchart of the application

Despite there are multiple modules related to the project, there two that are crucial where the hashing and the OTP are implemented, which are the Voting Process module and the Vote Verification module. Below are the figures illustrating the flow and the implementation of the methodologies suggested from the

previous parts of the report.

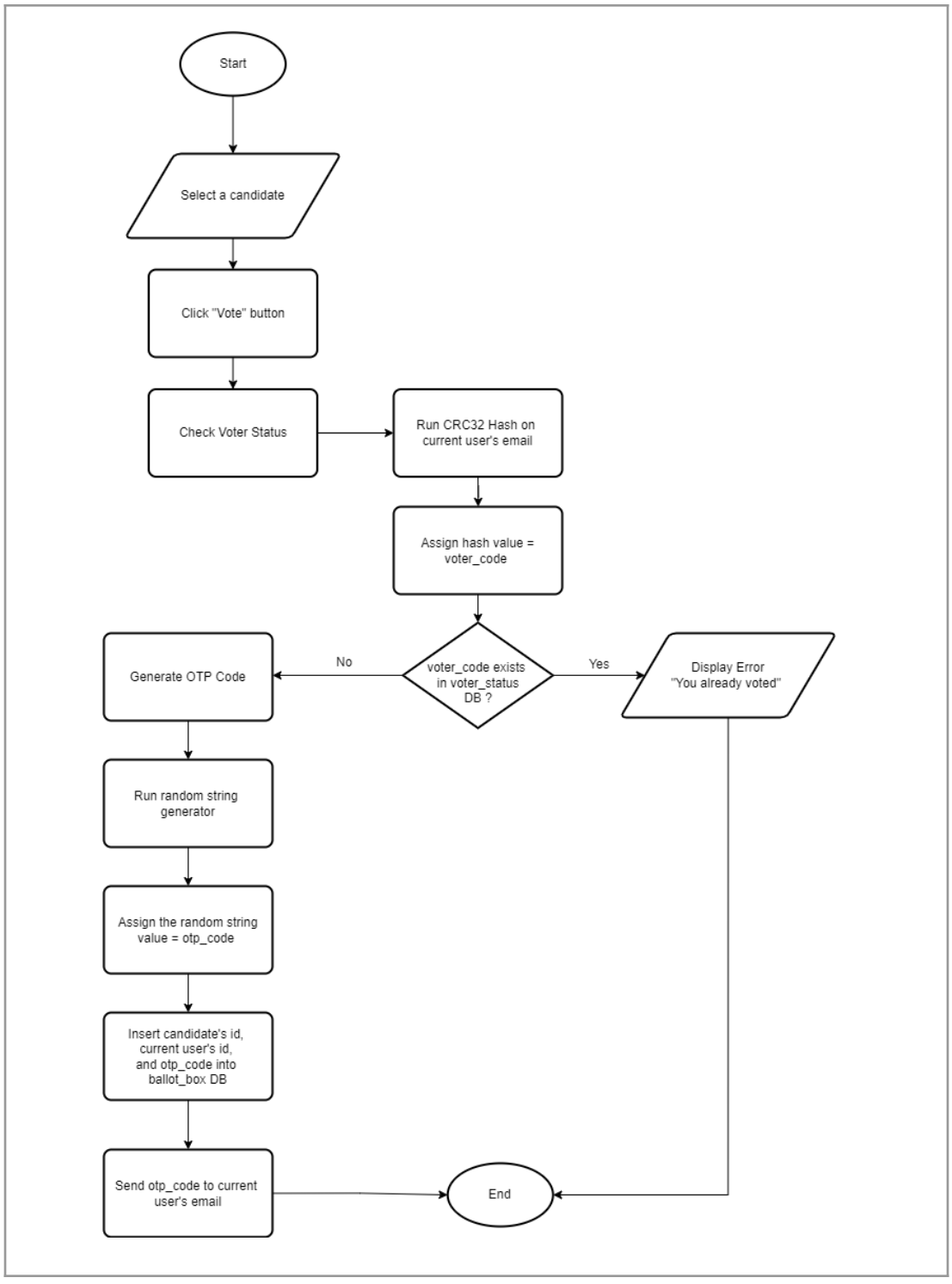


Figure 2: Flowchart of Voting Process module

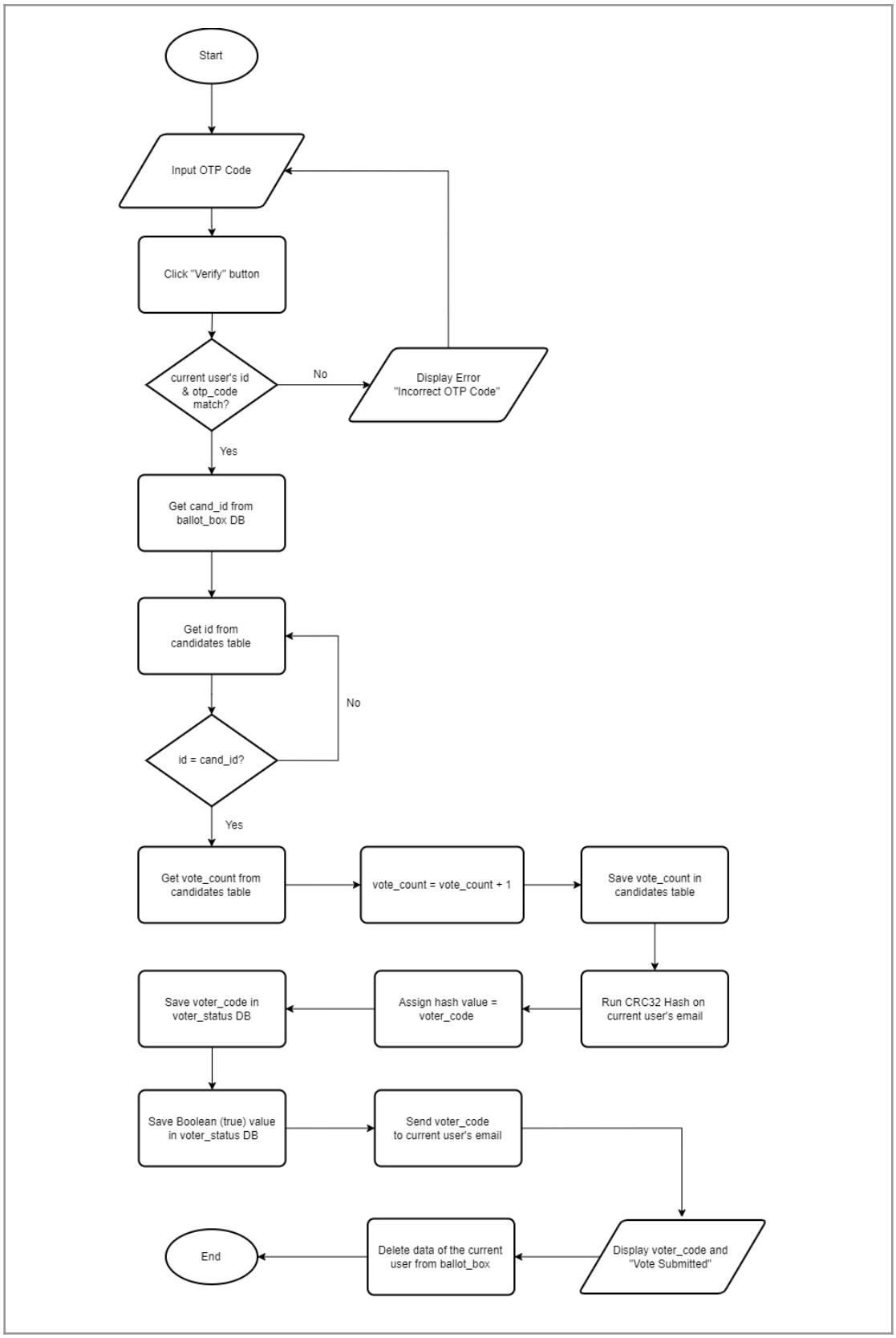


Figure 3: Flowchart of Vote Verification module

To simply put, the project is expected to gain a successful result with preserving the voters' anonymity by storing the ID or code generated from the hashing output instead of the plain text of the voters' email in the database. From figure 3, the ballot_box table in the database is deem as a placeholder and acts to hold the voting process data temporarily before and during the authentication of a valid vote, which includes data such as voter's ID, candidates ID, etc. Once the OTP is verified to match the respective voters' ID, only then the vote will be considered valid. A valid vote will trigger the program to save the voter's code in a table that lists the voters that have successfully voted for the election. The use of hashing to generate the voter code and the use of ballot_box that acts as temporary storage will preserve the anonymity of the voters as there will be no link between the voter's identity (in this case their email address) and the vote casted, while the use of OTP is simply to authenticate or validate the vote to deem it legitimate or not. The successful implementation of these methods is expected to result in resolving the problem statements of the project.

CONCLUSION

In conclusion, this paper discussed some practical considerations in the design of e-voting system that targets to keep the anonymity of the voters. To achieve the goals of anonymity of the voters, the use of a non-cryptographic hashing algorithm, CRC32, will be implemented. The hashed value is also used as part of the voters' authentication to verify its validation with the compliments of the use of One-Time-Password (OTP). The e-voting system is predicted to make sure the data in the database is intelligible in the human eyes and to successfully implement the OTP authentication for the validation of the vote. By using all of these technologies and methodologies within the development of the online e-voting application, it is predicted that the application's functionalities will work perfectly without any complications.

REFERENCES

Chowhan, R. S., & Tanwar, R. (2019). Password-Less Authentication. In *IGI Global bookstore* (pp. 190–212). https://doi.org/10.4018/978-1-5225-8100-0.ch008

De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2014). A Comparative Usability Study of Two-Factor Authentication. *Proceedings 2014 Workshop on Usable Security*. https://doi.org/10.14722/usec.2014.23025

Djanali, S., Studiawan, H., Nugraha, D. P., & Adi Pratomo, B. (2018). Vote identification and integrity of ballot in paper-based e-voting system. *Electronic Government, an International Journal*, *14*(1), 1. https://doi.org/10.1504/EG.2018.10010865

Fernandez-Navia, T., Polo-Muro, E., & Tercero-Lucas, D. (2021). Too afraid to vote? The effects of COVID-19 on voting behaviour. *European Journal of Political Economy*, *69*, 102012.

Hasta, K., Date, A., Shrivastava, A., Jhade, P., & Shelke, S. N. (2019). Fingerprint Based Secured Voting. *2019 International Conference on Advances in Computing, Communication and Control (ICAC3)*, 1–6. https://doi.org/10.1109/ICAC347590.2019.9036777

Jonker, H., & Pieters, W. (2010). Anonymity in Voting Revisited. In *Lecture Notes in Computer Science* (Vol. 6000). https://doi.org/10.1007/978-3-642-12980-3_13

K, D., & K, U. (2022). Blockvoting:An Online Voting System Using Block Chain. *2022 International Conference*

K, D., & K, U. (2022). Blockvoting:An Online Voting System Using Block Chain. *2022 International Conference on Innovative Trends in Information Technology (ICITIIT)*, 1–7. https://doi.org/10.1109/ICITIIT54346.2022.9744132

Kho, Y.-X., Heng, S.-H., & Chin, J.-J. (2022). A Review of Cryptographic Electronic Voting. *Symmetry*, *14*(5), 858. https://doi.org/10.3390/sym14050858

Landyshev, V., Blinovskaya, T., & Krakhmalev, D. (2020). The practice of using one-time passwords in modern corporate information systems. E3S Web of Conferences. https://doi.org/10.1051/e3sconf/202022401038

Nayaka K, P. S., Boban, J., & Bhargavi Ravi, A. v. (2019). Abnormal Pattern Analysis in Online Transaction. www.ijert.org

Oke, B. A., Olaniyi, O. M., Aboaba, A. A., & Arulogun, O. T. (2017). Developing multifactor authentication technique for secure electronic voting system. *2017 International Conference on Computing Networking and Informatics (ICCNI)*, 1–6. https://doi.org/10.1109/ICCNI.2017.8123773

Raut, S., Talekar, V., & Govardhan, A. (2021). Digital Electronic Voting Machine Using Raspberry Pi and Touchscreen Display. *2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*, 752–756. https://doi.org/10.1109/ICEECCOT52851.2021.9707960

Shacklett, M. E. (2021). *What is multifactor authentication and how does it work?* TechTarget. https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

Stevens, H. (2018). Hans Peter Luhn and the birth of the hashing algorithm. *IEEE Spectrum*, *55*(2), 44–49. https://doi.org/10.1109/MSPEC.2018.8278136

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, *94*, 30–37. https://doi.org/https://doi.org/10.1016/j.infsof.2017.09.012

Velioglu, S., Bolu, D. K., & Yemen, E. (2019). A New Approach to Cryptographic Hashing: Color Hidden Hash Algorithm. *2019 International Conference on Digitization (ICD)*, 170–173. https://doi.org/10.1109/ICD47981.2019.9105898