Hindawi
Mobile Information Systems
Volume 2022, Article ID 8705841, 11 pages
https://doi.org/10.1155/2022/8705841

Research Article

Development of an Efficient and Secured E-Voting Mobile Application Using Android

Anli Sherine,[1] **Geno Peter**,[2] **Albert Alexander Stonier**,[3] **Desmond Wong Leh Ping**,[4] **K. Praghash**,[5] **and Vivekananda Ganji**[6]

[1]*School of Computing and Creative Media, University of Technology Sarawak, Sibu 96000, Malaysia*
[2]*CRISD, School of Engineering and Technology, University of Technology Sarawak, Sibu 96000, Malaysia*
[3]*Department of Electrical and Electronics Engineering, Kongu Engineering College, Perundurai, Tamil Nadu 638060, India*
[4]*Operion Ecommerce & Software Sdn Bhd, Penang, Butterworth 12300, Malaysia*
[5]*Department of Electronics and Communication Engineering, Christ University, Bengaluru, Karnataka 560029, India*
[6]*Department of Electrical and Computer Engineering, Debre Tabor University, Debre Tabor, Ethiopia*

Correspondence should be addressed to Vivekananda Ganji; drvivek@bhu.edu.et

Received 13 June 2022; Revised 30 August 2022; Accepted 6 September 2022; Published 19 September 2022

Academic Editor: Saqib Hakak

Smart technologies, particularly the development of the Internet, are employed to enhance the quality of human existence. Thanks to the Internet's explosive expansion, more and more tasks can now be completed quickly and easily compared to the earlier times. E-voting is a relatively recent field that has been identified. Voting can be conducted in a variety of methods, including in person at a polling place, online, and via a mobile application. The security of applications cannot be disregarded given the internet's explosive growth. In order to prevent phishing attacks, we created an Android application and included a 3-step security process before voting. Students can now vote online from any location at any time using a mobile device. Android Studio is used to create and deploy the application. While creating the voting application, this research adheres to the software development life cycle. The result of this research is the creation of a mobile application that is user-friendly for students and serves as a practical tool for letting them vote with three levels of security.

1. Introduction

One of the most beneficial things a person can do for themselves and their community is to vote. On a broad scale, people typically believe that one person's vote has no bearing on their own. But people frequently overlook the significance of every vote. Voting gives people the ability to choose the kind of life they want for themselves and future generations. It is an opportunity to address issues that matter to people, including the kind of leader they desire. Voters make the decisions in elections. If you do not cast a ballot, someone else will decide for you. Even though elections are held annually, few individuals in this day and age recognise their importance. People's reluctance to visit actual polling places is one of the causes. E-voting is a method of casting a ballot online using a phone or other electronic device. It is often referred to as an electronic voting system. Voting through various channels, such as the phone, the internet, and private computer networks, has become increasingly powerful with the quick development of technology innovation. These methods have a number of advantages, including lower costs, accessibility for voters with disabilities, speedy installation, and ease of voting. However, there are security flaws in online voting systems that make the voting process open to major assault. Attackers may initiate a wide range of risky activities, such as utilising phishing assaults to sabotage the online vote and change the outcome, if the security is inadequate and the control mechanism is ineffective. Phishing is a type of social engineering assault in which administrators or end users are persuaded to provide their personal information by means of phone emails, messages, or phone calls. This technology seeks to provide

colleges the ability to vote on important and private internal corporate decisions. It uses three layers of security to prevent phishing attacks. Voting may be carried out from anywhere thanks to its adaptability. By implementing the necessary security measures, the election is conducted in complete secrecy, allowing the voter to select any of the participating candidates only provided they enter the correct voting code [1]. The student council is the official body that represents college students and allows them to engage in academic matters. In order to benefit the university and its students, the student council also works in conjunction with the administration and personnel of the university. The members of the student council are primarily other students, with support from university teachers and lecturers. Elections are held for a variety of activities, including clubs, in addition to the student council. Every two years, an electoral process for choosing the eligible student council members will be undertaken to choose the student council members. Despite the fact that voting is required of all students, the majority of them choose not to. A week prior to the election, the candidates for office must register with the election committee at the staff office. Voters are also thought of as the candidates themselves. Voters had to wait in a long line before casting their ballots, which added to the strain of the voting process. The majority of students decided not to vote in this situation. Regular voting will use paper and voters' time, and it may not be accurate. Voters have to submit the proper voting room key-ID in order to cast their ballots at the proper session for the research. To prevent any fraudulent activity, it included three-step verification features where the verification had to be completed by a mobile one-time password, e-mail verification, and fingerprint verification [2]. Many voters today do not enjoy waiting in lines because they are too busy with their own business or because they live far from polling places. These factors are causing a decline in the voting percentage. Voting nowadays takes a lot of time, is difficult and uses a lot of paper. In order to complete this process, a voter must physically visit a polling place and present the voting official with their identification card. When voting in person at a polling place, this identification card used is to be issued to obtain authentication. After completing the authentication procedure, the voter will proceed to the polling place and cast their ballot by placing a checkmark next to the candidate they choose to support. From the line to the vote, it will be a lengthy and time-consuming process. It is impossible for a voter to cast another ballot if indelible ink is visible on their right index finger. The expense of labour and paper at each polling place will be borne in part by the election commission. The voting station officer is responsible for transporting the vote boxes to a central location after the voting session to announce the results. The security along the route is a serious issue, as the ballot boxes might be changed during the time between the polling station and the central location.

2. Literature Review

This section includes publications that have addressed issues related to the examination of present methods for developing mobile applications. Online voting is a method of conducting elections that enables participants to electronically record and submit a secret ballot. A person or group of people express their opinions using this procedure. Voters can vote anywhere, at any time, and from any location with the ease of online voting. Using their own computers or smartphones, voters can cast their ballots from any location with Internet access with ease and comfort. Electronic voting technologies can expedite election results and lower election costs by drastically lowering the number of workers needed to run a physical polling place and tally the results. With the introduction of the electronic tabulation system, it allows the electronic counting of sheets or paper cards [3]. Direct-recording is the use of a ballot display with electro-optical or mechanical components where voters can record their ballots. Computer software can then process the data and store the results in memory components [4]. Direct recording electronics and electronic ballot printers are related. No vote information is saved using this technique. Only a token or piece of paper with voting options is printed by the printer. The ballot box, which may be electronic and count votes automatically, is then taken by the voter and placed inside. Voters can use a computer with internet access to cast their ballots using the internet voting system. It can be kept on any electronic device with internet connectivity and in an unsupervised, unrestricted place. The use of internet kiosks in actual polling places is one example of where it can happen in supervised and nonremote locations [5]. The voting system has a number of common aspects, one of which is the ability to specify in advance which users are permitted to vote and which are not. This method is employed in the private election section, where those who are not related to the party cannot vote. It can be used in the workplace, in a classroom, at a university, or even at a local event. The majority of voting applications display the voting results publicly. The outcome can be displayed in a variety of views, including pie chart and bar chart views. Trust is one of the main benefits of having expert influence over your election. Voters can feel secure knowing that their votes will be properly displayed and tallied thanks to a server and service that are separately controlled.

2.1. Existing Online Voting System. There are several existing online voting systems, which are discussed below

2.1.1. Easy Voting and Election. Figure 1 shows the application of easy voting and election that has been designed to simplify the voting by a group of people in a physical location. For example, one of the users creates a new vote, and the other user just needs to vote by passing the physical device from one person to another. The purpose is to create a tool that is simple and easy to use, and an internet connection is not required. The interface of this app is simple and easy to handle. When a user creates a new vote, the user needs to type in the name and choose the type of vote. These apps support two types of voting modes, such as in favour/against and single choice. The in favour/against type is suitable for voting on motions, resolutions, or proposals that

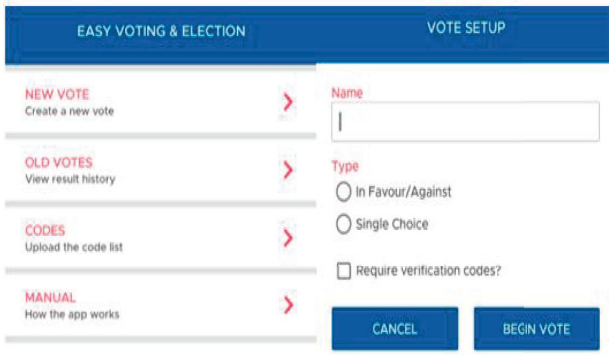

Figure 1: Easy voting and election.

can be either rejected or accepted, while the single choice allows the user to define multiple choices of answer to choose from, which can be used for custom elections such as offices. To ensure integrity of the voting process, users can choose and tick for required verification codes, for which users need to prepare and upload a list of verification codes. Through this method, voters who are authorized to vote will only be allowed to vote once and will be unable to vote twice. Each voter will receive their own unique code and the application will find the matches of their unique code in the list uploaded. In Figure 1 shown above, the old votes section allows users to see the result of past elections that have been created. The codes section allows users to upload the code list for verification of eligible voters. The section menu is to tell the user how the app works.

2.1.2. Mobile Voting. The mobile voting application shown in Figure 2 is created in a clean and simple user interface design. It is provided by Lukasz Liniewicz. It can conduct polls of large numbers of people. This voting app does not require any login account or internet connection. Users can create an election and vote anonymously. Users need to insert the name and the answer needs to be voted. Users just need to touch any of the answers, and the answer will be counted as one vote. The user just needs to vote by passing a device from one person to another.

2.1.3. Highly Secured Online Voting System over the Network. The aim of this system is to develop a voting system application that is interactive so that users are enabled to vote by using their own information that has been stored inside the database, while creating the voter's ID and information that needs to be renewed every six months for the verification of the user. Citizenship of India which is above age 18 years old and any sex only are to vote through this system without going to the physical polling station. Every user will be assigned a unique ID after registration. The technology of electronic voting can be included, such as voting kiosks, optical scans, and punched cards. They have implemented an online image verification system to increase the security of the e-voting system. This application consists of three phases: the first is to develop a front-end graphical for this system; second phase is the development of a method of

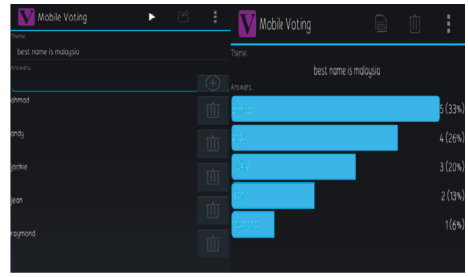

Figure 2: Mobile voting.

Figure 3: Homepage.

interaction with the webcams; and the third phase is the development of a web-based administration tool. This voting system requires the verification of every user through their username and password on the home page, as shown in Figure 3. The login and image stored in the database are used to compare with the image that has been taken while authentication is performed, as shown in Figure 4(a). After the successful authentication, the user will be directed to the voting page as shown in Figure 4(b). In this system, a methodology of integrating cryptography across the network has been used to present a higher level of security in online voting systems. The authentication process has been improved by adding both password security and face recognition.

2.1.4. Towards Secure E-Voting Using the Ethereum Blockchain. The aim of this application is to provide a secure voting environment and show that a reliable e-voting scheme is possible by using blockchain. It uses blockchain because bitcoin is only intended to validate coinage transactions, and the Ethereum network supports a broader range of use cases with the power of smart contracts. By using smart contracts, some applications that require a web server can be used without using any server. In this network, all operations are operated in real time. It also does not require any central authority to prove the work. The result can be calculated without any interface.

2.1.5. An Efficient Online Voting System. This system uses the ID and password created by the user to register the user on the voting website. The information of the voter will be

(a) (b)

Figure 4: (a) Image recognition. (b) Voting page.

Table 1: Comparison between existing systems.

No.	Type of system	Summarize	Shortcoming
1	Easy voting and election	(i) Does not require any account (ii) Able to view history vote (iii) Do not require any internet connection	(i) Complicated verification method (ii) One person can vote more than once (iii) User need to use the same device to vote
2	Mobile voting	(i) Do not require any account (ii) Do not require any internet connections	(i) One person can vote more than once (ii) User need to use the same device to vote
3	Highly secured online voting system over network	(i) Require face image recognition (ii) Can vote online through website	(i) System is complicated (ii) Everyone is eligible to vote
4	Towards secure e-voting using ethereum blockchain	(i) Does not require any server	(i) Unstable system (ii) Complicated system
5	An efficient online voting system	(i) Filter the eligible account and suitable candidate (ii) Required account to login the website	(i) Voters cannot view the overall result (ii) System is lack of security verification

saved in the database. The system can be used using the internet, e-mails, and e-SMS. The internet is used by voters who can vote anywhere and anytime. The e-mails are used to send error reports to the user that has entered the fault information. The e-SMS is used for voters who do not have internet access and e-mails that can be informed through SMS on their mobile phone. This online voting system requires storing a voter's information in a database, a voter's name, ID and password, a voter's vote in a database, and the total number of votes. Besides, there are several operational works that have been proposed in the system, which is recording information of the voter in database, checking of information filled by voter, discard the false information, and also each information is sent to election commission.

2.1.6. Comparison Between the Existing Systems. Table 1 below shows the comparison of summarization and shortcomings between each existing system.

3. Motivation

Incremental delivery is the software development methodology employed in this study. It is a process that will be applied to the system's design, development, testing, and

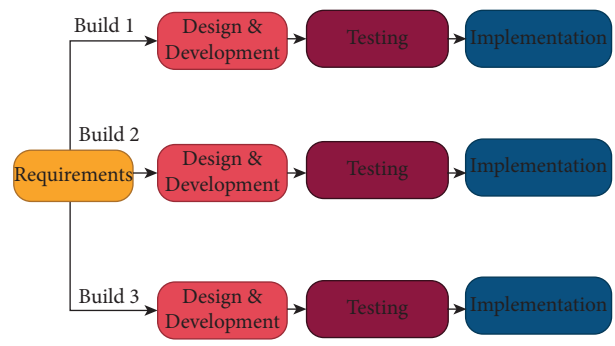

Figure 5: Incremental model.

implementation. This strategy, as displayed in Figure 5, is employed because it may break down software development from broad applications into more manageable components. It also enables straightforward, easy redesign, and deployment. The benefits allow developers to work incrementally and maintain concentration on one step before moving on to the next. If something is lacking, developers can go back to the previous phases.

3.1. Design and Development of E-Voting App. The specifications, features, and operations necessary to fulfil the

functional requirements of the proposed system that will be in place are outlined in detail throughout the design phase. After all requirements have been thoroughly defined and examined, the design is anticipated to happen. To make sure the final design satisfies the requirements, the suggested design should always be evaluated as shown in Figure 6. The success or failure of the research can be determined at this point, making it the most crucial. Measureable, testable, and traceable needs have been obtained. Google Forms have been used as the mechanism for gathering requirements [7]. A system will be created for this research to address the issue that has been encountered. It encompasses the deployment, architecture, and system interface of this system. The visualisation of what the system looks like and its attributes will be incorporated into the system interface. The three-step security in e-voting system environment is the main focus of the system architecture, which aims to stop phishing attempts.

The system will be developed with a number of features, including the ability to start a new election, join an existing one, verify voter eligibility via e-mail, phone OTP, or fingerprints, review previous joint elections, and more. This research will be applied through mobile applications in the system implementation. Users must download the app, which is available on the Google Play Store. The actual work begins during the development stage.

3.2. Testing and Implementation of E-Voting App. System integration and testing occur throughout the testing phase. The testing system will evaluate the system's overall functionality. Testing was necessary to ensure that the entire system functions in accordance with the specifications. The testing team and quality assurance (QA) will look for flaws and errors during the testing process and report their findings to the developers. The developers then send the programmes to quality assurance for retesting after fixing the flaws and errors. This process will keep on until the programme is functioning as the system requires. The majority of the program's code will be written during the implementation phase. In addition, it is where the systems that were described throughout the design process will be built. A certain amount of software is required to build this voting mechanism. A firebase database is mostly used to store data. To create an Android application, Android Studio is also necessary as a source code editor. Extensible Markup Language (XML) files and other types of code must be implemented inside the system using the Android Studio. To test the systems, an Android device is needed, such as a genuine smartphone or a virtual one that includes Google Play Store.

3.3. Mobile App Architecture. The application creation is carried out using Android platform, the software developers can easily publish their own programme right away because it provides a more stable integrated development environment than rivals such as Visual Studio. Android Studio is the integrated development environment of choice. Compared to other integrated development environment, Android

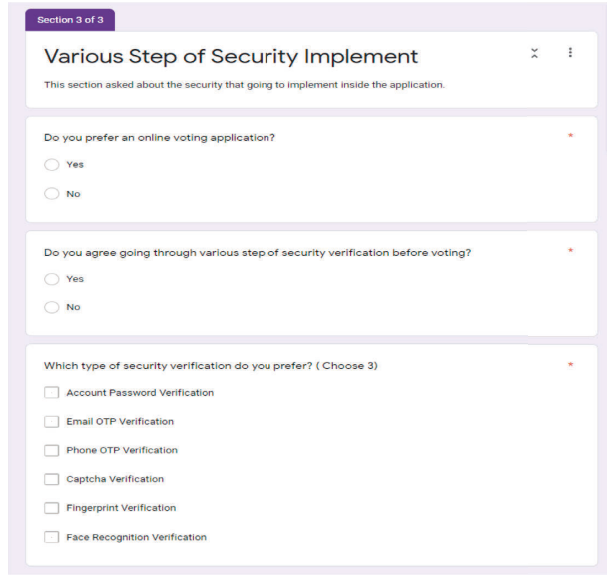

Figure 6: Research survey security question [6].

Studio also has a very simple user interface and enables drag and drop. The Java programming language, which is appropriate for creating Android mobile applications, is also used by the Android Studio. An industry and vendor-specific set of technologies and models known as mobile app architecture can be utilised to create fully structured mobile programmes. The mobile application architecture shown in Figure 7 below consists of three layers, such as the presentation layer, business layer, and data layer. Every layer has their own functionalities and each layer is essential and significant to develop mobile applications [2]. The presentation layer is a part that focuses on the modules of the user interface and also the process components of the user interface. While designing the presentation layer, the developers need to fulfil the requirements of the clients and also satisfy the designer [4]. While designing the application, the app developers should determine how the application will be presented in front of the end user. It is important to select the correct user interface components and their process components in order to build a successful application. For example, themes, colours, fonts, font size, and others.

Phishing attacks use emails and malicious web links to get the necessary personal information and data [8]. Phishers frequently utilise innovative techniques to deceive unsuspecting users and commit fraud in order to obtain and gather their sensitive and personal information. Phishers and cybercriminals are constantly looking for new ways to launch cyberattacks [9]. The standard phishing tools have always been expertly constructed in the form of forged SMS and e-mails; even these attack routes have raised the bar for sophistication and deceit. Attackers no longer bombard and spam users; instead, they use open-source intelligence (OSNT) technologies in conjunction with Internet sources to obtain minimal but required data on a target without their knowledge or consent [10]. Since phishing attacks do not contain any dangerous executable payload or malware, e--mail servers running antispam or phishing security programmes can struggle to identify phishing attempts [11].

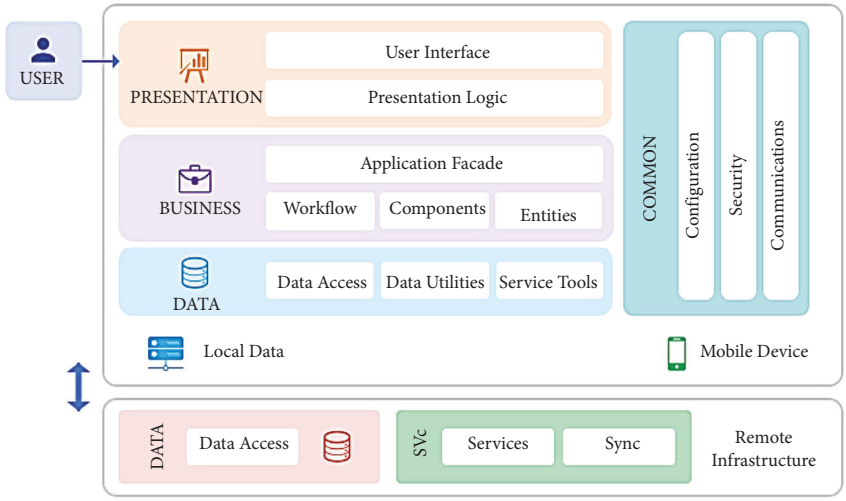

Figure 7: Mobile app architecture.

4. Results and Discussion

Confidential data transmission is one of the crucial and fundamental services in mobile e-voting systems. Sensitive client information is always protected from all types of assault, including phishing and man-in-the-middle attacks. Due to the present mobile authentication mechanisms, it is more difficult for users with mobile devices to recognise and prevent phishing attacks [11]. A mobile app prototype for e-voting with three levels of security has been created. The primary integrated development environment (IDE) tool is Android Studio. This chapter will also include a brief discussion of the interface design and its functionalities. The user interface that has been roughly designed will be displayed as the desired outcome. The user interfaces are divided into four sections, including the account page, home page, election page, and message page. In addition to the fragment page, it also includes separate pages for login, registration, and elections [6]. Android Studio is used to create this application. Open-source software is available on Android Studio. When making mobile applications, it is simpler and more practical. Once the application creation is completed, the software developers can easily publish their own programme right away. Since Android Studio provides a more stable integrated development environment than alternatives such as Visual Studio, it is the preferred integrated development environment. Comparatively speaking of other integrated development environment, Android Studio also has a fairly straightforward user interface and enables drag and drop. The Java programming language, which is appropriate for creating Android mobile applications, is also used by Android Studio.

4.1. Survey Data. Figure 8 below shows the three questions that have been asked of the respondent. For the first question, among 50 respondents, the majority of them prefer to have an online voting application. For the second question given by the researcher, the majority of the respondents agree and are willing to go through various types of security

Figure 8: Various steps of security implement in survey.

verification before voting. Furthermore, the third question given by the researcher concerns various types of verification that can be implemented inside the application [12]. The verification given by the researcher consists of six types, which are account password verification; e-mail OTP verification; phone OTP verification; captcha verification; fingerprint verification; and face-recognition verification [13]. As the result shown in Figure 5, the highest vote has been given to fingerprint verification, which has 45 votes with 90% of the respondents. The other one is captcha verification, which has 44 votes with 88% of the respondents. The

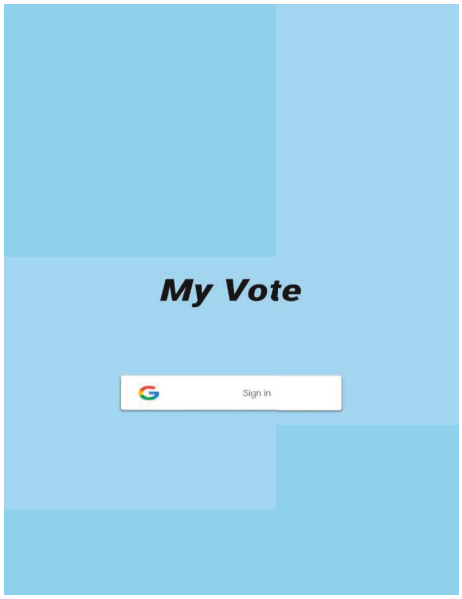

Figure 9: Registration interface.

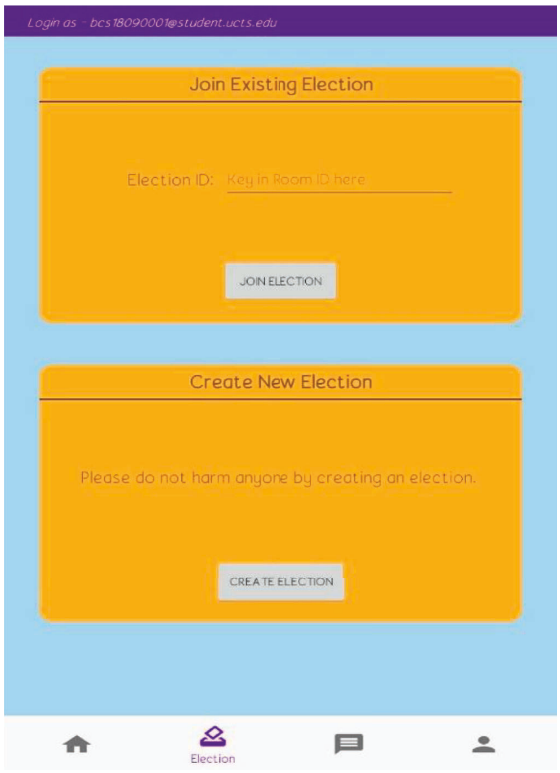

Figure 10: Election interface.

third one is phone OTP verification, which has 41 votes with 82% of the respondents. A majority of the respondents think that fingerprints are the most important, followed by captcha, and the third is phone OTP. The pilot survey was conducted based on 50 user responses [14].

4.2. Registration Interface. The registration interface is shown in Figure 9 below. E-mail, full name, contact number,

Figure 11: Account verification interface.

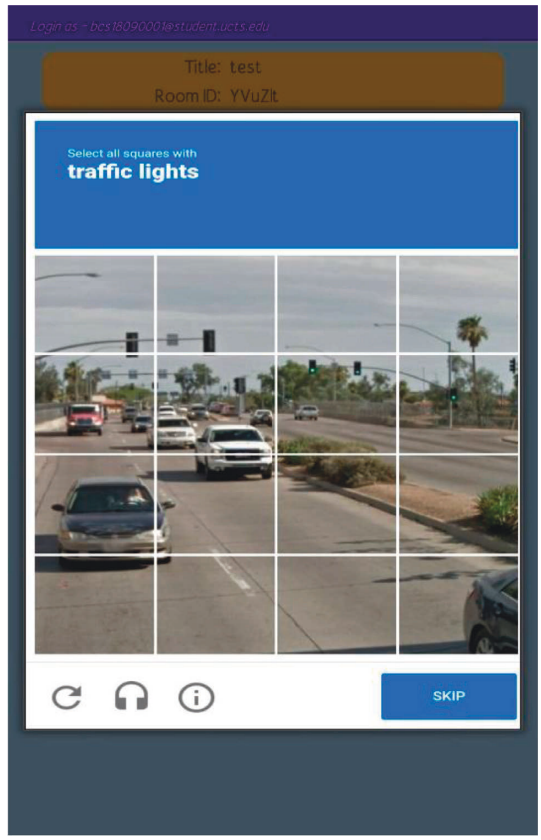

Figure 12: Captcha account verification.

student identity number, gender, and password are required for account registration. The user can log in with their e-mail and password if they already have an account.

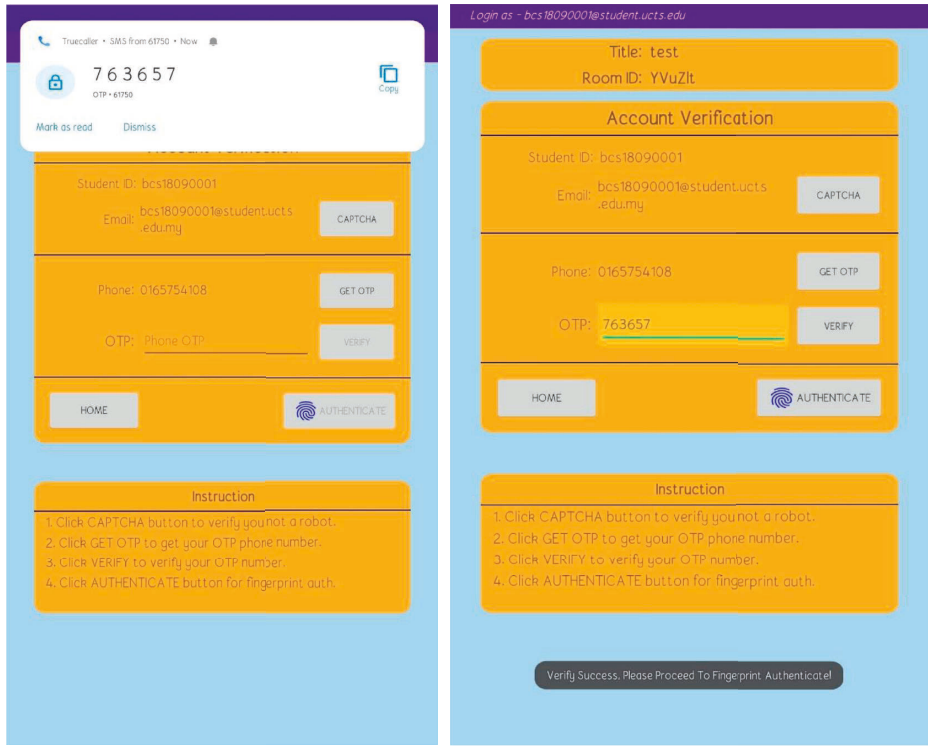

Figure 13: OTP verification.

4.3. Election Interface. The user interface for the election page is depicted in Figure 10 below. Joining an existing election and establishing new election sections make up this election page. A user who wants to participate in an election must enter the relevant election room ID in order to do so.

The user will be directed to the next stage, which is depicted in Figure 11 below, after entering the right election room ID. The student identity number, e-mail, contact number, and OTP are all listed on the account verification page. Each step must be verified by users. The database is used to get the student ID, e-mail address, and phone number, which cannot be changed [15]. If consumers need help using it, an instruction manual is available to walk them through the process step-by-step.

The graphs below demonstrate account verification using captcha. For users to prove they are not robots, they must click the captcha. When the user clicks the captcha button too frequently, Figure 12 will appear. The user can move on to the following phase if they are able to successfully verify the captcha.

Figure 13 illustrates how to verify a GET OTP. For their personal OTP, users must click the "GET OTP" button. The system will then send a 6-digit one-time password code to the user's phone number. The user must enter the proper one-time password when clicking the verify button after getting the one-time password. The user can move on to the following stage, as illustrated above, if they are successful in verifying their one-time password. The one-time password can only be used once, and each user is only permitted to use it once per day. The one-time password can only be given to a user three times each day. There will not be a one-time password given to the user's phone number if it is used more than 3 times [6].

The authentication using fingerprints is shown in Figure 14 above. After successfully completing the aforementioned three procedures, users are permitted to click this button. The user will be informed by the instruction if the fingerprint match was successful or unsuccessful. Based on the fingerprint of the user's device, fingerprint authentication is employed. To use fingerprint authentication, a user must enable their fingerprint on their own device [6].

4.4. Firebase Database. Figure 15 below shows the basis of the user profile. These data are stored in a Cloud Firestore. In the first collection, a user profile collection is created to store the user's information, which will store all user information under this collection. Inside this collection, a document is created every time a new user is registered. Each document in this field will be set to the user's university e-mail. Each document is represented by each user. Each document has a field which consists of all of the user's information. When a user registers, their information will be saved in the field. If an existing user updates their information, the data inside the field will be updated automatically.

Figure 16 below shows another collection inside the Cloud Firestore, which is voting information. This collection stores all the voting information that has been created by the user. Each document inside the collection information will be set as the title of the election that has been created by the user. Inside each document, it will be separated into two parts, which are the collection part and the field part. The

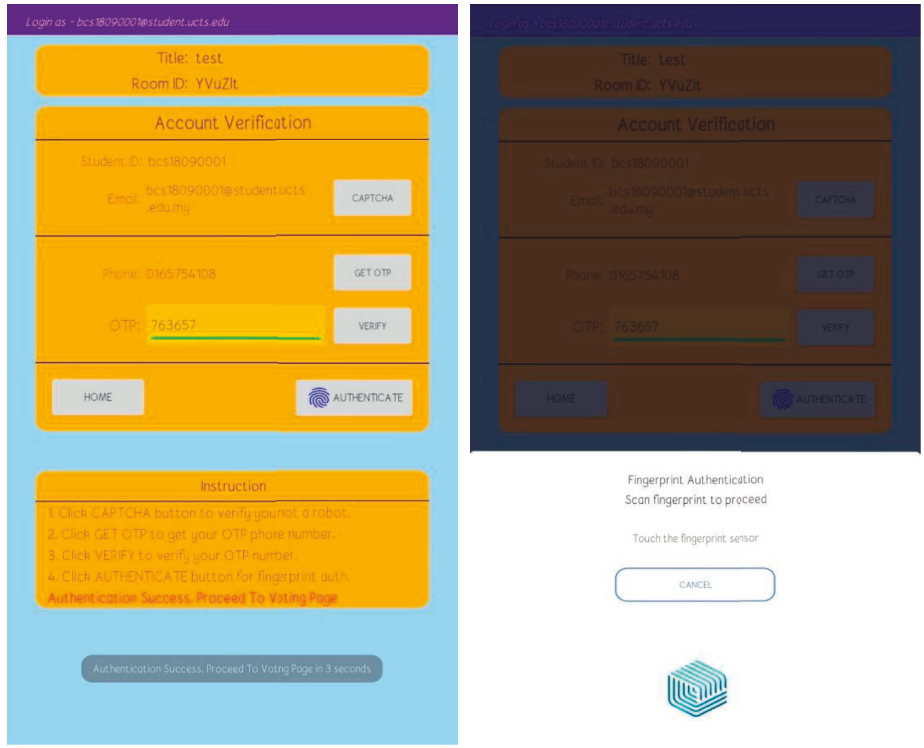

Figure 14: Finger print authentication [6].

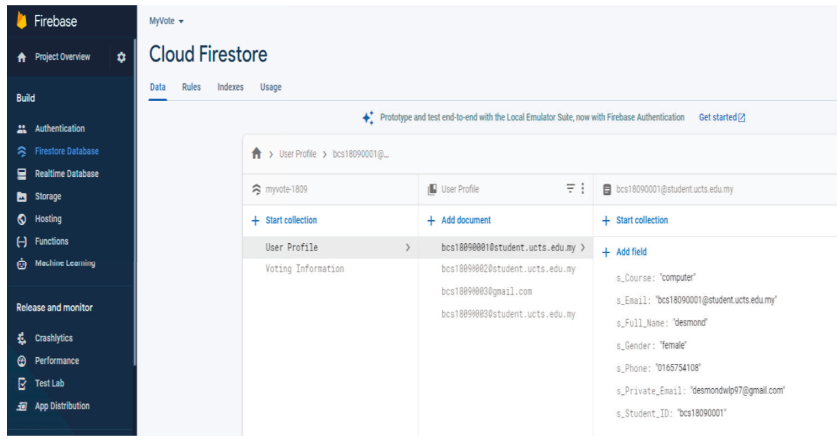

Figure 15: User profile firebase.

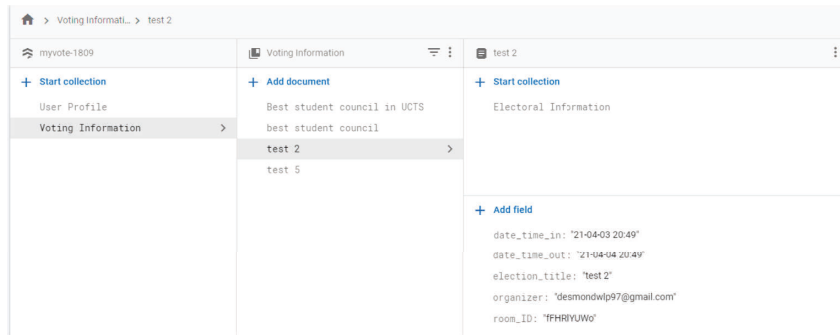

Figure 16: Voting information firebase.

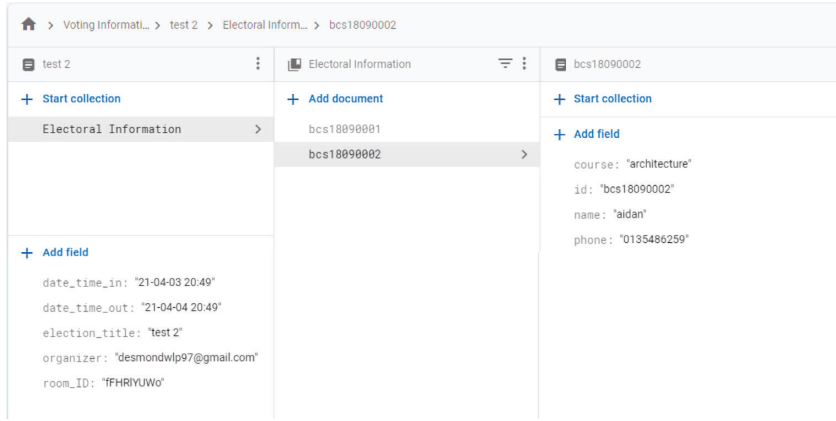

Figure 17: Voting electoral firebase.

collection part will store the electoral information while the field part will store the election information such as date, title, organizer, and room ID.

Figure 17 below shows the electoral information in the voting information collection under the Test 2 document. Inside the electoral information document, a bunch of documents will be created in which its name will be set as the electoral student ID. Inside each document, the electoral information will be stored here, such as course, ID, name, and phone number. All the information will be shown on the voting page except for the electoral phone number.

5. Conclusion

The proposed system has higher security compared to the existing system. The application was tested for the student leader election conducted on a university campus in Malaysia, and it proved workable. The only thing needed is an electronic gadget with the software installed on it along with an internet connection. No challenges were faced during the test run. Within this research, users need to register and log in to their own account before using the application. The user will directly go into the main page fragment, which consists of the homepage fragment, voting fragment, message fragment, and account fragment. The voting fragment page allows users to create a vote and join a vote. In this research, a 3-step security e-voting method for Android applications is proposed to guard against phishing attempts. Java and Extensible Markup Language (XML) are used in the development of the suggested system. Before the student submits his or her vote in this study, a three-step verification is put up. Captcha, phone OTP, and fingerprint verification make up the verification process. Phishing is an attempt by a person or group to obtain a victim's private information without their knowledge. To do this, fake websites that closely resemble the actual webpages are hosted. The message fragment will show the system messages and the voting message. While the account fragment allows users to edit their profile and logout, when a user wants to join a vote, they need to do a 3-step of verification in order to proceed. The first step is captcha verification, where the user needs to verify that he or she is not a robot by clicking the captcha button. The second step is that users need to get their own unique OTP number through their own phone number and insert it correctly. If the user successfully verifies the OTP number, then they can proceed with the third step. The third step is fingerprint authentication. After the user successfully verifies their OTP number, they are required to click the authentication button, and the fingerprint authentication will pop up. Users are required to scan their fingerprints to ensure that they are the owners of the phone in order to proceed to the voting page. Phishing scams are avoidable if you know how to correctly identify and prevent them. Firewalls are an effective way to prevent external attacks, acting as a shield between your electronic gadget and an attacker. However, future improvements can be made to fulfil the limitations and widen the scope of the research. The researcher can add some verification before creating a vote and also allow users to receive notification when a related field vote is created. Besides, a fully functional result will be added, such as a pie graph result, a real-time result, a percentage of the result, and the overall result. Electronic voting technology aims to speed up ballot counting, reduce the cost of paying staff to manually count votes, and improve accessibility for disabled voters. In the long term, expenses are expected to decrease. Results can be reported and published faster.

Data Availability

The required data can be obtained from the corresponding author upon an e-mail request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Sherine, G. Peter, A. A. Stonier, K. Praghash, and V. Ganji, "CMY color spaced-based visual cryptography scheme for secret Sharing of data," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 6040902, 12 pages, 2022.

[2] E. Yavuz, A. K. Koç, U. C. Cabuk, and G. Dalkılıc¸, "Towards secure e-voting using ethereum blockchain," in *Proceedings of*

the 2018 6th International Symposium on Digital Forensic and Security, IEEE, Antalya, Turkey, March 2018.

[3] A. Sherine and G. Peter, "A novel biometric recognition system for fingerprint using polar harmonic transform," *IJPR*, vol. 13, 2021.

[4] R. L. B. Abdullah and N. B. B. Haji Ahmad, *E-Voting System with 2-Step Verification Security Feature*, Universiti Teknologi Malaysia, Johor Bahru, Malaysia, 2017.

[5] G. A. Abandah, K. Darabkh, T. Ammari, and O. Qunsul, "secure national electronic voting system," *Journal of Information Science and Engineering*, vol. 27, 2014.

[6] A. Bhardwaj, F. Al-Turjman, V. Sapra, M. Kumar, and T. Stephan, "Privacy-aware detection framework to mitigate new-age phishing attacks," *Computers & Electrical Engineering*, vol. 96, Article ID 107546, 2021.

[7] G. Peter, A. A. Stonier, and A. Sherine, "Development of mobile application for E-voting system using 3-step security for preventing phishing attack," in *Proceedings of the 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering*, pp. 1173–1177, Greater Noida, India, April 2022.

[8] K. P. Kaliyamurthie and R. Udayakumar, "Highly secured online voting system over network," *Indian Journal of Science and Technology*, vol. 6, p. 1, 2013.

[9] P. Palanikumar and R. Karthikayini, "Online polling system," *International Journal of Scientific Research in Computer Science*, vol. 2, no. 3, pp. 09–14, 2017.

[10] Common Electronic Voting and Counting Technologies, "Retrieved from ndi," 2013, https://www.ndi.org/e-votingguide/%20common-electronic-voting-and-counting-technologies.

[11] S. Bojjagani, D. D. Brabin, and P. V. V. Rao, "Phishpreventer: a secure authentication protocol for prevention of phishing attacks in mobile environment with formal verification," *Procedia Computer Science*, vol. 171, pp. 1110–1119, 2020.

[12] G. Peter, A. Sherine, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, "Histogram shifting-based quick response steganography method for secure communication," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 1505133, 11 pages, 2022.

[13] G. Peter, J. Livin, and A. Sherine, "Hybrid optimization algorithm based optimal resource allocation for cooperative cognitive radio network," *Array*, vol. 12, Article ID 100093, 2021.

[14] I. Darmawan, "E-voting adoption in many countries: A literature review," *Asian Journal of Comparative Politics*, vol. 6, no. 4, pp. 482–504, 2021, https://doi.org/10.1177/20578911211040584.

[15] "Incremental model in SDLC: use, advantage Disadvantage, Retrieved from guru99," https://www.guru99.com/what-is-incrementalmodel-%20in-sdlc-advantages-disadvantages.html.