Development of cyber vote system using encryption approach

Ranpreet Singh, Bhupinder Kaur, Aby John, Bhupendra Singh ,Ritu Kumari
Lovely Professional University, Phagwara, Punjab

Abstract: Various approaches related to ballot-privacy, availability, completeness, equality, consistency, robustness, variability, and without use of receipt are commonly introduced to reduce risks. In addition, a variety of technologies such as decipherment and hashing have been implemented by the published protocols. The implementation of e- balloting in digital currency, in general, has now slowly become mature. Based on participants common security criteria, this we have proposed a chain based block protocol linked to ballot-privacy priorities, flexibility, accessibility, completeness, unique, robust.

1. INTRODUCTION

E - balloting, a modern comprehensive online balloting system based on the methodology of decipherment, has been slowly adopted and promoted by individuals. Compared to traditional elections, electronic balloting is a more open and unbiased alternative to the eco nomic system. As an e - balloting system, the Internet platform relies primarily on it. The key challenge for e - balloting is security.

Decipherment provides several advantages. It is very well may be utilized to perform errands, for example, encoding votes and computerized balloting stations, guaranteeing unmodified votes and programming, checking a voter's personality before throwing a balloting form, and helping with evaluating and tallying political decision results. Customarily, decipherment has been utilized to shroud data between two individuals utilizing a mystery key known to only them. After some time, the utilization of arithmetic to conceal data, secure protection, guarantee that documents are not modified and demonstrate the personality of a message's sender has ventured into the art and science [1]. Given the overarching value of vote secrecy and prevention of fraud, decipherment has proved to be a useful tool for countries using election technology. Keys are the information secret that is useful for encryption of data and decryption of data. Encrypted data cannot be recreated in its original form without the right decryption key. The protection of RSA is built on the strengths of two different functions.

In traditional systems, by auditing and controlling who has physical access to blank ballot stock, arbitrary individuals are prevented from forging votes. The supply chain is secured from the printer to the polling station. When votes are made, the excess ballots are discarded, and the completed ballots are placed into tamper-resistant containers and counted to the canvassing station. The system relies on trusting the employees who push the counting machines and handle the ballots. If there is enough collusion between workers, they can selectively invalidate ballots to achieve a desired result [2,3]. Protection is provided by

requiring the cooperation of large numbers of poll workers. In this paper we had made an online balloting portal where people can cast their vote irrespective for places. This portal is reliable, secure and user friendly.

In this paper we have used the firebase for database, firebase is a google-backed software to develop applications. Firebase offers several services, including analytics, authentication, security and real-time database.

2. EXISTING SYSTEMS

Standard ballots typically provide a typical voter with poor confidentiality. Some voters are unable to use standard vote ballots. The fine motor skills needed to fill out marksense or punchcard ballots can be difficult for the elderly or the infirm [4]. A special ballot will be required in each of these cases. Each group's balloting preferences can be determined because they are physically different in their ballots. Accidentally, identification of information is transmitted through the design of the ballot.

3. DESCRIPTION OF KEY GENERATION

Public Key Decipherment

Like symmetric key decipherment, there is no historical use of public key decipherment. Symmetric decipherment was appropriate for associations, for example, government, military, and huge money related enterprises engaged with grouped correspondences.

With the spread of more unbound PC organizes in most recent couple of decades, an authentic need was felt to utilize decipherment at bigger scale. The symmetric key was non-commonsense because of difficulties it looked for key administration. This offered ascend to the general population key cryptosystems [5]. The procedure of encryption and decoding is portrayed in the accompanying delineation.

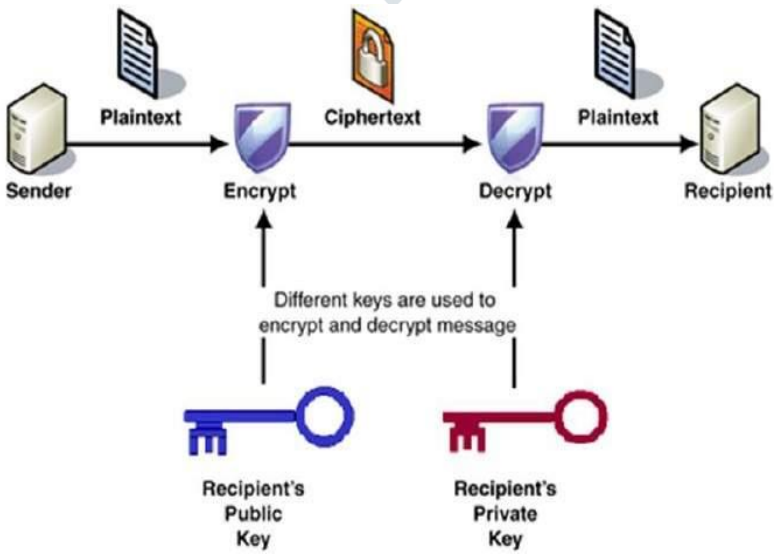


Figure 1 : Public Key decipherment

The most significant properties of open key encryption conspire are −

- Different keys are utilized for encryption and unscrambling. This is a property which set this plan not quite the same as symmetric encryption plot.
- Each beneficiary has a remarkable decoding key, for the most part alluded to as his private key.
- Receiver needs to distribute an encryption key, alluded to as his open key.

4. PROPOSED APPROACH

This main purpose of this paper is to solve the problems faced during the elections by the election commission and voters. This paper provides security to its users with the use of decipherment and it also help user to cast their vote from any place around the globe with a reliable internet connection. Decipherment provides electronic balloting and counting solutions with several advantages. It can be used to perform tasks such as encrypting votes and digital ballot boxes, ensuring unmodified votes and software, verifying a voter's identity before casting a ballot, and assisting in auditing and counting election results. Given the overarching value of vote secrecy and prevention of fraud, decipherment has proved to be a useful tool for countries using election technology. Encryption and decryption are among decipherment's most common uses. Encryption is the information obscuring process, and this process is reversed by decryption. Keys are the information secret that is needed to encrypt and decrypt data. Encrypted data is unintelligible and cannot be recreated in its original form without the right decryption key [8]. In this paper we used firebase for database, firebase is a google-backed software to develop applications. Firebase offers several services, including analytics, authentication, security and real-time database.

4.1 Advantages of proposed approach

Accessibility: E - balloting can be available in large networks if well-built so that people can still cast their votes from far back. This advantage saves both voters and government time and effort. Another way is to use the system is to use the power of multiple languages to help users use the system through headphones. Through listening to the voice of the system and interpreting it at the same time, it will be much easier for voters to fully understand the system

Speed: No one can deny that computers can do a great deal of work compared to people. Using this advantage can certainly reduce people's waiting time to get the result of the election. For some countries, after a few months, the election result is expected to finalize. With e - balloting, in a matter of days, people can get the result.

Accuracy: Computations and vote counting will be at ease for election volunteers since that e - balloting can do the counting for them.

Cost Reduction: It may be necessary to minimize tools such as ink, papers and other materials used in balloting. Voters can save money and get most of the elections with the help of information technology.

Validation: The capacity of the system to validate and audit votes diminishes the public's concerns about balloting or balloting.

Overall a Better Balloting System: People has the history and experience of having election done manually and it is undeniably true that people make it difficult.

5. IMPLEMENTATION AND FLOW DIAGRAMS

We have implemented our approach keeping in mind that it will satisfy all our customer need. While implementing this project there had been a lot of issues in design and coding phase, to resolve this issue we had to prepare number prototypes such that there will be no further problem in later phases [9]. We performed various feedback based on different sexuality and different age group of people. We asked them for what can be included and what can be omitted from the software to make it more responsive and user friendly.

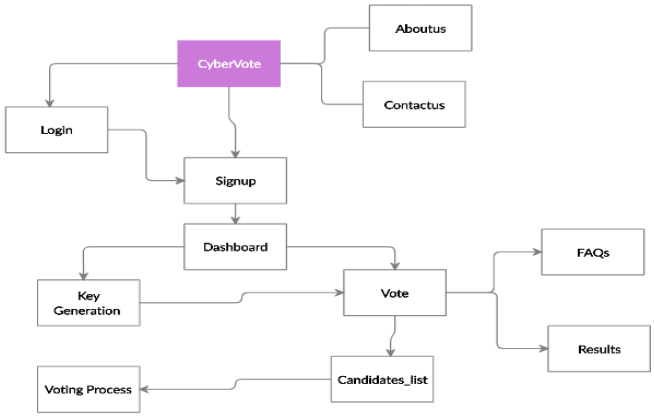


Figure 2: Flow chart of website

1. When you are at Cybervote the main page or index page of the website you can browse to login page, signup page, about us menu and contact us pages.
2. After signing in or logging in the website with your credentials you can browse to the dashboard
3. From dashboard you can move to key generation page and balloting page.
4. Once you are at balloting page you can go to candidate's list page or can also see the balloting results and browse to FAQs page.

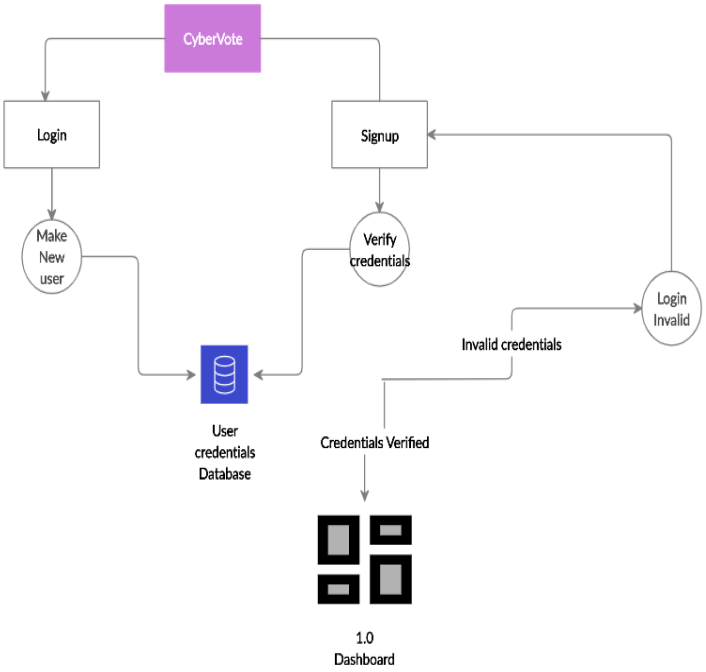


Figure 3: Flow chart for user login and verification

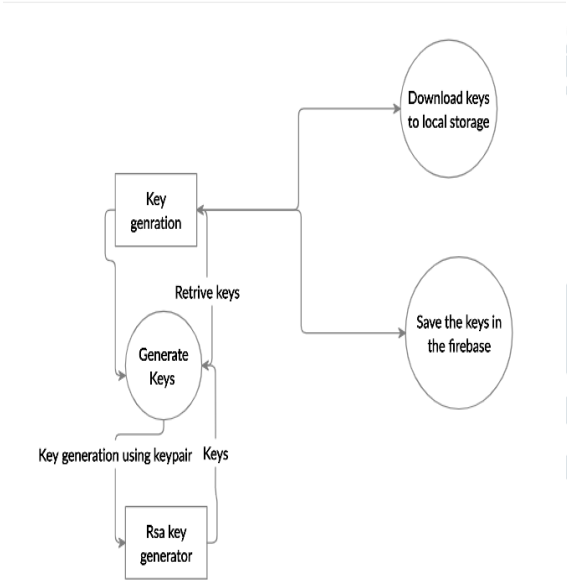


Figure 4: Flow chart for Key Generation

1. When you are at Key generation it will automatically generate key for a unique user.
2. By clicking on the download button, you can download the keys in the database as well as on your local storage.

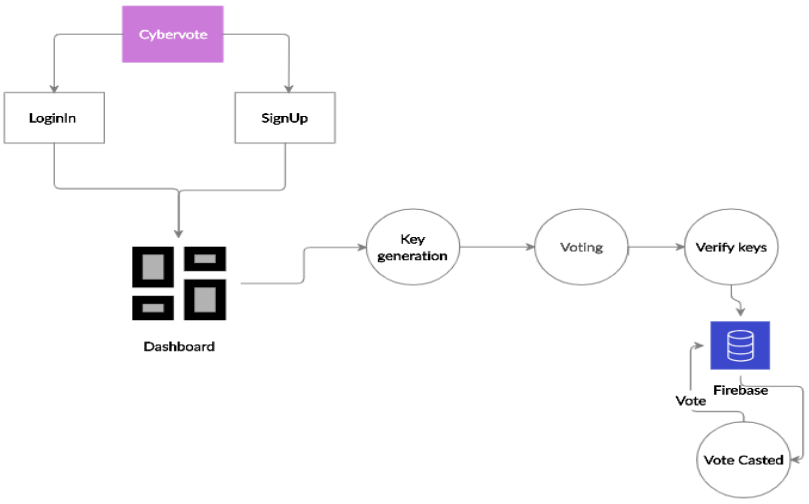
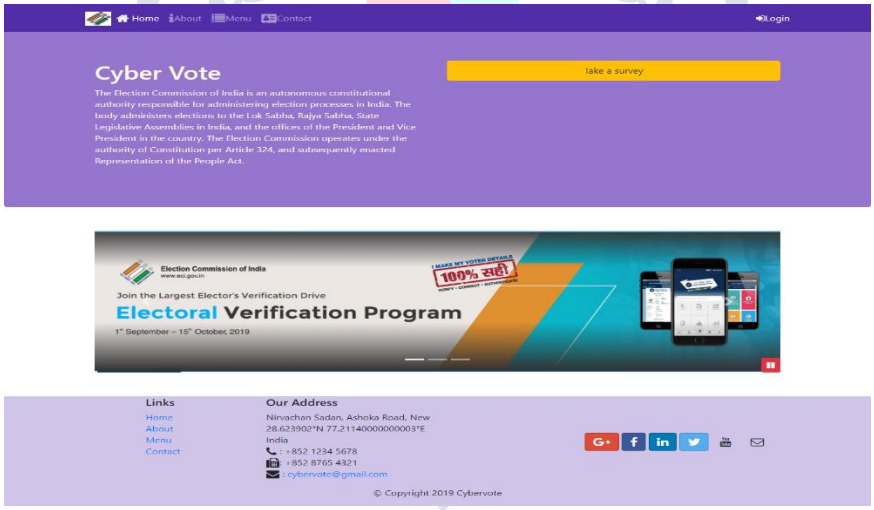


Figure 5: Flow chart for Balloting Process

1. When you are done with the generation of the keys you can cast a vote to your favorite representative only once.
2. The keys will be verified by the database and your vote will be registered.

This is home page of our web app. All the functionality of this website is explained as below:

Home Page



1. With the login button you can create an account using a verified Gmail id and password and login with your existing account credentials.

2. We can check about us page using navigation-bar.

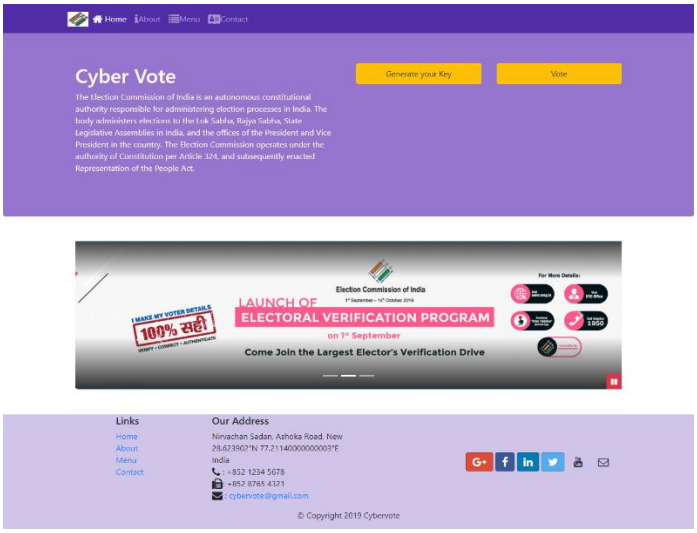
3. We can check contact us page using navigation-bar.

4. You can take a survey through home page by take a survey button.

5. You can see the new programs or events through the carousel bar.

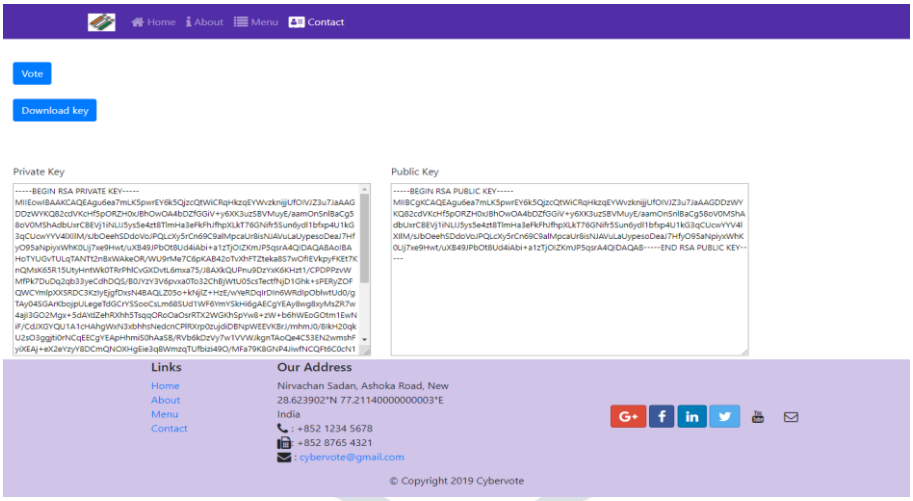
In this paper we have shown only limited pages of our websites.

MENU PAGE



1. You need to generate your keys using generate your keys button which will generate a key pair i.e. private and public key using rsa key generation algorithm.
2. After generating keys, you can vote your representative using vote button.

KEY GENERATION PAGE



1. You can download the key to your local storage using the download key button at the same time the keys will be stored to the firebase real time data base under the userid for whom the keys where generated.
2. You can use the vote button which will redirect you to a new page where you will get a list of candidates.

5. Conclusion

In this paper we used firebase for database, firebase is a google-backed software to develop applications. Firebase offers several services, including analytics, authentication, security and real-time database. Based on participants common security criteria, this we have proposed a chain based block protocol linked to ballot-privacy priorities, flexibility, accessibility, completeness, unique, robust.

References

[1] A. Basharat, "A Review of techniques used in E - balloting A Review of techniques used in E - balloting," no. January, 2017.

[2] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of E - balloting: the past, present and future," *Ann. des Telecommun. Telecommun.*, vol. 71, no. 7–8, pp. 279–286, 2016.

[3] T. Sobh and K. Elleithy, "Design, Analysis and Implementation of a Cyber Vote System," *Adv. Comput. Information, Syst. Sci. Eng. - Proc. IETA 2005, TeNe 2005, EIAE 2005*, no. June 2007, 2006.

[4] S. Bell *et al.*, "STAR-Vote: A secure, transparent, auditable and reliable balloting system," *Real-World Electron. Balloting Des. Anal. Deploy.*, vol. 1, no. 1, pp. 375–403, 2016.

[5] Aviel D. rubin Secutiy Considerations for remote electronic balloting "REMOTE," no. 12, 2000.

[6]http://www.dgalindo.es/mscprojects/yifan.pdf

[7]https://www.cs.hmc.edu/~mike/public_html/courses/security/s06/projects/chrisd.pdf

[8] https://www.geeksforgeeks.org/rsa-algorithm-decipherment/

[9] http://www.ijtrd.com/papers/IJTRD185.pdf

[10] T. Kadam, "Online Balloting System," *Int. J. Eng. Trends Technol.*, vol. 37, no. 5, pp. 273–276, 2016.