Secure Voting System using Hardware Key Based Sessions

Akarsha K.S[1], Anirudh M Belathur[2], Krishna M.V[3], Navneeth C.S[4], Smt. Nandini B M[5]
The National Institute Of Engineering, Mysuru

***Abstract*–** Current remote electronic voting frameworks are intended to give vote protection and evidence. The framework is platform autonomous online application, i.e a web-based application is intended to be especially straightforward and lightweight as far as its structure, the cryptography it utilizes, and the client experience.It has the adaptability to permit making of choice from any remote spot, The decision is held in full confidentiality by applying fitting safety efforts to enable the voter to vote in favour of any participating candidatesjust signing in into the framework by entering the right username, secret key.Our proposed method is an online voting framework that uses a simple hardware device at the voter's end which grants voter to cast a ballot free of area through secured gateway portals.The proposed plan is savvy and in the meantime fulfils the security necessities of a web based online voting system.

Keywords- Voting, Remote election device, RSA security algorithm.

I. INTRODUCTION

The most essential part of the vote based system is the capacity of the general population to elect their leader by exercising vote, One of the strategies that is used is of a web based vote casting ballot via the internet. Arrays of such decision frameworks are utilized by organizationsand associations where the individuals are in remote locationsand postal polls where voters residing in areas that aredistantly located in cases of general elections in the country.

There are two primary classifications of such frameworks. In the primary class, voters vote in surveying stations utilizing electronic voting machines, for example, direct recording electronic voting systems or scanners. On the contrary the second class of voting system, called remote electronic voting, where voters vote over the Internet using Their own devices.

II. TRADITIONAL METHOD

India is one of the largest democracies in the world. Democracy in itself means to provide the power among the citizens of the country to be able to choose the leader through direct or indirect means of voting. The Right to Vote has been instilled as one of the statutory rights or legal rights to the citizens of India.

The nation progressively moves forward in providing the best resources to make sure that the process of casting votes is highly secure and provides anonymity to the people of India. Today, the Election Commission is the government body that conducts the elections in India. It is highly important that any system provides services such as - anonymity, non-duplication of votes, etc. The election is conducted is by segregating the country into different constituencies. The election commission defines the timeline for the elections in the respective constituencies. The interested candidates register themselves for the elections by following the set of criteria defined in the Constitution Of India.

On the day of the elections, the citizens of each constituency have to cast their votes in the designated polling booths. This system makes extensive use of human resource and use of paper trail to keep track of events at those polling booths. Even to this date, the ombudsmen in the polling booths make use of indelible inks to mark signs of vote on voters hands. This is a system to prevent duplication of votes. The Electronic Voting Machines are set up at all polling booths to capture the votes. These Electronic Voting Machines(EVMs) are highly sophisticated machines that are well configured to provide all the services as needed by the system.

But unfortunately, the system uses up immensely large amounts of monetary funds, extensive human resources. Also, the concept of polling booths have increased threats of booth capturing and other illicit activities that deprives the voting rights of the people and fails to exhibit any functionalities of a democratic nation In the paperR.Kusters[1],a lightweight system sElect had been implemented as web based application which is simple and secure and is mainly meant for low-risk elections. The presented proposed system can be used for all kinds of elections used by the democratic nations.

III. PROPOSED SYSTEM

Generally elections takes place with the people present in their respective constituencies. This system instills the fundamental right of voting, back to people whoare unable to exercise their vote away from their constitutency.This system will gradually help in increasing the overall voting and also transparency in the entire process. As online systems are in trend in recent decade, using proposed system user can cast vote more easily from their remote places. A special hardware device is provided to each and every person who are unable to vote from their constituencies due to various reasons.

The system has an election portal for election commission where the election date, timeframe, constituency and the list of candidates who are contesting in the respective constituency are decided. The election portal will be opened on that particular day of election where people are allowed to vote and each and individual votes are recorded. Finally in the counting phase all d recorded votes are counted and the respective candidate with the highest votes is declared as the winner of the respective party.

Vote counting Module, which is responsible for votes that has been received and declaring the results with the candidate, no of votes and the party.

It is highly secured module which avoids duplication of the votes from the same person and keeping the identity of the person anonymous. Finally it is the responsibility of the EC to announce the results which can be viewed by all.

In the voters end, a special hardware device is issued to every person who are unable to exercise their vote from the constituency and on the day of election the corresponding portal is opened from EC,each and individual person is authenticated and verified. In the specific timeframe they vote and the votes are encrypted using RSA and sent to the election commission portal which is decrypted at the thatend. Finally it's the job of the election commission to count the votes using vote counting module and finally declare the results.

A techstackMERN (Mongo DB, Express. js, React. js, Node. js)is an open source, used to implement this system. It is mainly a framework for building dynamic applications. The techstack is made up of :

Mongo DB: It is utilized by the backend application to store information in JSON group and is fundamentally a NOSQL DB. It is an open source, database which gives persistence to application information and stores JSON records in accumulation with dynamic constructions as opposed to putting away information in lines and segments.

NODE.js:It is JavaScript runtime condition that runs the backend applicationand it is an offbeat ,occasion driven engine where the application makes a demand and after that keeps chipping away at other valuable errands as opposed toslowing down while it hangs tight for a reaction. On fulfillment of the asked for undertaking, the application is educated of the outcomes through a callback. This empowers expansive quantities of tasks to be performed in parallelwhich is basic when scaling applications.

Express.js:It keeps running as a module inside the nodejs environment and is fundamentally a web application framework that runs the backend. It basically handles routing of requests to the particular piece of the application. It tends to be utilized to give a REST API which is, for the most part, giving the front end application the assets that it needs to access.

ReactJS:It is fundamentally a JavaScript library for structure interactive UI's.Front end application is separated into segments and every part can be accessed independently which makes react different from others. Each part has its own state and a parent can pass its state to child components and vice versa(through call back functions). They are ordinarily executed in JSX-an extension of JavaScript that enables HTML syntax to be inserted inside this code. It is solitary page engineering for the frontend, which gives security from assailants.

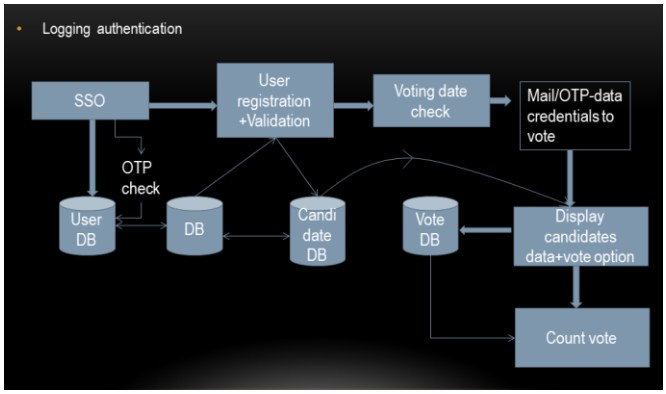

Fig.1:Design of the backend

IV. AUTHENTICATION

Security is one of the most important services that is to be presented when building a system that aims at serving a functionality that the entire nation will use. The authentication module is a service in itself with the objective of taking care of the log in requests from client services. In figure 2, the client services may include, the requests from the election commissionportal orthe people signing in via their device to vote during the elections. The authentication module, basically acts like a micro-service that talks to a database containing information about the user login ids and passwords. The service makes use of highly secure encryption algorithms like sha256 to secure the passwords. A second layer of encryption in the databases will be provided using GUIDs. The authentication module aims at providing Single Sign On(SSO) service. The service will integrate the use of phone prompts to enable two step verification for the user.

This will be a stand alone service that will clearly take care of the entire sign in service and will allow other services to talk to it's database via the service and not directly. This promotes the usage of cleaner distributed databases. The system as a whole, will have background jobs that are necessary to take of database consistency.

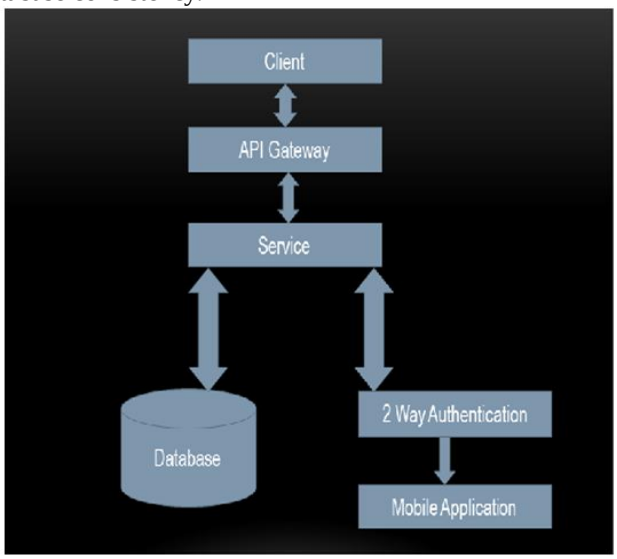

Fig.2:Authentication portal

V. ELECTION COMMISSION PORTAL

Election commission of India assesses the importance of this constitutional institution in the large system of democratization in India. The more advantageous function of Election Commission has a lot to do with the upward thrust of alliance politics and coalition rule in India. During the election on the voter's end the corresponding portal is opened from Election Commission called election commission portal. This portal will have a key role to play in the remote voting technique. Election Commission portal includes precious statistics provided by Election Commission inclusive of the election begin and end date, names of respective constituency's applicants together with electorate listing and does the task of counting outcomes at the give up as shown in figure 3. The portal is accessible to Election Commission to feed necessary details pertaining to the election into the portal however,is open to voters only on the particular timestamp during the election as fixed by Election Commission.Here each and every individual voter is authenticated and verified additionally proper security measures like proper security measures like session ID and Mac ID is used to prevent duplication of votes at the voter's end. Votes are encrypted with an end to end encryption algorithm. Finally, the number of votes are counted using vote counting module and the result is declared in Election Commission portal.

VI. ELECTION TIMELINE

The Election Commission has the complete authority on running the elections, conducting them and collating the results to provide the consolidated vote scores. The Election Timeline proves to be one of the major features of the product design. The Election Timeline is specified by the Election Commission, which generally acts as the admin for the ecosystem in place. The Election Timeline is in its true essence the sequence of events that will take place for the hassle free conduction of elections. The timeline comprises of the order of events.

The Election Commission, first sets a date window or a time frame during which the election will be held. Implicitly, this means that, the users will API endpoint is not available for the users to cast their vote before the opening of the date window and the closing of the date window. Further, the Election Commission has to specify the constituencies where the election will be held. This is a high valued information for seamless flow of elections.

The users, pertained to that constituencies are the only ones who are allowed to vote. Then the candidates, along with their party name and symbol(if contesting from a party) is to be fed to the database. This is needed to provide the voters with the list of the candidates in their constituencies specifically and to allow the vote calculation engine to determine the right results. Then the voting lines will be opened only during the voting date window, to give access to the voters to exercise their votes. On a later date, the Election Commission will request for the results from the Vote Calculation Engine that will summarize the results and present it to the Commission. It is then the final duty of the EC to publish the results.

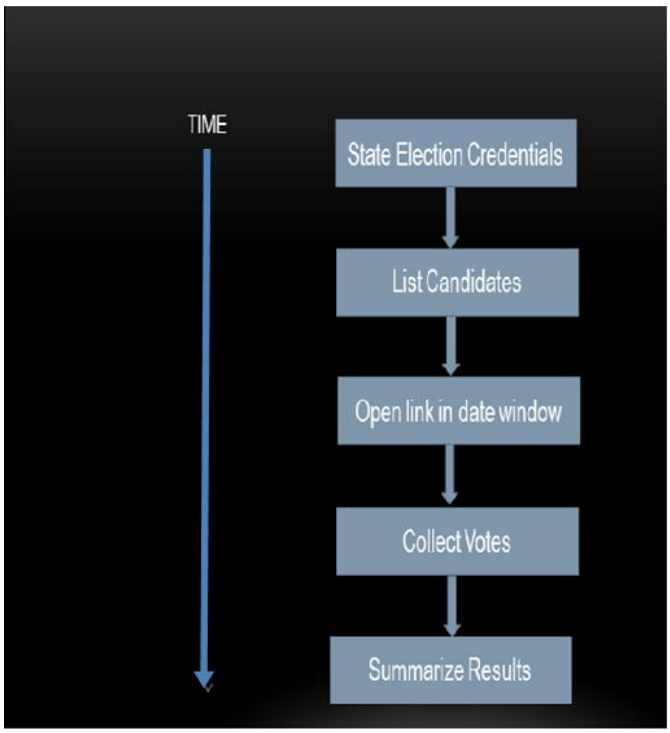

Fig.3:Election commission portal

VII. RESULTS AND CONCLUSION

This product gives easy and secure access to people living in remote places to vote. It uses modern cryptographic techniques such as RSA encryption algorithm which makes it highly secure and preserves the anonymity of the voter. The system has 2 way authentication that makes sure the system cannot be breached. The proposed system is platform independent and the hardware is low cost and affordable, as well as easily portable. The setup and user interaction is seamless and hassle free. As a democratic nation, each and every vote is important and this system helps in increasing the number of votes. The entire system will be deployed on cloud infrastructure and there cannot be any manipulation with the votes. The system is tamper proof and helps in enforcing much better democratic principles.

VIII. REFERENCES

[1]. R. Küsters, J. Müller, E. Scapin and T. Truderung, "sElect: A Lightweight Verifiable Remote Voting System," 2016 IEEE 29th Computer Security Foundations Symposium (CSF), Lisbon, 2016

[2]. N. Kate and J. V. Katti, "Security of remote voting system based on Visual Cryptography and SHA," 2016 International Conference on Computing Communication Control and automation (ICCUBEA), Pune, 2016

[3]. A. Rodríguez-Pérez, "Secret suffrage in remote electronic voting systems," 2017 Fourth International Conference on eDemocracy&eGovernment (ICEDEG), Quito, 2017

[4]. Figure 2:Authentication portal[1]. R. Abdelkader and M. Youssef, "UVote: A Ubiquitous E-voting System," 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, Vancouver, BC, 2012