# E-Voting System based on Mobile using NIC and SIM

Balaji Ghate
Pimpri Chinchwad College of Engg.
Pune, India.

Satish Talewar
Pimpri Chinchwad College of Engg.
Pune, India.

Sanket Taware
Pimpri Chinchwad College of Engg.
Pune, India.

J. V. Katti
Pimpri Chinchwad college of Engg.
Pune, India.

## ABSTRACT
Mobile is emerging technology and center of attraction for worldwide end-user. The proposed system suggest solution called mobile voting application to solve geographical restriction for casting vote and to avoid complexity and standing in a queue for the longer time. The security is an important concern in any voting system. This system provides security by applying the authentication. User's identity issue is solved by secure authentication strategy. The primary goal of authentication is a prevention of any unauthenticated person from duplicating various users. The proposed system uses encryption technique to store the user's information into the encrypted form to achieve a greater level of security. The application protocol consists of three phases. The first phase is voter registration, the second phase is vote casting and vote collecting and the third phase is result phase. For authentication of authorizing end-user, the application generates 4 digit pin from NIC(National Identification Code) and SIM(Subscriber Identity Module). The purposed protocol provides secure and efficient voting approach. Vote Encryption is done using AES Encryption algorithm.

**Keywords**
Encryption, security, Authentication, NIC, SIM.

## 1. INTRODUCTION
Democracy plays very major and crucial role in the development and strengthens of countries like India the future of country goes into the people hands. Who will run the whole country? Once they are elected from the citizen of the country so it is very important to bring transparency, increase participation of voter and avoid the fake voting. Smooth voting and simple way of voting is the actual need to mitigate this requirement. So the mobile voting application provides the techniques to casting the votes through cell phones. The security is an important concern in any voting system. This system provides security by applying the authentication. User's identity issue is solved by secure authentication strategy. The primary goal of authentication is the prevention of any unauthenticated. a person from duplicating various users. E-voting system authentication is done generating by NIC (national identification code). using the user details like name, date of birth, mail and other related information. Unique NIC get generate successfully. When the NIC get to generate the application does the combination of NIC and SIM then it will generate the 4 digit pin number. These credentials will be mail to the user provided the email. The user will login into the system by providing accurate login credentials. It will be authenticated if it is authorized he/she will get the list of nominees and then select one of the nominees whichever he/she wishes to vote. Then the vote will be recorded. Once all the user has cast vote within the time limit given by election commission. Afterward, the counting of voting and the results will be announced. The first challenge in the application is user must have the smart phone or android phone without this he /she will not be able to part of the election process and the second challenge is that once the user has been registered with his mobile number he /she has to cast the vote using the same SIM number. The cause is pin is generated by using SIM number otherwise he/she has to reregister with new SIM number and he/she will get other newly generated credentials. The key characteristics of the proposed system of mobile voting application are as the following.

- **Cost-effectiveness:**
  The application installation and efficient to use and affordable to everybody.
- **Fairness:**
  Until and unless the whole election process gets complete. No one is able to access the election outcome.
- **Integrity:**
  The vote can't be modified, deleted or replaced because it is highly secure using encryption technique.
- **Security:**
  No one is able to understand how voting has been taken placed.
- **Accuracy:**
  Election commission will record the each and every ballots precisely.

## 2. RELATED WORK
Mobile Phone voting is the relative area of development and research to boost the mobile technology. so these are the past existing work related to mobile phone voting application.

K. Hayam has given the mobile phone voting method by applying public key encryption algorithm RSA. The proposed system mainly consists of three stages: access control phase; voting phase and election administrator server phase. The first phase will be responsible for validation and identification of the authorize voter. Voting gets done by encrypting voter data using the RSA as encryption algorithm. Once user cast his vote election administrator decrypt the received encrypted data using the RSA private key. The proposed protocol suffering from online registration and very high computational cost and duplication of communication due to use of RSA encryption algorithm.

Polling System by GSM Facility [2], presents the electronic voting system using GSM mobile technology. When a voter wants to do the voting, then voter send a message to GSM modem. Then the voter which sends the message that contains the voter's mobile id and candidate's id and then GSM

modems receive the votes which are end by a voter and then voting is done.

Smart Device Based Election Voting System Endorsed through Face Recognition [3], provides the online voting system through facial recognition using ADHAR CODE NO verification. Then it fetches the voter's details using its database and then matches it with ADHAR code data and if it matched then only he/she can allow voting.

H. Shaun put approach of GSM mobile [4] phone voting system to cast the vote without a need of registering for voting in initial and going to a polling booth. System strictly prevents the duplicate voting for the security concern. He has not used any cryptographic algorithm used in the system to protect the database from the third party like the hacker.

Y. Qui suggests [5] mobile phone intermediate e-voting system implemented on the extended puller's encryption technique. The main aim of the method is to enforce the cut-of-the choose method to ignore the computational zero-knowledge evidence and will express effectiveness of the system. Proposed application is slightly safe in the simulation-based.

R. Lakhotia has proposed the mobile phone voting system which uses the mobile phone communication in which the GSM authentication used to ensure genuine voter, high security, voter mobility and reduce the public key overhead for registration propose. Voter of particular country will get voter ID for the authentication and identification purposes. To vote voter has to activate their mobile number and only one vote will be cast each and every mobile number. The protocol consists of major three stages: pre-voting and intermediate and post voting stage. Whenever user wishes to cast his/her vote then he/she has to just press the "vote " button and now the base station will instruct the user through to switch off the mobile during the voting process mobile only be reserved for voting. The mobile will not received and incoming and outgoing calls during the election process. Whenever the authentic user cast his/her vote to any nominee through SMS election commission will get notification of India.

Highly Secured Online Voting System over Network presents the online voting system. The people above 18 years old can only give vote by online systems. Then election commission Officer he/she verify candidates. Also here the proposed software works of Ethernet and then allows online voting. Here all users or voters do login by using username and its password and then only he can do vote.

## 3. PROPOSED SYSTEM

To overcame the challenges and weaknesses of the previously existing system. The protocol purposed smooth and simple way of voting which is highly secured. The application is based on the lesson and deep analysis of existing mobile voting system which will contribute to overcame the significant challenges in the existing system. The proposed system consists of following stages.

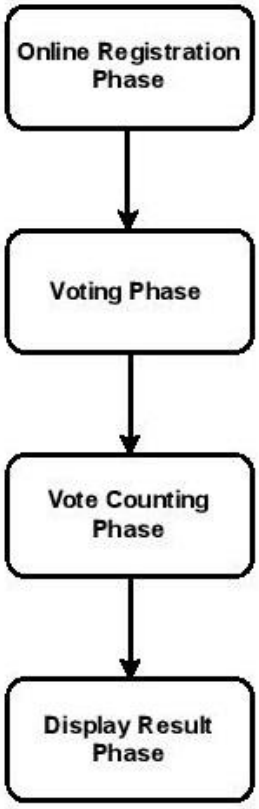



**Fig 1.**

### 3.1 Online Registration Phase

In the first phase of online registration, the candidate or user has to provide his details. The details name, date of birth, email, and other details required for registration along with these all details his SIM(Subscriber Identity Module) code number gets automatically detected by the application. Once the registration process gets successfully complete. The application will send the login credentials to the candidate/user email address which is provided by the end-user while registration. He will get the username and pin as the password to his registered email address. Here the user has to keep this login credentials secure and he/she should not reveal login credentials to any third party. Login credentials are the soul for application

Following are the required steps for online registration.

Step 1:

Voter will enter his/her all registration details.

Step 2:

Receiving this election commission server will encrypt this data.

Step 3:

The server will process this users data and generates unique NIC number for each voter.

Step 4:

The server will retrieve SIM card number from mobile SIM module. If Dual SIM, then from Slot number 1 of SIM Module the SIM card number will be retrieved.

Step 5:

Retrieved SIM card number and NIC number are combined to generate unique PIN for each voter.

Step 6.

NIC and PIN will be sent to voters registered e-mail.

Step7:

Eventually, the server will store encrypted data to a database. In this way, online registration phase will be completed.

Step 8:

Offline registration phase which will be used in case someone registers his/herself on genuine user credentials.

Step 9:

When the genuine user registering his/herself with election commission server, ECS will send registration problem message of can't register through online registration phase and will request his/her to come to ECO for correction of their registration as someone already register his/herself on genuine user credentials.

Step 10:

In such circumstance, a user should go to election commission office. The previous registration will be canceled and a genuine user will be registered by Election commission office (ECO).

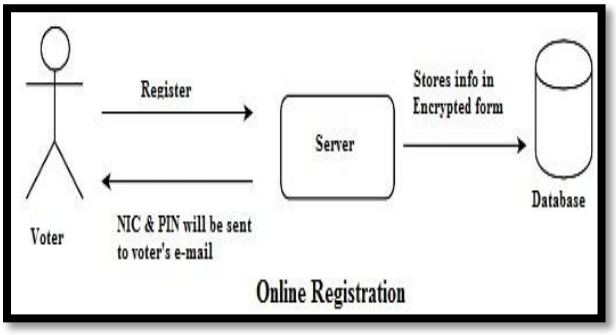



**Fig 2.**

## 3.2 Voting And Collecting Phase

In the second phase of the application, the candidate will be entered into the system. The application takes the whole responsibility that the unauthorized person must not be able to enter into without prior authorization. Once he/she will enter into the main soul of the application there will be a list of nominees who are contesting the election. The user is able to select the anyone nominee then he/she has to simply click/press the vote button to cast the vote for the desired candidate. The vote will get recorded into the system and voting status of that user will get off. it means that particular user can not vote more than once. The application strictly avoids the replication of the vote in order to bring the transparency and avoid the replication of voting which will harm the trust and policy of the application. In this way, a user will enter into the third phase of the application.

### *3.2.1 Login Phase*

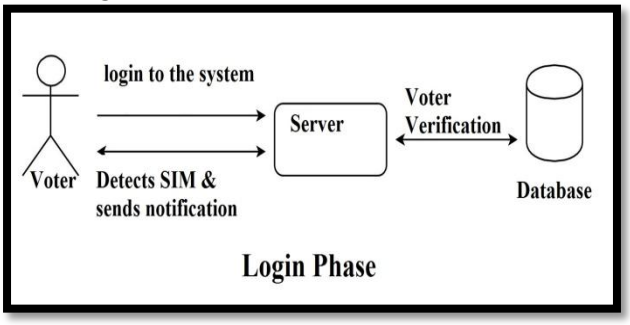



**Fig 3.**

Step 1:

In this first step of the second phase, now during the phase of login as shown voter will log into the system using his NIC and PIN which has been sending to his/her e-mail.

Step 2

The server will detect SIM card number from mobile SIM module. If Dual SIM, then from Slot number 1 of SIM Module the SIM card number will be retrieved.

Step 3:

Verification of voter will be done and for that server will retrieve NIC from a database and merge it with SIM card number and PIN will be formed.

Step 4

The PIN will be compared with the entered PIN by the voter and if it matches then the voter is verified and a voter can vote.

### *3.2.2 Voting Phase*

Step 1:

On the voting day ECS which has the entire authenticated voter list will send candidate list to each voter. This will ensure that the candidate list message only send to the authenticated voter list. This method also prevents the unauthorized voter to cast vote as illegal user will not be receiving this message.

Step 2:

On the voting day after receiving the nominee list, voter will have all nominee list.

Step 4:

In this step voter will select their candidate from the candidate list. After selecting their favorite candidate voter will then encrypt the message with ECS public key, concatenate PIN encrypt both and again concatenate NIC number and send to ECS via SMS.

Step 5:

ECS will NIC number. Then it will decrypt the remaining part with user symmetric key. ECS will mark only the PIN part of the message for the record purposes and to avoid double voting. The remaining encrypted candidate list message will be forwarded to the vote collecting and result phase server.

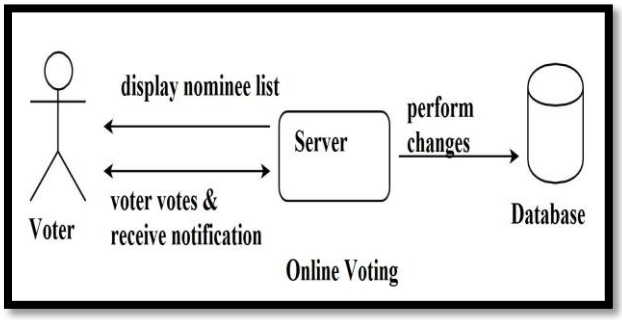



**Fig 4.**

## 3.3 Counting And Displaying Result

In the third phase of the proposed protocol actual process of announcing the result start. The vote will be counted by the system. The application ensure that the every vote should be counted there should be no duplication and any other way which may mislead the result. It has been designed in such way that the application would produce the transparent result.

So that there should maintain balance between the ethics and transparency.

Step 1:

Before the start of the election, time lock mechanism should be implemented on VCRPS. It will keep the vote in encrypted form until the official time of the election ended. Implementing this restriction on this server, the decryption of the votes will be started after the end of the election time. No third party will know the result before the official time ends, thus prevents unfair seeing of the election results. Moreover, anonymity is maintained.

Step 2:

At the end of election time, each vote will be decrypted by using ECS private key.

Step 3:

At the last step of the election process, votes will be counted and the results will be officially announced to the public.

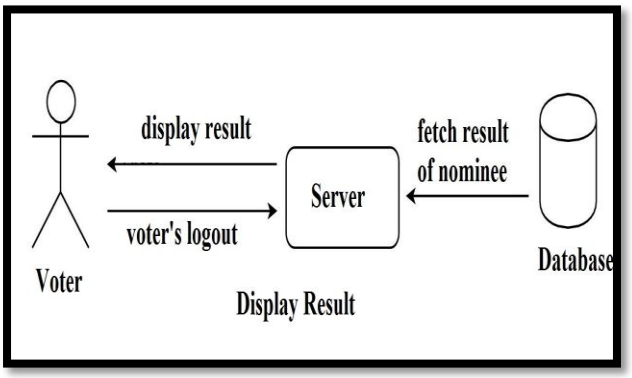



**Fig 5.**

## 4. IMPLEMENTATION DETAILS:

For the implementation of this project the Ionic framework and node JS and Cordova have used. To build the mobile application which will run on the different platform. The team has design application in such way that the application will compatible to all different kind of mobile operating system. To design front end have used the HTML and javascript for input validation. Following are the screenshot of the design application. The screenshot shows the authentication which is strictly checked by system cloud server database. To log in for the vote, a user has to provide his NIC and 4 digit pin for authentication if he provides incorrect details. Login failure takes place.

### 4.1 Login Failure:

Step 1:

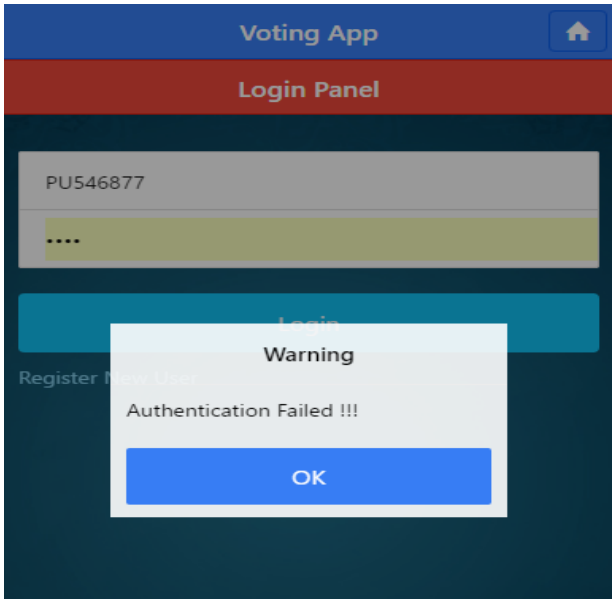
The end user will enter the NIC code as his/her username.

Step 2:

The end user will enter the four digit pin number as password to login into the system.

Step 3:

Database Administrator will match the end user provided username and password. If his/her claim is incorrect then the authentication failure message will be displayed.




### 4.2 Login Successful:

Step 1:

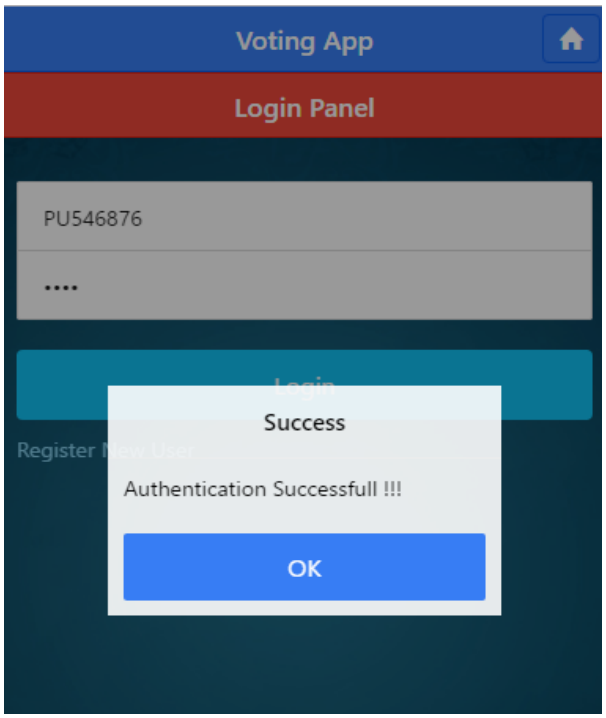
End user will enter the NIC code as his/her username.

Step 2:

End user will enter the four digit pin number as password to login into the system.

Step 3:

Database Administrator will match the end user provided username and password. If his/her claim is correct then the authentication successful message will get displayed.



## 5. PROJECT FUTURE SCOPE

The mobile voting application is suffering from privacy and security issues which are the real challenge in the mobile voting applications. It is very difficult to address these issue. The application provides necessary security feature to contest election process for school and colleges and universities. The future scope will be offline voting through mobile short message service and expansion of application area in democratic government election process developing highly secure and consistency, precise and cost effective solution using mobile technology which will address lengthy, complicated and costly, more time consuming and geographical restriction to cast election process. The more efficient and secure electronic voting system.

## 6. CONCLUSION

The mobile voting system provides many merits as compared to a traditional voting system such as cost, access easily and everywhere, preciseness, quick response, secure and efficient voting protocol as the application uses NIC and SIM info for authentication as well as to cast the vote. The voting process will be easier and restriction of geographic location so the system will contribute to maximizing the participation. It also uses encryption technique to store the user data privacy details which are almost difficult for the third party to decrypt it. The uniqueness of this e-voting system is that NIC is generated using user data and once this NIC used for voting automatically voting status of the user gets disable.

## 7. REFERENCES

[1] Hayam. A. Annie, "E-Voting Protocol Based On Public-Key Cryptography," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[2] Hemlata Sahu, Anupam Choudhary, "Polling System Using GSM Facility", International Journal of Scientific & Engineering Research Volume 2, Issue 10, Oct-2011.

[3] risha Patel, Maitri Chokshi, Nikhil Shah, "Smart Device Based Election Voting System Endorsed through Face Recognition", International Journal of Advance Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013

[4] K. Kim, and D. Hong, "Electronic Voting System using Mobile Terminal," World Academy of Science, Engineering and Technology, pp. 33-37, 2007Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[5] H. Shaun, and A. Choudhary, "Intelligent Polling System Using GSM Technology," International Journal of Engineering Science, vol. 3, 2011Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.