An Assurable E-Voting System That Ensures Voter Confidentiality and Voting Accuracy

Ketaki Bhoyar
Assistant Professor
Padmashree Dr. DYPIEMR
Akurdi, Pune-44.

Pranav R. Patil
Student
Padmashree Dr. DYPIEMR
Akurdi, Pune-44.

Ashish R. Zaware
Student
Padmashree Dr. DYPIEMR
Akurdi, Pune-44.

Arvind S. Pawar
Student
Padmashree Dr. DYPIEMR
Akurdi, Pune-44.

ABSTRACT
The word "vote" means to choose from a list, to elect or to determine. The main goal of voting (in a scenario involving the citizens of a given country) is to come up with leaders of the people's choice.

In our conventional voting system we have problems when it comes to voting. Some of the problems involved include ridging votes during election, insecure or inaccessible polling stations, inadequate polling materials and also inexperienced personnel.

Due to such problems the percentage of voting in India is getting decrease year by year.

This E-voting system seeks to address the above issues. They will able to vote from their places using internet. In this system, assuming that every person has smart phone we will design a smartphone compatible application. In this application we will authenticate the user by its aadhar card number along with biometrics such as face recognition or finger print recognition. After authenticating user will able to see list of candidates. Then the vote of user will be stored on database server. This transmission of data from end user application to database server will be encrypted by using cryptography. For this purpose AES algorithm will be used.

General Terms
Election, Voting, Democracy, Graphical Password

Keywords
E-Voting, Election Commission Server, Election Commission (EC), Database, E-Aadhar, Cued Click Points.

1. INTRODUCTION
The paper addresses the democracy-oriented legal and constitutional requirements that an electronic voting system has to comply with. The scope of this paper covers every election or decision making process, which takes place through voting. Due to mainly the current technological limitation, electronic voting cannot be proposed as a universal means of voting but rather an alternative option and extension to traditional voting means. An electronic voting process must be designed in such a way that it guarantees a general, free, equal and secret character of elections. In a democratic context an electronic voting system should ensure attributes and properties such as verifiability, accountability, security and accuracy. Only then it can foster and promote the participation of the citizens, the legitimacy and the democratic transaction of the election process. E-voting is considered as an alternative capability, which may facilitate the participation of the voters. Taking into account the associated organizational difficulties, a specific registration or declaration that the voter is willing to make use of the e-voting option constitutes neither exclusion nor discrimination using.

2. LITERATURE SURVEY
As indicated by Haijun Pan et al, Authors of "E-NOTE: An E-voting System That Ensures Voter Confidentiality and Voting Accuracy", E-voting framework in view of and enhanced from our past work (Name and vote isolated E-voting framework, NOTE). The proposed E-voting framework, alluded to as Enhanced NOTE (E-NOTE), is upgraded with another convention outline and guard dog equipment gadget to guarantee voter classification and voting precision. This paper also enhances the plan, other than the Election Committee (EC) and Vote Counting Committee (VCC), an unprejudiced outsider, Ballot Distribution Center (BDC), is proposed to assume the liability of conveying polls. The votes and the hopefuls' names are isolated into two sections when the voters cast their votes. The guard dog gadget records all voting exchanges to avoid voter fakes. Author identified with voter secrecy, voter fakes, and voting exactness, accordingly giving a system to reasonable races [1].

According to views of XukaiZou, Author of "Assurable, Transparent, and Mutual Restraining E-voting Involving Multiple Conflicting Parties", E-voting procedures and frameworks have not been broadly acknowledged and sent by society because of different concerns and issues. One specific issue connected with numerous current e-voting procedures is the absence of straightforwardness, prompting the inability to convey voter certification. In this work, we propose an assumable, straightforward, and shared limiting e-voting convention that adventures the current two-party political elements in the US. The proposed e-voting convention comprises of three unique specialized commitments widespread variable voting vector, forward and in reverse shared lock voting, and in-procedure check and authorization that, in mix, determines the obvious conflicts in voting, for example, namelessness versus responsibility and security

versus variability. Particularly, the trust is part just as among counting powers who have conflicting intrigues and will actually limit one another. The voting and counting procedures are straightforward to voters and any outsider, which permit any voter to check that his vote is in reality numbered furthermore permit any outsider to review [2].

Tomasz Truderung et al, Authors of "Clash Attacks on the Variability of E-Voting Systems" says Variability is a focal property of cutting edge e-voting frameworks. Naturally, variability implies that voters can watch that their votes were really checked and that the distributed aftereffect of the race is right, regardless of the possibility that the voting machines/powers are (in part) untrusted. The fundamental thought behind this assault is that voting machines figure out how to give distinctive voters the same receipt. Subsequently, the voting powers can securely supplant tickets by new tallies, and by this, control the decision without being identified. This attack does not seem to have attracted much attention in the literature. Even though the attack is quite simple, we show that, under reasonable trust assumptions, it applies to several e- voting systems that have been designed to provide variability. In particular, we show that it applies to the prominent Three Ballot and VAV voting systems as well as to two e-voting systems that have been deployed in real elections: the Wombat Voting system and a variant of the Helios voting system [3].

Authors Hrushikesh S. Deshpande, et al, explain implementation of AES algorithm based on architecture which gives good performance and consumes less space. Efficiency parameter being most important this method will help us to design our proposed system [4].

Ashwini R. Tonde, et al, Authors of "Review Paper on FPGA Based Implementation of Advanced Encryption Standard (AES) Algorithm", explains the implementation of AES algorithm by software which costs less resources but offers limited security and slowest process. Which is not suitable for our proposed system [5].

Sonia Chiasson, et al, authors of Persuasive Cued Click Points: Design, Implementation, and Evaluation of Knowledge based Authentication Mechanism explains advantage of Graphical password over the knowledge based passwords and biometric passwords. Implementation of such technique for setting the graphical password and using it for authentication is explained in detail in this paper. According to them such graphical passwords encourages user to select more random, and hence more difficult to guess, click points [6].

3. PROPOSED MODEL

This proposed system provides registration of voter, after registration voters will cast their vote and result will display. In this proposed system we are developing a smart phone compatible (Android) application.

Registration will not be part of that application. From that

application, user can login and cast his vote and also can see the results.

For proposed system it required following elements.

(1) Mobile Phone
(2) Election Commission Server(ECS)
(3) Election Commission Databases(ECD)

3.1 System Scope

Process enables voters to cast a secure and secret ballot over the android application. In the framework, an e-voting process may fall in one of the following categories:

(1) Public elections and referenda at state and/or local level.

(2) Internal elections and similar decision procedures.

(3) Privacy Preservation using E-Aadhar No, Email supported OTP and Graphical Password (CCD).

(4) Result Declaration

3.2 Design And Implementation Constraints

Utilizing a Persuasive Cued Click Points as a secret key conveyance the aggressors can figure the watchword in the past graphical secret key plans. Without the framework direction the vast majority of the clients taps on the hotspot in every picture.

In this strategy the framework impact the client to choose more images, furthermore keeps up the client memorability.

In this plan when the picture is shown the haphazardly chosen square called the perspective port just obviously seen out. The various parts of the picture are shaded, so that the client can click just inside the perspective port. This is the means by which the PCCP impact the client to choose the position of the snap point. The perspective ports are chosen by the framework haphazardly for every picture to make a graphical secret key. It will be hard for the aggressors to figure the snap point in every one of the pictures.

3.3 System Phases

(1) Registration Phase

In this phase we will provide the one highly secured Application for registration purpose. After that user have to SIGN IN there and fill its whole information including AADHAR Number, EMAIL & Mobile Number. After pressing submit button, server send one public key to them which encrypt the whole information and send over the server.

During Registration process, AADHAR Number, EMAIL Address and Mobile Number entered by user will be checked under 2 conditions:

(a) Entered value is previously not associated with any other user [i.e. repeating].

(b) Entered value is genuine, for this purpose server will send verification code to email and will scan QR code printed on AADHAR card of user. Where user has to enter correct code in 5 minutes session time.

Then user have to generate Cued Click Point based Image Authentication code, as below mentioned steps:

1. Server will generate many images, from where user have to select one or many.

2. After selecting image user has to set Cued Click Point as a password for voting.

After this a unique E-AADHAR number is allotted to every registered user.

And then server sends data to database server in encrypted format [Encryption algorithm used is AES]. User must have to

keep this key secret. Because this key is required on day of election. Election commission server should keep two updated databases. First database consists of E-AADHAR Number and second database contained email id from the concern authorities for user verification and authentication purposes at the Login time.

(2) Voting Phase

(a) In this phase, EC will send candidate list to authenticated voter according to their constituency on their mobile EVOTEAPP. This will ensure that the candidate list only sent to the authenticated voter. This method also prevents unauthorized voter to cast their vote.

(b) In this step voter will select their candidate from the candidate list. After selecting their candidate voter can vote to Candidate, provided he has to enter all the password associated things properly. Like email, verification code, mobile no., verification code, set and sequence of image, location of cued click point on images.

(3) Result phase

In this phase, EC will send Result on mobile app, after closing of voting time, which will save time also, as it is in auto counting mode.

3.4 System Architecture

An electronic voting process must be designed in such a way as to guarantee the general, free, equal and secret character of elections. In a democratic context an electronic voting system should respect and ensure attributes and properties such as transparency, verifiability, accountability, security and accuracy. Only then can it foster and promote the participation of the citizens, the legitimacy and the democratic transaction of the election process. E-voting is considered as an alternative capability, which may facilitate the participation of the voters. Taking into account the associated organizational difficulties, a specific registration or declaration that the voter is willing to make use of the e-voting option constitutes neither exclusion nor discrimination using.

Election Commission organizes voter registration through its dashboard. This registration phase will not be part of our EVOTEAPP.

This registration process is only for unregistered users. Registered user can directly login inti the application for voting purpose.

All the data of registered user is stored on Election Commission database. The structured form of data i.e. user's general information is stored on database server in the form of tables and the unstructured data such as image for graphical password in cued click point's sequence is stored in EC file server.

After successful login of voter, voter is provided with list of available candidates in his territory only. Candidates from any other territory will not be seen by the voter.

Then he have to select the candidate of his choice and should cast his vote by authenticating through his graphical password. The casted vote is stored on database in form of tables.

Then after completion of Voting period votes are automatically counted by system. And the elected voter will be shown as part of result. On demand a voter is able to see the whole statistics of result also.

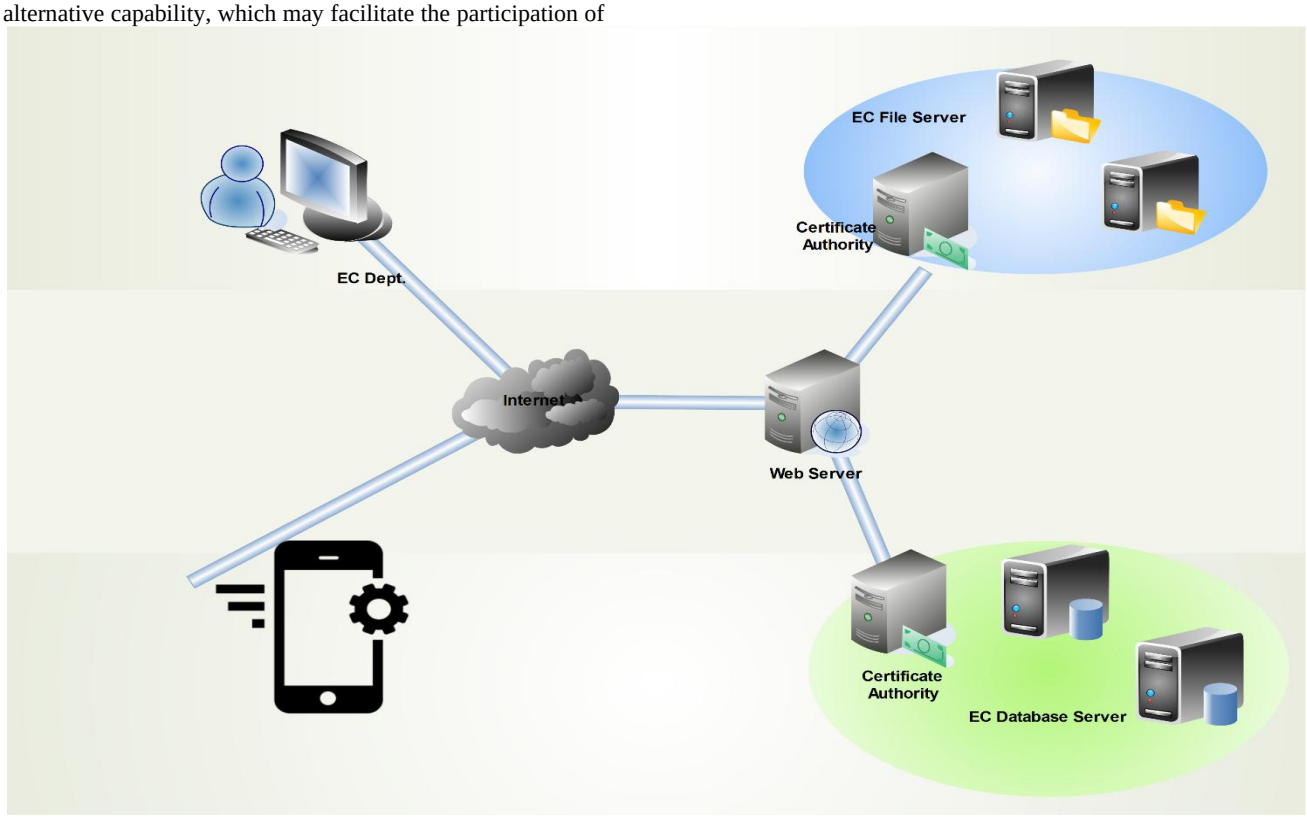

Fig 1: System Architecture.

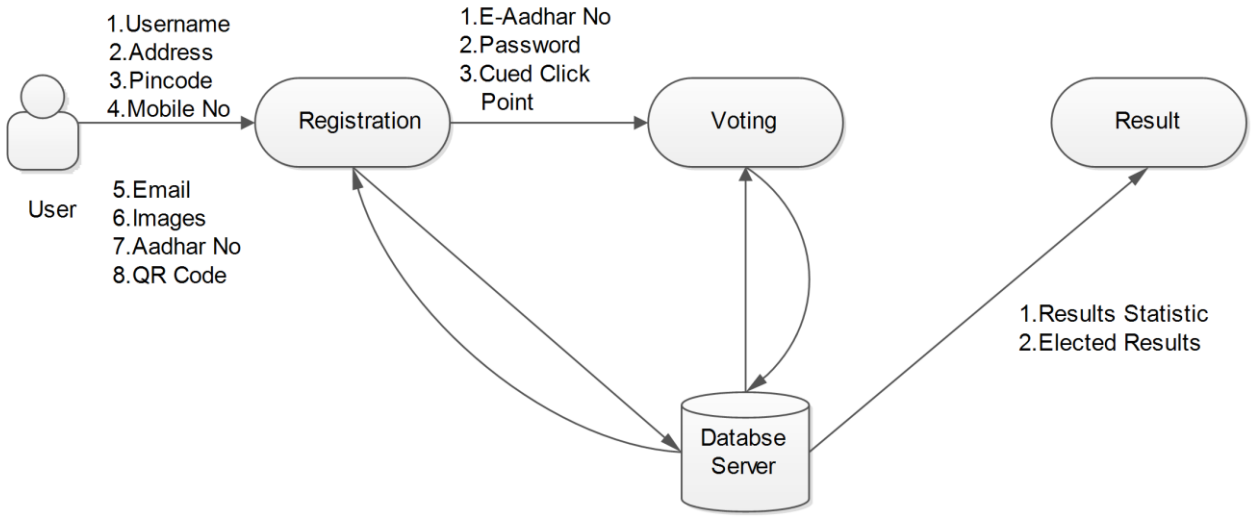

Fig 2: Functional Diagram

4 CONCLUSION

In traditional voting system the percentage of voting is getting low year by year. There are so many security issues also due to which frauds happens in voting system. Thus from this paper we address an e-voting system which will be a highly secure. Through this system a user can cast his vote from any remote location. And hence percentage of voting will increase and fraud also will decrease. Such a highly secure voting system is also very useful in decision making process in any organization.

5 ACKNOWLEDGEMENT

As we know any project has hidden efforts of lot of people. We want to take this opportunity to express our gratitude towards all of them. We would like to thanks our project guide Prof. Ketaki Bhoyar for their guidance.

We sincerely appreciate the inspiration, support and critical advice of our HOD Mrs. P. P. Shevatekar and all the faculty members of DYPIEMR.

6 REFERENCES

[1] E-NOTE: An E-voting System That Ensures Voter Confidentiality and Voting Accuracy , Haijun Pan, Edwin Hou, Senior Member, IEEE, and Nirwan Ansari, Fellow, IEEE 2012.

[2] Assurable, Transparent, and Mutual Restraining E-voting Involving Multiple Conicting Parties, XukaiZou IEEE 2014.

[3] Clash Attacks on the Veriability of E-Voting Systems, Tomasz Truderung and Andreas Vogt, IEEE 2012.

[4] Efficient Implementation of AES Algorithm on FPGA, Hrushikesh S. Deshpande, Kailash J. Karande, Altaaf O. Mulani, PISER 2014.

[5] Review Paper On Fpga Based Implementation Of Advanced Encryption Standard (AES) Algorithm, Ashwini R. Tonde, Akshay P. Dhande, IJARCCE 2014.

[6] Persuasive Cued Click Points: Design, Implementation, and Evaluation ofKnowledge based Authentication Mechanism, Sonia Chiasson, Robert Biddle, IEEETransaction On Secure Computing, Vol 9, No 2, March/April 2012.