Survey on Secure Online Voting System

Smita Khairnar
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune-44

Reena Kharat
Department of computer Engineering,
Pimpri Chinchwad Collage of Engineering
Pune-44

ABSTRACT
This paper aims at creation of secure online voting system providing biometric security. Online voting system used for government elections. Online voting system is publically available system so there are various types of attacks to hack this system. Propose a new secure online voting system by using biometric and steganographic authentication. The vote casting and recording also secure using homomorphic encryption, blind signature to solve the problem of voter votes hacking and destroying system. Here an image based and biometric authentication is used. Use of homomorphic technique encrypts the casted vote stored securely in vote casting and recording server. Also the system is very user friendly. It is reliable system for outside voters.

Keywords
Homomorphic encryption, blind signature biometric security, steganography.

1. INTRODUCTION
Now a day's election process is play a very important role in Indian government. Election is a process to select a perfect candidate for who will lead our nation. In democracy people choose there leader by giving their valuable vote.

Recently used Indian voting system is an electronic voting system, In that system voter availability is compulsory, is the drawback of electronic voting system. So online voting system is the solution for this drawback voter can be voting the candidate for everywhere from specified Election Day and date.

Online voting system security is main concern. In online voting process maintain the strict privacy and uprightness of the vote casted and authentication before the voter is cast their votes. In online voting vote casting transference is also considered. And votes are calculated automatically after election time is released and automatically sort the votes.

In online voting system authentication is the main is problem, only authenticated user is voting for candidate. Only authorize person can give their vote. Person can be authorizing by some methods that can be personal identification number (PIN), secrete message or user identity proof. All authenticated data can be collocated by user. All authentications are verified by main database then allow for that voter. Authentication is verified by biometric identification process.

2. LITERATURE SURVEY
1. Jambhulakar, chakole and pradhi [3] proposed a novel security for online voting system by using multiple encryption schemes. Provide security for cast vote when it is submitted from voting poll to voting server. Multiple encryptions to avoid DOS attack. Security provide submissive as well as active interloper. This system is to take a judgment of certain issues. This paper use cryptography concepts to take pros of digital signature. Encrypting the send forth vote to client server then send to voting server with the help of net. After sending encrypted vote then server side decrypt the vote before counting.
On server side decryption of that vote is done before counting. We require two keys for this purpose one for encryption on voter system, which should be publicly known and second key for decryption of encrypted vote before counting on voting server, this key must be private. So for this purpose we need a pair of asymmetric keys. To provide security from active intruder who can alter or tamper the casted vote when vote is transferring from voter to voting server, we are using digital signature. When a voter cast his/her vote after that he/she will digitally sign on that by using his/her own private digital signature, and send this to voting server, on voting server side that signature is checked by digital signature verifier of that voter which is publicly known. For this purpose each voter should have a private digital signature and a public digital signature verifier, for this we are using a pair of asymmetric keys for each registered voter.

2. Pashine, ninave and kelapure [4] proposed an android platform for online voting system. This application provide diversion of long process also provide security to the voter and its voter comfort system voter no need to go polling booth easily vote for candidate in hometown itself. And also provide the option of gesture recognition but authentication is the problem of android platform.

In this application which is partitioned into three panels on the basis of its users as follows:
Admin Panel: This panel will be specifically used by members of election commission to administer all the electoral processes including registrations of candidates & voters; and monitor all other actions carried out by them.
Candidate Panel: This panel will be specifically used by electoral candidates to interact with the election commission & voters which will help them to work efficiently not only before the election but
also after the election if elected.
Voter Panel: This panel will be specifically used by each individual voter who is eligible for casting his vote i. e. a person ageing 18 years or the above. These are the main users, for whom the application is developed.

3. Khasawneh [2] Proposed An E-Voting System For Biometric Security Is Providing A Two Sided Solution Such As Server And User Side. After Casting The Vote System Will Generate Hardcopy For Voter And Also Generate Unique Number. This Unique Number And Voter Name And Identification Number Is Secured. All Content Are Stored In Special Box This Box Is Secured Box, This Information Is Used For Verifying The Vote Before Stored In Final Database. This Side Copy Is Printed With Unique Barcode That Can Be Easily Readable Automatically And Scanned Then Randomly Choose One Copy, Then This Copy Is Tested

This two sided process providing verification and correctness for the system.

4. Shridharan [1] Implemented a three models such as, Authentication model, franchise excising model, distributed database and central server model. In authentication model voter with smart card and voter identification number and also gives the biometric information this all information is used in future election voting process. After verification and validation voting interface means candidate name and sign are displayed, this is verified by vote casting database, and then votes are counted and declared the result. In this system security and traceability also ensures to auditing the vote and voter information.

In such a system, the correctness burden on the voting terminal's code is significantly less as voters can see and verify a physical object that describes their vote and are allowed to vote in terminal only after their identity is proved. The voters, who cast multiple votes during the process of voting is ensured to be prevented. Also to ensure the maintenance of authenticity, any biometric identification of the voters could be used for accessing the terminal to cast their vote and restricting them to cast again. The process of online voting could be deployed with three phases - the voter registration online vote capturing and the instant online counting and result declaration.

5. Firas I. Hazzaa, Seifedine Kadr [6] This paper deals with the design and development of a web-based voting system using fingerprint in order to provide a high performance with high security to the voting system also we use web technology to make the voting system more practical. The new design is proposed an election for a university for selecting the president of the university. The proposed EVS allows the voters to scan their fingerprint, which is then matched with an already saved image within a database.
Developed Web-based Voting System using Fingerprint Recognition. This system has provided an efficient way to cast votes, free of fraud, and make the system more trustable, economic and fast. We have used Minutiae-based fingerprint identification and matching with high accuracy.

6. Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi [7] Using Cryptography and Steganography at the same time, we try to provide Biometric as well as Password security to voter accounts. The scheme uses images as cover objects for Steganography and as keys for Cryptography. The key image is a Biometric measure, such as a fingerprint image. Proper use of Cryptography greatly reduces the risks in these systems as the hackers have to find both secret key and the template. The basic idea is to merge the secret key with the cover image on the basis of key image. The result of this process produces a stego image which looks quite similar to the cover image but not detectable by human eye. The system targets the authentication requirement of a voting system.

In this paper we proposed a method for integrating cryptography and steganography. The strength of our system resides in the new concept of key image. We are also able to change the cover coefficients randomly. This strategy does not give any chance to steganalytic tools of searching for a predictable set of modifications. Also, considering the complexity of elections, we have provided sufficient proof of authenticity of an individual in form of both biometric measures and secret key.

7. Himanshu Agarwal and G.N.Pandey [8] proposed aadhar id based online voting system for Indian election is proposed for the first time in this paper. The proposed model has a greater security in the sense that voter high security password is confirmed before the vote is accepted in the main database of Election Commission of India. The additional feature of the model is that the voter can confirm if his/her vote has gone to correct candidate/party. In this model a person can also vote from outside of his/her allotted constituency or from his/her preferred location. In the proposed system the tallying of the votes will be done automatically, thus saving a huge time and enabling Election Commissioner of India to announce the result within a very short period.

This system is much secure and efficient than the traditional voting system. Manipulation of votes and delay of results can be avoided easily. A unique AADHAAR identity is the centre point of our proposed model. It leads to the easier verification of both voters and candidates. This AADHAAR Identity number is unique for every citizen or voter of India. This AADHAAR Identity number has been introduced by government of India and this also recognizes the constituency of the voter. But the registration of the voter should be completed only after the verification of all documents by the field officer. The field officer also verifies AADHAAR Identity Number from the main AADHAAR card database. After completing verification, the registration of the voter should be complete and the voter will get auto generated e-mail which has all these information of the voter with the system generated password. The Voter can use this password for login and he/she can also change the system generated old password. Voter can also set the verification keys to ensure security. There should be restriction to use only virtual/on screen keyboard to type password or to change password. Main purpose of using virtual/on screen keyboard is to stop capturing password, if voter changes his/her password from some public place.

8. K. P. Kaliyamurthie1, R. Udayakumar, D. Parameswari and S. N. Mugunthan [9] The aim of this paper is to people who have citizenship of India and whose age is above 18 years and of any sex can give their vote through online without going to any physical polling station. Election Commission Officer (Election Commission Officer who will verify whether registered user and candidates are authentic or not) to participate in online voting. This online voting system is highly secured, and its design is very simple, ease of use and also reliable. The proposed software is developed and tested to work on Ethernet and allows online voting. It also creates and manages voting and an election detail as all the users must login by user name and password and click on his favorable candidates to register vote. This will increase the voting percentage in India. By applying high security it will reduce false votes.

Method for integrating cryptography over network to present a highly secure online voting system. The security level of our system is greatly improved by the new idea of random cover image generation for each voter. The user authentication process of the system is improved by adding both face recognition and password security. The recognition portion of the system is secured by the cover image. This system will preclude the illegal practices like rigging. Thus, the citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy. The usage of online voting has the capability to reduce or remove unwanted human errors.

9. Gianluca Dini [10] This proposed system is based on replication and tolerates both benign and fully arbitrary failures of servers. If enough servers are correct, service availability and security are ensured despite the presence of

faulty servers and any number of faulty voters. A voter that suffers a crash failure can vote after recovery. The proposed service satisfies common voting requirements including voter eligibility and privacy, and tally accuracy. In addition, the service satisfies a further important requirement, namely tally verifiability without any intervention of voters. Anyone, including an external observer, can easily be convinced that the election outcome is fairly computed from the ballots that were correctly cast. It follows that the proposed voting scheme strengthens the security properties of the electronic voting procedure, and simplifies the interaction of voters with the electronic voting system.

4. PROPOSED IDEA

Proposed Architecture is online voting system. In this system there are three models.

i. Voter registration server

ii. Authentication server

iii. Vote recording and casting server.

In voter registration server, voter will be registered personal information and biometric information eg. Thumb Impression. Only registered users are allowing to vote at the time of election. The proposed system is shown in fig. 1.

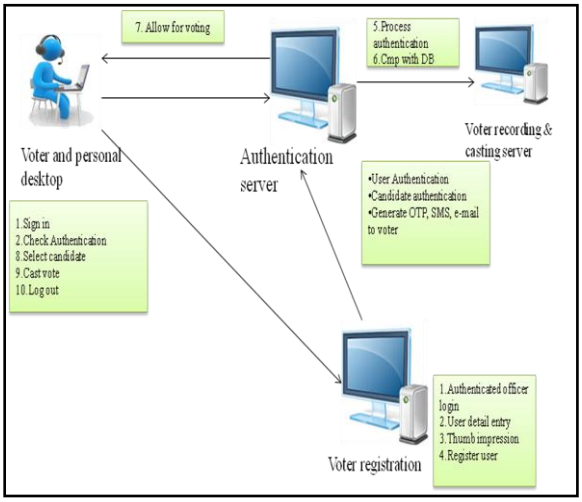

Fig. 1 Architecture of Online Voting System

In proposing system user does registration process first. Send all information to authentication server send password and ID to voter after he/she is login. If it is authenticated then allowing for voting after voter cast his/her vote and this vote is encrypted form stored in vote casting and recording server.

5. CONCLUSION

In this paper different online voting system is technique is studied based on homomorphic encryption, blind signature. From study we proposed a secure online voting system and user friendly system using biometric authentication. In previous system cannot provide casted vote is not stored securely or separately. We can provide security casted vote and only authenticated person is cast their vote. A system provides strong security of the online voters and protects them against various security attacks. It is reliable system for casting votes and recording vote.

6. REFERENCES

[1] Srivatsan Sridharan , " Implementation of Authenticated and Secure Online Voting System", 4th ICCCNT 2013, Tiruchengode, India No.6, July 2013. IEEE – 31661.

[2] Divya G Nair, Binu. V.P, G. Santhosh Kumar," An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation", arXiv: 1502.07469v1 [cs.CR] 26 Feb 2015

[3] Prof. S.M. Jambhulkar, Prof. Jagdish B. Chakole, Prof. Praful. R. Pardhi "A Secure Approach for Web Based Internet Voting System using Multiple Encryption", 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies,2014.

[4] Pranay R. Pashine, Dhiraj P. Ninave, Mahendra R. Kelapure, Sushil L. Raut, Rahul S. Rangari, Kamal O. Hajari," A Remotely Secure E-Voting and Social Governance System Using Android Platform", International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 13 - Mar 2014

[5] Ms. Ashwini Walake, Prof. Ms. Pallavi Chavan," Efficient Voting system with (2,2) Secret Sharing Based Authentication", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 410-412

[6] Firas I. Hazzaa, Seifedine Kadry, Oussama Kassem Zein,"Web-Based Voting System Using Fingerprin Design and Implementation",International Journal of Computer Applications In Engineering Sciences ISSN: 2231-4946.

[7] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A.Barbhuiya, Sukumar Nandi, *"* Online Voting System Powered By Biometric Security Using Steganography*"* Second International Conference on Emerging Applications of Information Technology, 2011.

[8] Himanshu Agarwal, G.N.Pandey, "Online Voting System for India Based on AADHAAR ID", Eleventh International Conference on ICT and Knowledge Engineering 2013.

[9] K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan , "highly secured online voting system over network", 4833 Indian Journal Science and Technology Print ISSN: 0974-6846 Online ISSN: 0974-5645 Vol 6 (6S) May 2013.

[10] Gianluca Dini "Increasing Security and Availability of an Internet Voting System", Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02) 1530-1346/02 $17.00 © 2002 IEEE.

[11] Xun Yi, EijiOkamoto, "Practical Internet voting system", Journal of Network and Computer Applications 36 (2013) 378–387.