Review On Mobility Based Secured E-voting System

Jayshree Gajabe, Mrs. Rashmi Jain
(Computer Science & engineering, Rajiv Gandhi College of Engineering, Nagpur.
Email: jayashree56gajabe@gmail.com)
(Computer Science & engineering, Rajiv Gandhi College of Engineering, Nagpur
Email: rashmil_jain@rediffmail.com)

Abstract:
The objective of voting system is to select the leader from people's choice. In our traditional voting system we have problems when it comes to voting. Some of the problems involved include ridging votes during election, inaccessible polling stations, inadequate polling materials, man power is needed, declaration of result take too much time. Because of such problems the percentage of voting is getting decrease year by year.

So this E-voting system try to address the above issues. candidates will able to vote from their places using internet connection. In this system we assuming that 80% to 90% of people have a smart phone so we will try to design a Smartphone compatible application. In this application we will authenticate the user by its aadhar card number , mobile number or by his/her email addresses. After authenticating user will able to see list of candidates. and user can vote to their favourite candidate ,Then the vote of user will be stored on database server in encrypted formats using encryption algorithm. This transmission of data from user application to database server will be encrypted by using cryptography .

The main aim of the work is to allow mobile users for e-voting . It will verify whether the voting is done by an authorised user or not and provide the vote count after e-voting

Keywords — Election, e-voting, Android app, Web server.

I. INTRODUCTION

Secure E-Voting system based on public-key encryption cryptosystem is proposed in this work. This protocol is summarized in three processes: firstly, access control process which involves the identification and authentication phases for the applied citizens. Secondly the voting process which will be done by ciphering the voter information using public-key encryption cryptosystem, to be submitted over an insecure network to the specified government election server. Finally, the election server administrator will sort the final result by deciphering the received encrypted information using private key. Actually, this E-Voting protocol is more efficient than traditional Voting protocols since the voter can vote from his/her own mobile application without any extra cost and effort. The main aim of the work is to allow mobile users for e-voting with the help of distributed system. It will verify whether the voting is done by an authorized user or not and provide the vote count after e-voting.

II. LITRATURE SURVY

a method to encrypt data which can only be decrypted at specified time this can be useful to encrypt some time sensitive data like bidding offer or electronic vote. They used a combination of public key encryption and hash function to enable decryption only at certain time. But this method does not cover communication between client and server and how to store votes in the database in a secure manner[1].

To protect the confidentiality of the voters, they design a paper ballot that will be teared after people have given a vote. The teared paper ballot then can be used to count the voting result while maintaining voter privacy. Unlike the conventional paper ballot which always have parties and candidates printed on the same order, this method randomized the order, but still can be correctly counted[2].

There are some related research regarding this issues. The overall design of e-voting infrastructure was proposed in this. They built a working ecosystem to deploy a remote voting and ensure its security especially the verifiability to ensure the votes are valid and able to detect unauthorized one. The mechanism was to match several parts of the secure key in some servers[3]. The attack to the verifiability of vote data was given in this. The clash attack was simple since it exploited the voting machine to supply different votes from the same voter. The author provided the countermeasure by using the serial number on printed receipt to Wombat and Helios e-voting systems[4].

Another ballot integrity procedure was proposed by employing entanglement between two parties[5].

There were three phases included: initial, voting, and verification phase. A formal model for both weak and strong verifiability. They proof the proposed model to Helios-C(Helios with Credential) system. However,we propose another system to provide more secure ballot in e- voting environment built on top of our own system[6].

In this system, assuming that every person has smart phone they had design a smart phone compatible application. In this application they had authenticated 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[7].

Technology moulds the life style of human in a promoting manner. We prefer reducing time and efforts in all our chores. One of the systems used majorly for this purpose is ON-LINE where security is the major concern. This paper provides a secure approach for online voting system using the concept of encryption and digital signature. We have implemented the concept of AES and RSA algorithm[8].

The E-Voting means the voting process in election by using electronic device. In this proposed system described how the android mobile phones are efficient and can be used for voting. The android platform is used to develop an application. Our system support simultaneous voting due to the distributed nature of the database. During election electronic device is used for voting process. A voter may only need to register only once for a particular election and that does all, voter need to cast his /her vote without actually have to present at the voting cell. The registration process must be done at Booth application for once then voter is been given a facility to vote from his/her Android mobile phone irrespective of his/her location. This proposed system suppose to propose a new e-voting system, which ensures voter confidentiality and voting accuracy, thus providing an important framework that based on unique identification ADHAAR ID (U-ID) number. An online solution is very useful as the information about the voters and the election committee is also made available to the people in this system[9].

Voting is an important part of the democratic process. The electorate makes a decision or expresses an opinion that is accepted for everyone. Some parts could be interested in the election results deviation without anyone else noticing it. However, ensuring that the whole voting process is performed correctly and according to current rules and law is, then, even more important. We present in this work a review of existing verification systems for electronic voting systems, from both academia and the commercial world. To do so, we realize a fair comparison against a set of representative voting verification systems, by using an evaluation framework. We define this framework to be composed of several properties and covering important system areas, ranging from the user interaction to security issues. We then model the natural evolution of verifiability issues on electronic voting systems, which are influenced by restrictions on current laws and by technological advances[10].

Remote voting has been an active research field for application of cryptographic techniques in the last two decades with many schemes and systems in publication. In this paper we present an overview of recent efforts in developing voting schemes and security models that involve a variety of real world constraints to ensure election integrity. We classify voting schemes based on their primary cryptographic techniques. We analyze recent typical schemes and systems against the basic and counter attack requirements with brief description. Such analysis shows difference among these security requirements and aids in design of future schemes. Our conclusion is provided regarding suitability of a particular voting system/scheme under various conditions[11].

III. ALGORITHM COMPARISON TABLE

Name	Description	Advantages	Disadvantages
RSA Algorithm	RSA is a cryptosystem which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission	1.it is public key cipher 2.RSA algorithm is hard to crack. 3.RSA algorithms the public key to encrypt data.	1.Slow signing and decryption, which are slightly tricky to implement securely. 2.Very slow key generation. 3.Key is vulnerable to various attacks if poorly implemented.
Diffie Hellman	A simple public-key algorithm is Diffie-Hellman key exchange . This protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms.	1.The sender and receiver have no prior knowledge of each other. 2.Communication can take place through an insecure channel. 3.Sharing of secret key is safe.	1.can not be used for symmetric key exchange. 2.can not used for signing digital signatures. 3.the nature of diffie-hellman key exchange does make it susceptible to man in the middle attacks in the exchange.
Digital Signature	DSS is uses the secure hash algorithm a digital signature is an authentication mechanism that enable the creator of a message to attach a code that acts as a signature.	1.Non repudiation, because the author cannot be denied of his work(he created and sent). 2.Imposter prevention Integrity of data, ever change will be detected.	1.Expiry:Digital signatures, like all technological products, are highly dependent on the technology it is based on.
Hash Function	Hash function also called as message digest and one way encryption, are in some sense use no key.	1.the main advantage is syncronization. 2.in many situations, hash tables turn out more efficient than lookup	1.hash collisions are practically unavoidable . 2.hash tables becomes quite

		structures.	inefficient when there are many collisions.

VI. 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. So our proposed 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.

REFERENCES

[1]R.L.Rivest, A. Shamir and D.A Wagner (1996), " Time lock puzzles and time related Crpto", Research Showcase @ MIT.

[2] H. Pan, E. Hou, and N. Ansari (2011), "Ensuringvoters' and candidate confidentiality in E-voting systems*"*, 34th IEEE Sarnoff Symposium.

[3] A. Hassan and X. Zhang (2013), "Design and build a secure e-voting infrastructure," IEEE Systems,Technology and Applications Conference.

[4] R. Kusters, T. Truderung and A. Vogt (2012), "Clash attacks on the verifiability of e-voting systems," IEEE Symposium on Security and Privacy.

[5] H. Alshammari, K. Elleithy, K. Almgren, and S. Albelwi (2014), "Group signature entanglement in e-voting system," IEEE Systems, Application and Technology Conference.

[6] V. Cortier, D. Galindo , S. Glondu, and M.Izabachene (2014), "Election verifiability for Helios under weaker trust assumptions," Computer Security- ESORICS.

[7] Ketaki Bhoyar, Pranav R. Patil ,Ashish R. Zaware ,Arvind S. Pawar (2015), "An Assurable E-Voting System That Ensures Voter Confidentiality and Voting Accuracy," *International Journal of Computer Applications.Volume 132 – No.14, December2015*

[8]Jena Catherine Bel.D, Savithra.K , Divya.M "A Secure Approach for E-Voting Using Encryption and Digital Signature",2015 IJEDR | NC3N 2015

[9]Akshay Akhare A,Manoj Gadale R,Rajashree Raskar S,Bhagyashree Jaykar V,Mrs. D.A.Phalke"Secure Mobile Based E-Voting System", International Journal on Recent and Innovation Trends in Computing and Communication

[10] Jordi Pujol-Ahulló, Roger Jardí-Cedó, and Jordi Castellà-Roca "Verification Systems for Electronic Voting:A Survey".

[11] Huian Li, Abhishek Reddy Kankanala, Xukai Zou ,"A Taxonomy and Comparison of Remote Voting Schemes",