iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3726

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Implementation of Mobility Based Secured E-Voting System

Jayashree Gajabe[1], Mrs. Rashmi Jain[2]
[1]*Student, Computer Science & engineering, Rajiv Gandhi College of Engineering, Nagpur.*
[2] *Lecturer, Computer Science & engineering, Rajiv Gandhi College of Engineering, Nagpur.*

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 favorite 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 authorized 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. LITERATURE REVIEW

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. PROPOSED MODEL

Fig(1).Mobile Voting System

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 be part of that application. From that application, user can login and cast his vote and also can see the results.

Proposed system is divided into the four modules that are

A. Registration Phase

Fig(2). 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 Name Address ,gender & Mobile Number. After pressing submit button, it generate the id and password During Registration process, Mobile Number entered by user will be checked under following conditions:
(a) Entered value is previously not associated with any other user [i.e. repeating].

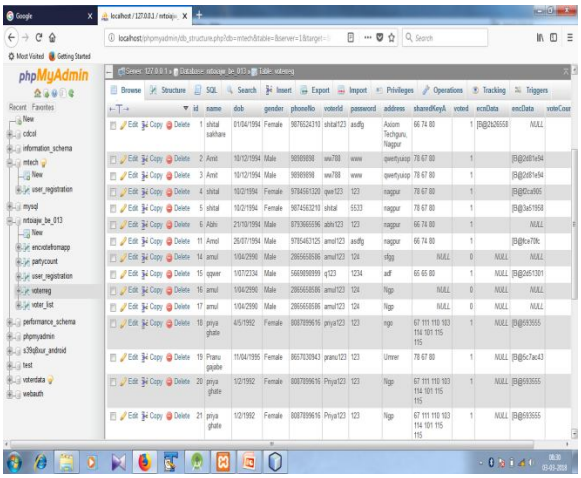
B. Voting Phase

Fig(3). voting phase

In this phase ,user can enter his id and password then the candidate list is provided to the user by administrator then user can cast his vote to his favourite candidate then that vote is converted into the encrypted format for security purpose This will ensure that the candidate list only seen to the authenticated voter. This method also prevents unauthorized voter to cast their vote.

B. Sever Connection And Data Encryption

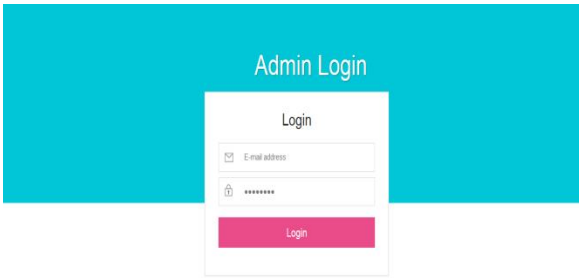
The server connection and data encryption is the second module in this section after the user gives his vote successfully to his favourite candidate the user vote is store in the server side database in encrypted format, for the encryption of user vote we use the encryption algorithms i.e diffie-hellman ,DES and for the connectivity between application and server side database we use the XAMPP control pannel, in server side database complete details of successfully voted candidate list is also available which is shown in following fig.



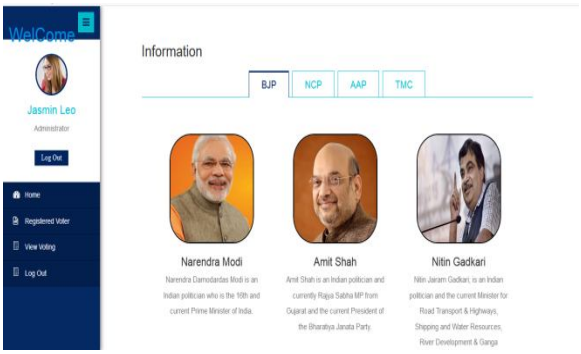
Fig(4). Database Details

C. Data Description And Admin Section.

On other side there is administrator in admin section who can able to count the vote, decrypt the encrypted vote and shows the result to whom user voted and administrator can able to calculate the number of votes after voting time is closed. we also provide the unique ID and PASSWORD to the administrator with the help of id and password only authorized person can login to admin section and handle the complete admin section which is shown in following fig.



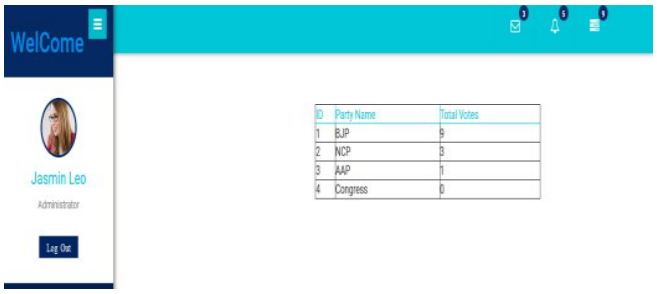
Fig(5). Admin Section



fig(6).Details on admin Section

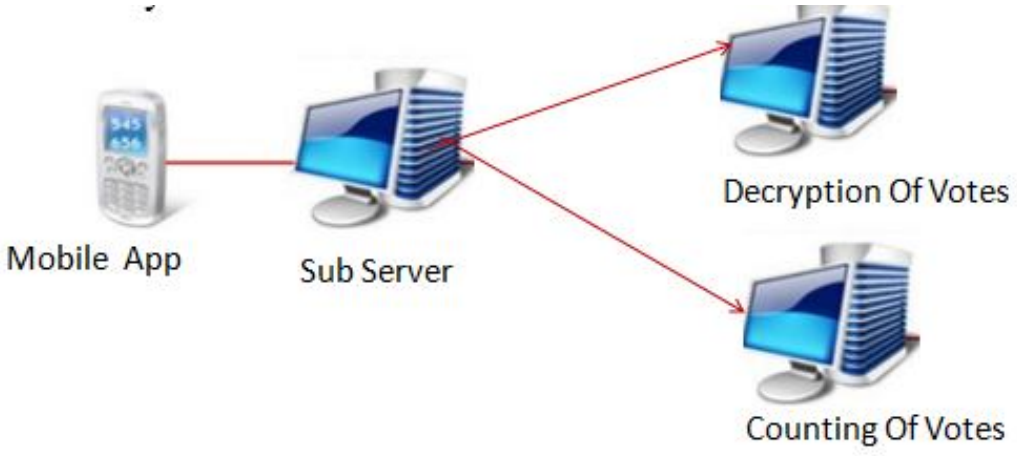
D. Voting Result and Result Analysis

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



fig(7).Result Analysis

IV. SYSTEM ARCHITECTURE



Fig(8). Functional Diagram

above figures show the logical representation of user Registrations and administrative section. we have made the application for the user to register for the vote after the registration the user can login and cast his vote to his favorite candidate .Then user vote is converted into encrypted format for security purpose for encryption we the encryption algorithms . On other side there is administrator in admin section who can able to decrypt the encrypted vote and shows the result to whom user voted and administrator can able to calculate the number of votes. Below is the description of encryption and decryption Algorithms: In this section we are discussing about the proposed algorithm used in our paper for implementing the secured e-voting system. We have used the DES and Diffie hellman algorithm for the encryption and decryption of vote. Diffie hellman algorithm is used to generate the key for the encryption and decryption using DES algorithm.

A. Steps for Encryption

1) Generate public and private keys for sender and receiver using diffie hellman algorithm.
2) Exchange public keys
3) Generate common secret key for Sender using sender's private key and receiver's public key
4) Generate common secret key for Receiver using receiver's private key and sender's public key
5) Send input text i.e. Vote for encryption
6) Encrypt input text using "DES" algorithm.

B. Steps for Decryption

1) Get the encrypted message.

2) Convert it into byte array format.
3) Pass for decryption.
4) Get decrypted output.

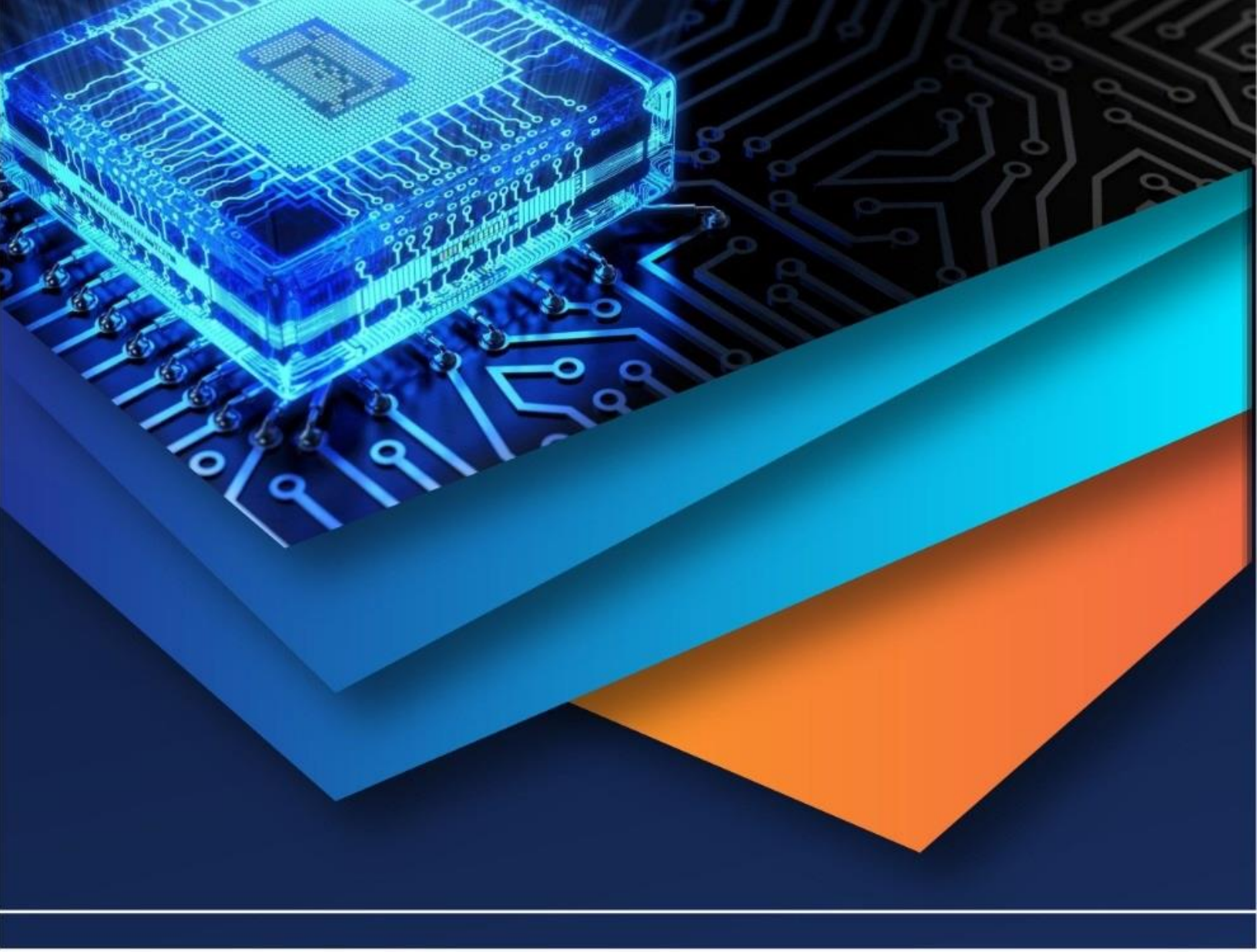
V. CONCLUSION

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

A. Papers

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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY