CHAPTER 38
A Review of Advanced E-Voting Application Using Android Platform

Dr. R. Kannan
Nehru Institute of Engineering and Technology, Coimbatore, India

Dr. V. Jayaraj
Nehru Institute of Engineering and Technology, Coimbatore, India

Dr. M. A. Raja
Nehru Institute of Engineering and Technology, Coimbatore, India

Dr. M. Maheswaran
Nehru Institute of Engineering and Technology, Coimbatore, India

ABSTRACT

The proper execution of democratic rights has become linked to the availability and reliable functioning of advanced information and communication technology (ICT).While modern societies fully reply on ICT for business, work and leisure time activities ,the use of ICT for democratic decision making is still in its infancy Countries all over the World are examining evoting .for it has some striking advantages over traditional paper voting, including security for casting votes, accuracy of counting and analyzing votes, options to conduct voting in a centralized and decentralized manner etc.

Another issue with e-voting is educating the voters. We cannot consider that all the users are computer gurus and they will use the e-voting systems easily. When e-voting is designed it needs to be easy to use. We should consider the fact that a large portion of the voting public has a very little knowledge about the computers. According to some of the research done by the Public Policy Institute of California over 50% of 18-44 years of age voters prefers Internet voting . Some recent studies have focused on e-voting, its security concerns and making it more secure. Below is the list of related literature about e-voting:

Keywords: *information and communication technology , e-voting, California etc*

INTRODUCTION

In traditional elections, a voter usually goes to the voting stations. After direct person-person verification with some IDs, the voter is allowed to vote. The voter is then given a ballot which allows a single vote. Once the ballot is used, it cannot be used again. However, this ballot must also be anonymous. The ballot must identify the voter as being permitted to vote, but not reveal their actual identity, and the voter must also be given assurances of this. Traditional polling methods trust a lot of parties during the election. The current methods require an attacker interact directly with the voting process to disrupt it. There is a greater chance of getting caught as there will be physical evidence in the traditional polling. On the other end, internet is harder to control and manage the security as Network and internet related attacks are more

ISBN: 978-93-5782-920-5, www.aetsjournal.com —Handbook of research in Big data Analytics, Artificial intelligence and Machine learning

difficult to trace. In the traditional polling, you know who is in the election room. Also with the internet or network related voting, from all around the world you will have attackers, not only by the few people in the room . the hierarchy of the voting schemes just discussed Online Another issue with e-voting is educating the voters. We cannot consider that all the users are computer gurus and they will use the e-voting systems easily. When e-voting is designed it needs to be easy to use. We should consider the fact that a large portion of the voting public has a very little knowledge about the computers. According to some of the research done by the Public Policy Institute of California over 50% of 18-44 years of age voters prefers Internet voting . Some recent studies have focused on e-voting, its security concerns and making it more secure. Below is the list of related literature about e-voting.

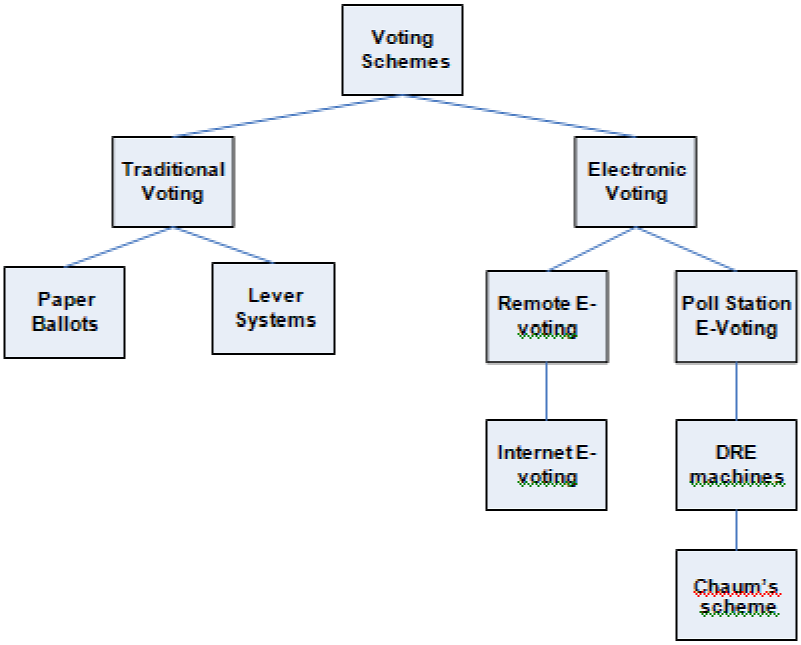

Figure 1: The categorization of the voting schemes .

LITERATURE SURVEY

2.1 O.Kogeda , N.Mpekoa and Alshaher,2014, J.C.Aker,2011 at given that

The goal of this study is to design an efficient and effective prototype that allows Students in universities to instantly cast vote without time limit during the Election period . The Proposed design promotes Reusability through the use of standard services implemented and deployed By employing a platform as a service, Mobile devices are the most Adopted means of communication in developing countries such as Kenya with its penetration higher than that of all other electronic devices put together Therefore mobile devices are considered a good potential alternative for voting platforms and any other activities. Thus a simple prototype application that can be installed on user mobile phones with limited pictures or graphics

2.2 Jameson and Nielsen at given that

The three properties that a good adaptive interface should possess are controllability ,predictability and transparency and obtrusiveness. Controllability

refers to the degree to which users can occurrence of particular actions. Users Should be the ones who make decisions on what a system has to do. Predictability refers to the degree to which users can predict what will happen after they perform certain actions. Transparency refers to the degree that the users can understand the system behaviouror has aclear picture of how a system works. Unobtrusiveness refers to the degree to which users can concentrate on their tasks demands of attentions to interface argues that usability is quality attribute that assesses how easy user interfaces are easy to use .It is defined by five Quality Components.Leamability that is how easy is it for users to accomplish basic tasks the first time they encounter the design ,Efficiency deals with how users can re-

establish proficiency aftera period of not Using the design ,errors that is how many errors do users make, how severe are these errors and how easily can they recover from the errors and lastly satisfaction that is how pleasant is it to use the design.

2.3 Tadayoshikohno,AdamStubblefield,AvielD.Rubin, Dan S.Wallach at given that

Voting Alerts are focused ,timely and relevant emails that keep Voters informed about election dates, important deadlines.ElectronicVoting and Couting technologies pose a challenge to ensuring transparency ,since many visually verifiable steps in a traditional election are automated inside a machine and therefore cannot be seen by the voter and others. In such circumstances, particular efforts must be made to provide transparency in each steps of the process Automated elections mean that people can trust the results because it allows for a process that is so audible ,transparent and secure of course, electronic voting also helps reduce human error.

2.4 Quesenbery,2011 and David Evans at given that

The word usability has become a catch –phrase for products that word better for their users, but it is difficult to pin down just what people mean by it. Is a result software that is usable a process, also called user centered design for creating usable software, a set of techniques, such as contextual observation and usability testing, used to achieve the result; or a philosophy of designing to meet user needs? The different meanings can be described in four key requirements

2.5 David L.Dill,BruceSchneier,and Barbara Simons at given that

Public key cryptography also known as asymmetric cryptography ,is a form of cryptography in which each user will have a key that didn't have to secret .Having this public key will not inhibit the systems secrecy as a message encrypted with the public key decrypted only with the corresponding private key. The private key is kept secret ,while the public key may be widely distributed. The public and private keys are related mathematically. The private key cannot be practically derived from the public key .

2.6 Adam Stubblefield,AvielD.Rubin ,Dan S.Wallach and Tadayoshi Kohno at given that

The encryption algorithm E( ) is homomorphic if given E(x)and E(y)Obtain without decrypting x;y for some operation.In that case,homomorphic encryption is a special type of cryptography in which the sum of two encrypted values is equal to the encrypted sum of the values. In simple mathematics this is equivalent to the communicative property of multiplication .For a majority of cryptographic algorithm ,this doesnot hold true.It is one of the schemes that can be used in E-voting especially to be totally the votes even through the results are encrypted. There are few cryptosystems which uses homographic encryption. They will be discussed in the next section.

2.7 I. Damgard, M. Jurik, J. Nielsonat given that

In Cryptography it is often needed to prove some statement to someone without giving extra information.This is accomplished by zero knowledge proofs .Especially for the authentication systems Zero Knowledge proofs can be used.Forexample,a party might want to prove his identity with secret information and does not want the other party to learn anything about this secret.In other words ,Second party can only known the correctness of the statement or identity of the first party and no more information.

2.8 B.Harris,(2003),A.D.Rubin at given that

In voting systems, privacy and security are desired but are not always simultaneously achievable at a reasonable cost. In online voting sisters , verification is very difficult to do accurately and anonymity is difficult to ensure .This document shows some of the many problems with practical E-voting and why public elections are too important to trust it. When E-voting system scheme is considered there are different Modules involved to consider the security and design .Three important phases of having secure systems are considered as design, development and deployment. In other words, it is important have the foundations in designing a secure and practical E-voting scheme to procedure a secure ,efficient and publicly acceptable implementation of voting scheme in the real world.

2.1. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography, also known as asymmetric cryptography, is a form of cryptography in which each user will have a key that didn’t have to be kept secret. Having this public key will not inhibit the system’s secrecy as a message encrypted with the public key can be decrypted only with the corresponding private key. The private key is kept secret, while the public key may be widely distributed. The public and private keys are related mathematically. The private key cannot be practically derived from the public key. The two main branches of public key cryptography are:

Public key encryption — a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality .

The problem with the public key encryption is the intruder can easily replace the private key with his when the sender requests the public key. This means the newly received public key will have the intruder’s private key and he can easily decrypt the message. To avoid this issue digital signature can be used.

Digital Signatures — a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This is used to ensure authenticity .

Conversely, Secret key cryptography, also known as symmetric cryptography uses a single secret key for both encryption and decryption. It is also known as one-key or private-key encryption. The requirement is the shared secret that both parties should have a copy. In this e-voting prototype shared keys will be used for the users’ encryption in our tests.

2.2. HOMOMORPHIC ENCRYPTION

The encryption algorithm E ( ) is homomorphic if given E(x) and E(y), one can obtain E(x Φ y) without decrypting x; y for some operation Φ.

In that case, homomorphic encryption is a special type of cryptography in which the sum of two encrypted values is equal to the encrypted sum of the values. In simple mathematics, this is equivalent to the communicative property of multiplication. For a majority of cryptographic algorithms, this does not hold true.

It is one of the schemes that can be used in e-voting especially to be able to tally the votes even though the results are encrypted. There are few cryptosystems which uses homographic encryption. They will be discussed in the next section.

2.3. ZERO KNOWLEDGE PROOFS

In cryptography it is often needed to prove some statement to someone without giving extra information. This is accomplished by Zero Knowledge Proofs. Especially for the authentication systems Zero Knowledge Proofs can be used. For example, a party might want to prove his identity with secret information and does not want the other party to learn anything about this secret. In other words, second party can only know the correctness of the statement or identity of the first party and no more information.

2.4. THRESHOLD CRYPTOGRAPHY

Threshold Cryptography is a term used to describe a cryptosystem in which the ability to perform a cryptographic function can be distributed amongst several participants in such a way that only through cooperation of a specified subset of the participants can the operation be performed. In addition, if less than the required number of participants' attempts to perform the action, no useful information can be constructed or obtained. The threshold value is typically denoted by the letter t. In a threshold system as defined here, only t+1 cooperating authorities can perform the desired cryptographic operation.

The essential components of a threshold cryptography system are a key generation algorithm, an encryption algorithm, a share decryption algorithm, and a combining algorithm [5]. First, the key generation algorithm generates the public key parameters, a set of secret key "shares", and a set of "verifier keys". The secret key shares are distributed to the participants in a secure manner. The encryption algorithm provides encryption services for an appropriately-sized message m by applying the public key parameters and an encryption algorithm to generate the cipher text c. The share decryption algorithm is used by each participant with a secret key share to "partially decrypt" the encrypted message c. Each participant also uses the verifier key corresponding to the secret key share to generate a proof of correct encryption. The combining algorithm takes all of the "partial decryptions" or "decryption shares", verifies their corresponding proofs, and combines the decryption shares to reveal the original message m. The combining step only succeeds if t+1 valid decryption shares are used.

2.5. CRYPTOGRAPHIC VOTING PROTOCOL

Basic requirements for electronic voting

- Privacy – All votes should be kept secret

- Completeness – All valid votes should be counted correctly
- Soundness – Any invalid vote should not be counted
- Unreusability – No voter can vote twice
- Eligibility – Only authorized voters can cast a vote
- Fairness – Nothing can affect the voting

Extended Requirements for electronic voting

- Robustness – faulty behavior of any reasonably sized coalition of

participants can be tolerated. In other words, the system must be able to tolerate to certain faulty conditions and must be able to manage these situations.

- Universal Verifiability – any party can verify the result of the voting
- Receipt-freeness – Voters are unable to prove the content of his/her vote
- Incoercibility – Voter cannot be coerced into casting a particular vote by a coercer.

There are four main approaches to efficient and fully secure elections:

- Schemes based on homomorphic encryption
- Schemes based on mixnets
- Heterodox schemes
- Schemes based on secret sharing among several mutually
- distrustful election authorities.

2.6. ISSUES IN SECURE E-VOTING SYSTEM

The issues behind e-voting need to be examined conservatively before such potentially dangerous moves are made. In a voting system, privacy and security are desired, but are not always simultaneously **achievable** at a reasonable cost. In online voting systems, verification is very difficult to do accurately, and anonymity is difficult to ensure. This document shows some of the many problems with practical e-voting and why public elections are too important to trust to it.

When e-voting system scheme is considered there are different modules involved to consider the security and design. Three important phases of having a secure system are considered as design, development and deployment. In other words, it is important tp have the foundation in designing a secure and practical e-voting scheme to produce a secure, efficient and publicly acceptable implementation of voting schemes in the real world.

2.7. COMPLETELY AUTOMATED PUBLIC TURING TEST TO TELL COMPUTERS AND HUMANS APART (CAPTCHA)

Any additional check for the security or spam will decrease the security concerns users have today for the e-voting systems. A CAPTCHA is a program that can generate and grade tests that humans can pass but current computer programs cannot. In our project this is used to confirm that users are trying to vote instead of the automated computer systems. CAPTCHAs have several applications for practical security like preventing comment spam in blogs, protecting web registrations, online polls where you want to make sure that humans are voting not the programs, preventing dictionary attacks, search engine bots, worms and spasm etc. Official Captcha site has published some guidelines for it.

Accessibility: It should be easily accessible for reading the text. If it is a problem due to legal reasons audio CAPTCHA can also be used.

Image Security: Images should be distorted randomly. Without random distortion, application will be open to the attacks.

Script Security: By using this, systems are closed to any computer attacks. However we also need to make sure that scripts used are not easily accessible so that attacker will find the easy way around them to use the systems.

Security Even After Wide Spread Adoption: Some of the sites might be using the sites that have CAPTCHAs setup. It is important that the security level kept the same and these sites are still secure even after a significant number of sites adopt them.

CONCLUSION AND FUTURE SCOPE

The percentage of people those who cast votes are increased since this E-Voting application is available in the play store so that they no need to travel for casting the votes, which is registered in their native. It offers the facility of online voting and saves individuals time while standing in the queue. The transportation charge will be decreased for carrying the Electronic voting machine to pooling booths. To avoid crowd in this pandemic E-Voting system is much more important.

REFERENCES

[[1] Dr.Aree Ali Mohammed and Ramyar Adbolrahman Timour,Efficient E-voting Android Based System, IJARCSSE,vol.3,Issue 11,2013

[2] A.S. Belenky and R.C. Larson, “To Queue or not to Queue?,” OR/MS 27, October 2013, pp. 30-34.

[3] “An Electronic Polling Service to Support Public Awareness Using Web Technologies”, Christos

Bouras, Nikolaos Katris, Vassilis Triantafillou.

[4] “E-voting on Android System” paper (International Journal of Emerging Technology and Advanced Engineering) prepared by : Kirti Autade, Pallavi Ghadge, Sarika Kale ,Co-authors- Prof. N. J. Kulkarni, Prof. S. S. Mujgond, February 2012.

[5] “Electronic Voting,” Encyclopedia of Computers and Computer History, prepared by Lorrie Faith Cranor and edited by Raul Rojas, published by Fitzroy Dearborn, 2001.

[6] “Voting – What is, What Could be,” Caltech/MIT Voting Technology Project (VTP) Report, July 2001.

[7] Java Cryptography an e-book by Jonathan B. Knudsen, First edition May 1998, ISBN:1-56592-402-9