ISSN 2395-1621

Implementation of E-Voting: Using NFC

[#1]Heena Bawalal Naikwadi, [#2]Prof. B. B. Gite.

[#1]heenanaikwadi1@gmail.com,
[#2]bbgite.sae@sinhgad.edu

[#12]Computer Engineering Department,

SAE, Kondhwa Pune,
Savitribai Phule Pune University, India, 411048.

ABSTRACT

Voting is duty of every citizen of this country. But people face so many problems such as fake voting, name not found, don't know the exact place of poll, don't have enough time etc. There are also some political influences over the poling and tendency of people for not voting. Considering all these problems we have come up with a solution. A system with web application as well as android application. Android application is using NFC tags for identification and poling. The vote will be counted accordingly hence the less fraud probability. The web application is for managing all election related activities. Managing date, time and area are some of its main features. It will make elections easier and will increase the voting percentage. An electronic voting (e-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. There are many security challenges associated with the use of Internet voting solutions. Authentication of Voters, Security of voting process, Securing voted data are the main challenge of evoting. This E-Voting system mainly for those people who are unable to come to the voting booth due to on duty leave or the people who are physically handicapped. In voting system there are many processes. This system having main four processes: firstly, application control process which involves the identification and authentication phases for the applied citizens. Secondly, the voting process which will be done by voter information. In Third section confirmation process, in this system check the image captured in application duration and match the image of voter which is online for giving vote for their identification. Finally the election server, administrator will sort out the final result by decipher the received encrypted information using private key.

Keywords: Encryption, Decryption, NFC Card.

ARTICLE INFO

Article History

Received: 18th June 2017

Received in revised form :

18th June 2017

Accepted: 21st June 2017

Published online :

21st June 2017

I. INTRODUCTION

Voting is a process at the heart of a democratic society. Voting schemes have evolved from counting hands in early days, to systems that include paper, punch card, mechanical lever, and optical-scan machines. Internet census takes precautions to prevent people from stuffing the ballot box; they generally do so at the expense of voter privacy. Recent democratic elections using voting machines have shown that the winning margins could be less than the error margins of the voting systems themselves, making election an error prone task. Electronic voting systems provide some characteristic over traditional voting technique. Formerly when elections were made traditionally, organizers determine who is eligible to vote. This may involve a formal registration period or an announcement that anyone who is a member of a certain group as of a certain time may vote. Once the election begins, administrators may validate the credentials of those attempting to vote. This way could involve asking voters for identification cards or passwords. Generally, this procedure also involves keeping track of who has already voted so that eligible voters may vote only once. Moreover, the traditional way of voting generates more constraints; election fraud could be prevented by using physical security measures,

Audit trails, and observers representing of all parties involved. But the prevention of election fraud is made more difficult by the frequent requirement that votes remain private [1]. Contrarily to the traditional way of

voting, electronic voting is essential because it considers ways in which the polling tasks can be performed electronically without sacrificing voter privacy or introducing opportunities for fraud. In order to determine whether a system performs these tasks well, it is useful to develop a set of criteria for evaluating system performance. The criteria to be developed are such as accuracy, democracy, convenience, flexibility, privacy, verifiability and mobility [7]. The aim of this paper is to develop a general prototype system that provides security and trusted electronic voting system.

This system presents a novel e-voting framework that satisfies the security prerequisites of e-voting. The proposed framework is executed on an android mobile phone which acts as a voting machine. The framework utilizes NFC to store all conditions that conform to the rule of the government to check eligibility of voter. NFC is one of these proficient technologies. It is a short range radio communication technology and uses Radio Frequency Identification (RFID).

The software engineering challenges:

i. **Accuracy:**
   It is not possible for a vote to be altered eliminated the invalid vote cannot be counted from the finally tally.
ii. **Democracy:**
   It permits only eligible voters to vote and, it ensures that eligible voters vote only once.
iii. **Privacy:**
   Neither authority nor anyone else can link any ballot to the voter.
iv. **Verifiability:**
   Independently verification of that all votes have been counted correctly.
v. **Resistance:**
   No electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting.
vi. **Availability:**
   The system works properly as long as the poll stands and any voter can have access to it from the beginning to the end of the poll.
vii. **Ability:**
   The system allows any voter to interrupt the voting process to resume it or restart it while the poll stands the existing elections were done in traditional way, using ballot, ink and tallying the votes later.

Problem Background

Electronic voting is an emerging social application of cryptographic protocols. A vast amount of literature on electronic voting has been developed over the last two decades. While e-voting has been an active area of research for the past two decades, efforts to develop real-world solutions have just begun [5], posing several new challenges. The use of insecure Internet, well documented cases of incorrect implementations, and the resulting security breaches have been reported recently [4]. These challenges and concerns have to be resolved in order to create public trust in e-voting. An important step towards streamlining this effort is to develop a framework and identify necessary properties that a secure and trusted evoting system must satisfy to reduce discovery redundancy. Such a framework will allow us to evaluate as well as compare the merits of existing and future candidate e-voting schemes.

Problem Statement

Making the electronic voting system has a security and confidence system by the user, usually user can access to the electronic voting system and voting on the text without security system, that any user can access to the electronic voting system through the ID number for another user and he/she can vote more than one time at the same text, The users could know the result of voting during the process of voting which make the system dicey and mistrust, The user can dominate the result of voting by the access that he or she has of the result before the end of election day

Research Objective

The main objective of this study is: To develop a general prototype system that provides security and trusted electronic voting.

Scope Of Study

The scope of the project is that it will use the ID of the user as the main security to the votes system.

II. 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.

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.

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.

III. SYSTEM ARCHITECTURE

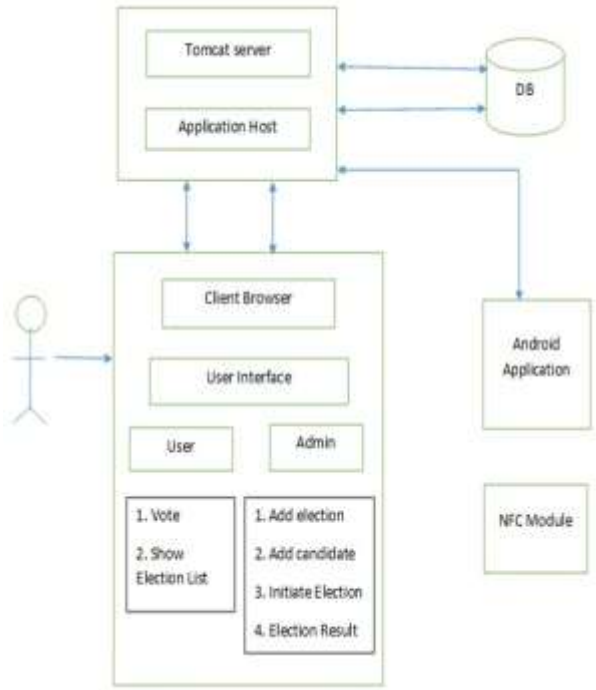

Fig-1:-A simple block diagram of E-Voting system.

IV. MATHEMATICAL MODEL

System Specification:

S= {S, s, X, Y, T, f_{main}, DD, NDD, f_{friend}, memory shared, CPU_{count}}

- **S (system)**:- Is our proposed system which includes following tuple.
- **s (initial state at time T)** :-GUI of Advanced Technique E-Voting using NFC. The GUI provides space to enter a query/input for user.
- **X (input to system)** :- Input Query. The user has to first enter the query. The query may be ambiguous or not. The query also represents what user wants to search.
- **Y (output of system)** :- List of URLs with Snippets. User has to enter a query into Advanced Technique E-Voting using NFC then Advanced Technique E-Voting using NFC generates a result which contains relevant and irrelevant URL's and their snippets.
- **T (No. of steps to be performed)** :- **6**. These are the total number of steps required to process a query and generates results.
- **f_{main}(main algorithm)** :- It contains Process P. Process P contains Input ,Output and subordinates functions. It shows how the query will be processed into different modules and how the results are generated.
- **DD (deterministic data)**:- It contains Database data. Here we have considered Advance Technique E-Voting using NFC NDD.
- **f_{friend}** :- WC And IE. In our system, WC and IE are the friend functions of the main functions. Since we will be using both the functions, both are included in f_{friend} function. WC is Web Crawler which is bot and IE is Information Extraction which is used for extracting information on browser.
- **Memory shared**: - Database. Database will store information like list of receivers, registration details and numbers of receivers. Since it is the only memory shared in our system, we have included it in the memory shared.
- **CPU_{count}**: - 2. In our system, we require 1 CPU for server and minimum 1 CPU for client. Hence, CPU_{count} is 2.

- Identify the processes as P.

S= {I, O, P....}

P= {EV, NFC_auth}

  - EV is E-Voting System.
  - NFC_auth tag for Vote .
  - P is processes.

- **EV= {U, MAX, CV}**

.Where,

  - U= vote as a input Query
  - MAX = {1, 2, 3, … , n}
  - CV is output of vote taken through NFC tag.

- **NFC_auth= {V, DB Techniques, Info}**

Where,

  - V is input which is taken from user via NFC tag given to NFC .
  - DB is use for Storing Votes, showing election results to Admin.

V. ALGORITHM

AES 128 bit Encryption Decryption algorithm :

The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

System will include 2 Roles

Voter

Step 1: Register Voter.
Step 2: Login Voter.
Step 3: call NFC_auth function
  Step 3.1: Home Page.
  Step 3.2 : Show Elections
  Step 3.3 : Vote

Admin

Step 1: Login.
Step 2: call auth function.
  Step 2.1: Home Page.
  Step 2.2 : Add Elections
  Step 2.3 : Add Candidate
  Step 2.4 : Initiate Election
  Step 2.5 : Election Result

VI. OBJECTIVE

The main motto to develop the E-Voting System is to increase a voting count in our country because of only few people are going to voting Centre due to their tight schedule or remote work. So the people can vote from any location in the word with using this system.

The E- Voting System is to make secure with some algorithm and techniques. There is no need go at any voting Centre. Avoid the phishing attackers, decrease bogus voting and provides the security to the system.

Proposed system does not require large scale hardware interfaces only internet connection is needed so easily accessible from any position.

This system is useful for election commission to conduct their elections for different posts. The elections can be conducted easily and effectively in a proper manner with Proper security.

VII.IMPLEMENTATION

The final stage in this approach is the implementation phase. In this phase, user is encouraged to use the system. The new system is transfer to a working environment. This experiment is important and crucial since the efficiency and the functionality of the system can be tested in this phase. Any error with the system can be corrected once the system is being use by the user. Minimal instructions of the system also will be given to the user so that the user can understand the system easily. It is also at this stage that documentation is done in order to put into writing all stages of how the system works. User by reading such document should be able to use the system comfortably.

VIII. RESULTS

A comprehensive system testing is carried out for different modules of system .The summary of the result are shown in table 1.

S/N	Test Case Description	Number of times test carried	Actual Results for correct/wrong		Percentage correct	Severity Average (H-High, M-Medium, L- Low)
			C	W		
1	Login	5	5	0	100	Low
2	Register	4	4	0	100	Low
3	Vote A	5	5	0	100	Low
4	Vote B	7	7	0	100	Low
5	Result	4	4	0	100	Low
6	Search	5	5	0	100	low

TABLE 1: SUMMARY RESULT

IX. CONCLUSION

This system is designed for election commission to conduct their elections for different posts. The elections can be conducted easily and effectively in a proper manner by using this Mobile based voting system using NFC module because the voter can vote from the place where he is working by using this system. It can be converted for public elections and also parliament elections. Proposed E- voting system is very effective and it will be useful for voters in many ways and it will reduce the cost and time. Internet-based voting offers many benefits including low cost and increased voter participation. Voting systems must consider security and human factors carefully, and in particular make sure that they provide voters with reliable and intuitive indications of the validity of the voting process.

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]. Gajendra Singh,Gajendra singh, " A Hyper Modern Cryptography Algorithm to Improved Data Security: HMCA" Vishwa Gupta etal, International Journal of Computer Science & Communication Networks,Vol 1(3), 258-263 258 ISSN:2249-5789.

[6]. Hayam K. Al-Anie," E-VOTING PROTOCOL BASED ON PUBLIC-KEY CRYPTOGRAPHY", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[7]. Xin Zhou," Research and Implementation of RSA Algorithm for Encryption and Decryption" 2011 The 6th International Forum on Strategic Technology, 978-14577-0399-7/111$26.00 ©20111EEE.

[8]. Rasmi P S et al," An Implementation of a New public key System based on RSA which leads hackers solve multiple hard problems to break the cipher" 12th International Conference on Intelligent Systems Design and Applications (ISDA),2012.

[9]. Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[10]. Hussein Khalid Abd-alrazzq1, Mohammad S. Ibrahim2 and Omar Abdul Rahman Dawood 3 "Secure Internet Voting System based on Public Key Kerberos", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012.

[11]. Menezes, A., P. Van Oorschot, and S. Vanstone, (1996), Handbook of Applied Cryptography, CRC Press, pp.4-15, 516.
[12]. I. Branovic, R. Giorgi, E. Martinelli, (2003) "Memory Performance of Public-Key Cryptography Methods in Mobile Environments", ACM SIGARCH Workshop on Memory performance: Dealing with RSA Laboratories, (2007) "What is a Hard Problem. RSA the Security Division of EMC"
13]. Robert Gripentog, Yoohwan Kim, "Utilizing NFC to Secure Identification", 978-1-4799-8679-8/15/$31.00 copyright 2015 IEEE ICIS 2015, June 28-July 1 2015, Las Vegas, USA.
14]. Smita Khairnar, Reena Kharat, " Survey on Secure Online Voting System", International Journal of Computer Applications (0975 – 8887) Volume 134 – No.13, January 2016.
15]. Ms. Tanzila Afrin , Prof.K.J.Satao, " E-Voting System for on Duty Person Using RSA Algorithm with Kerberos Concept", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013.
16]. Oluwafemi Osho*, Victor Legbo Yisa, awale Joshua Jebutu, "E-Voting in Nigeria: A Survey of Voters' Perception of Security and Other Trust Factors", 2015 INTERNATIONAL CONFERENCE ON CYBERSPACE GOVERNANCE (CYBER-ABUJA)