ISSN 2395-1621

Secure Internet Voting System using NFC and Thumb Matching

[#1]Prof. Madhura Sanap, [#2]Madhuri Borkar, [#3]Rohini Deshmukh,
[#4]Ritika Jujgar, [#5]Mrunal Kaware

[1]mesanap.sae@sinhgad.edu
[2]mborkar8@gmail.com
[3]rohinideshmukh246@gmail.com
[4] ritikajujgar@gmail.com
[5] kawaremrunal09@gmail.com

[#12345]Department of Computer Engineering,
SAE Kondhwa (Bk) Pune.

ABSTRACT

In earlier times people were using various systems for electing their representative. But those systems were inefficient and had many drawbacks such as process were very time consuming, location constrained was crucial problem, less secured, laborious work etc. The proposed system "Secure Internet Voting System using NFC and Thumb Matching" resolves all drawbacks of existing system. Important advantage of the system is that less time consuming, secured, location constrained is avoided, accuracy, minimum requirement of equipment's and skills.

Keywords : **Thumb matching, NFC, NFC tag, NFC tag Reader, Arduino, AES, Native similarity, Base 64.**

ARTICLE INFO

Article History

Received: 16th May 2016

Received in revised form :

16th May 2016

Accepted: 20th May 2016

Published online :

25th May 2016

I. INTRODUCTION

This paper has been developed in an attempt to provide an objective introduction to the internet voting system including the information about the voting system technologies into the voting process. In this paper we are going to present the overall structure and working of internet voting process by using NFC and thumb matching. The voting system is improving step by step, advancement in the new system eliminates the drawbacks of the previous system. 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 e-voting. This E-Voting system is mainly for those people who are unable to come to the voting booth due to some reasons.

II. PROPOSED SYSTEM

The proposed system that is "Secure Internet Voting System Using NFC and Thumb Matching" is made intelligent which can give the access to internet voting system to the voter by reading the NFC tag. The authentication is provided by the thumb matching. The vote count is not kept into the same machine itself instead of it is stored in the remote server. System is secured by the encryption algorithms like AES, Base 64 and template matching algorithm like native similarity hence there is no chance of increasing the vote count of machine. Even in case of damage to voting machine there will not be harm to continuity of the election process. This system having main four processes: firstly, application control process which involves the registration and authentication phases for the applied citizens. Secondly, the voter will read his NFC tag by NFC tag reader present on the booth. In Third section confirmation process, the system will match the image of thumb taken from the user and the image which is already saved on system. Finally the election server, administrator will sort out the final result by decipher the received encrypted information using private key.

Now let us take the short review of keywords of proposed system:

A. NFC: NFC is the short range near field communication technologies which allows two hardware's to communicate and exchange data with each other.

B. NFC Tag: NFC tags are data storage tags which can be read or write by NFC device. They typically contain the data of size 96 and 8,192 bytes. It is read only in normal use but it is rewritable.

C. NFC reader: NFC reader is used for reading the NFC tag and sending the information to other device.

D. Arduino: Arduino is a single board microcontroller which is designed by the Arduino software company. The Arduino programs can be written in any programming languages which work as a mediator between two devices.

Algorithms used in this project are as follows:

A. **Native similarity (For template matching):** In our project as thumb matching is used for authentication we are using native similarity (template matching). At the time of voting to check weather authenticated person is voting or not we are using native similarity.

Following are the steps of algorithm:

1) The features for our test will be 25 RGB triples, corresponding to the average of the RGB values on the 25 regions marked in the figure on the left.

2) The image will be normalized to 300x300 pixels. No texture or variance feature will be stored, only the color averages.

3) Each region has 30x30 pixels. Each image will be represented, then, a 25x3 feature vector.

4) To calculate the similarity measure between two images A and B we will take each of the 25 regions, calculate the Euclidean distance between the regions and accumulate.

The distance from A to A will be, by definition, zero. The upper bound (maximum Possible distance between two images, using this similarity measure method) is Calculated as 25*(Math.Sqrt ((255-0)*(255-0) + (255-0)*(255-0)+ (255-0)*(255-0))) or a Little bit over 11041.

B. **AES (For Encryption and Decryption):** As thumb image is used for authentication so to provide security we are using AES (Advanced Encryption Standards). At the time of registration the user uploads the thumb image which is stored in the database in the encrypted format. At the time of voting the system decrypts the thumb image which is stored in the database to match with the recently uploaded thumb image.

Following are the steps of algorithm:

1) The key that is provided as input is expanded into an array of forty four 32-bit words, w (i).

2) Four different stages are used, one of permutation and three of substitution.

3) For both encryption and decryption, the cipher begins with an Add Round key stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.

4) Only the Add Round key stage makes use of key.

5) The Add Round key stage is, in effect, a form of Vernam Cipher and by itself would not be formidable.

6) Each stage is easily reversible.

7) The decryption algorithm makes use of the expanded key in reverse order.

8) Only it is established that all four stages are reversible, it is easy to verify that decryption does recover the plaintext.

9) The final round of both encryption and decryption consist of only three stages.

C. **Base64 (For Encryption and Decryption):** Base64 is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. We are using Base64 function to encrypt and decrypt total count of votes.

III. OBJECTIVE AND SCOPE

1) E-Voting machine is made intelligent which can give the access to internet voting system to the voter to vote the candidate by reading NFC tag and thumb matching.
2) The web based e-voting system is more secure than the present system.
3) The location constraint is avoided in our system.
4) In future we can extend our project to cast a vote using NFC thorough desktop.
5) New encryption algorithms can be applied in future to provide more security.
6) To increase the percentage of voting.

IV. SYSTEM ARCHITECTURE

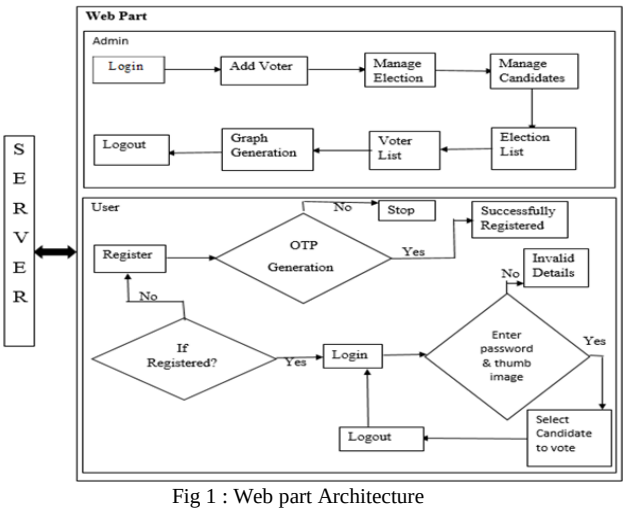

Fig 1 : Web part Architecture

In our system web side and android both can be used for registration and voting purpose but the difference is admin part is given only on the web part and for more security we are using NFC(Near Field Communication).

A. Web part-

1) Admin: Admin is responsible to check and handle all the processes going on. He can perform following functions such as adding voters, manage elections, manage candidates those standing for elections, calculation of votes and display of results.

2) User: User has to go through registration wherein he can fill up his personal information. After entering information, for verification purpose OTP is generated which send on the mobile no. is given by the user. If OTP is valid then the user is successfully registered. If the user is already registered he can go for voting else he has to register himself. Before voting user has to give his password as well as upload thumb image for authentication. If the password and thumb image are same as that of stored in database then the user can cast his vote else he has to go through the process again.

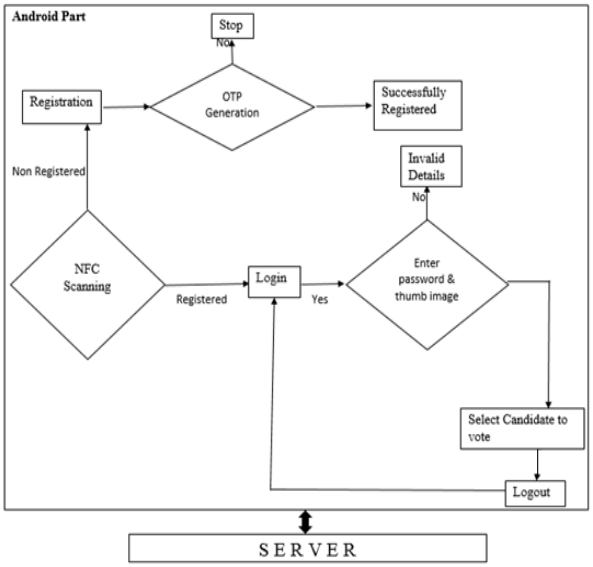

Fig 2. Android part Architecture

B. Android part-

The user must have NFC tag with registered id in it. For voting purpose the user has to scan the NFC tag using NFC tag reader. If NFC tag is not registered with the specific user then he has to go through registration. The registration and OTP generation process is same as above. . If NFC tag is already registered with the specific user then he can log into the system. Voting process on android part is same as discussed above in web part.

V. RESULTS

If the functioning of voting is accurate then it generates a pi-chart and a table. In the table it shows names of candidates standing for election and the number of votes give to each individual as well as the total number of users who casted their votes. The pi-chart, diagrammatically shows the percentile of individual votes to candidates.

Candidate Votes		
Sr. No	Names	No. of Votes
1.	Rahul Jadhav	200
2.	Gaurav Kaware	125
3.	Shubham Jujgar	225
Total		550

Table 1 : Results table

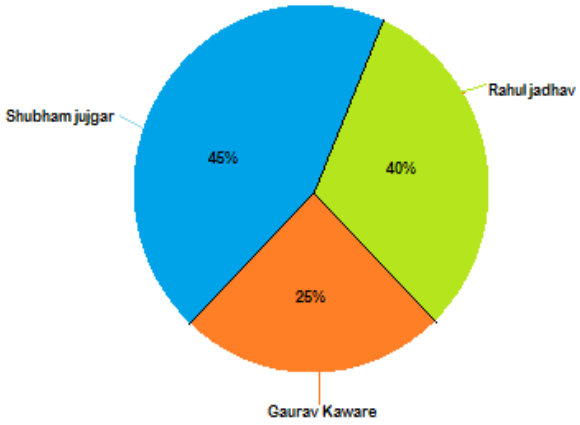

Figure 2 : Results Pi Chart

VI. CONCLUSION

Thus this system can be used for internet voting. The secure web-based e-voting system provides high level of security, authentication, reliability, and corruption-free mechanism. In this e-voting system minimum manpower is utilized, hence mechanism is error free.

REFERENCES

[1] International journal of advance research in computer engineering and technology, Volume 2, July 2013.

[2]Security Analysis of India's Electronic Voting Machines_NetIndia, (P) Ltd.

[3] Hyderabad y the University of Michigan April 29, 2010.

[4]IEEE Transactions of circuits and systems for video technology, Volume 25, April 2015.

[5]IEEE Transactions on pattern analysis and machine intelligence.

[6]R.Mercuri.Explanation of voter-verified ballot systems. ACM Software Engineering Notes (SIGSOFT), 27(5). Also at http://catless.ncl.ac.uk/Risks/22.17.html.

[7]Drip to Chatterjee, JoyshreeNath, SuvadeepDasgupta, AsokeNath "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.

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

[9]Communication Software and Networks, 2010. ICCSN'10.Second international conference.

