Remote Electronic Voting System

Kumsetty Nikhil Venkat
181IT224
Information Technology Department
National Institute of Technology Karnataka (Deemed)
Surathkal, India
nikhilvenkat26@gmail.com

Ankit Gupta
181IT107
Information Technology Department
National Institute of Technology Karnataka (Deemed)
Surathkal, India
ankitgupta6252@gmail.com

Ayush Rahandale
181IT109
Information Technology Department
National Institute of Technology Karnataka (Deemed)
Surathkal, India
ayush22081993@gmail.com

Abstract— **Online Voting System (OVS) Using Cryptography protocols aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow casting of vote from any remote place, the election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct username, password. Our proposed technique is a Terminal based voting system that permits voter to vote independent of location. Security of any information is concerning issue and it very sensitive for Remote electronic voting system. Proposed system does not use any biometric application, without using biometric function authentication of the voter is done. In this system votes are encrypted by RSA encryption algorithm to provide the security. Rivest, Shamir, and Adleman (RSA) encryption algorithm is faster and encryption is done in minimum time. So, it saves the time and improves the performance of system. The proposed scheme is cost effective and at the same time satisfies the security requirements of an online voting system**.

Keywords—Terminal, Cryptographic protocols, RSA

I. INTRODUCTION

The most important aspect of the democracy is the ability of the people to choose their ruler by vote. This makes the electoral process of utmost importance and increasing its requirement to the strictest levels. With the advent of technology, a number of e-voting systems have come into existence. The term e-voting includes several types of voting including when user is casting the vote and the counting of the votes. This technology includes punch scan, optical scan and specialized voting kiosks[1].

II. PROBLEM STATEMENT

One of the methods is that of online voting using internet. Such type of election system are used by corporations and organizations where the members are in a far off location and is also as a substitute similar to postal ballots for voters at different unreachable locations, for general elections in a country.

This system provides security by applying the authentication. User's identity issue is solved by secured authentication strategy.

III. OBJECTIVES

Primary goal of authentication is prevention of any unauthenticated person from duplicating various users. Authentication is handled by very strong Secret sharing methods in system. Secret sharing methods are appropriate for sensitive data storing which are very important. Secret sharing is also called as secret splitting. Secret sharing is technique for assigning a secret between a set of participants. Each participant allocated is part of the secret. It uses t shares out of n no of shares for rebuilding. This system uses the appropriate idea of a new polynomial of degree (t-1) to any set of t points that lie over the polynomial. Line is defined in two points, three points utilized to define a quadratic and cube-shaped curve defined by four points and so on. Means, creation of the polynomial of degree t-1 it gets t points. Method generates a polynomial of degree t-1 with the secret due to beginner coefficient as well as the rest of the coefficients random selected. It searches n points over the curve and gives one to each of the participants. . Once a minimum of t out of the n participants disclose their points, there's decent information to match a (t-1) degree polynomial to them and additionally the start coefficient being the secret.

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys which are a Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private Key is kept private. An example of asymmetric cryptography:

- A client (for example browser) sends its public key to the server and requests for some data.
- The server encrypts the data using client's public key and sends the encrypted data.
- Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So, if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or

2048 bits long, but experts believe that 1024-bit keys could be broken in the near future.

IV. LITERATURE SURVEY

In this paper [1], safe sensor network to observe interaction performance by AES encryption algorithm on the basis of plaintext size as well as value of operation per hop related to the network scale.
In this paper [2] author describes biometric cryptosystem on the basis of AES encryption and decryption. AES is proposed to secure secret information through utilizing iris as a biometric key. Data is original or modified is checked by the CRC.
Author proposed web based internet voting system [3], in that author justifies the protection to vote. Mainly security is needed when vote travel from voting client to voting server. Author strong tools are the concept of number of encryption and decryption.
A new e-voting system is proposed [4] to accomplish protection by e-voting. Provided security is rely on homomorphic property and blind signature method. Embedded system is utilized as voting machine and on that machine proposed system is implemented. All rules of government is stored with use of RFID to analyze voter is eligibility.
Quality of voting system [5] is an important thing to analysis the on the basis of extremely huge elections. This method consists with one drawback such as mix-net addresses ballots including with a duplicate credential. It is possible by increasing electronic watermarking lessening the amount of operations in computing section. Founded same authorized as well as duplicate watermarked ballots and elimination of duplicate watermarked ballots may decreases the amount of ballots within input of mix net Author has ability to utilize algorithm introduced by Walton in JCJ method to assure integrity of ballot and particularly the prop00erty of coercion protection. JCJ method is possible practically if author utilize watermarking and mitigates difficulty of calculating.

V. DESIGN

Pseudo code of RSA algorithm:

1. Generating Public Key
   - •Select two prime numbers p, q.
   - •Calculate n (first part of public key) n= p*q
   - •Assume a value of 'e' such that 'e' is integer; not a factor of n; 1<e<f (n) where f (n) = (p-1)*(q-1)
2. Generating Private Key
   - •f (n) = (p-1)*(q-1)
   - •Private Key d= (k*f (n) + 1)/e for some integer k.
3. Encryption and Decryption.
   - •Suppose the word 'AI': A=1 I=9
   - •Encrypted data c= (19^e) mod n
   - Decrypted data x= (c ^d) mod n where d is the private key.

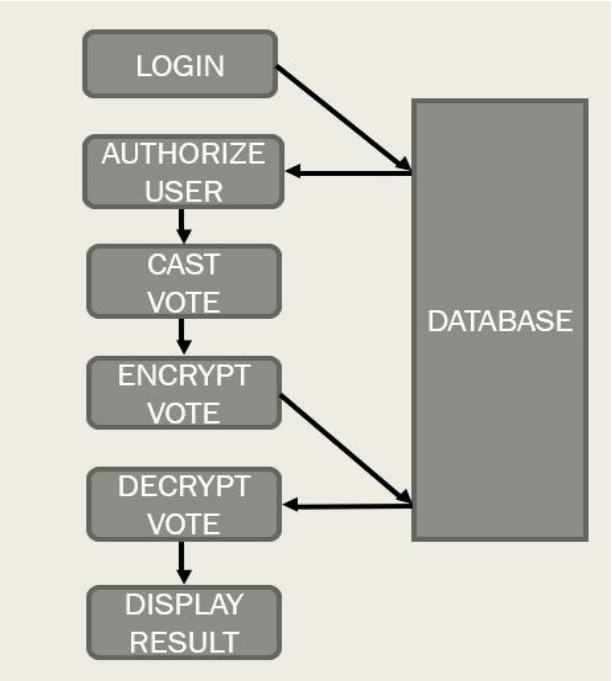

Fig. 1: Block Diagram of e-voting System.

VI. IMPLEMENTATION

A. System Overview:

Our system helps to those organizations which have their Branches in number of cities. Systems main goal is to provide security to casted vote between transmissions from voter to storage server. Our main concentration is to provide security to the data. The Public Key is given to everyone and Private Key is kept private. To prevent passive attack, we encrypt the vote in user's system and further forward it to server through internet. Once voting process is over, decryption of the votes is done. The decrypted votes are then counted. Vote is encrypted by RSA encryption algorithm in the system. As RSA is one of the fastest algorithm it preserves time for encryption ad decryption of process. Voter encrypts casted vote by a key and after that, encrypted vote through his private key and forwarded both to server. Advantage of using this system is that without using digital signature vote is casted and authentication is done.

1. Registration phase
In the registration phase, user register himself by providing personal details of the user. After filling all the personal information, message digest of the voter's data is generated. Then the data is embedded in the server database.

2. Authentication phase
During this phase user will send his share to server. Then server will stack His and user's share to regenerate the data. If match found, user is an authenticated user and will be allowed to cast his/her vote. If match not found permission is denied to cast the vote.

3. Voting phase
In this phase ballet will be open only to the authenticated user. User will cast his/her vote. The casted vote is encrypted using RSA and then stored in the database.

4. Counting phase
Counting phase starts with decryption process of all encrypted votes. Once decryption of all votes is done counting starts. After end of counting votes results are announced. RSA algorithm is easy to deploy and requirement of processors has low cost as well as less memory is needed.

VII. RESULTS AND ANALYSIS

A. Results and observations:

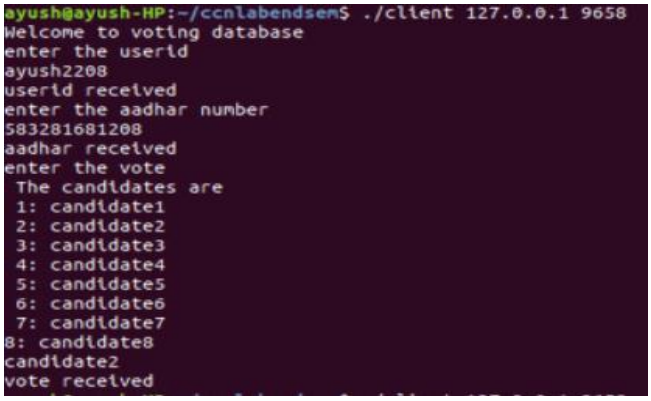

Fig. 2: Output displayed at the client1

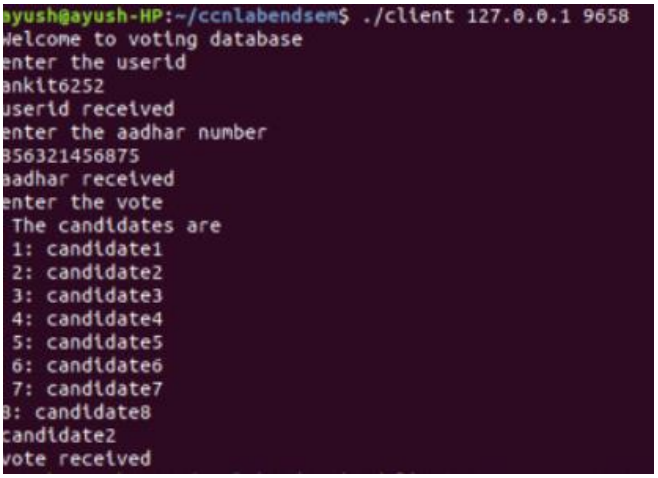

Fig. 3: Output displayed at the client2

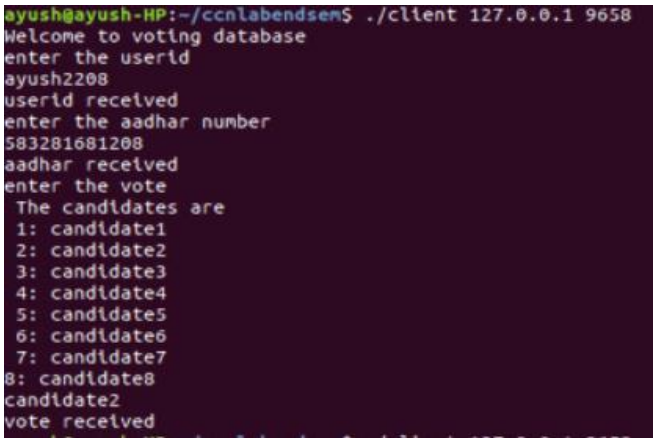

Fig. 4: Output displayed at the client3

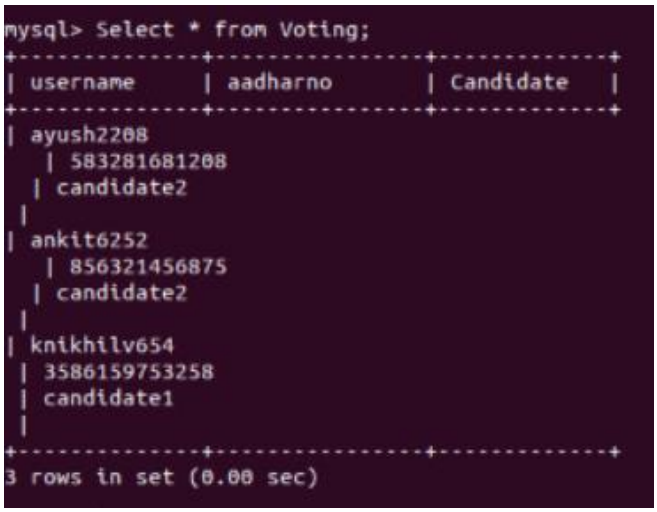

Fig. 5: MySQL database 'Voting'.

Fig. 6: Output displayed at the server.

B. Analysis:

The proposed remote e-voting system provides number of benefits such as increasing numbers in voter as well as minimum cost for setup election procedure. When system offering benefits along also give security. The proposed system effectively provides enhanced security in online voting system. This system has a vital issue in process and it is prevented by implementing robust security by authentication. Secure authentication is implemented by utilizing encryption algorithm. RSA algorithm is implemented to provide stronger security by encrypting the votes. Proposed system takes less time as it is using visual cryptography and RSA algorithm.

VIII. CONCLUSION

The developed system describes the essential security properties of remote electronic voting systems. It is aimed to design and implement a real application for an electronic voting system for an organization. It satisfied the important properties such as security, verifiability, authentication, integrity, efficiency and robustness, saves money, time requirement. The opportunity of casting an individual's vote using one of the most convenient medium among the e-voting remotely is observed in this system. The adoption of the integrated system increased the level of participation in the institution because of the ease of voting and its tendency to eliminate electoral fraud such as vote rigging due to denial of service (Dos/DDos) attacks, SQL injection. More rudiments to be focused on biometric technology to capture the real identity of the voter and broaden the security requirements of non-repudiation.

REFERENCES

[1] Hyubgun Lee, Kyounghwa Lee, Yongtae Shin, "AES Implementation and Performance Evaluation on 8-bit Microcontrollers", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009.

[2] R. Jubiya, M. Keirthi, M. Anupriya, A. Muthukumar," IRIS Authentication Based On AES Algorithm", Volume 3, Special Issue 3, March 2014.

[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.

[4] Hussien, H., Aboelnaga, H., "Design of a secured e-voting system", Computer Applications Technology (ICCAT), 2013 International Conference on Date of Conference: 20-22 Jan. 2013.

[5] Souheib, Y., Stephane, D., Riadh, R, "Watermarking in e-voting for large Scale election", Multimedia Computing and Systems (ICMCS), 2012 International Conference on Date of Conference: 10-12 May 2012.

[6] https://en.wikipedia.org/wiki/Electronic_voting.

[7] Rahil Rezwan, Huzaifa Ahmed, M. R. N. Biplob, S. M. Shuvo, Md. Abdur Rahman "Biometrically Secured Electronic Voting Machine", 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC).

[8] D. Ashok Kumar, T. Ummal Sariba Begum," Electronic Voting Machine – A Review", Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012.

[9] Shashank S Kadam, Shashank S Kadam, Sujay Dandekar, Debjeet Bardhan, Prof. Namdeo B Vaidya, "Electronic Voting Machine with Enhanced Security", Proceedings of the International Conference on Communication and Electronics Systems (ICCES 2018).

[10] Afrina Ali, "Is Bangladesh going for e-voting?", [Online] 06 February, 2017. [Cited: 4 August, 2017.] Available:http://www.thefinancialexpressbd.com/2017/02/06/61143/IsBangladesh-going-for-e-vote [Accessed 04 August 2017]

[11] Remmert, M. (2004): "Toward European Standards on Electronic Voting", The Council of Europe [accessed 23 March 2017]

[12] Bhuvanapriya R., Rozil Banu S., Sivapriya P. and Kalaiselvi V. K. G., "Smart voting" , 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, 2017, pp. 143-147.

[13]ArduinoWebsite http://arduino.cc/en/Main/arduinoBoardUno[accessed 8 August 2017]

[14] "GT-511C3 datasheet" [Online] Available: https://cdn.sparkfun.com/datasheets/Sensors/Biometric/GT511C3_datasheet_V2.1_20161025.pdf [Accessed 10 August 2017]

[15] "Product GT-511C3" [Online] Available: https://www.sparkfun.com/products/11792 [accessed 08 August 2017]

[16] "Fingerprint Scanner-TTL" [Online] Available: https://github.com/sparkfun/Fingerprint_Scanner-TTL [accessed 10 August 2017]