Secured Aadhar Based E-Voting Application using RSA

B.Bhaskar Rao, P.Chandra Sekhar, V. Sunil Kumar, K. Sandeep Varma

Abstract: ***The invasion of wireless, mobile phones and various internet technologies has resulted in the new implementation, making the e-voting method very quiet and effective. The E-voting ensures the option of a suitable, simple and secure manner of incarceration and the complete number of votes in an election. This study work offers the e-voting requirements and necessities using a platform based on Android or the internet. E-voting implies voting through electronic devices or websites in the election. An e-voting application is developed using the android or web platform. This request enables the user cast the ballot without going to the polling booth. To prevent fraud respondents using the scheme, the application utilizes adequate authentication steps. Once the polling process is completed in the electronic device, the outcomes can be obtained in a fraction of seconds instantly. All voting counts of applicants are encrypted using RSA and stored in the database to prevent third-party attack and disclosure of outcomes. Upon completion of the meeting, the admin can decrypt the count of votes and publish the outcome and finish the voting process.***

Keywords: ***E-voting, RSA, Encryption, Decryption.***

I. INTRODUCTION

Voting is the process of selecting candidate from the group of people or from states or with in a country. The elected candidate will make a collective decision with help of members, who are also elected by the people. The voting can be in different ways, one can be done in paper ballots and without a paper (online). By using paper ballots one has to visit the polling station booth to cast his vote by standing in the queue. For this process one has to provide security and infrastructure to conduct the peaceful elections. There are chances for rigging and the corruption. In present elections, only 62% of the people are participating in the voting and remaining are busy in jobs, business and other works. The voting process can be increased with help of online voting (E-voting).

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Dr B Bhaskara rao*, Associate Professor in Department of CSE, Gitam University.visakhapatnam, Andhra Pradesh,India

Dr P.Chandra Sekhar, Associate Professor in Department of CSE, Gitam University . visakhapatnam, Andhra Pradesh,India

V. Sunil Kumar, Assistant Professor in Department of CSE, Gitam University . visakhapatnam, Andhra Pradesh,India

K.Sandeep Varma, Assistant Professor in Department of CSE, Gitam University . visakhapatnam, Andhra Pradesh,India

Now a days the Indian government agencies are using Electronic Voting Machines ("EVM") to cast the vote in the place of paper ballots. For this procedure the also the voter has to visit the election booth and has to stand in the queue for the hours to cast his vote.

In this Conventional election process, there is possibility of calculation of errors and fraud. The technology is growing very rapidly and everyone is aware of the technology by using simple android mobile devices and other laptops. These devices became ubiquitous and affordable. With help of these conditions one can propose an Electronic voting (E-voting) system using android and web platforms. With help of E-voting, Voters got an opportunity to cast their vote easily and quickly from anywhere in the country. The counting process can be finished in secure manner.

E-voting is secure because the casting votes are transmitted and saved in the encrypted form and anonymized form. In order to provide security one can implement the cryptographic algorithms to safe guard the data. Out of all algorithms, the RSA (Rivest- Shamir Adleman) is the best to provide the security. The RSA is asymmetric cryptographic algorithm which is used to perform different encryptions and decryptions techniques using public keys and private keys. This algorithm provides a high security then other symmetric algorithms. This algorithm is resistant to different types of attacks including brute force technique.

This application is purely used to cast the vote from mobile device or any other device which is connected to the internet. This E-voting can be done using portable electronic device with help of RSA algorithm.

II. RELATED WORK

In March 2000, using the private company votation.com, the Arizona Democratic Party ran its presidential primary over the internet. Each registered party member got in the mail a personal identification number. Citizens had an alternative to cast their votes at a specified place or online to select their candidate from their own home convenience. Voting electors who cast their ballot online must require a PIN and one must answer the private questions provided during the registration period. If the data is true, then in the upcoming election one casts the ballot. Estonia had the ultimate innovative to exploit the Internet voting system in 2009. Every citizen in Estonia has a unique national ID card that is used to define the country's citizen.

In Estonia elections, the ID card is used to provide safety, ensuring accuracy in votes and system. Security administrators said the current scheme has no problems. They have not found in the scheme the single fraud or tampering.

A research of internet voting in two Swiss constituencies in 2017 discovered that it had no impact on participation based on the proportion of votes and on peaceful conduct of elections. By eliminating inequalities, a paper on "remote electronic voting and turnout in Estonian parliamentary elections in 2007" showed better outcomes. E-voting helps digitize the technology, with the assistance of which a big proportion of the greater socioeconomic groups took part in the election. People who have lived far from the state can cast their votes from any place resulting in the proportion of votes being increased. These individuals are extremely trained and technology-conscious.

III. BACLGROUND

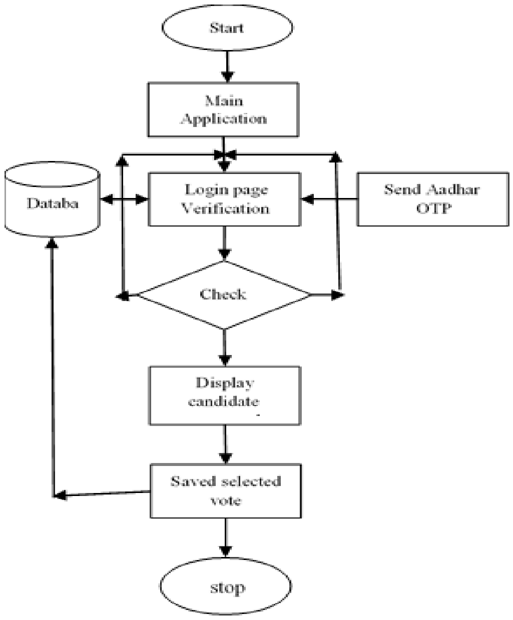
In traditional electronic voting system, the citizens of the nation use ballot papers to cast the vote. In this system the illiterate people can cast their vote easily without prior training. In this procedure, one need an infrastructure like ballot papers, ballot boxes, small room, chairs, electric fans, transportation and security. All these preparations are done by using manpower. To arrange all these things, one need a proper planning in advance and it is time consuming process. In this process the results cannot be declared instantly because all the ballot boxes have to be collected from all the remote locations. In this process the citizens have to stand in the queue for long time to cast their vote. To stockpile the ballot boxes, one need a lot of space with highly secured concrete buildings for few days till the results are announced. The above are the drawbacks in traditional system. In electronic voting system one can remove the all the procedures, partly can remove the security and infrastructure.

In this method, all the citizens need an electronic device or laptop or an electronic device or any other device which supports internet facilities. Every citizen having electronic gadgets has a part of their life and such device are not burden or expensive to the government to conduct the E-voting smoothly. Every citizen cast their vote using a simple android application or web application by providing flexibility, portability, privacy, security and accuracy. It can be done easily without disturbing their private life or job profile or business life at any time. This can be done by designing an unpretentious software interface which is understandable to a common man which includes self-description. In order to cast the vote one has to register with national ID or social security number or aadhar number, Voter ID number and a mobile number and the registration includes password and user id. Using the user id and password one has to login the application selects the party symbols which is given against the candidate’s name and the after this step, one has to click the submit button to cast the vote. Electronic voting can be characterized in 4 phases that embrace the e-commerce, individual verifiable, trust authority and universally verifiable, these classifications are presented on the basis of security, privacy and trust [6].

In case of electronic commerce, security is guaranteed to communication network only and no security for voter privacy, stuffing ballot box and vote tempering. In case of trust authority, voter privacy, integrity and tempering are preserved. In present system individual citizen is verifiable, system software is intelligent and secured. It validates every citizen, who are going to cast their valuable vote [8]. Software developers and researchers are employed parallel for developing this application from the past twenty years. Finally, the built an application which are use useful to the real world. Identification of citizen can be verified by using aadhar or social security number or any other national id by using the biometrics. These biometrics are very good in identifying a person uniquely. There are still some small issues in electric voting that include implementation, insecure internet, and security.

IV. PROBLEM STATEMENT

Indian elections, electronic voting machines ("EVM") are used. In Indian local, state and general (parliamentary) elections, EVMs have substituted paper ballots. There have been previously claims about the tamp arability and safety of EVMs. The present scheme has several unresolved problems. A candidate may understand how many individuals voted for him from a polling station. This is an important problem, especially if lop-sided votes are cast for / against a candidate in individual voting stations and the winning candidate may demonstrate favoritism or grudge over particular fields. Although there is a simple and unconditionally secure protocol to do this, the control units do not electronically transmit their results back to the Election Commission. Indian EVMs are intended as stand-alone units to avoid any intrusion during the transmission of outcomes electronically. Instead, in the presence of candidates ' polling officials, the EVMs are gathered in counting stations and tallied on the allocated counting day(s). Our suggested scheme can overcome all these vulnerabilities.



V. RIVEST SHAMIR ADLEMAN (RSA)

One of the first public-key cryptosystems, RSA (Rivest–Shamir–Adleman) is widely used for secure data transmission. The encryption key is public in such a cryptosystem and is different from the secret (private) decryption key. There are four steps in the RSA algorithm: important generation, important allocation, encryption, and decryption. RSA have fundamental principles that are found with modular exponentiation (m) three very big positive integers e, d, and n.

A. Key Generation

RSA's most complicated aspect is the key generation algorithm. The key generation algorithm's objective is to produce both public and private RSA keys. Sounds pretty easy! Weak key generation, unfortunately, makes RSA very susceptible to attack. So it's got to be done right. To encrypt the plaintext signal, the RSA algorithm uses a public key (e, n). RSA uses personal key (d, n) to decrypt the cipher text. The formula below for calculating Cin is cipher text and Mes is plaintext.

B. Key Distribution

Suppose A wishes to give B data. A must understands B's public key to encrypt the message if they decide to use RSA, and B must use its personal key to decrypt the message. B transmits its government key (n, e) to A via a secure but not necessarily secret route to allow A to transmit its encrypted emails. The personal key (d) of B will never be allocated.

C. Encryption

- Assume that the sender wishes to send a text message (Mes) to a person whose government key is (n, e).
- The sender then displays the plaintext as a sequence of numbers below n.
- First plaintext P encryption, which is a module number n. Simple mathematical move is the encryption method as Cip= (Mes)e mod n• Cip (Ciphertext) is encrypted text. Before encryption, plaintext is what you have, and cipher text is the encrypted outcome.
- Mes is the plaintext converted into Numeric code.
- The value of e and n is a public key pair generated through the process of key generation.

Here are the following RSA encryption flowchart shown as Figure 1.

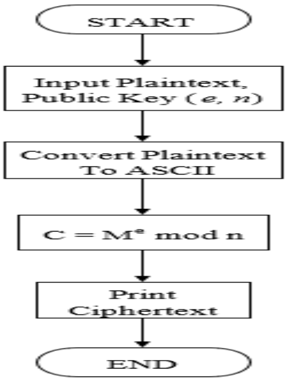


Fig. 1: RSA encryption Flowchart

- Mes (plain text) before encryption is what you have.
- Cip is a cipher text or encrypted document to convert to plaintext.
- The d and n values are private key pairs generated by the key generation process.

D. Decryption

The RSA decryption method is also very simple. Suppose a cipher text Cip has been obtained by the public-key pair (n, e) receiver. The Receiver calculates the Cip power of d (private key). One will get the plaintext Mes by calculating the result value modulo n that is given in below equation.

$$Mes = (cin)^{d} \bmod n \qquad (1)$$

The following figure 2 shows RSA decryption flow chart.

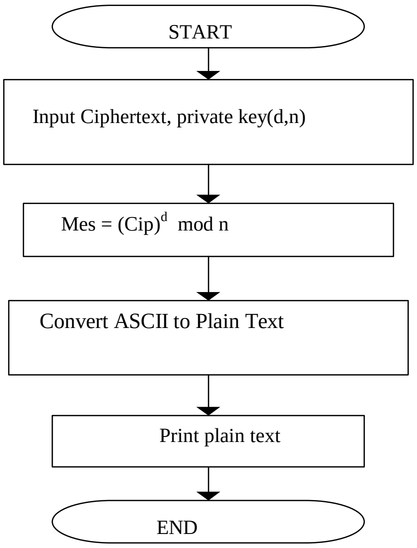

START
Input Ciphertext, private key(d,n)
Mes = (Cip)^d mod n
Convert ASCII to Plain Text
Print plain text
END

Fig. 2 RSA decryption Flowchart

VI. IMLEMENTATION

Data Transmission Using RSA:
The following are explanations on the sending of information on RSA application:
Step 1: Start the application in android to initiate the public server

Step 2: The RSA algorithm require two prime numbers p, q for public key and private key generated by the server, the pubic key will have sent to the application by the server.

Step 3: The message M is encrypted by the application to ASCII values. The encoded data will have sent to the candidate. The ASCII values M is encrypted to cipher text using public key.

Step 4: The developed application will send the cipher text C using URL to the Server.

Step 5: The Server will receive the Cipher Text C.

Step 6: The Server will decrypt the cipher text using the Private key using functions in PHP. Then the server the matches the decrypted text with original message M.

Step 7: The Server stores the data in MYSQL.

A. Data Process Analysis

- There are four choices for the user to choose from in this voting implementation, each choice reflects a specific party. each party to be represented by a number 5,8,9,6. This application denotes the preferred option as encrypted information amount. In any voting method, prime numbers are also chosen randomly automatically in order to prevent wiretapping fraud. Because prime numbers are chosen using random technique, the user is then specified to calculate prime numbers, i.e. 47 and 89. The following is the starting RSA encryption and decryption calculation method: 1024 is the size of the main encryption duration to be determined. The suggested key length for RSA security is 1024 bits at this moment.
- To randomly determine the value of p and q where p and q are free numbers. For example, we have p= 47 and q= 89 manual calculations. These numbers were chosen as prime numbers because they were not too large and not too small. Prime numbers p and q were randomly chosen in the calculations because the application automatically generates numbers p and q, making it hard to detect an amount of app chosen.
- Calculate the modulus n (public key) and Euler's Totient function:

$$\mathbf{\Phi(n)} \text{ with formula } \mathbf{n = p * q} \qquad (2)$$

Table II shows the calculation of encryption for each amount of applicants. Thus, information with value 2472 will be sent to the first applicant with serial number 5. The information with value 4113 will be sent to the second applicant with number 8. The third candidate with number 9 will send 1141value information, and 2693 value information will be sent to a fourth candidate with number 6. The data decryption process is the reverse of the data encryption process that will process the cipher text obtained from the encryption using the formula Mes= (Cip)d mod n to obtain the original plaintext. The table below describes the information decryption calculation.

- Calculate the modulus n (public key) and Euler's Totient function Φ(n) with formula n = p * q.
- n = 47 * 89= 4183 Φ(n) = (p-1)(q-1)
  = (47-1)(89-1) = 46* 88 = 4048
- Find e, where 1 < e < Φ(n) and GCD (Φ(n), e) = 1. Table I. results that we have to choose e = 3 because that numbers included in the first five Fermat numbers so can make modular exponentiation process be faster.
- Calculate d with formula **d * e mod Φ(n) = 1** ***d*** *** 3 mod 4048= 1** from the above one can obtain the value of d is 2699. Data encryption process conducted with formula **Cip=(Mes)^{e} mod n.** The data will have sent in the form of Message taken as input and it converts into to ASCII values. These values pass as arguments to RSA algorithm in turn returns cipher text.

Table- I: Encryption Calculation

Mes	**ASCII**	**Cip = (Mes)^{e} mod n**	**Cipher Values**
5	53	53^3 mod 4183	2472
8	56	56^3 mod 4183	4113
9	57	57^3 mod 4183	1141
6	54	54^3 mod 4183	2693

Table I shows encryption calculation for each number. So, for the first serial number 5 will sent data with value 2472. For the second number 8 will sent the data with value 4113. The third number 9will sent the data with value 1141, and for a fourth candidate with the number 8 will sent data with value 2693. Data decryption process is the reverse of the encryption data process which cipher text obtained from the encryption will be processed by the formula **Mes = (Cip)^{d} mod n** to get the original ASCII values and these ASCII values converts to plaintext. The following table outlines the calculation of the data decryption.

Table- II: Decryption Calculation

Cip	**Mes = (Cip)^{d} mod n**	**ASCII values**	**Original text Mes**
2472	2906^{2699} mod 4183	53	5
4113	538^{2699} mod 4183	56	8
1141	368^{2699} mod 4183	57	9
2693	529^{2699} mod 4183	54	6

Table II. shows decryption calculation from cipher text value. So, once decrypted, the ASCII value of the cipher text is obtained, then the ASCII value are converted into the original value. The results are 2472 for result 5, 4113 for results 8, cipher text 1141 for result 9, and the cipher text 2693 for result 6.

B. Architecture of System Analysis

There are three components which are present in the Voting system architecture and they are Smart mobile phone, application interface and Server. When the user application interface appears, describes the user's authentication permit application type in the android or IOS smartphone model, explaining the RSA algorithm that used the server segment describes the RSA model algorithm used with information source applications such as MySQL database.

C. Analysis of Voting System and System Design

The method of system analysis describes what the system should do to satisfy the requirements of customers. Figure 3 illustrates case for system use describing system function from a user view.

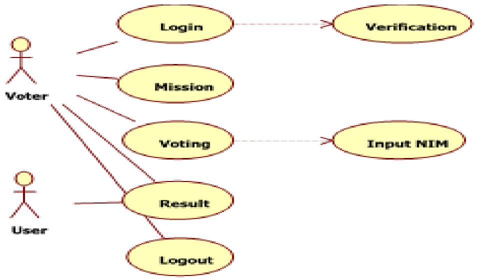


Fig. 3 Use case for E –Voting System

D. Storing of E-Voting Data in Database

The database for mobile voting is created using the MySQL database. The front end application is created and PhpMyAdmin is an option in the software to connect the MYSQL database. The tables can be created in this application which are required for the user and different party details. The sample table is given below.

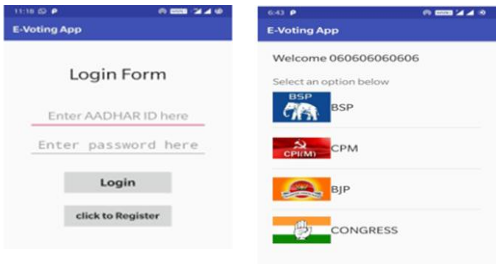
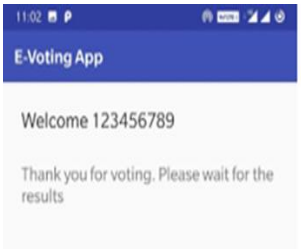


Figure 4. Login Page & Party Symbols of E-Voting



Welcome 123456789

Thank you for voting. Please wait for the results

Figure 5. Thank you

VII. CONCLUSION

Based on the safety of RSA voting data transmission on android or IOS based studies, it can be concluded as follows: A safe E-Voting scheme enables quality and reliable information to be collected. Our proposition fulfils the criteria in several areas to be used. Its instant implementation is to replace or complement existing voting systems, fresh democratic leadership systems (e.g. eCognocracy), or to securely and reliably collect data in marketing surveys. Implementing a secure E-Voting system requires the fulfilment of a set of features in such a way that there are no flaws in their implementation. This document shows a true application using ring signatures of a safe E-Voting platform. Free and verifiable software was used to create the scheme. A nice outcome is the use of the RSA algorithm in the safety of information transmission on the smartphone. This is because the RSA algorithm is an excellent way to secure the amount of safety. This portable Ios & android-based vote with an RSA algorithm may stop the election outcomes from being rigged as it has been encrypted.

REFERENCES

1. Lambrinoudakis, Secure Electronic Voting: Trends and Perspectives. 2002.
2. D. Boneh, Twenty Years of Attacks on the RSA Cryptosystem. 1999.
3. P. S. . Pardede, "Analisis dan Perancangan Keamanan Informasi Pada Electronic Voting Menggunakan Algoritma Kriptografi Kunci Publik," 2012.
4. H. K. Al-Anie, M. A. Alia, and A. A. Hnaif, "E-VotingProtocol Based on Public-Key Cryptography," Int. J. Netw. Secur. Its Appl., vol. 3, no. 4, 2011.
5. Nawindah and A. Sofwan, "Analisa Perancangan dan mplementasi Sistem Informasi E-Voting untuk Pemilihan Ketua BEM pada Himpunan Mahasiswa Jurusan Teknik Grafika dan Penerbitan," Pros. Semin. Nas. Multidisiplin Ilmu Univ. Budi Luhur, 2014.
6. A. B. Handoyo, "Sistem Pengamanan Data Pemilihan Umum e-Voting dengan Menggunakan Algoritma SHA-1," Makal. IF3058 Kriptografi - Sem. II, 2013.
7. K. Ok, V. Coskun, and M. N. Aydin, "Usability of Mobile Voting With NFC Technology," 2013.
8. C. R. K. Stradiotto, T. C. . Bueno, and V. O. Mirapalheta, "Web 2.0 E-Voting System Using Android Platform," 2014.
9. D. A. M. G. Wisnu, A. Suharsono, and D. S. Rusdianto, "Rancang Bangun Sistem E-Voting dengan Menerapkan Hash dan Digital Signature untuk Verifikasi Data Hasil Voting," 2013.
10. Adnan, "Kinerja Tanda Tangan Digital RSA 1024 bit pada Simulasi E-Voting Menggunakan Prosesor Multicore," Semin. Nas. Apl. Teknol. Inf., 2014.
11. P.Chandra Sekhar ,Srinivasa Rao, K., Srinivasa Rao, P.," Segmentation of natural images and retrievals based on the mixture of pearson type III distributions", IJITEE,pp. 2038-2042, 2019.
12. P.Chandra Sekhar, K.Srinivasa Rao & P.Srinivasa Rao,"Image Segmentation Algorithm for Images having Asymmetrically Distributed Image Regions", International Journal of Computer Applications (0975 – 8887) Volume 96– No.21, 2014, pp 64-73.
13. K. Srinivasa Rao, P. Chandra Sekhar & P. Srinivasa Rao, "Image Segmentation for Animal Images using Finite Mixture of Pearson type VI Distribution", Global Journal of Computer Science and Technology: Graphics & Vision Volume 14 Issue 3 Version 1.0,2014 pp.1-12.
14. B.Bhaskara Rao, V.Valli Kumari, "Clustered Hierarchical Concept Based Semantic Closeness Between Two Concepts Using WordNet", IJCSI Vol. 11(4), 2014.
15. B.Bhaskara Rao, V.Valli Kumari, "Concept Based Ranking of Results using an Ontology and Fuzzy Network for a Personalized Web Search Engine", IJCA vol. 81(13), 2013.

AUTHORS PROFILE

Dr B Bhaskara rao is presently working as Associate Professor in Department of CSE, Gitam University . He published several papers in various international conferences and journals. His current research interests are Cryptography, Data mining and web mining.

Dr P.Chandra Sekhar is presently working as Associate Professor in Department of CSE, Gitam University . He published several papers in various international conferences and journals. His current research interests are Cryptography, Speech & Image processing.

V. Sunil Kumar is presently working as Assistant Professor in Department of CSE, Gitam University . He published several papers in various international journals. His current research interests are Cryptography and CyberSecurity.

K.Sandeep Varma is presently working as Assistant Professor in Department of CSE, Gitam University . He published several papers in various international journals. His current research interests are Cryptography, Vulnerability & Eithical Hacking.