International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9, Issue-7, May 2020

Secure Radio Frequency Transmission for Paperless Voting System

Anshu Banerjee, Ananya Tewari, Renuka Bhandari

Abstract*: In any democracy, elections play an important role. If the traditional Electronic Voting Machine (EVM) is secured by encryption, it could be made more reliable. Traditional voting process provides security through the use of a paper audit trail which is not environment friendly making it unfit for use in the long run. This paper proposes the use of Blowfish algorithm for encryption along with secure transmission using radio frequency and verification of the cast vote. In this approach, the cast vote is encrypted using Blowfish encryption algorithm and transmitted to the server through radio frequency. At the server, the data is decrypted and sent back to be displayed on the screen of the EVM, eliminating the paper audit trail. This approach will account for a considerable amount of cost reduction without compromising on the security and sanctity of the election process.

***Keywords*: Blowfish Algorithm, Encryption, Radio Frequency, Decryption, Cloud**

I. INTRODUCTION

Elections are conducted using electronic voting machines (EVM).[1] They have been developing over the past two decades and have replaced the process of voting through ballot papers, thus making the election process much easier by avoiding manual tallying of ballot papers.[2] EVMs are fast and reliable, and save lot of time and manpower. However, there are many security loop-holes and threats, which may lead to tampered results in the election. Security and privacy are main concerns in the EVM. An implementation of secure voting system has been proposed that improves the security.

II. HISTORICAL BACKGROUND

Voting in India was conducted using ballot boxes till 1982.[2] Ballot boxes had many major security concerns. Apart from that, they were difficult to transport and required specific storage conditions. Ballot boxes were then replaced by EVMs.[2]

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
Anshu Banerjee*, Department of Electronics and Telecommunication, Army Institute of Technology, Savitribai Phule Pune University, Pune, India. Email: amshubanerjee_16383@aitpune.edu.in
Ananya Tewari, Department of Electronics and Telecommunication, Army Institute of Technology, Savitribai Phule Pune University, Pune, India. Email: ananyatewari_16654@aitpune.edu.in
Dr. Renuka Bhandari, Department of Electronics and **Telecommunication**, Army Institute of Technology, Savitribai Phule Pune University, Pune, India. Email: rbhandari@aitpune.edu.in

A. Electronic Voting Machines (EVM)

Electronic Voting Machine (EVM) is a device that is used to record votes electronically. It is made up of two Units – a Control Unit (CU) and a Balloting Unit (BU). A five-meter cable joins these two units.[2] There exists a Presiding/Polling Officer who watches the CU while the voting compartment houses the BU. Instead of issuing the ballot papers, the Polling Officer who is in-charge of the CU releases a ballot by pressing the Ballot Button on the CU. The voter then casts his vote by pressing a blue colored button on the BU against the candidate and symbol of his choice. In this way, the possibility of casting an invalid vote is completely eliminated as opposed to paper ballot system where invalid votes were cast in large numbers. This has enabled EVMs to reflect a more authentic and accurate choice of people. EVMs, also reduce the printing of millions of ballot papers needed for every election, and make the counting process very quick (result can be declared within 3 to 5 hours as opposed to 30-40 hours, on an average, under the conventional Ballot paper system).[2]

B. Voter Verifiable Paper Audit Trail (VVPAT)

Voter Verifiable Paper Audit Trail (VVPAT) or Verifiable Paper Record (VPR) is an independent system attached to the EVM. It facilitates the voters to verify that their votes are cast as intended. After a vote is cast, a paper slip is printed containing the serial number, name and symbol of the candidate. It is shown through a transparent window for about 7 seconds. After this period of time, the printed slip falls in a box that is sealed. This process is automated. This process helps detect malfunction or possible election fraud and the electronic results can be audited.[2]

III. THE PROBLEM

The traditional EVM is susceptible to several security threats such as: Before voting- The unit may be replaced with a fraudulent one which may be pre-programmed to transfer a certain set of the votes in the favor of a previously decided candidate. After voting- The EVM's memory can be manipulated in between the election and the counting phase. Manipulation of the data is done using an on-clip interface by swapping the vote from one candidate to another. EVM's may also be hacked with a Bluetooth device. Moreover, the VVPAT which is used to confirm the vote, unnecessarily creates infrastructural burden and large amounts of waste paper. To avoid problems such as BU manipulation, fake votes and duplication of votes, cryptography can be used to ensure security and the voter's privacy.[3]

Exploring encryption algorithms:

1) Data Encryption Standard (DES): It is a symmetric- key block cipher. It was released in 1977 as FIPS-46 in the Federal Register by the National Institute of Standards and Technology (NIST).

This algorithm works on a 64-bit plain text to produce a 64-bit cipher text. During decryption, a 64-bit cipher text is converted into a 64-bit plain text. A 56-bit cipher key is used for both the processes of encryption as well as decryption. 48-bit round keys are used for encryption which are obtained from cipher key using a predefined algorithm. The encryption blocks are made of two permutations (P-boxes), the initial and the final permutation box , and there are 16 Feistel rounds. The function has four sections: • Expansion P-box • S-boxes • A whitener (that adds key) • A straight P-box.

2) Advanced Encryption Standard (AES): The algorithm is a symmetric- key block cipher issued by the National Institute of Standards and Technology (NIST) in the month of December 2001 as FIPS-197 in the Federal Register. A non-Feistel cipher is used here. The algorithm can encrypt block size of 128-bits. It applies 10, 12, or fourteen rounds. The size of the key size can be 128, 192, or 256 bits as per the number of rounds. AES does work on a 4×4 column major order matrix of bytes.

3) RSA (Rivest–Shamir–Adleman): The RSA algorithm has four steps, given as follows: Generation of key, distribution of key, encryption and decryption. The very basic principle that goes into this algorithm is that finding three extremely large positive integers i.e. e, d is very viable and n is with modular exponentiation for the integers m. The algorithm includes a public key and a private key. The public key can be accessed by everyone, and it is used for the encryption of messages. The messages encrypted with the public key can only be decrypted using the private key. After carefully studying the characteristics of various encryption algorithms, Blowfish algorithm was found out to be the most reliable encryption method. The Blowfish algorithm has been discussed further, in detail, later in the paper. The comparative results have been displayed in fig 2 and 3.

IV. PROPOSED SOLUTION

Along with cryptography, to make the entire voting process more environment friendly, the use of paper for auditing can be completely eliminated. The proposed method solves both the problems by use of Secure Radio Transmission. This system can be implemented by interfacing the encryption and decryption technologies within the traditional Balloting Units and Control Units. This will also reduce the number of Control Units to one single unit all over the nation that can be overseen by authorized officials to avoid tampering.

A. Participants and Phases

The participants are: the voter, voting server and the voting authority. The system will be comprised of the following phases: Authentication, Voting, Encryption, Transmission, Decryption, Storing and Confirmation. The voter is asked to enter his voter ID so as to compare with the database and confirm existence of the said voter. The voter selects the candidate of their choice and pushes a button corresponding to their choice. The vote made is then recorded by the microcontroller and encrypted using the blowfish algorithm. The encrypted message is transmitted to the server using the GSM module over Radio Frequency. This message is received by the GSM module at the server. The microcontroller at the receiver (server) decrypts the message. This decrypted message goes to a national database stored on the cloud which maintains counts of the votes received by a particular party/candidate. Simultaneously the decrypted message is also sent back to the Balloting Unit to confirm to the voter that the message has been received and what the received message is.

B. Security through Encryption

After comparison with various other encryption methods through simulation, blowfish was found out to be the most suitable due to its speed and its secure nature.

The Blowfish Algorithm: Blowfish is a cipher designed to be an improved replacement to the DES algorithm. It is a symmetric-key Feistel block cipher. It is much faster than DES and the rate of encryption is high. There is to date no crypt analysis method found that has proved to be effective. The algorithm includes S-boxes that are key-dependent and a highly complex key schedule. The added advantage is that the algorithm is patent-free and can be used for general purpose. This algorithm is used by various applications and e-commerce software which are practically implemented.[1]

Key features of Blowfish are:

1. Block Size = 64 bit
2. Key Size = 32 - 448 bit (variable size)
3. Number of Sub-Keys = 18
4. Number of rounds = 16
5. Number of S-boxes = 4 (Substitution-boxes)

As shown in Fig. 1, the algorithm has also been tweaked a little to render more safety to it.

C. Encryption

The 64-bit plaintext, goes through 16 rounds of encryption to produce the ciphertext. The round function (refer to fig 3.1) consists of the following actions:

- STEP 1 XOR left half (L) of the data with the i^{th} P-array entry.
- STEP 2 The input for Blowfish's F-function is the XORed data.
- STEP 3 XOR F-function's output is with the right half (R) of the data
- STEP 4 Swap L and R3

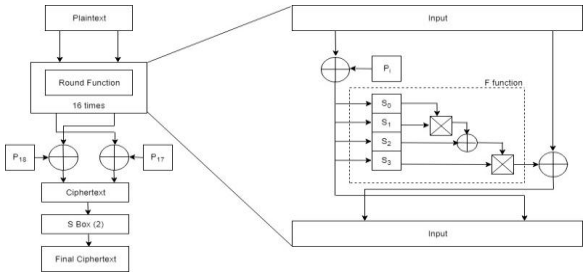

Fig 1: Modified Blowfish Algorithm

D. Sub-Key Generation

In the beginning of the key schedule, the P-array (18 32- bit entries) and S-boxes (4 S-boxes with an array of 256 32-bit entries each) are initialized with values obtained from the digits (hexadecimal) of pi. Thus, there is no obvious pattern. The secret key K is then XORed with the P-entries in order (the key is cycled if required). For example,

If [K] = K_1, K_2, K_3, ..., K_{14} (32-bit each. Total = 448 bits) Then, P-box entries are modified as:

$P_1 = P_1$ XOR K_1, $P_2 = P_2$ XOR K_2...$P_{14} = P_{14}$ XOR K_{14}, $P_{15} = P_{15}$ XOR K_1, $P_{16} = P_{16}$ XOR K_2, $P_{17} = P_{17}$ XOR K_3, $P_{18} = P_{18}$ XOR K_4

In the next step, an all-zero block of 64-bit is entered into the system to be encrypted with the algorithm. The resultant ciphertext replaces P_1 and P_2. The ciphertext is then encrypted again with the new sub-keys, and P_3 and P_4 are replaced by the new ciphertext. This continues, replacing the entire P-array and all the S-box entries. Thus, the algorithm runs 521 times to generate all the sub-keys. The last swap is undone after the 16^{th} round, L is XORed with K_{18} and R is XORed with K_{17}.

E. The F Function

The F function splits the input (32-bit) into four eight-bit quarters which are used as inputs to the S-boxes. The most significant and the least significant bits of the 8-bit input is used to index the rows and the middle bits are used to index the columns. In this way, the an 8-bit input is replaced by a 32-bit input by the S-box. The outputs are then added and XORed which produces the final 32-bit output.

F. Added Security

For making the algorithm more secure, an additional substitution box, S-box (2) (refer to fig 3.1) has been added at the end. The values of this S-box are pre-defined and known only to the transmitter and the receiver. It maps the cipher text to a particular value, producing the final cipher text.[4]

Fig. 2 and 3 show the time comparison between the discussed algorithms. It shows how blowfish takes the least time. It is also observed that modified blowfish is takes a little more time than the original algorithm (0.002097s), but it is much more secure due to the additional substitution box.

G. Data Encryption

For encrypting a particular plain text, it is simply passed through the algorithm.

H. Decryption

Being a Feistel network, Blowfish can be inverted simply by XORing P_{17} and P_{18} to the ciphertext block, then using the P-entries in reverse order.

V. RESULTS AND DISCUSSION

Table 1 and Fig 2 Show the time comparison between the discussed algorithms. We can observe that blowfish takes the least time. Although modified blowfish takes a little more time than the original algorithm (0.002097s), it is much more secure due to the additional substitution box.

Table 1: Time comparison of encryption algorithms

ALGORITHM	TIME TAKEN
DES	1.309676s
AES	0.716540s
RSA	0.633598s
MODIFIED BLOWFISH	0.011267s
BLOWFISH	0.009170s

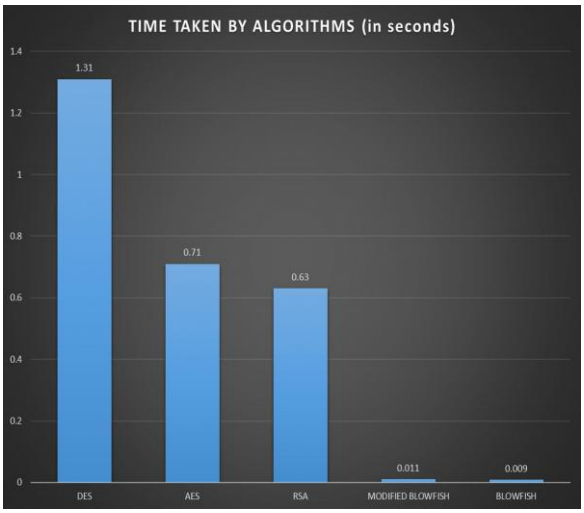

Fig 2: Graphical Representation of Time Comparison

The implementation is based on the secure transmission of messages through radio frequency to reduce the security threats as well as to eliminate the usage of paper in the voting process. The paper also proposes to reduce the paper used in maintaining logs of the registered voters by making it a digitized system.

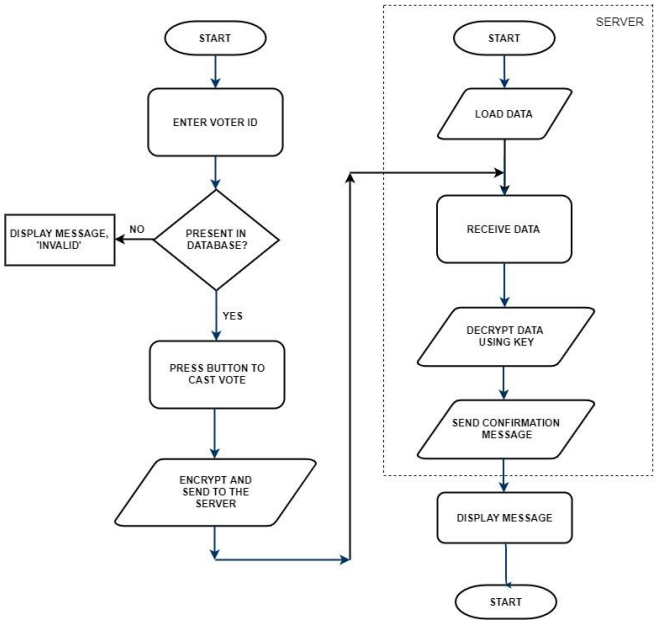

Fig. 3: Flowchart

A. Authorization

The voter must enter their registered IDs in the system through the GUI so as to confirm their existence as a registered voter.

This database is maintained locally according to the constituency that the process is taking place in. If the voter does not exist in the database then they are denied from voting. If the voter does exist, then they may proceed to vote.

B. Voting

The voter proceeds to select the desired candidate using the buttons interfaced with the microcontroller. This message is then encrypted and sent to the GSM Module for transmission.

C. Encryption

The encryption is carried out in the microcontroller using the modified Blowfish algorithm. The algorithm has been described above.

D. Transmission and Reception

The transmission is done through radio frequency, this is done by employing GSM modules on both ends, the Balloting Unit and the central national server. The central server receives the encrypted message which contains the name of the party/candidate who has been voted for.[5][6]

E. Decryption

The message is decrypted in the microcontroller on the server end. After encryption the decrypted message is sent to two paths:

1) Cloud Storage: This is the national database which is updated each time a vote is cast, and is used to tally the results.[7]

2) Confirmation: The decrypted message is also sent back to the Balloting Unit to display the cast vote to the voter so as to confirm that the vote has been recorded for the correct candidate without any tampering.[8]

This process is now repeated for the next voter. This eliminates the need to use paper while also securing the voting process.

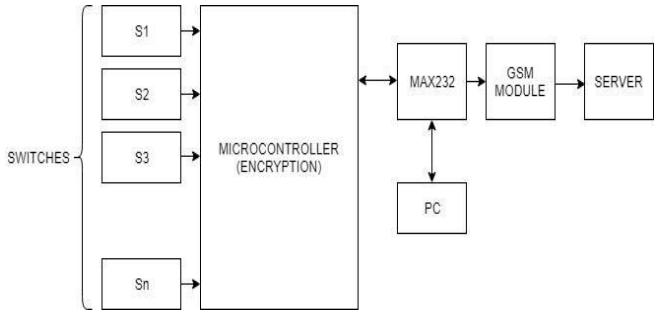

Fig 4: Transmitter Block Diagram

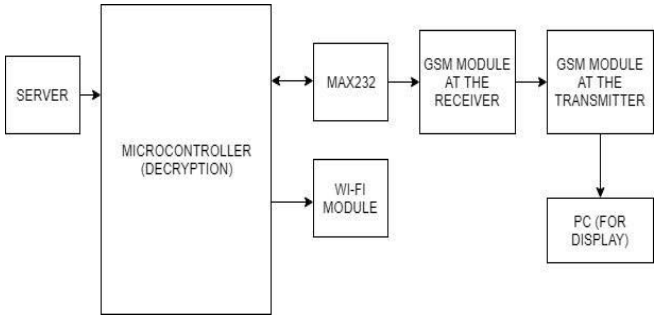

Fig 5: Receiver Block Diagram

VI. CLOUD STORAGE

In order to deploy a seamless as well as centralized data storage and accessing system, cloud technology is used. The motivation behind choosing this is how the cloud involves minimal investment along with ability to apply algorithms which will also ensure security of data. It performs the following two functions:

1. Ensures that the voter is registered.
2. Stores data regarding the tally of votes collected.

VII. APPLICATION

This proposed idea can be implemented by interfacing the encryption and decryption technologies within the traditional Balloting Units and Control Units. This will reduce the number of Control Units to one single unit (Server) all over the nation, that can be overseen by authorized officials to avoid tampering. This may be implemented in election processes at various levels as long as the required technology is available.

VIII. CONCLUSION

The proposed system eliminates the use of paper completely, while also securing the entire process through the modified blowfish algorithm. The main purpose is to be able to implement an environment friendly paperless voting system without compromising on the security sanctity of the election process. It can be implemented by interfacing the encryption and decryption technologies within the traditional Balloting Units and Control Units. This will also account for a large amount of cost reduction in conducting elections.

REFERENCES

1. Panem. Charan Arur, M. Sai Chandrasekhar, S. Sai Sreeram, K. Ram Kishore, S. Venu Gopal, ”Secure Data Transmission using Blowfish Algorithm”, International Journal of Innovative Research in Science and Engineering, ISSN (Online): 2347-3207
2. Election Commisiion of India FAQs, https://eci.gov.in, Accessed on: 18-08-19 at 17:40
3. P. Ashok, P. Annadurai, R. Lavanya, P. Raghuvara Pandian, ”A Survey on Crypt- Algorithms in Voting System”, Indian Journal of Science and Technology, Vol 9(38), October 2016, ISSN (Print) : 0974-6846
4. Gurjeevan Singh, Ashwani Kumar, K. S. Sandha, ”A Study of New Trends in Blowfish Algorithm”, International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326, ISSN: 2248-9622
5. Dr. Poongodi. S, Manivel. N, Marakatha Kumar, Sangeetha and Shalini. D, ”Implementation of aadhar based voting machine using arduino with GSM”, International Journal of Intellectual Advancements and Research in Engineering Computations, Vol 6 Issue-I, ISSN: 2348-2079
6. Sneha Pallav, S. Dhanalakshmi S. Aiswarya, ”Mobile Voting using Global System for Mobile Communication (GSM) Technology and Authentication using Fingerprinting Biometrics and Wireless Networks”
7. Jena Catherine Bel. D, Savithra. K, Divya. M, ”Jena Catherine Bel. D, Savithra. K, Divya. M A Secure Approach for E-Voting Using Encryption and Digital Signature”, International Journal of Engineering Development and Research, ISSN: 2321-9939-2015
8. Adam Aviv, Pavol Cerny, Sandy Clark, Eric Cronin, Gaurav Shah, Micah Sherr, Matt Blaze, ”Security Evaluation of ESS Voting Machines and Election Management System” G. O. Young, “Synthetic structure of industrial plastics (Book style with paper title and editor),” in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

AUTHORS PROFILE

Anshu Banerjee is currently pursuing her Bachelor of Engineering (BE) in Electronics and Telecommunication from Army Institute of Technology, Savitribai Phule Pune University. Currently in her fourth year, her research interest is in Cryptography and Network Security, Artificial Intelligence and Wireless Communication.

Ananya Tewari is currently pursuing her Bachelor of Engineering (BE) in Electronics and Telecommunication from Army Institute of Technology, Savitribai Phule Pune University. Currently in her fourth year, her research interest is in Cryptography, Wireless Sensor Networks and Machine Learning.

Dr. Renuka Bhandari received her Bachelor of Engineering degree from RGPV Bhopal and her Masters in engineering (Digital Communication) degree from DAVV University Indore. She received her Ph.D. (Electronics & Telecommunication Engg.) from Savitribai Phule Pune University, Pune. She has been in the field of Engineering Education for last 25 years. Presently she is working as an Asst Professor, Dept. of Electronics & Telecommunication Engineering in Army Institute of Technology, Pune, India. She has more than 15 publications in international conferences and journals.