E-voting in cloud using Cryptography Algorithm

P.Pooja
Department of Computer Science and Engineering
Dr.Mahalingam College of Engineering and Technology
Pollachi,Coimbatore,India
ppooja2603@gmail.com

C.Elakkiya
Department of Computer Science and Engineering
Dr.Mahalingam College of Engineering and Technology
Pollachi,Coimbatore,India
nilaela296@gmail.com

S.Soundharya
Department of Computer Science and Engineering
Dr.Mahalingam College of Engineering and Technology
Pollachi,Coimbatore,India
soundharyasakthi7@gmail.com

***Abstract*— This project aims at creation of a voting system by providing a cost effective solution ensuring non-traceability and integrity of the votes cast while providing great convenience to voters. This system is developed robustly to ensure that all eligible voters having a Universal Identification Number (UID) of their country is allowed to cast their respective vote. The voters, who cast multiple votes during the process of voting is ensured to be prevented. Also it provide guarantee for maintenance of authenticity. The process of online voting could be deployed with three phases - the voter registration, online vote capturing and the instant online counting and result declaration. Automated Tallying removes human fallibility from the tabulation process and makes election results available within seconds of the close of the election.**

The additional feature of the model is that privacy of casted vote is preserved using Advanced Encryption Standard (AES) encryption algorithm. When voters enter the details it would be stored in the encryption format, so that they are secured. As it is implemented in both hardware and software, it is more robust security protocol. It uses higher length key size such as 128,192 and 256 bits of encryption. Hence this algorithm makes more robust against hacking. For 128 bit, about 2^128 attempts needed to break. This makes it very difficult to hack it, as a result it is very safe protocol. In this model a person can also vote from outside of his/her allocated electorate or from his/her chosen location.

Keywords—AES algorithm, Biometric sensor, cloud computing

I. INTRODUCTION

Earlier, Voting is a privilege of living in a democracy. To take this step further concept of online voting system is designed. India's recent initiative to give Unique Identification Number (UIQ) for every citizen will help to implement this online voting system using cloud computing. In traditional voting system the voter must come to polling booth for doing their democracy duty. So we have proposed a system for voting. Using this system, we can vote for the candidate wherever we are. Main objective of proposed system are, to minimize the time consumption for voters. It supports only the authenticate person to elect the candidate. User can vote at any place at time during the election time.

B. Overview

The evolution of cloud computing over the past few years is potentially one of the major advances in the history of computing. Cloud computing is a centralized cloud storage environment which can have ability to store large amount of data. With organizations today shifting large amounts of data from physical storage to the cloud, the demand for cloud services has only increased. One of the foremost advantages of moving to cloud is the reduction in cost of storage while organizations can focus on their day-to-day operations. Amazon has established itself as a market leader in terms of provider of cloud services with its various offerings. Amazon Web Services (AWS) is a comprehensive, evolving cloud computing platform provided by Amazon. It provides a mix of infrastructure as a service (IaaS), platform as a service (PaaS) and packaged software as a service (SaaS) offerings. In AWS provides Relational Database Services (RDS). RDS web services that makes it easy to setup, operate and scale the database in cloud. Low level database admin work is handled automatically by AWS. This support Postgre SQL, MYSQL, MSSQL and Oracle database. Amazon RDS automatically patches the database software. Enables point in time recovery.

A. Objective

The main objective is to allow only the legible voters to vote and avoid duplicate voting by providing authenticity. Once the voting session is completed it takes less time to calculate results, therefore time consumption is reduced. To prevent the data from hacking, high data security is maintained.

The literature identified presented a brief overview of the existing literature on this topic. The

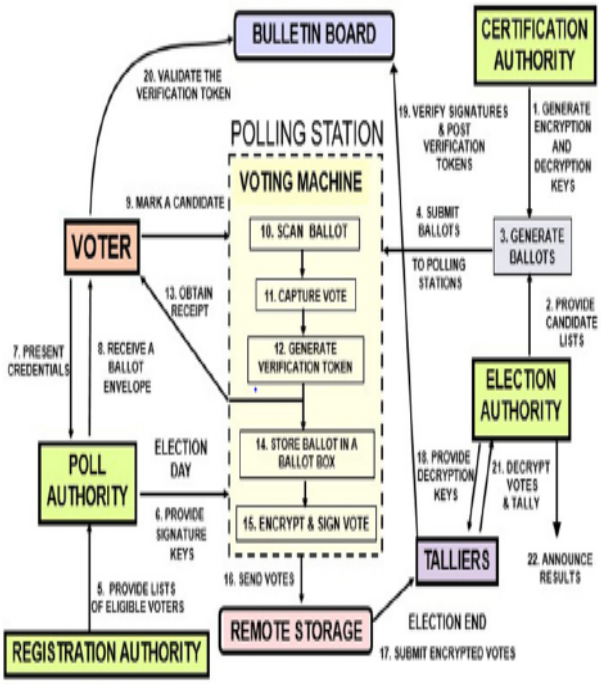
algorithm used for the encryption of the details. This include validation of the input data from the application. This also provide the results of the vote analysis. The performance of the system is also analysed based on evaluation metrics. Methodology describes the implementation of the application.

II. METHODOLOGY

Current system which is present now is Electronic voting system where the counting of votes is difficult. This system requires high manpower and resources. To overcome this problem the online voting system is designed. This system reduces the manpower, where the voter can vote through an application and the voter need not come to polling station. Thus the system makes counting process efficient. The result can be produced in short period of time. The data would be secure and prevents from manipulating the votes.

A. Existing System

The existing E-voting scheme takes place at the polling station with votes being casted in controlled environment. The scheme really operates in three stages- pre election, vote capture and post election. The existing system is shown in Figure 1 .



Stage 1 is the pre election stage. Most of the procedures presented in this stage are only implemented by the election authorities, and they are transparent to ordinary voters. Pre-election setup requires the election authorities to create sets of digital certificates with the aid of a trusted certification authority (CA). Each certifi- cate has a public/private key pair of a public key cryptosystem. Polling stations are provided each with a public key (encryption key) from the set of polling stations digital certificates. The polling station private key (decryption key) is kept secret by dividing it into shares using a threshold secret share technique. Pre-election stage requires voters' participation in the enrollment of voters' bio- metric fingerprints. This is required for the authentication and sub- sequent authorization of the voters inside the polling stations in the vote capture stage. . Pre-election setup also requires the creation of paper ballots with a randomized candidate list. Election authorities will create a set of authorities digital certificates with the aid of a trusted certification authority.

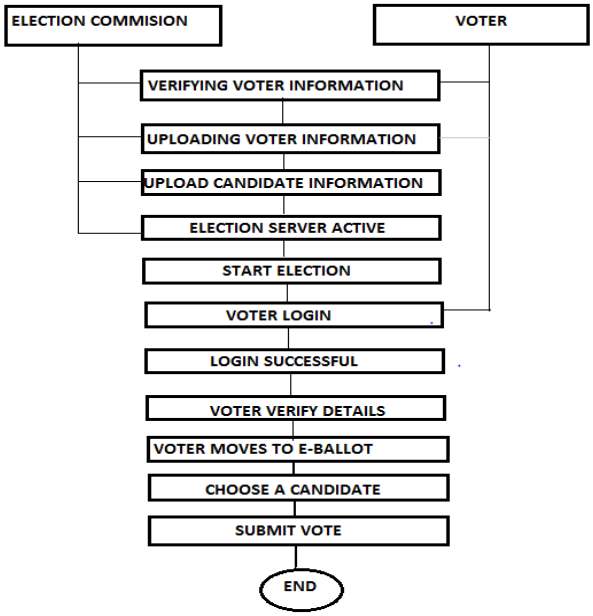
Stage 2 is the vote capture "cast vote" stage. This stage begins with the start of the Election Day. A voter arrives to the polling station and identifies himself to the local electoral commission with an ID card and his finger print. The national ID card is used to fetch the template record of a specific voter, while the biometric finger print is used for authenticating the voter. The authentication is done by comparing the voter's own biometric template (previously enrolled and stored in a template database) with the one he used to identify himself (one-to-one comparison). After a successful authentication, the electoral commission either hands the voter exactly one closed envelope or he randomly chooses one himself. The envelope contains a ballot form sealed inside the envelope. In the polling station's booth, the voter privately extracts his ballot form from the envelope, and makes his selection by placing a mark in the right hand column against the candidate of choice (plurality voting), or, in the case of a Single Transferable Vote (STV) system, he marks his ranking against the candidates. Once the selection has been made, the voter separates the LHS and RHS parts along the perforation and keeps the LHS temporarily. The voter then leaves the booth, head towards an official operating a voting machine, and casts the RHS ballot part representing his protected vote in the presence of the official. In order to process the vote, the RHS is placed over an optical scanner connected to the voting machine. The scanner records the barcode of the RHS and an index value indicating the cell into which the voter's choice was marked. The recorded data is considered as the digital representation of the vote.

Stage 3 is the post-election stage. This stage starts after the end of the election period. Post election processes includes tallying of votes and announcing the results.

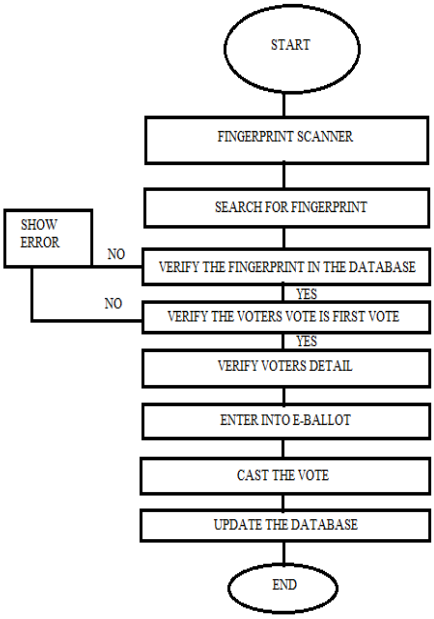
B. Proposed System

The Online voting system is shown in Figure 2

will employ fingerprint Authentication for casting their votes for the candidate and the application is deployed in cloud so that it is accessed from anywhere.



2. Flow Diagram of Proposed System



3. Flow Diagram of Finger print sensor

C. System Requirements

The implementation requires the following software and hardware:

- Netbeans IDE – version 8.1
- Oracle database
- AWS
- Fingerprint sensor

NetBeans IDE – Net Beans is an open-source integrated development environment (IDE) for developing with Java, PHP, C++, and other programming languages. Net Beans is also referred to as a platform of modular components used for developing Java desktop applications. Net Beans is coded in Java and runs on most operating systems with a Java Virtual Machine (JVM), including Solaris, Mac OS, and Linux. NetBeans uses components, also known as modules, to enable software development. NetBeans dynamically installs modules and allows users to download updated features and digitally authenticated upgrades. NetBeans IDE modules include NetBeans Profiler, a Graphical User Interface (GUI) design tool, and NetBeans JavaScript Editor. NetBeans framework reusability simplifies Java Swing desktop application development, which provides platform extension capabilities to third-party developers.

Oracle Database Software - Oracle DB rivals Microsoft's SQL Server in the enterprise database market. There are other database offerings, but most of these command a tiny market share compared to Oracle DB and SQL Server. Fortunately, the structures of Oracle DB and SQL Server are quite similar, which is a benefit when learning database administration. Oracle DB runs on most major platforms, including Windows, UNIX, Linux and Mac OS. Different software versions are available, based on requirements and budget. A key feature of Oracle is that its architecture is split between the logical and the physical. This structure means that for large-scale distributed computing, also known as grid computing, the data location is irrelevant and transparent to the user, allowing for a more modular physical structure that can be added to and altered without affecting the activity of the database, its data or users.

AWS - Amazon Web Services (AWS) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow. Amazon Web Services (AWS) is a comprehensive, evolving cloud computing platform provided by Amazon. It provides a mix of infrastructure as a service (IaaS), platform as a service (PaaS) and packaged software as a service (SaaS) offerings. Amazon Elastic Compute Cloud (EC2) provides virtual servers -- called instances -- for compute capacity. The EC2 service offers dozens of instance types with varying capacities and sizes, tailored to specific workload types and applications, such as memory-intensive and accelerated-computing jobs.

AWS also provides an Auto Scaling tool to dynamically scale capacity to maintain instance health and performance.

III. Features and Processes involved in Proposed System

The proposed system has the following modules:

- Validation of voter information
- Validation of Candidate information
- AES algorithm
- Result calculation phase

A. Validation of voter information

During registration of voter details in admin module, the voter details such as fingerprint, Aadhaar number, voter ID, name, address, phone number, date of birth, pincode are collected and stored in cloud. The voter details are validating by their length and it should be in specific format. The voter age is above 18 or not. If the provided details are invalid it would be providing error. Each voter should register with their Unique Identification Number (UID) and the details provided by the voters are verified and stored in the database. During voter login module, the voter login with the help of fingerprint. If the fingerprint is present in database then the voter is able to cast their votes. On successful login, the voters details would be displayed and the voter would be able to choose their respective candidate. After casting the vote the vote should be stored in secured way by applying AES algorithm.

B. Validation of Candidate Information

Every candidate participating in Election should register with UID number and required details such as Aadhaar number, phone number, Address, pin code, date of birth, name needed for registration. The system would be validating the details whether they are in specified format and length. When voter is casting vote by recognizing the candidate representation symbol.

C. AES Algorithm

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time. Thus the Electronic code block (ECB) mode is used in this algorithm. The EBC mode is deterministic where the blocks of data are sequentially processed by the key.

ENCRYPTION PROCESS:

The steps to be followed in encryption process:

STEP 1: Derive the set of round keys from the cipher key.

STEP 2: Initialize the state array with the block data (plaintext).

STEP 3: Add the initial round key to the starting state array.

STEP 4: Perform byte substitution, shift rows, mix columns, add round key for nine rounds.

BYTE SUBSTITUTION:

The 16 input bytes are substituted by looking up a fixed table (S-box). The result is in a matrix of four rows and four columns.

SHIFT ROWS:

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows :

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MIX COLUMNS:

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

ADD ROUND KEY:

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

STEP 5: Perform the final round of state manipulation and copy the final state array out as the encrypted data (ciphertext).

DECRYPTION PROCESS:

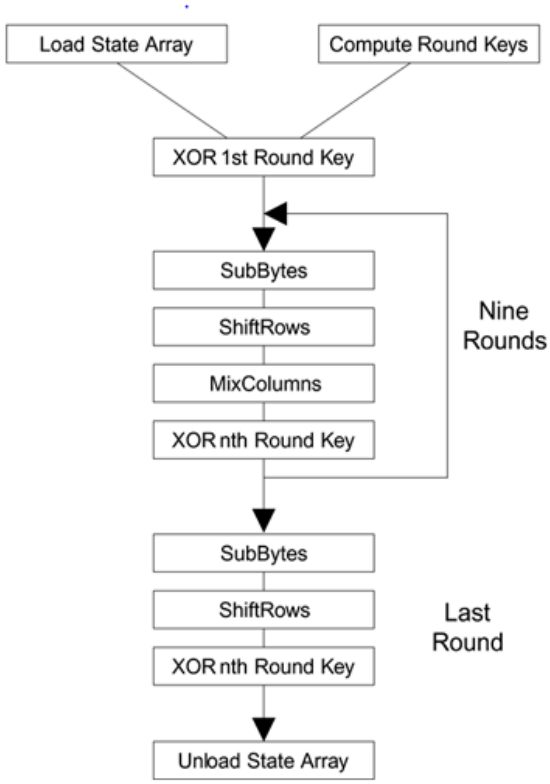
The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order:

INVERSE ADD ROUND KEY – Performs XOR operation between the cipher text and intermediate expanded key corresponding to that particular iteration.

INVERSE SHIFT ROW – This step rotates each ith row by i elements right wise in the matrix.

INVERSE SUB BYTES – This step replaces each entry in the matrix from the corresponding entry in the inverse S-Box.

INVERSE MIX COLUMN - The Inverse MixColumns operation performed by the cipher, along with the shift-rows step, is the primary source of all the 10 rounds of diffusion.



4.AES Algorithm

D. Result Calculation Phase

By the admin can know entire details above voter registration and different party candidate details. By this election commission or the admin can know the voters count by constitution wise. As the vote is casted for candidate the vote count value is incremented and final result is obtained. All received votes of polls are saved in the system, the numbers of voters and the information of polls are also available (in Poll, Poll_Members, Poll_Response, Poll_Answer tables). All checking, validation of received votes is done completely by stored procedure API (invoked from middleware layer) and acceptable votes are saved. For example, checking non-duplicate receiving votes from a member, receiving between start and end time of an open poll, validity of received information and all verification is done. According to the type of each poll the result of voting can be calculated. In this section, algorithm for calculating final results is described.

The algorithm takes the total number of votes received for each candidate as input for the algorithm.

DISTRIBUTED STATION ALGORITHM:

STEP 1: If the number of votes received is greater than half the number of voters.

STEP 2: Each voting candidate is taken.

STEP 3: Checks that the voting candidate is having votes more than 50 percentage of the total votes received.

STEP 4: If the candidate is having votes more than 50 percentage, then the candidate is considered to have highest number of vote count.

STEP 5: Then the candidate is declared as winner.

At the end time of poll (at deadline) or when all members have been voted, The candidate who has the maximum selecting percentage among the selected candidates are declared to have highest count.

IV. RESULTS

A. EVALUATION METRIC

Performance is evaluated for the proposed algorithm based on the several metrics which are best suited for the cryptographic algorithms. The performance is evaluated separately for text data encryption. The metrics that are selected for the evaluation are encryption time, decryption time, throughput of encryption, throughput of decryption, CPU process time, and CPU clock cycles, power consumption and memory utilization.

Encryption time: The encryption time is the total time taken to produce a cipher-text from plain-text. The calculated encryption time is then used to calculate the throughput of the encrypted algorithm. It gives the rate of encryption.

Decryption time: Decryption time is the total time taken to produce the plain-text from Cipher-text. The calculated decryption time is then used to calculate the throughput of the decrypted algorithm. It gives the rate of decryption.

B. Experiments and results

To evaluate the influence of the configuration parameters of the AES algorithm on the encryption and decryption time, a sequence of experiments was developed varying the experimental factors. For each execution platform, various factors are taken into consideration:

- The key sizes varies such as 128 bits, 192 bits , 256 bits.
- There are two chaining modes: ECB (Electronic code block) and CBC (Cipher chaining block)
- The padding of bits to the text.

For different file sizes 1, 25, 50, 75, 100 Mbytes.

B. Summary of result

Thus the system uses an encryption algorithm called Advanced Encryption Standard which encrypts all voter credentials that include voter id , Aadhaar No, name, address, phone number, pin code, state and Candidate details also. This algorithm increases the security level of voters details. Thus the result analysis is done for the algorithm based on the encryption and decryption time which varies for different information size. Thus the time efficiency is calculated. Thus the fingerprint authentication gives high security.

V. CONCLUSION

Generally voting has to be performed by user by going to the voting centre. Many users like army person or NRI cannot come to the voting place. The proposed online voting system where users can vote over the online. The Online Election System provides high level of Security, Authentication, Reliability and Corruption free mechanism. There is a database which is maintained by the Election Commission of India in which all the names of voter with complete information is stored. The Online Voting system will manage the voter's information by which voter can login and use his voting rights. The system will incorporate all features of Voting system. Thus the result would be given within a hours after a completion of voting. It decrease the Cost and Time of voting process. It is very easy to use, less time consuming and easy to debug.

REFERENCES

[1] KareemM.AboSarma, AhmedA.AbdelHafez, Ghazy M.R.Assassa, Mona F.M. Mursi, "A pratical, secure, and auditable E-voting system," *Journal of Information security and applications,* pp. 69-89, 2017.

[2] Parag Chatterjee,Ashok Nathe, "Biometric Authenication for UID based smart and Ubiquitous services in India," *IEEE computer society*, pp. 662-667, 2015.

[3] Veeru Talreja, Terry Ferrett,Matheew

C.Valenti, Arun Ross "Biometric-as-a-service : A Framework to promote Innovative Biometeric Recognition in the cloud" ," *IEEE international confrence on consumer Electronics* , pp. 1-6, 2018.

[4] Victor Mateu.Francesc sebe, magda valls, "Constructing creditional based E-voting system from offline E-coin prorocols," *Journal of Network and computer application*, pp. 39-44, 2014.

[5] Ahmed Hassan, Xiaowen Zhang, "Design and build A secure E-voting Infrastructure,"*IEEE Explore, pp.1-7*,, 2013.

[6] Kristjan Vassil, Mihkel solvak, pritik Vinkel, Alexander H.trechsel, R.micheal Alvarez, "The Diffusion of internet voting. Usage patterns of internet voting in estoian between 2005 and 2015," *Science Direct*,Volume 33 pp.453-459,2016.

[7] Gurpreet singh matharu, Anju mishra, Pallavi chhikara, "A cloud based Framework to modernize the indian election voting system," *IEEE International Conference on computational Intelligence and computing Research* , pp.1-7, 2014.

[8] Joseph .D. Enoch, Nne .R. Saturday "Biometric Online Voting System in Nigeria". *International Journal of Computer Trends and Technology (IJCTT)* V49(1):18-26, July 2017.

[9] Rachna Jain, Sushila Madan, Bindu Garg " E-Voting System using Homomorphic Encryption in a cloud Based Environment ", *International Journal Of Security And its Application*, Vol.11, pp 59-68, 2017.