ISSN 2347 - 3983
Volume 8. No. 9, September 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter202892020.pdf
https://doi.org/10.30534/ijeter/2020/202892020

Dactylogram Based Voting System Using Image Encryption and Symmetric Key Encryption

Dr.G.Amudha[1], Nandhini.R[2], Gomathi.S[3],Hansika.V.R[4]
[1]R.M.D. Engineering College, India, gav.cse@rmd.ac.in
[2]Newgen Software Technologies, India, ucs16218@rmd.ac.in
[3]R.M.D. Engineering College, India,ucs16122@rmd.ac.in
[4]R.M.D. Engineering College, India,ucs16126@rmd.ac.in

ABSTRACT

In Online, Security plays an important role including payments, social activities, electoral application educational sites, etc. The Secure voting system and its process are ensured by an encryption and decryption process and its main goal is to provide high security and authorization to the data involved in the process and also the data that has been stored in the database. Security is the priority needed in every activity that is involved in the process. Using Triple-DES encryption and decryption algorithm, the fingerprint of the user has been captured from the dataset and it undergoes Triple-DES encryption and decryption to provide security to data of each user. Here Dataset is used to store the fingerprint of each user after obtaining the fingerprint from the fingerprint scanner. The advantage of this security process is to secure data that cannot be breached by any unauthorized users and to provide ease of use and easy maintenance. The proposed method DBVS is efficient compared to RSA based algorithms.

Key words: Dactylogram, Fingerprint, Image Encryption, Triple-DES Encryption, Voting System.

1. INTRODUCTION

In recent days, voting system is being conducted in a fashion that the user details have been captured through a manual process in a paper format which contains their Name, DOB, Age, Address, Phone number, Aadhaar number, etc. has been captured and manually their generate a number for each user and prepare their id as a card and send back to the user.

2. TWO SORTS OF CRYPTOSYSTEM

2.1 Symmetric Cryptosystem

It uses the same key to perform encryption and decryption.

2.2 Asymmetric Cryptosystems

It uses a public key that encrypts the data accessed by anyone and the receiver uses his/her private key that is not known to anyone and even not to the sender. It is otherwise called a public- key cryptosystem.

On successful completion of the project, securely protects the voting system, that the unauthorized voter or user cannot vote more than one time that several people perform during the time of voting. This leads to multiple time voting of the same person to several parties and thus leads to fixtures during the voting time.

3. CRYPTOSYSTEM

The word Cryptography means the user can use any ofthe encryption algorithm Enc(x) and passes the encrypted text to the receiver, with this the receiver uses his/her private key to get back the plaintext which is the same as sender's text. The user will use the most secure algorithm to encrypt the plaintext so that the intruders cannot access the plaintext by guessing the key. This cipher text is then reached to the other end-user so they use some of the decryption algorithms by using the key that is used by the source user. To provide security in transferring the data the user will use the algorithm that follows these properties: Confidentiality, Security[19], and Authentication so the information sent by the user will be more protected and cannot be accessed by the intruders. Two cryptographic systems were used. One is Symmetric uses the same key to perform the encryption and decryption and the other one is Asymmetric uses a public key that encrypts the data accessed by anyone and decrypts with receivers private key to get the original data.

4. EXISTING SYSTEM

4.1Literature Survey

The security of the cloud data has attracted increasing attention from various communities, and a lot of fruitful research has been successful SumitA. Hirve et al. (2017). For example, this system allows eligible voters to vote even though they are away from their hometowns. The essential target of the proposed framework is to raise the general rate of voting by giving voting offices to individuals far from the place where they grew up. This framework includes enlistment of the voters intrigued by voting from their present city which is far from their home city. Registration requires voters to specify thedetails including name, address, phone number, email id, date of birth, Aadhaar Id, and fingerprint scan. These additional measures are used to make this system secure against manipulation and hacking. The officer in charge

will maintain a database of all the entries of voters. Secure Hash Algorithm (SHA1) using UTF8 encoding is used to encrypt the Aadhaar id and fingerprint scan while storing it in the database. This cryptographic algorithm will prevent original data from being manipulated or leaked. After the vote has been successfully cast, a confirmation mail will be sent to the respective voter. It is also stated that there is a drawback of cloning attack [9] or replica attack in this type of voting system; Balkrushna Bhagwatrao Kharmate et al.(2015)has explained thatAuthentication of the voters and their casted votes is the main goal in the electronic voting system. Since many fraudulent activities are happening during the voting period. The Security and Privacy of the data should be achieved so that the fake voting process can be achieved in the future generation. The Security not only be provided by avoiding unauthenticated users, it should be provided through a secured voting machine. If Voting Machine is having faults in its operation there will be a chance of fault votes happening during the election. The security of the data, Privacy of the votes, and the increase in the percent of casted voted plays a major role in deciding once the position in the election. This can be achieved by an Online voting System where the people can cast their votes from anywhere and at any time. The voter's authentication can be done with the help of UIDAI data and registration through fingerprint to the admin. The scanner senses the fingerprint and matches the stored image in the database and allows his/her to cast their votes in the election. The voter's details and cast votes for the particular user will be shared with the database which is nearby to the administration over the private network. Casting the votes and after the completion of the election, the captured votes are calculated and stored in the same database itself. It ensures the complete authentication of the users, security of the data, and privacy of the information [24] are protected against from unauthenticated users. The main thing is that distance does not matter allot. The person can deliver their votes from anywhere in the world and at any time. So this leads to the increase in voting percentage which will gradually raise the percentage to the winning candidate in the elections; Stephen Gibengo Fashoto et al. (2017) Electronic-Voting system is a significant part of the election process. The main goal of this process is to ensure the security of the votes and privacy of the voter's details who are casting their votes in the election. This process has been incorporated in many governmental and non-governmental organizations. But the main goal is to provide the security and privacy of the data. So we have provided an RSA algorithm technology where votes cast by the voters will be under complete privacy and security against intruders. The performance measures of this algorithm have been tested under the university elections over a network. This voting process will be initiated by the server system where all the nodes which act as subsystem will be connected to the server system. The votes are captured in the computer nodes where these votes are performed under the RSA algorithm and it is passed to the server system using the node and voters ID number. Thus this algorithm provides a good level of security to the votes and privacy of voter's details against the intruders or unauthenticated users over the network.

Ruchita Tekade et al.(2016) In this, we will provide security to the voting system by authenticating the users. Here the fingerprints of each user will be gathered and stored. The scanner will scan all the user's fingerprint and the Share Construction algorithm is used to divide scanned images into two shares, where one is stored in the database.The other share will be stored in Voter's ID Card (VIC). These two images are reconstructed and fresh images are gathered at the time of voting and both images are matched at the time of voting. If it is matched then the user is allowed to vote. After this, Homomorphic Encryption is used to perform the results gets counted. It makes a secure procedure against illegal activities;Friðrik Þ. Hjálmarsson et al. (2018)in this work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. The paper proposes a novel electronic voting system based on blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing an e-voting system. In particular, we evaluate the potential of distributed ledger technologies through the description of a case study; namely, the process of an election, and the implementation of a blockchain-based application, which improves the security and decreases the cost of hosting a nationwide election.

The drawbacks of the bitcoin system is even though it decreases the cost of hosting a nationwide election, it is highly not affordable for implementing this kind of system. Another major drawback of this kind of system is that bitcoin does not provide scalability;Mohammed Khasawneh et al. (2018)in this paper we propose a multi-faceted online e-voting system. The proposed system is capable of handling electronic ballots with multiple scopes at the same time, e.g., presidential, municipal, parliamentary, amongst others. The system caters for integrity of an election process in terms of the functional and non-functional requirements. The functional requirements embedded in the design of the proposed system warrant well-secured identification and authentication processes for the voter through the use of combined simple biometrics. Data breaches – the biometrics can still be hacked. Tracking and data – Biometric devices like facial recognition systems can limit privacy for the users;N. Aditya Sundar.M.V. Kishore et al (2018)Secure Voting System is very secure, efficient and easy for casting of votes. In this paper we will use RSA [1, 2] and MD5 [1, 2] algorithms for security purposes.Our proposed system provides a new e-voting system which fulfills the security requirements of e-voting process. In our project we have total three steps are required e-registration of voter, vote uploading and result display.Proposed system provides secure and efficient e-vote uploading and also paper ballot system if e-voting fail MD5 implementation: All the attacker needs with a 128-byte block of data, aligned on a 64-byte boundary of this algorithm. Safdar Shaheen, Muhammad Yousaf. et al.proposes that Free and fair elections are indispensable to quantify the sentiments of the populace for forming the government of representatives in democratic countries. Due to its procedural variation from different country and its

complexity, to maneuverer, it is a risky task. Since the Orthodox paper-based electoral systems are slow and error-prone, therefore, a secure and efficient electoral system always remained a key area of research. In this article, proposes a new secure and efficient electronic voting scheme based on public key cryptosystem dubbed as Number Theory Research Unit (NTRU). An effective and robust three factors authentication protocol based on a personalized memorable password, a smartcard, and bio Hash is proposed to ensure the validation of the legitimacy of a voter for casting a legal vote. NTRU based blind signatures are used to accommodate the anonymity and privacy of vote and voters, hence the accuracy of secure and reliable counting of votes is achieved through NTRU based homomorphic tally.

5. PROPOSED SYSTEM

The content involved in the process is that the voting system with the dactylogram (i.e.).The fingerprint[22] of each user is captured and then the obtained image is stored in the dataset where all the images of the fingerprint of the user are stored. These images are then encrypted Encrypt (image [I]) where I represents each user, the encryption algorithm preferred is Triple DES algorithm using three keys. Finger print that are generated by the user are encrypted using triple DES algorithm and output of the encrypted text is cipher(X) obtained is decrypted Decrypt (cipher(X)) with the same generated three keys to obtaining back the plaintext. This plaintext is stored in the dataset and the fingerprint is retrieved through SQL queries. On the login of the user, these fingerprints are fetched from the dataset by uploading the file from the dataset through their Name and DOB details that are stored in the database.

6. MODULES USED

6.1 Admin

This is the primary module utilized in our project which incorporates like admin name, their dob, the password has to be gathered if it's a replacement admin and if it's already existing admin they will use their name and password to log in with their account to manage the user's account. This module also has the responsibility of adding new users and allowing them to cast their votes and release their voting results.

6.2 User

6.2.1 Existing User

In this module the user has got to enter his or her details like Name, DOB and Aadhaar id alongside this, their fingerprint has been captured from the dataset. These details are checked with a database during which it contains of these details that are stored in the database If the credentials are passed then they're allowed to vote by selecting the candidates from the list and count is taken and therefore the results are released after the whole voting is completed.

6.2.2New User

In this module if the user may be a new one they need to enter their details like Name, Father's and Mother's Name, DOB, Age, Address, State, City, Phone number, District, Pin code and their ward Number, Ward Address and their valid Aadhaar number along with this their fingerprint has been taken. The fingerprint will be encrypted and decrypted using the Triple-DES algorithm and the secured information is stored within the dataset.

6.2.3Casting Votes

In these modules, the user has to enter their details such as Name, DOB, Aadhaar id, and their fingerprint has been captured and matched with the database. If the credentials are passed and they are allowed to move to the voting page where they can select the candidates from the available list, select them, and the count will be incremented by one, which will be updated in the database automatically. Here the credentials are encrypted and stored.

6.2.4 Declaring Results

In these modules each candidate is granted with some votes that are polled by the users and the count is credited automatically and the result is being directed by reading the details from the database by the admin.

7. ALGORITHM USED

7.1 Triple Des

Figure 1. Block diagram explains about Triple DataEncryption Standard (TDEA or Triple DEA), is a symmetric-keyblock cipher, which performs the DEScipher algorithm thrice to each data block. It uses a key size of 112 or 168 or 56 bits. It is the basic form of Feistel structure which includes 48 rounds that each block could perform. This is the first module used in our project which includes such as admin name, their dob, the password has to be gathered if it is a new admin and if it is already existing admin they can use their name and password to log in with their account to manage the user's account. This module also has the responsibility of adding new users and allowing them to cast their votes and release their voting results.

Here the fingerprint is encrypted using DES algorithm where cipher text is generated and again it is encrypted using the second set of key, finally the generated cipher text is encrypted using the thir*d key*.

This final cipher text is been stored in the database. Our results show that time taken to perform triple DES algorithm outperforms theRSA algorithm and DES algorithm due to its increase in key size.

7.2 Data Set

In this module, if the user is a new one they have to enter their details such as Name, Father's and Mother's Name, DOB, Age, Address, State, City, Phone number, District, Pin code, and their ward number, Ward Address and their valid

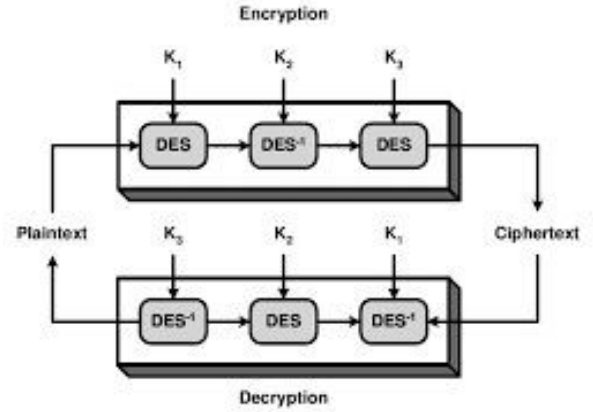


Figure 1: Triple 3-DES

Aadhaar number along with this their fingerprint have been taken. The fingerprint has been encrypted and decrypted using the Triple-DES algorithm and the secured data is stored in the dataset. From the dataset, the fingerprint is uploaded in the database. From the dataset, the fingerprint is matched during the time of voting. Here more number of encrypted fingerprints are stored. Our test shows that the time taken to retrieve the fingerprint image from the database is very less. Similarly time taken to decrypt the data which is retrieved from the dataset is also feasible.

7.3 Components of a Data Set

A data set consists of the following components:

7.3.1 Element: The data values collected for each entity. Entities considered are Name, Age, Date of Birth, Aadhaar number, Biometric parameter like fingerprint.

7.3.2 Variable: A characteristics values of each data element. For each of the entities specified the values are been stored and the validation for each entity is been specified.

7.3.3 Observation: The package of measures for each element. Based on the values entered the observation is made and stored to identify the entity.

7.4 DBVS

Our DBVS algorithm basically accepts the parameters as specified in the data set. In that one of the entity is fingerprint. As shown in the below diagram, first fingerprint from our hand istaken as input. This is the raw data received from the user. Now the encryption process is started where the raw data is converted to an encrypted message .The scanned image is processed by Triple DES Encryption algorithm by using generated keys (k1, k2, k3) from which Cipher text is generated. Key are generated using pseudorandom function. Encrypted fingerprint is now decrypted by Triple DES Decryption algorithm using generated keys (k3, k2, k1).

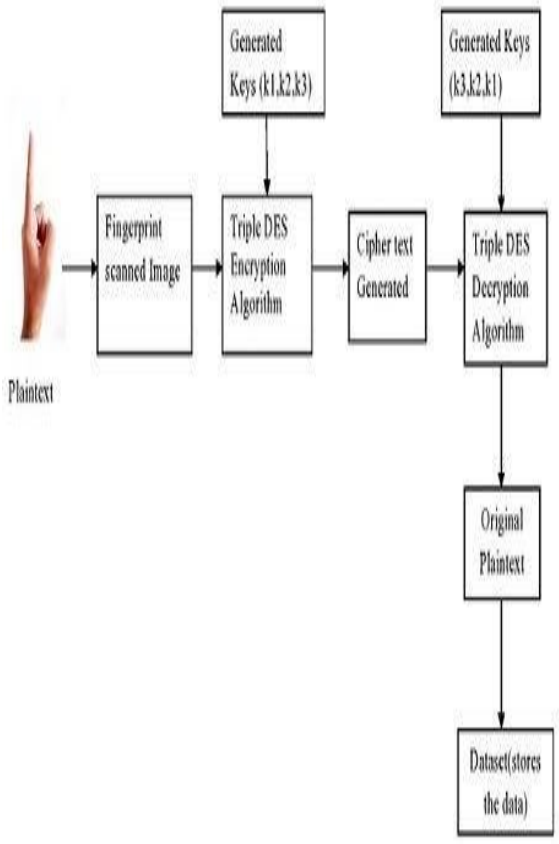


Figure 2: Architecture Diagram for generating 3-DES using keys

Figure 2 explains as, Keys which are used in encryption are used in reverse in the decryption process. Now we have obtained the original plain text as output. This decryption is done while casting the vote. User validation is done by this image comparison.

Open the application is on, it will take you to the user login page. The website prompts you to enter the Name, Date of Birth, Aadhar card number and fingerprint. Kindly enter the details required. If the data entered matches with the existing database of the application, the user will be taken forward to the viewing page.

In the viewing page, the user can be able to see the list of polling candidates, that is, the list of candidates who are participating in the election.

The user can vote for his/her preferred candidate by selecting the name of the candidate. Thereby, the user's vote will be marked for the respective person and can exit the application.

If the data entered in the login page of the application did not match with the existing database, the user will be prompted to create a new user credential by signing up.

During signing up, the user must give his details and fingerprint. The fingerprint thus collected will be saved in the database after encryption and will be used for further use after decryption. Once the user creates a new login, he can move on to cast his vote following the steps mentioned earlier.

8. PSEUDOCODE

```
private TripleDESCryptoServiceProvider des = new
TripleDESCryptoServiceProvider();
public DES(string key)
{
des.Key = UTF8Encoding.UTF8.GetBytes(key);
des.Mode = CipherMode.ECB;
des.Padding = PaddingMode.PKCS7;
}
public void EncryptFile(string filepath)
{
byte[] Bytes = File.ReadAllBytes(filepath);
byte[] eBytes =
des.CreateEncryptor().TransformFinalBlock(Bytes,0,Bytes.
Length);
File.WriteAllBytes(filepath,eBytes);
}
public void DecryptFile(string filepath)
{
byte[] Bytes = File.ReadAllBytes(filepath);
byte[] dBytes =
des.CreateDecryptor().TransformFinalBlock(Bytes,0,Bytes.
Length);
File.WriteAllBytes(filepath,dBytes);
}
```

9. RESULT ANALYSIS

Figure 3 explains as,The login page has two options for Admin and User .For admin to login, he/she can select admin and enter their name and password, if it is a new admin then enter Admin Name, Date of Birth, along with their password. Once entered the admin can manage user's account and release the results. For Users, they have to select user from the login page, and enter their details which includes their Name, Date of Birth, and Aadhaar id along with their fingerprint .Once checked and verified with details in the dataset, the user is taken to the list of polling candidates to cast their vote. If their login details does not match or the user is a new user then ,the user have to sign up by giving their details, where includes their Name, Father's andmother'sname,DateofBirth,Age,Address,state,City,Phonenumber,District,Pincode,ward number and address, valid Aadhaar id and also finally their fingerprint. These details are stored in the dataset. Once giving all the details, now the user can login and give their votesAadhaar details are used to validate the user. Admin can be able to update the candidate details using the console.After user registration, users can login and can be able to cast the vote using his fingerprint.

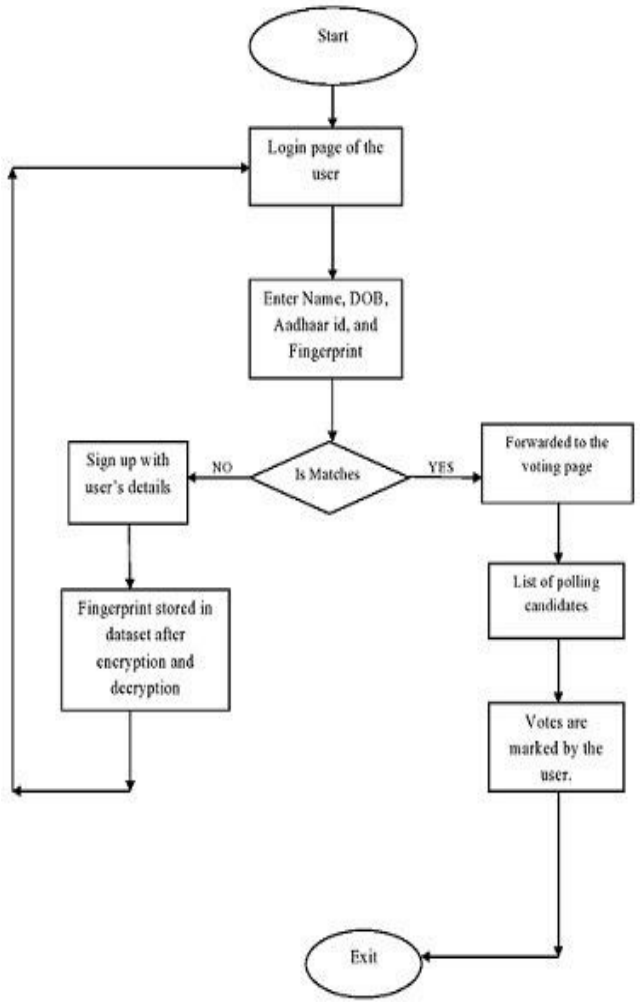


Figure 3: Flowchart for the Process

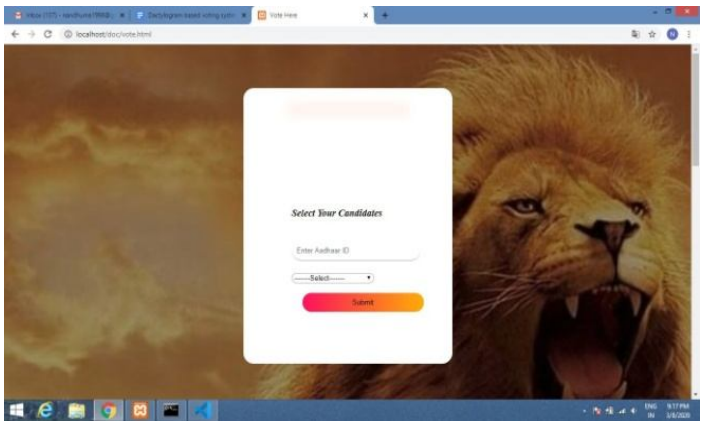


Figure 4: Admin and User Module

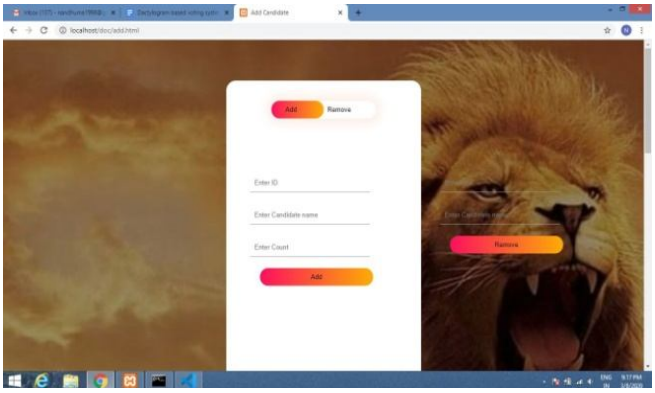


Figure 5: Admin Login and Register Page

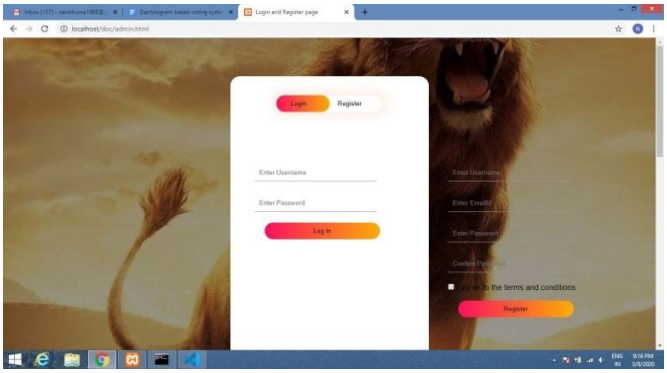


Figure 6: User Login and Register Page

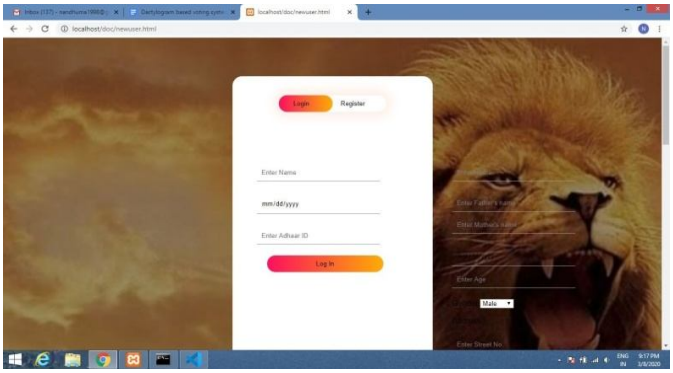


Figure 7: Add and Remove Candidate by Admin

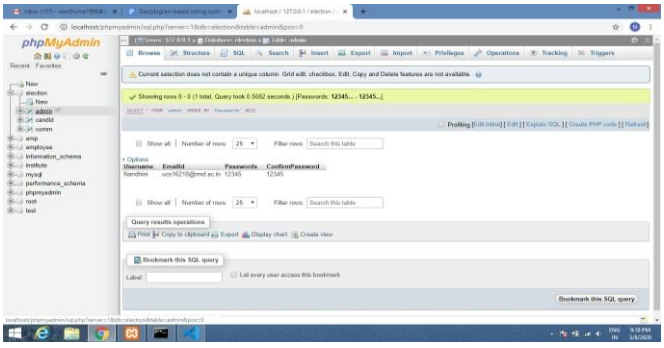


Figure 8: Database of Admin Module

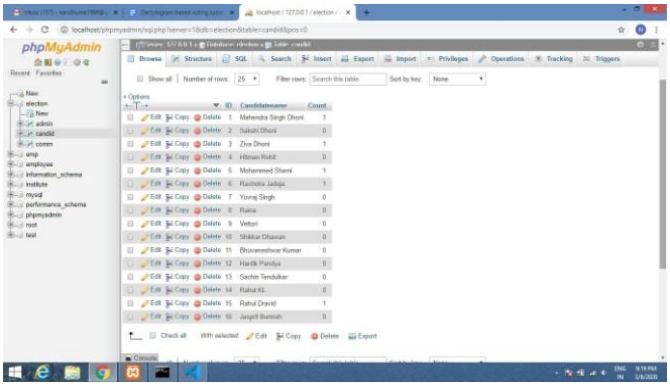


Figure 9: Database of Candidate Module

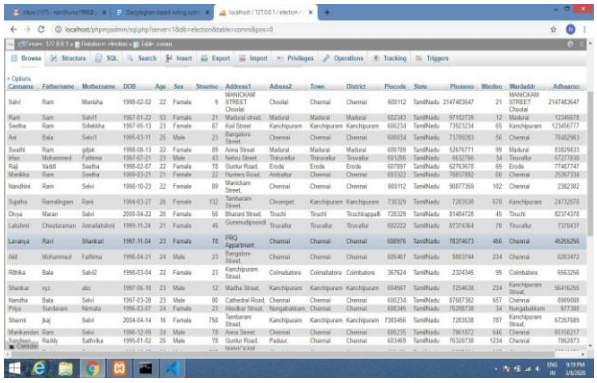
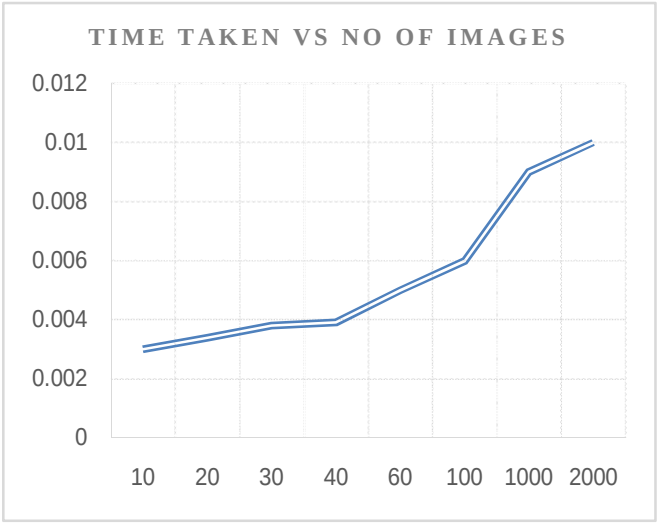


Figure 10: Database of User Module

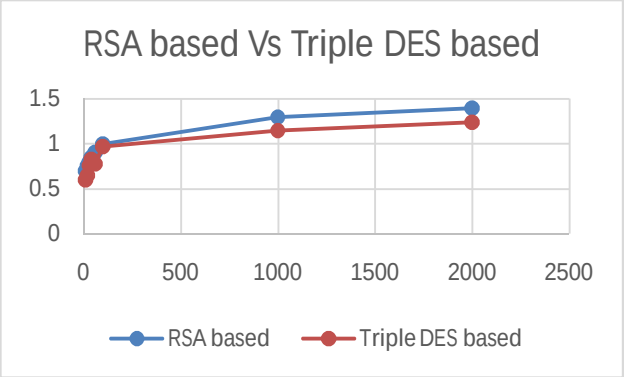
Figure 4-7 represents about the login of the user and admin, Register of the user and admin. The admin has the rights to add the candidate and Remove the candidate.
Figure8-10represents the database screenshots of the Admin. User and the Candidate.

9.1 Latency

If the number of images increasing also time taken is not that much increased.



9.2 No of Keys



In Triple DES there are three keys are used which makes the man in the middle attack to be impossible. This depicts that time taken to implement the image encryption is enhanced in Triple DES.Whereas the time taken is more in RSA based algorithm in the e-voting system.

10.CONCLUSION

Thus it provides a secure voting system that can provide a secure and smooth way of the voting process. It also protects fraudulent activities such as voting more than once can be avoided. Through this Authentication, Confidentiality and Security can be provided. Hence the security process proposed in this paper ensures that the secure data that cannot be breached by any unauthorized users and to provide ease of use and easy maintenance.

REFERENCES

[1] R.Rivest, A.Shamir, and L.Adheman. **A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM,** 21(2): 120-126, 1978. Computer Science pages 223-238. Springer, 1999

[2] G.I. Davida, Y. Frankel, B.J. Matt, **Secure offline Biometric Identification**, Oakland, 1998.

[3] Payal V.Parmar, Shraddha B.Padhar, Shfika N.Patel, Niyatee I.Bhatt, Rutvij H.Jhaveri, "**Survey of various homomorphic encryption algorithms and schemes**," International Journal of Computer Applications. Vol. 91(8), April 2014.

[4] Saarinen, M.-J.O., **Cryptanalysis of block ciphers on SHA-1.** Lecture notes on Computer Science Vol.2887- 2003.

[5] A.Rose, A.Othman. **Visual Cryptography for Biometric Privacy** Pages 70-81 Volume-6, Issue 1; March 2011.

[6] A Deshpande2, Bhagat3, Bhagia4, P. Zavar5, **Fingerprint Recognition with Cryptography Algorithm** - 2017.

[7] Punithavathi Ramesh, Geetha Subbiah, **Visual Cryptography for Secure Images-VIT** University - June 2018.

[8] Richard Clayton, **Times Higher Education Supplement** (U.K.), October 2005.

[9]Gunasekaran, Amudha; Narayanasamy, P.**Analyzing the Network Performance of Various Replica Detection Algorithms in Wireless Sensor Network**, - Journal of Computational and Theoretical Nanoscience, 2018, doi:10.1166/jctn.2018.7188, Volume 15, Number 3, March 2018, pp. 989-994(6)

[10] Agarwal H. and Pandey G., "**Online Voting System for India Based on AADHAAR ID**," in Proceedings of 11th International Conference on ICT and Knowledge Engineering, Bangkok, pp. 1-4, 2013. Alsaidi N. and Yassin.

[11] "BITRU: Binary Version of the NTRU **Public Key Cryptosystem via Binary Algebra**," International Journal of Advanced Computer Science and Applications

[12] Arooj A. and Riaz M., **"Electronic Voting with Biometric Verification Offline and Hybrid Evms Solution**," in Proceedings of 6th International Conference on Innovative Computing Technology, Dublin, pp. 332-337, 2016.

[13] Canard S. and Sibert H., "Votinbox-**A Voting System Based on Smart Cards,**" France Telecom, Research and Development, 42 rue des Coutures, BP 6243, F-14066 Caen Cedex 4, France, 2008.

[14]http://williamstallings.com/NetSec/NetSec3e.html

[15] R. Mercuri.**Electronic vote Tabulation Checks and Balances**. PhD thesis, university of pennsylvania, philadelphia,P.A,October 2000.

[16] Online voting,Parliamentary Office of Science and Technology May 2001.

[17] McGaley margarer,McCarthy Joe,**Transparency and eVoting democratic Vs Commercial interests**.

[18] Top-to-Bottom Review I California Secretary of State, 2007.

[19] Sanaa Sharaf, "**Security Issues in Serverless Computing Architecture**" International Journal of Emerging Trends in Engineering Research (2020)., https://doi.org/10.30534/ijeter/2020/43822020

[20] Liquid democracy uses blockchain to fix politics and now you can vote for it, 2018.

[21] Ajit Kulkarni, "**How to Choose Between Public And Permissioned Blockchain For Your Project**" in Chronicled, 2018.

[22] Ramya K Josephine B Praveen K Maruthi M Kumar C. "**An efficient and secured biometric authentication for IoT",**International Journal of Emerging Trends in Engineering Research (2019) 7(11) 604-609, 10.30534/ijeter/2019/327112019

[23] Nicholas Weaver, Secure the Vote Today, 2016.

[24]L. Ramprasad and G. Amudha, "**Spammer detection and tagging based user generated video search system — A survey,"** *International Conference on Information Communication and Embedded Systems (ICICES2014)*, Chennai, 2014, pp. 1-5, doi: 10.1109/ICICES.2014.7033826.