

Implementation of E-Voting Using Fingerprint Recognition with Cryptographic Algorithm

Sumit A. Hirve¹, Manali A Deshpande², Bilquees B Bhagat³, Puja C Bhagia⁴, Nikita P Zavar⁵

Assistant Professor, Department of CSE, M.E.S College of Engg, SavitribaiPhule Pune University, Pune, India¹

B.E Student, Department of CSE, M.E.S College of Engg, SavitribaiPhule Pune University, Pune, India²

B.E Student, Department of CSE, M.E.S College of Engg, SavitribaiPhule Pune University, Pune, India³

B.E Student, Department of CSE, M.E.S College of Engg, SavitribaiPhule Pune University, Pune, India⁴

B.E Student, Department of CSE, M.E.S College of Engg, SavitribaiPhule Pune University, Pune, India⁵

ABSTRACT: As India is a making country, voting recognize a fundamental part to pick the possible destiny of the country and its subjects. Electronic voting (otherwise called e-voting) will be voting utilizing electronic intends to either help or deal with the tasks of throwing and numbering votes. Electronic Voting Machine (EVM) is a basic electronic gadget used to record votes set up of ticket papers and boxes which were utilized before in ordinary voting framework. Since Voting is the basic right of every Indian, each individual should be given equal opportunity to vote. Voting in this day and age is accessible just for voters who are available in the place where they grew up amid race period. This system allows eligible voters to vote even though they are away from their home towns. The essential target of the proposed framework is to raise the general rate of voting by giving voting office 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 their personal details including name, address, phone number, email id, date of birth, aadhar 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 aadhar 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.

KEYWORDS: E-voting, offline voting, security, SHA1, Fingerprint recognition, UTF-8 Encoding.

I. INTRODUCTION

The web based voting framework is the framework actualized to make the voting framework simple for booth polling and furthermore for the head to view and check the outcome for every region individually. Here the voting is done from current place with notwithstanding the region in which they were raised. Electronic voting is frequently observed as an apparatus for making the appointive prepare more proficient and for expanding trust in its administration. E-voting significantly lessens coordinate human control and impact in this procedure. In E-voting framework, a voter can utilize his/her voting ideal to vote online with no trouble. Legitimately actualized, e-voting arrangements can build the security of the vote, accelerate the preparing of results and make voting simpler. Nonetheless, the difficulties are extensive. If not painstakingly arranged and composed, e-voting can undermine the trust in the entire discretionary process.

The voters interested in using this system need to register first with the system administrator. Enrolment is principally done by the framework manager for security reasons. The framework Administrator enrolls the voters on the framework by essentially filling an enlistment shape to enlist voter. Natives looking for enrolment are relied upon to contact the

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

framework overseer to present their points of interest. New client can be just made by the head of the system. Security is the main concern of this system, therefore, we are making use of cryptographic algorithm to encrypt the aadhar id and the fingerprint scan of the voters before storing it in the database. The algorithm is named as Secure Hash Algorithm (SHA1). The algorithm uses UTF-8 Encoding for storing the hash value in the database.

Aadhar id is used for authentication purpose to authenticate whether the person is who he says he is. Aadhar card is used since it is exceptional for every individual. Fingerprint recognition is implemented for verification of the voter casting vote. Fingerprint scan taken at the time of registration is compared to the fingerprint scanned at the time of voting. If both the fingerprints match then voter is allowed to cast his vote. Fingerprints remain constant throughout life and they are unique for each individual. Fingerprint scan being a type of biometric system is more secure than passwords or tokens.

Biometric innovation deal with the physical attributes, similar to face, irises, veins or behavioural qualities like your voice, you're penmanship. Biometric verification is that each individual is one of a kind and every individual can be distinguished by his or her natural or conduct attributes. Biometric technology can perceive a man on the premise of the novel components of their face, unique mark, mark, and DNA or iris example and after that grant a safe and advantageous strategy for validation purposes.

Advantage of using Biometric system over password:

The obvious favourable position of biometric innovation contrasted with more customary or conventional validation techniques, for example, individual ID cards, attractive cards, keys or passwords, is that it is naturally connected to a distinct individual and subsequently not effectively traded off through robbery, conspiracy or misfortune.

Most bio-metric frameworks are anything but difficult to utilize and this rearranges client administration bringing about cost reserve funds to the relevant provider or industry. Clients don't have to recall passwords or PIN numbers and client accounts can't be shared. In the event that enhanced dependability or security is required, it is conceivable to utilize a mix of at least one biometric advancements, for example, facial and voice acknowledgment.

II. RELATED WORK

A few governments joined these two societal improvements to electronic voting. In any case, to bounce from paper vote into web voting requires a great deal of middle of the road ventures, through voting machines, remote paper ticket and after that remote e-voting. The mama chine had the motivation behind recognizing contrasting options to mechanize the voting procedure and characterize the measures fundamental for its execution, beginning from the 1996 races in more than 50 municipalities.

The hardware, in charge of 100% of the robotization of the decisions, was then discharged in Brazil in 1996 and today fills in as a model for some different nations that have tried the capacity of the mama chine for the usage of their constituent procedures. E-voting has been embraced in different countries on the planet, both created nations, for example, the United States of America, Japan, Ireland, Canada, France, Belgium, Austria and Switzerland and creating nations, for example, Brazil, India, Russia, Paraguay, Philippines, Kazakhstan, Venezuela, and Estonia. As a result of the diverse conditions pertaining in these nations the act of e-voting has delivered shifted comes about, some fruitful, others unsuccessful. By 2011 five nations had relinquished e-voting. One of them was the Netherlands, the primary nation to have presented e-voting (exactly 20 years prior). The others were Germany, the United Kingdom, Ireland and Australia. The fundamental explanations behind surrendering e-voting were worries about information security, unquestionable status and accreditation and cost.

III. ALGORITHMS USED

Message Digest 5 (MD5):

We start by assuming that we have a b-bit message as info, and that we wish to discover its message digest. Here b is an arbitrary nonnegative whole number; b might be zero, it require not be a numerous of eight, and it might be arbitrarily huge. We envision the bits of the message recorded as takes after:

$$m_0 m_1 \dots m_{\{b-1\}}$$

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

The accompanying five stages are performed to register the message digest of the message.

Step 1. Appending Padding Bits. The original message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. The padding rules are:

- The original message is always padded with one bit "1" first.
- Then zero or more bits "0" are padded to bring the length of the message up to 64 bits less than a multiple of 512.

Step 2. Appending Length. 64 bits are appended to the end of the padded message to indicate the length of the original message in bytes. The rules of appending length are:

- The length of the original message in bytes is converted to its binary format of 64 bits. If overflow happens, only the low-order 64 bits are used.
- Break the 64-bit length into 2 words (32 bits each).
- The low-order word is appended first and followed by the high-order word.

Step 3. Initializing MD Buffer. MD5 algorithm requires a 128-bit buffer with a specific initial value. The rules of initializing buffer are:

The buffer is divided into 4 words (32 bits each), named as A, B, C, and D.

- Word A is initialized to: 0x67452301.
- Word B is initialized to: 0xEFCDAB89.
- Word C is initialized to: 0x98BADCFE.
- Word D is initialized to: 0x10325476.

Step 4. Processing Message in 512-bit Blocks. This is the main step of MD 5 algorithm, which loops through the padded and appended message in blocks of 512 bits each. For each input block, 4 rounds of operations are performed with 16 operations in each round. This step can be described in the following pseudo code slightly modified from the RFC 1321's version:

Do the following:

```
/* Process each 16-word block. */
```

```
For i = 0 to N/16-1 do
```

```
/* Copy block i into X. */
```

```
For j = 0 to 15 do
```

```
Set X[j] to M[i*16+j].
```

```
end /* of loop on j */
```

```
/* Save A as AA, B as BB, C as CC, and D as DD. */
```

```
AA = A
```

```
BB = B
```

```
CC = C
```

```
DD = D
```

```
/* Round 1. */
```

```
/* Let [abcd k s i] denote the operation
```

```
a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s). */
```

```
/* Do the following 16 operations. */
```

```
[ABCD 0 7 1] [DABC 1 12 2] [CDAB 2 17 3] [BCDA 3 22 4]
```

```
[ABCD 4 7 5] [DABC 5 12 6] [CDAB 6 17 7] [BCDA 7 22 8]
```

```
[ABCD 8 7 9] [DABC 9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
```

```
[ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]
```

```
/* Round 2. */
```

```
/* Let [abcd k s i] denote the operation
```

```
a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s). */
```

```
/* Do the following 16 operations. */
```

```
[ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20]
```

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

```
[ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24]
[ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]
[ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]
```

/* Round 3. */

/* Let [abcd k s t] denote the operation

$a = b + ((a + H(b,c,d) + X[k] + T[i]) \lll s)$. */

/* Do the following 16 operations. */

```
[ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
[ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]
[ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]
[ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]
```

/* Round 4. */

/* Let [abcd k s t] denote the operation

$a = b + ((a + I(b,c,d) + X[k] + T[i]) \lll s)$. */

/* Do the following 16 operations. */

```
[ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]
[ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]
[ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]
[ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]
```

/* Then perform the following additions. (That is increment each of the four registers by the value it had before this block was started.) */

A = A + AA

B = B + BB

C = C + CC

D = D + DD

end /* of loop on i */

Step 5. Output. The contents in buffer words A, B, C, D are returned in sequence with low-order byte first.

Secure Hash Algorithm(SHA-1):

SHA1 algorithm consists of 6 tasks:

Task 1. Appending Padding Bits. The original message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. The padding rules are:

- The original message is always padded with one bit "1" first.
- Then zero or more bits "0" are padded to bring the length of the message up to 64 bits less than a multiple of 512.

Task 2. Appending Length. 64 bits are appended to the end of the padded message to indicate the length of the original message in bytes. The rules of appending length are:

- The length of the original message in bytes is converted to its binary format of 64 bits. If overflow happens, only the low-order 64 bits are used.
- Break the 64-bit length into 2 words (32 bits each).
- The low-order word is appended first and followed by the high-order word.

Task 3. Preparing Processing Functions. SHA1 requires 80 processing functions defined as:

$f(t;B,C,D) = (B \text{ AND } C) \text{ OR } ((\text{NOT } B) \text{ AND } D)$ (0 ≤ t ≤ 19)

$f(t;B,C,D) = B \text{ XOR } C \text{ XOR } D$ (20 ≤ t ≤ 39)

$f(t;B,C,D) = (B \text{ AND } C) \text{ OR } (B \text{ AND } D) \text{ OR } (C \text{ AND } D)$ (40 ≤ t ≤ 59)

$f(t;B,C,D) = B \text{ XOR } C \text{ XOR } D$ (60 ≤ t ≤ 79)

Task 4. Preparing Processing Constants. SHA1 requires 80 processing constant words defined as:

$K(t) = 0x5A827999$ (0 ≤ t ≤ 19)

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

$K(t) = 0x6ED9EBA1$ (20 $\leq t \leq 39$)

$K(t) = 0x8F1BBCDC$ (40 $\leq t \leq 59$)

$K(t) = 0xCA62C1D6$ (60 $\leq t \leq 79$)

Task 5. Initializing Buffers. SHA1 algorithm requires 5 word buffers with the following initial values:

$H0 = 0x67452301$

$H1 = 0xEFCDAB89$

$H2 = 0x98BADCFE$

$H3 = 0x10325476$

$H4 = 0xC3D2E1F0$

Task 6. Processing Message in 512-bit Blocks. This is the main task of SHA1 algorithm, which loops through the padded and appended message in blocks of 512 bits each. For each input block, a number of operations are performed. This task can be described in the following pseudo code slightly modified from the RFC 3174's method 1:

Input and predefined functions:

$M[1, 2, \dots, N]$: Blocks of the padded and appended message

$f(0;B,C,D), f(1;B,C,D), \dots, f(79;B,C,D)$: Defined as above

$K(0), K(1), \dots, K(79)$: Defined as above

$H0, H1, H2, H3, H4, H5$: Word buffers with initial values

Algorithm:

For loop on $k = 1$ to N

$(W(0), W(1), \dots, W(15)) = M[k]$ /* Divide $M[k]$ into 16 words */

For $t = 16$ to 79 do:

$W(t) = (W(t-3) \text{ XOR } W(t-8) \text{ XOR } W(t-14) \text{ XOR } W(t-16)) \lll 1$

$A = H0, B = H1, C = H2, D = H3, E = H4$

For $t = 0$ to 79 do:

$TEMP = A \lll 5 + f(t;B,C,D) + E + W(t) + K(t)$

$E = D, D = C, C = B \lll 30, B = A, A = TEMP$

End of for loop

$H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E$

End of for loop

Output:

$H0, H1, H2, H3, H4, H5$: Word buffers with final message digest

Output. The contents in $H0, H1, H2, H3, H4, H5$ are returned in sequence the message digest.

IV. PROPOSED WORK

The proposed algorithm for the system is given as follows:

1. As in the smart e-voting system there are totally work on digital information and digital data. There are multiple database uses for verification and authentication and data processing. The front end is web page by using which the voter interact with voting system and donate vote. Biometric system used for the user verification and it works online.
2. First voter are scan finger by using biometric scanner then the given data passes to the online database for verification after the data are verified the voter are allow for donate their vote. The Biometric scanner which is main connectivity of voter to the voting system.
3. The web page which front end to voter. Interactions with whole system are through this web page which provides multiple links for multiple users. Also the important data are allocated by using this web page.
4. The multiple databases such as SQL which is backend of whole system are working for data gathering, sorting, listing and providing security to vote as well as voter data. Login details are stored as hash values in database.
5. The whole data can be stored and process by under administration on the centralised database this approach are reduced data complication and duplication. Only administrator who's having authority to access the internal data

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

- by passing some security. In case of data duplication the database first finding match if duplication found discard the duplicate data and record for future use.
6. Middle layer is connectivity through which the whole process can be made to work. The connectivity of the front end to the backend is done by using middle layer which is the network layer. Network is secure and it is totally different from public domain which provides data security and hides from outer world.
 7. The SMS Gateway is used for user satisfaction. After user donate their vote only voting satisfactorily message are forward to user by using services.
 8. The counting of the votes and finding result for every election area are process done by using centralised server which is Hub of information and data of voting systems.
 9. The whole system process done based on digitally and on network based.

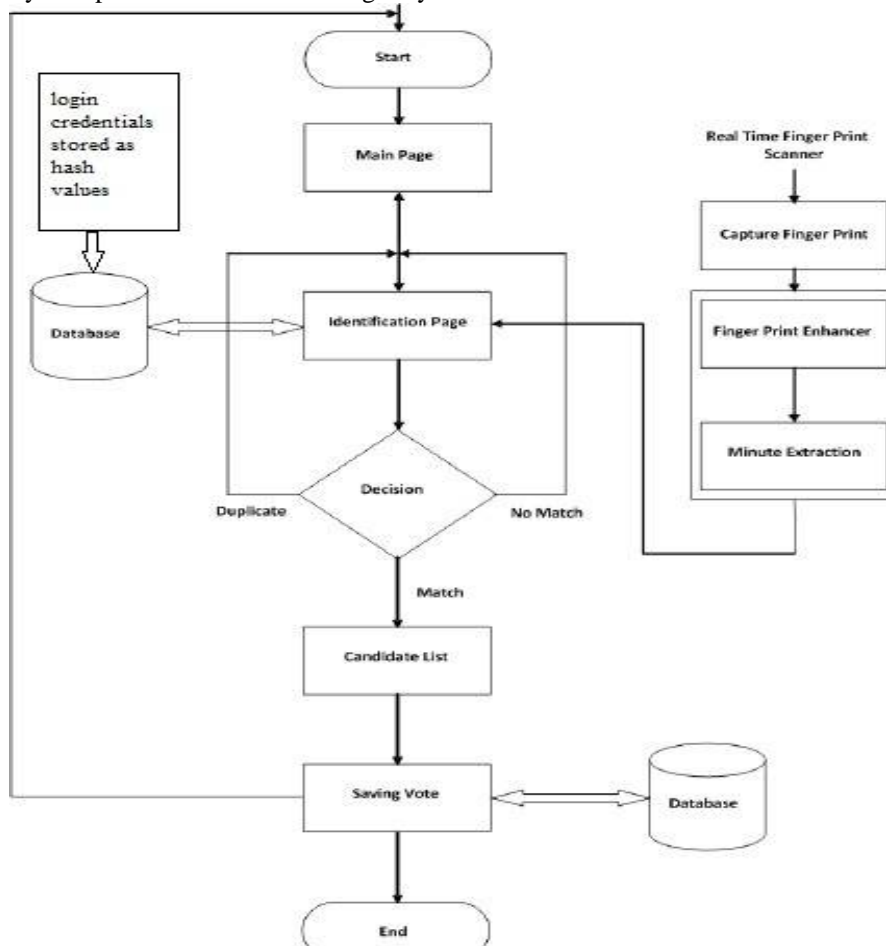


Fig 1: System implementation

Fig. 1 shows system implementation of the project. The various steps involved in the project is demonstrated using the above system architecture.

V. EXPERIMENTAL RESULTS

The GUI is prepared by making use of Eclipse IDE and SQLYog is used at the backend for storing data. Apache tomcat 8 is used to run servlet and JavaServer Pages (JSP) based web applications. Tomcat can also be used as HTTP server.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

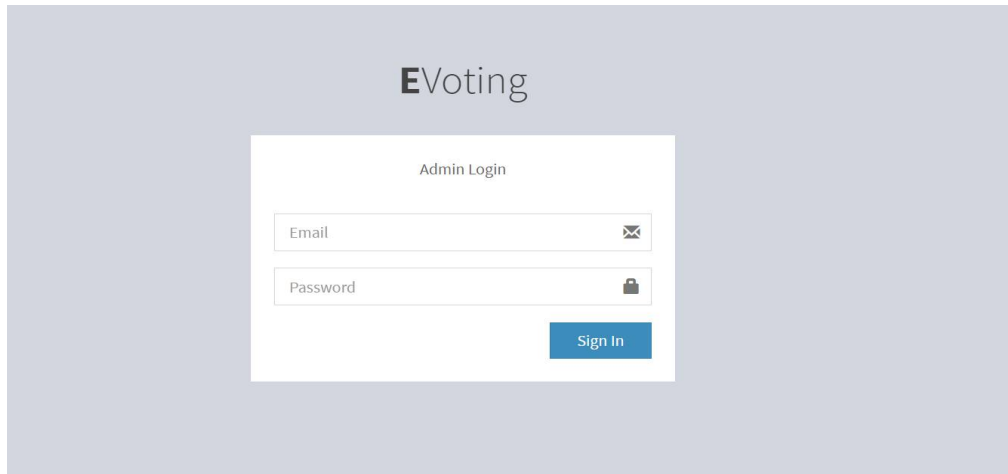


Fig 2:Admin Login

Fig. 2 shows admin login page of the project. Admin has to login using email id and password. The password is encrypted using Secure Hash Algorithm (SHA1) using UTF-8 Encoding.

After successful login, the admin can perform the following tasks:

1. Access voting panel to allow the voters to vote.
2. Perform registration of voters
3. Access voters list.
4. Perform registration of candidates.
5. Access candidates list.
6. Logout

id	fullname	email	contact	passwrđ	role
1	Bilquees	abc@gmail.com	4569412165	8w1DW+duKL8wTrClI4iduw==	admin
2	Admin	admin@gmail.com	9568563512	8w1DW+duKL8wTrClI4iduw==	admin
(Auto)	NULL	NULL	NULL	NULL	NULL

Fig 3: Admin Table in SQLYog

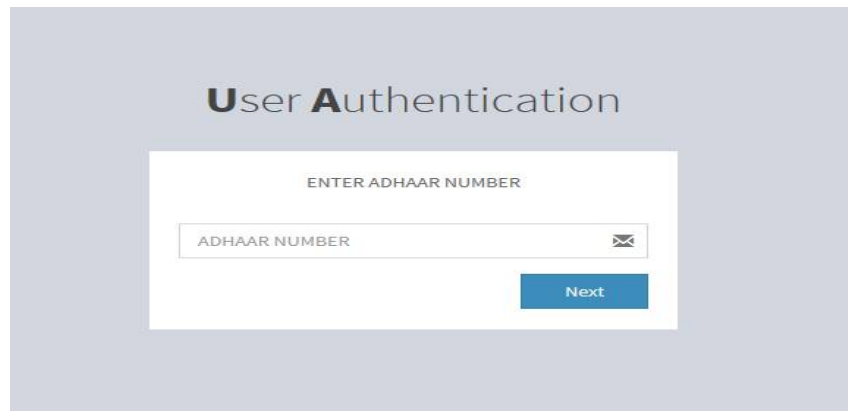
Fig. 3 shows the admin entries in the database. SHA1 algorithm is used to encrypt admin's login password while storing it in the database. This additional step will help in making the system more secure against hackers and will protect the system against any manipulation.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017



The image shows a web interface for user authentication. At the top, the text "User Authentication" is displayed. Below it, a white box contains the instruction "ENTER ADHAAR NUMBER". There is a text input field labeled "ADHAAR NUMBER" with a small envelope icon to its right. A blue button labeled "Next" is positioned below the input field.

Fig 4: Voting Panel

Fig. 4 shows the voting panel which will be available for the voters at the day of Voting. Voters have to enter aadhar id for verification purpose before they cast their vote. This step is taken to ensure that only eligible and registered voters cast their votes and it will also reduce chances of identity theft.

VI. CONCLUSION

Distinguishing proof of suitable innovation and its degree to use for secure electronic voting is the prime worry in discretionary process. Accomplishment of electronic voting relies on upon trust level and subsequently security issues should be tended to appropriately in configuration prepare remembering the social and political ramifications. This examination endeavours to fuse Fast and Accurate Biometric procedure into the E-Voting System to keep an unapproved individual to vote. This work has many focal points over the customary voting framework like decreased surveying time, less issues in discretionary planning, solid confirmation component, simple and precise tallying, and adaptability to voter for vote cast independent of land area. The proposed model and structure improves the security issues into the electronic voting framework regarding disposing of sham voting and vote redundancy, less race consumption, more straightforwardness. This system is expected to overcome the issues and vulnerabilities of current voting structure.

REFERENCES

- [1] Jean Bacon, Fellow, David Eyers, Thomas F. J.-M. Pasquier, Jatinder Singh, Ioannis Papagiannis and Peter Pietzuch, "Biometrics using Electronic Voting System with Embedded Security", IEEE Transactions on Network and Service Management, VOL. 11, NO. 1, MARCH 2014.
- [2] Adem Alpaslan Altun and Metin Bilgin, "Web based secure e-voting system with fingerprint authentication", Scientific Research and Essays Vol. 6(12), pp. 2494-2500, 18 June, 2011.
- [3] Reem Abdelkader and Moustafa Youssef, "UVote: A Ubiquitous E-Voting System", 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing.
- [4] Claudia Garcia-Zamora, Francisco Rodriguez Henriquez, Daniel Ortiz-Arroyo, "SELES: An e-Voting System for Medium Scale Online Elections," enc, pp.50-57, Sixth Mexican International Conference on Computer Science (ENC'05), 2005.
- [5] Hsing-Chung Chen and Rini Deviani, "A Secure E-Voting System Based on RSA Time-Lock Puzzle Mechanism", 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications.
- [6] Balkrushna Bhagwatrao Kharmate, Shahebaz Shaikh, Prashant Ravindra Kangane, Tushar Anant Lad, Prof. Ashvini Y. Bhamare, "A Survey on Smart E-Voting System Based On Fingerprint Recognition", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 9, September 2015. Aria Pezeshk and Richard L. Tutwiler, "Automatic Feature Extraction and Text Recognition from Scanned Topographic Maps", IEEE Transactions on geosciences and remote sensing, VOL. 49, NO. 12, 2011
- [7] Sanjay Kumar, Manpreet Singh, "DESIGN A SECURE ELECTRONIC VOTING SYSTEM USING FINGERPRINT TECHNIQUE", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

- [8] Alaguvel.R, Gnanavel.G2, Jagadhambal.K , “Biometrics using Electronic Voting System with Embedded Security”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.
- [9] M.O Yinyeh, K.A. Gbolagade, “Overview of Biometric Electronic Voting System in Ghana”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.
- [10] FirasHazzaa, SeifedineKadry, New System of E-voting Using Fingerprint, International Journal of Emerging Technology and Advanced Engineering”, Vol 2, pp 355-363, 2012
- [11] Muhammad Imran Razzak, RubiyahYusof and Marzuki Khalid, “Multimodal face and finger veins biometric authentication”, Scientific Research and Essays Vol. 5(17), pp. 2529-2534, 4 September, 2010.
- [12] Mrs. S.M.Shinde, Mrs. PritiSubramanium, “BIOMETRIC GSM VOTING SYSTEM”, International Journal of Technical Research and Applications, Volume 1, Issue 4, PP.103-107, September- October 2013.