ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Survey on Secured Biometrics Based Automatic Voting Machine

Shinde Rajashree Revaji, Thosar Devidas S.

Assistant Professor, Dept. of Electronics & Tele-Communication Engineering, SPPU, Pune, India

Assistant Professor, Dept. of Computer Engineering, SPPU, Pune, India

ABSTRACT: An electronic voting system is a selection system in which the election data is recorded, stored and processed primarily as digital information. India is a democratic country, where Voting plays important role in the Election process. Voting is considered as our central tariff as responsible citizens of the nation. An election voting system is used to store the vote which is in digital format. The electronic-voting can be done On-line. The On-line voting can be done using Internet connection. In case of traditionally voting system, voters need to go to distributed places like polling booths. The most important thing while dealing with e-voting system is Voter Authentication, E-voting process and the voted data. So while designing an e-voting system, system need to take care of the privacy of voter's data and provide security to the election system. So this project mainly works on the Security, Reliability and accessibility. This proposed system can achieve the security of an e-voting system, Availability and Ease of use to voters. System is also very cooperative for administration purpose to declare the result within minute, and to avoid the duplication of voting. Electronic Voting can play a really vital role in the democracy of our life. In this paper, we propose an electronic voting protocol. Our scheme does not require a special voting channel and communication can occur entirely over the current Internet. This method integrates the Internet convenience and cryptology. This paper analyses the various existing protocols such as simple protocol, Two Agency protocol, Blind Signature Protocol. In the existing protocol the Tallier has to wait until the decryption key is received from the voter. So it will consume lot of time. Instead of getting the decryption key value from the voter, the Tallier maintains the key information securely in the database. So, comparatively the proposed protocol consumes less time. This paper also analyses the various security issues involved in an electronic voting like security, privacy, authentication, anonymous, uniqueness, accuracy, fairness, efficiency and enforceability.

KEYWORDS: E-voting, Security, Privacy, Anonymity, Online Voting, Cryptology, Privacy, Security and Internet, Case diagram.

I. INTRODUCTION

E-voting is an election system that allows the populace to choose their representative by recording his or her secret ballot by some electronic means. In today's era internet voting, have won considerable surveillance as possible that promise to make the electoral process much simpler and efficient for political parties, candidates, election administration, and most importantly, for electors. In 2004, it's estimated that almost 30% of the voting population in the US used some form of e-voting technology. Security is a staple in e-voting process. Therefore the necessity of designing a secure e-voting system is important. There are different levels of maintaining e-voting security. Security must be applied to hide votes from outsiders. For countries like Brazil, India and the Philippines, e-voting and electronic counting means that people can get authoritative election results seconds, instead of days or weeks.

This paper finding the information related to e-security of computer science are focusing on e-secure election system to search extracting will able to make voting technically controlled, more secure and time consuming. The e-secure election system is most useful for public to voting. The procedure of election has very tough media reporting mostly if happen wrong something. It will improve system security of level to assurance of voter. The voting system defined the online voting system is most useful to voter can vote from anywhere to vote. The online voting system can be reduced the counting of votes and ballots. To online voting system is very hard to trust on online system because it requires more security as compared to physical system. Privacy is important in online system because any one cannot find votes to given to which party. Administrator register voter information of the election process as below first step begin with

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

voter basic information like voter name, voter age, voter address, sex ,voter id etc. In the central database which is mentioned by election commission. Then next registration phase voter face photo stored in database. Then next administrator scan left forefinger and stored in central database. This information validate when voter come for voting at election date.

II. PRESENT VOTING SCENARIO IN INDIA

Now the election seems to be a great messy proceeding. On or before election days transport system totally ceases and maximum surface transport vehicles are taken off the road for election purpose. Moreover official works in a majority of public sectors are suspended during election months. Officers and staffs from public sectors are appointed on election duties. As a result the public sectors have to face a complete disorder and the employees, customers related to it also suffer a lot. Schools, colleges and other related institutions are taken as polling stations or DCRCs (Distribution Centre cum Receiving Canters) for distribution and collection of voting equipments, related documents & applications, to the polling officers. For these, the official works, classes are suspended and the students have to face various problems.

On a particular election day, the election booths become heavily crowded. People have to stand in the scorching sunlight for hours just to cast “a vote”. Aged people and senior citizens have to face the same problems. Pregnant women and women with kids face great difficulty for the lack of various facilities; as a result a great percentage of these women do not come to the booths to cast their votes.

Fig. 1: Old & aged person standing in a long vote queue waiting for her turn

III. EXISTING SYSTEM

Social Many Parts has been divided by the election process. It is necessary to provide security to election system. So lots of man power is needed to election system and it conflict to manage by the system. Booths are provided by the election commission system and Booths will maintain by the schools. Voter has known about the booth location that where it will arranged. Time and place has been given by the election commission [10]. Thereafter, at the day of voting, voter has to go to the polling booths to do vote as shown in figure 2. Then identification is done by the officers of the voter. After that on voter’s left forefinger, marking is done by the officer using the ink. Then on register signature has to do. Then voter is going for the voting. Red lamp is blink and beep sound is hear when voter press the button of electronic ballot and that is indicate voting is done and it is stored [11] [12]. Every time this process is repeated. Lots of man power is required to this process.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

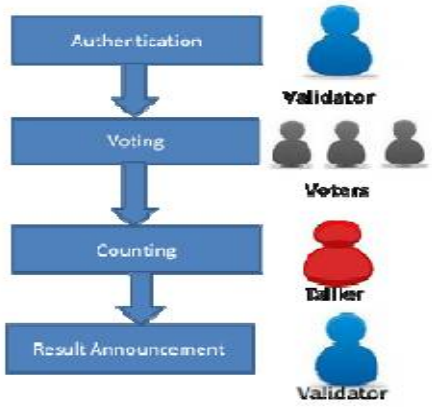

Fig. 2. Phases of Conventional Voting

Conventional Voting consists of the following four phases given in Fig 2. Authentication – Alice walks into a voting precinct and authenticates herself by showing her voting credentials; this step is public and verified by the officials present in the room. At the end of the authentication process, Alice is given a paper ballot on which to write her vote. Vote – The vote takes place in a protected booth where she cannot be seen by anyone. Alice casts her vote by writing it with a pencil on the paper ballot; she then folds the paper ballot and puts it in the ballot box where all the votes are mixed. Since no one can see what Alice writes and there are no marks on the paper ballots, Alice's vote is anonymous. Count votes – At the end of the voting time, the officials open the box containing the paper ballots and publicly count the votes; the results are then announced. Verification – Various types of verification are used or possible; most procedures are indeed public and overseen by representatives of competing parties. The opposite interests of the parties warrant the first level of protection against fraud. A recount is also possible if there is a presumption of fraud or error.

A. *ISSUE IN CONVENTIONAL VOTING:*

Conventional voting (such as voting by paper or signature voting) has many problems.

- Printing of ballot paper is expensive.
- Voting consumes lot of time.
- Counting is prone to errors.
- Maintaining convenient poll booths is very difficult.
- There is no good relationship between the government and popular, popular cannot trust the government and depend on it, voter here is like a blind person that must rely on the other person to vote for him.
- Sometimes, government coerced and carries on the voters to vote for a particular candidate, and eliminate them from voting freely.
- Some candidates trying to win by buy the votes from the voters.
- Government can cheat by substitute the original ballot by derivative ones.

According to all what is mentioned above, the whole world is moving on towards the trend of e-voting. Electronic voting systems are expected to be the solution for the weakness in traditional voting systems.

B. *ANALYSIS OF THE PROPOSED PROTOCOL:*

- **Privacy and Fairness** This scheme achieves privacy and fairness issues because no one can acquire any information about the tally result before the voting deadline. Before announcing the election outcome, each ballot will be in an encrypted form. Therefore no one can learn or predict the outcome of each vote before the tally announcement.

- **Uniqueness** No voter is able to vote more than once, by maintaining the status bit information; it prevents the double voting and because of this, it achieves uniqueness issue.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

- **Efficiency** The Transactions in the existing protocol are multiple, as the Tallier has to send the receipt to the voter to get the decryption key to decrypt the encrypted votes. This scheme achieves efficiency because these functions are carried out in a single transaction, as the Tallier does not have to wait for the decryption key from the voter. The advantages of the proposed scheme over the existing protocols are less complexity in implementation and consumption of very less time in the voting process.

- **Security** The proposed scheme achieves security by encrypting and decrypting the vote using RSA 512- bit public key algorithm. As the key size increased, it is very difficult for the hacker to find out the key to decrypt the encrypted vote during the time of transferring the vote from the voter to Tallier. The time to guess the key will be more and the whole process will be over by the time the key is guessed.

- **Anonymity**: In the existing protocol, to guarantee verifiability, the voter's encrypted vote will be sent to the voter with the key value to decrypt that vote. By decrypting that vote, the voter can verify that the voter's vote has been counted correctly. If it is verified by the voter, it violates the anonymity and Uncoercibility. So, this protocol advocate those voters not are allowed to verify their votes by themselves. It is not necessary to allow voter voters to verify (or Show to bribers) their votes in the announcement phase.

- **Uncoercibility**: This Scheme does not support uncoercion, since the voter is at a remote location, we cannot be sure that the voter is who she avows to be, unless we use a biometric authentication protocol. Even with the use of biometrics to authenticate, both eligible person and Eve (political person) sit in front of the same system (reserved for election) doing the authentication and Eve voting or monitoring the votes, as he wants. If voter wants to sell her vote, and Eve is not present, she can take a picture of his voting and give it to Eve as proof. In any case, the remoteness of the voter makes the abolition of the sale of votes impossible to fulfill for online voting.

IV. PROPOSED SYSTEM

Before talking about the proposed electronic voting system, we need to define the biometric token (smart card) and the nature of that token and why we use it in our system, and how it can be useful for the voters in election. In the proposed electronic voting system we will use biometric with smart token and we will use the iris pattern as a template, to verify the voter in the election. Once the Smart card is inserted by the voter into the poll machine match the Iris pattern template that is stored in smart card with the real time Iris pattern taken via camera using VeriEye techniques automatically. If the captured iris pattern matches the iris pattern templates in the smart card, the voter will be verified for the system. In this system, smart card is used as a storage media to store the information of the voters, other personal data and the Unique Id (11-digit number TN/99/0000012—In this, TN specifies the State, Next two digit specifies District Id and third one specifies the Unique id for each eligible voter) and Iris pattern (unique for each user-static one). Because it is a temporary storage media, andan anonymous media, which provide a secure way to save the information of the cardholders. In this system we are using 16 Kbytes EEPROM ACOS 3 smart card. The memory area provided by the card chip is basically segregated in internal data memory and user data memory.

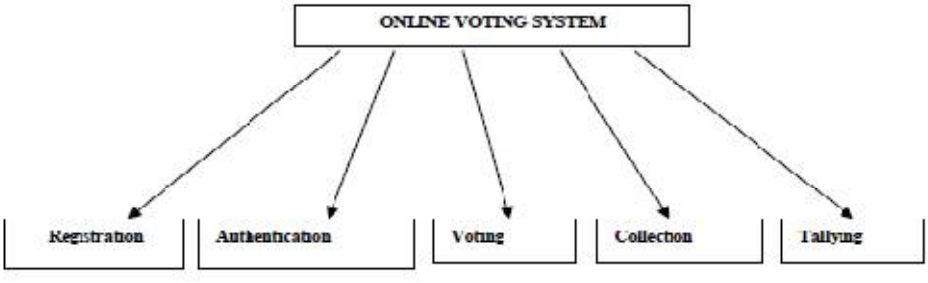

Fig. 3. Tasks of Online Voting System

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A. Registration

The process of voter registration is always done by Administrator before few days of the election process as follows: 1) Registration phase begins by storing the Voter information such as Unique Voter ID (11-digit number TN/99/0000012—In this, TN specifies the State, Next two digit specifies District Id and third one specifies the Unique id for each eligible voter), Name, Age, Sex, Address and District in the database. 2) Obtaining the Iris pattern of the voter and storing it in the Smart card. 3) Testing and issuing of the Smart card to the voter. This is a preparation step for implementing this system, only after the issue of the smart card after proper authentication and testing the smart card can be used. So, this step has to be started and completed before the process of election. In this phase, the corresponding public key and private key will be generated automatically using RSA algorithm for each voter. The Key information will be maintained by the Administrator securely.

B. Authentication

The voter identification (Authentication) is the first step in the process of voting according to this system as follows:

1) Obtaining the iris pattern of voter using an iris recognition device on the polling booths.
2) Obtaining the approved iris pattern of the voter from the smart card provide through smart card reader.
3) Comparing the two patterns to know whether they match or not. (To match the iris patterns, VeriEye technique is used)
4) On matching the voter identification is confirmed and further steps are taken.

5) On mismatch the voter is notified regarding the mismatch and proper enquiry and alternate solutions is done. Once the voter is authenticated, tallier checks the validity against the database whether the voter can cast vote or not. It extracts the Voter ID (unique id) from the smartcard, using that it compares the status of the voter whether it is 0 or 1. If status = 1, the voter can't cast vote. If status = 0, the voter is allowed to cast vote.

C. Voting

Once the voter is authenticated then, the Validator sends the confirmation message to the Tallier to conduct the vote. After this voter is provided with the graphical user interface to cast his/her vote.

The various steps involved are done by Validator as follows,

- Selection of the candidate by the user.
- Asked for confirmation of selection in the form of message box.
- On confirmation the vote is updated to the local database.
- On non-confirmation the voter is taken back to the candidates list screen to get the voters selection. The selection and confirmation of the vote is the user part in this module the connectivity and the updating of the local database which stores the votes are programmed to work in the background of the software.
- If the status is 0 then Tallier provides the voting page to voter to give vote.
- The voter selects the option by clicking the options.
- Immediately that vote will be updated in the local databases and the count will be incremented and the status is 1 will be updated for that voter.
- The vote will be encrypted with the Public key and sends the encrypted vote through the network. By this time all the votes that are casted are stored in the local database of each booth are sent to the distributed database for further processing like counting, announcement of results and record maintains.

D. Tallying

This part is completely hidden to the voter and this process is started only when the time for polling is over.

After receiving the encrypted vote the Tallier performs the following operations during counting phase:

- Tallier gets the private key and decrypts the vote.
- Immediately that total number of vote will be counted in the distributed databases and will be updated. Since the data are in the form of digital nature the counting process becomes very easy and the possibility of error in counting is negligibly small.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Cryptography for security: This protocol adopted with the existing Public key RSA algorithm. The protocol provides security taking the key size 512 bits. As the key size increased, it is very difficult for the hacker to find out the key to decrypt the encrypted vote during the time of transferring the vote from the voter to tallier. The time to guess the key will be more and the whole process will be over by the time the key is guessed.

V. USE CASE DIAGRAM

The following diagram depicts the use case specification of different modules.

Analysis of the Properties of the Proposed Protocol In this section, we will verify that the protocol previously proposed satisfies the main indispensable requirements to any electronic vote scheme.

Security Issues: The protocol provides security taking the key size 512 bits. As the key size increased, it is very difficult for the hacker to find out the key to decrypt the encrypted vote during the time of transferring the vote from the voter to tallier. The time to guess the key will be more and the whole process will be over by the time the key is guessed.

Single Transaction/Efficiency: The Transactions in the existing protocol are multiple, as the tallier has to send the receipt to the voter to get the decryption key to decrypt the encrypted votes.

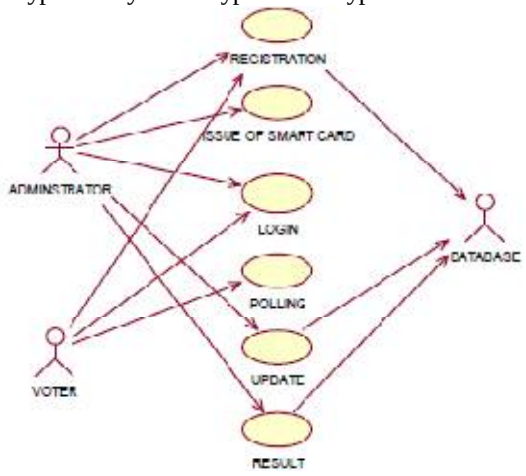

Fig. 4. Main Use Case Diagram

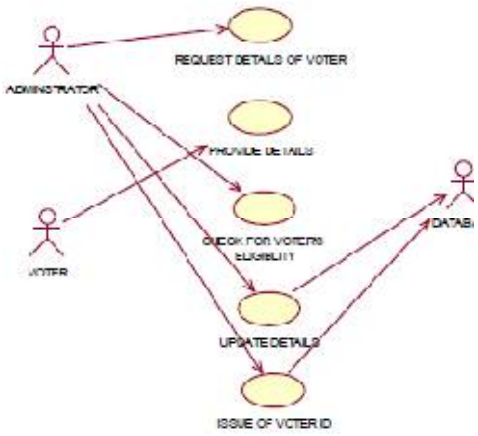

Fig. 5. Registration Use Case Diagram

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

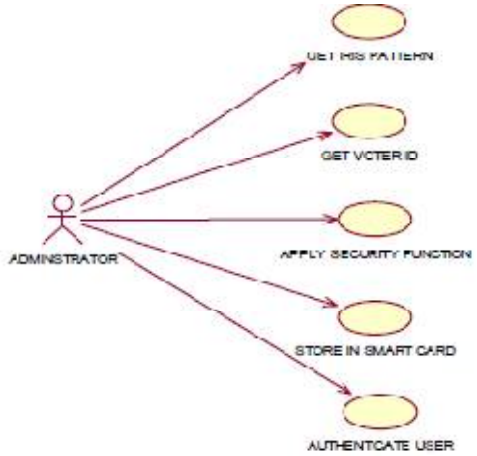

Fig. 6. Smart Card Use Case Diagram

In the proposed protocol these functions are carried out in a single transaction, as the tallier does not have to wait for the decryption key from the voter. The advantages of the proposed single transaction voting protocol over the existing protocols are less complexity in implementation and consumption of very less time in the voting process.

Comparison of the Existing Voting Protocols and the Proposed Protocol

The Comparison of the existing voting Protocols and the proposed protocol is given in Figure 7.

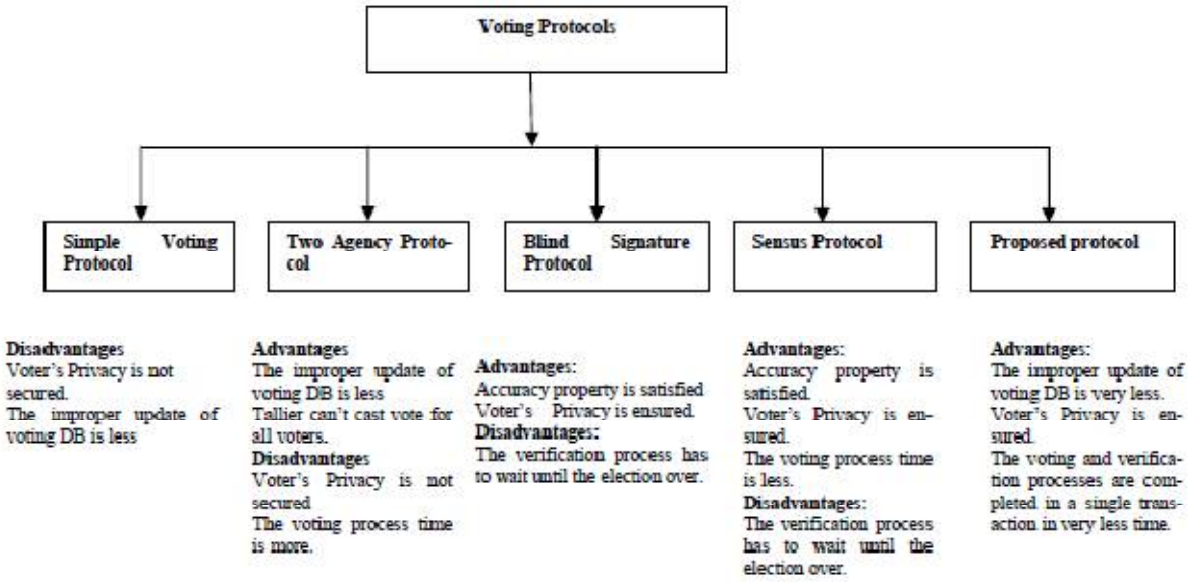

Fig. 7 Comparison among different protocols

VI. Conclusion and Future Work

The challenge for the system, and for this Administrative unit, is to face the difficulty revealed with each election and to commit processes that allow the system to acquire from one election to the next. This report attempted to highlight the reforms that can make a substantial difference in addressing the most recent set of concerns and describes the proposed model of E-Election system mostly for organization. The proposed system is much secure and expeditious than the normal electoral system. Influence of ballot and postponement of results can be avoided simply with the use of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

this E-Election system for voting. In the planned hypothesis, this paper will try to build a secure E- Election system that is free from unauthorized access throughout casting votes by the elector. It is expected that the proposed E-Election system will increase the reliability, opacity and security of the existing election system.

REFERENCES

1. Soumadip Sen, Sankhadip Sen, "Automatic Voting Machine – An Advanced Model for Secured Biometrics Based Voting System", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 7, July 2015.
2. Alaguvel.R, Gnanavel.G, J agadhambal.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.
3. Kalaichelvi Visvalingam, R. M. Chandrasekaran , "Secured Electronic Voting Protocol Using Biometric Authentication", Advances in Internet of Things, 2011, 1, 38-50 doi:10.4236/ait.2011.12006 Published Online July 2011
4. KALAICHELVI V, Dr. RM. CHANDRASEKARAN, "DESIGN AND ANALYSIS OF SECURED ELECTRONIC VOTING PROTOCOL", Journal of Theoretical and Applied Information Technology Vol. 34 No.2, 31st December 2011..
5. Masayuki Abe. Mix-networks on permutation networks In Advances in Cryptology |ASIACRYPT '99, vol. 1716 of LNCS, pp. 25-273. Springer-Verlag, 1999.
6. Markus Jakobsson. A Practical Mix. In Advances in Cryptology | EU-ROCRYPT '98, vol. 1403 of LNCS,pp. 448-461, Springer-Verlag, 1998.
7. W. Juang and C. Lei, "A secure and practical electronic voting scheme for real world environment," IEICE Trans. On Fundamentals, E80-A(1), January 1997.
8. Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In Proc. Of Workshop on Security Protocols '97, vol. 1361 of LNCS, pp. 25-35.Springer-Verlag, 1997.
9. Kazue Sako. Electronic voting schemes allowing open objection to the tally. In Transactions of IEICE, vol. E77-A No.1, Jan.1994.
10. Josh Cohen Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In Proc. 26th ACM Symposium on the Theory of Computing (STOC), pp. 544-553.ACM, 1994.
11. Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In Advances in Cryptology |AUSCRYPT '92, pp. 244-251, 1992.

BIOGRAPHY

Shinde Rajashree Revaji is a Assistant Professor in the Electronics & Tele-Communication Engineering Department, Sir Visvesvaraya Institute Of Technology, Savitribai Phule Pune University. She received Master of Engineering (ME) degree in 2014 from Savitribai Phule Pune University, MS, India.

Thosar Devidas S. is a Assistant Professor in the Computer Engineering Department, Sir Visvesvaraya Institute Of Technology, Savitribai Phule Pune University. He received Master of Engineering (ME) degree in 2015 from BAMU, Aurangabad, MS, India.