Journal of Theoretical and Applied Information Technology
31st December 2011. Vol. 34 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DESIGN AND ANALYSIS OF SECURED ELECTRONIC VOTING PROTOCOL

[1]KALAICHELVI V , [2] Dr.RM.CHANDRASEKARAN
[1]Asst. Professor (Ph. D Scholar), SRC- Sastra University, Kumbakonam, India
[2]Professor, Annamalai University, Annamalai Nagar, India
E-mail: [1]kalaichelvi2k@yahoo.com, [2]aurmc@sify.com

ABSTRACT

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 analyzes the various existing protocols such as simple protocol, Two Agency protocol, Blind Signature Protocol and Sensus 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 analyzes 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 and Internet*

1. INTRODUCTION

1.1 CONVENTIONAL VOTING

Conventional Voting consists of the following four phases given in ***Fig 1.***

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.

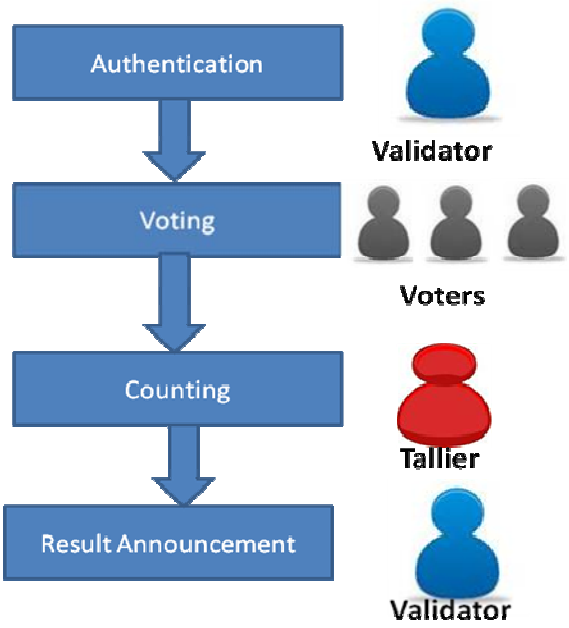

Fig 1. Phases of Conventional Voting

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1.2 ISSUES 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.

1.3 PROPERTIES/ISSUES / REQUIREMENTS OF AN ELECTRONIC VOTING:

The requirements in conventional voting (paper vote) are also apply for electronic voting, the requirements can be expected to be universal, and any system must try to apply these requirements:

Fairness : No one can learn the voting outcome before the tally.

Eligibility : Only eligible voters are permitted to vote.

Uniqueness : No voter should be able to vote more than once.

Privacy : No one can access any information about the voters vote.

Accuracy: All valid votes should be counted correctly.

Uncoercibility: No voter can prove how he voted to others to prevent bribery.

Anonymity: There should be no way to derive a link between the voter's identity and the marked ballot.

Efficiency: The computations can be performed within a reasonable amount of time.

Robustness : A malicious voters cannot frustrate or disturb the election.

Verifiability: Voters can check if their ballots have been correctly counted.

The rest of the paper is organized as follows: Section 2 presents the literature survey. Section 3 describes the existing voting protocol. Section 4 presents the problem definition of the proposed protocol, module description and features of the proposed protocol. Section 5 discusses the analysis of the proposed protocol and results. Section 6 presents the conclusion.

2.0 RELATED WORK

In the last few years a numerous number of researches propose different e-voting systems, and some countries and states around the world implement their e-voting system. However, this numerous number of e-voting schemes can be categorized into three main categories. The categories based on the cryptography mechanism used to build the system. The first category is e-voting system based on blind signature technique [1-3] The second category is e-voting system based on Mix-Nets [5-6]. The third and the last category is e-voting system based on homomorphic signature Properties [4-11]. Chaum was the first one to introduce blind signature and mixed nets. In general this different proposed system agree that the system should not be verifiable voting system (which mean the voter has no way to prove their voting activity) as a prevent technique against vote buying problem. However, some other e-voting system allows voter to prove their voting activities. Since the voting buying and the privacy of the voter is a critical problem in the Jordanian voting system we design our scheme as anonymous and unverifiable e-voting system, which categorize under the first category "blind signature-based e-voting system".

3.0 METHODOLOGY

3.1 EXISTING VOTING SCHEME

This section gives a brief introduction to the approaches used in various voting schemes.

3.1.1 SIMPLE PROTOCOL

This protocol is designed without employing any cryptographic techniques. In this voters would submit their vote along with a unique identification number to a Validator who would then take their name off on a list of registered voters. Then the Validator would then strike off the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Unique Identification number and submit just the votes to the Tallier who would count the votes. Although this system has the advantages of being flexible, convenient and mobile, this system is far from secure. If the Validator is compromised votes can be easily traced back to the voter or votes could be changed. Both privacy and accuracy lack with this protocol. There is no way to ensure the voter's privacy and the Tallier accurately records the votes.

3.1.2 TWO AGENCY PROTOCOLS

In this two agency protocols, the electronic Validator distributes a secret identification tag to each voter just prior to the election. The Validator then sends the Tallier a list of all identification tags, with no record of the corresponding voters. Each voter sends the Tallier his /her identification tag and an encrypted file containing a copy of the tag and the voted ballot. At this point the Tallier can make sure the identification tag is valid, but the program has no way of examining the contents of the ballot. The Tallier publishes the encrypted file, and the voter responds by sending the Tallier the key necessary to decrypt it. When the election is over, the Tallier publishes a list of all voted ballots and the corresponding encrypted files. This protocol also has several problems. Most importantly it doesn't protect the voter's privacy if the Tallier and Validator collude.

3.1.3 BLIND SIGNATURES

Blind signatures allow a document to be signed without revealing its contents. The effect is similar to placing a document and a sheet of carbon paper inside of the envelope. If somebody signs the outside of the envelope, they also sign the document on the inside of the envelope. The signature remains attached to the document, even when it is removed from the envelope [1-3]. The voter prepares a voted ballot, encrypts it with a secret key, and blinds it. The voter then signs the ballot and sends it to the Validator. The Validator verifies that the signature belongs to registered voter who has not yet voted. If the ballot is valid, the Validator signs the ballot and returns it to the voter. The voter removes the blinding encryption layer, revealing an encrypted ballot signed by the Validator. The voter then sends the resultant encrypted ballot to the Tallier. The Tallier checks the signature on the encrypted ballot. If the ballot is valid, the Tallier places it on a list that is published after all voters vote. After the list has been published, voters verify that their ballots are on the list and send the Tallier the decryption keys necessary to open their ballots. The Tallier uses these keys to decrypt the ballots and add the votes to the election tally.

3.1.4 SENSUS POLLING PROTOCOL

One of the drawbacks of the Blind Signature protocol is the voter has to wait till the voting has ended before the voter can verify the casted vote was the correct one, which is not in line with the property of flexibility. Sensus system is closely based on the Blind Signature protocol. The major difference between the schemes emerges after the voter has submitted the encrypted ballot to the Tallier. Instead of waiting till the voting ends the Tallier sends a receipt to the voter when his/her ballot has been received. This receipt is no more than a confirmation the vote has been transferred to the Tallier correctly. The voter may submit the decryption key immediately after receiving this receipt, completing the entire voting process in one session. The implemented Sensus system employs a pollster agent that performs all cryptographic functions and transactions with the election programs on the voter's behalf. Tests conducted with a prototype implementation of Sensus indicate that the entire voting process can be completed within a few minutes.

4.0 PROPOSED PROTOCOL

Before talking about the proposed electronic voting protocol we need to define the biometric token (smart card) and the feature of it, and why we use it in our system, and how can it be useful for the voters in election.

4.1 SMART CARD:

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) and the ***public key*** information. But why smart token, why it is the best for electronic voting?. Because it is a temporarily store media, and an 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. The internal data memory is used for the storage of configuration data and it is used by the card operating system to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to manage certain functions. The user data memory stores the data manipulated in the normal use of the card under the control of the application. Memory area is possible within the scope of data files and data records. The maximum number of data files allowed in ACOS 3 is 31. A data file can contain up to 255 records. User data files are allocated in the personalization stage of the card lifecycle. Once the **personalization bit** has been programmed there is no possibility of resetting the card back.

4.2 BIOMETRIC AUTHENTICATION

Biometrics is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition.

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During **Enrollment**, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison.

Biometric recognition can be used in **Identification** mode, where the biometric system identifies a person from the entire *enrolled* population by searching a data-base for a match based solely on the biometric. For ex-ample, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in **Verification** mode, where the biometric system authenticates a per-son's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an ac-count, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user. This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought unique and static one.

The proposed voting scheme is divided into a number of phases as drawn in ***Fig.4.1 – Fig.4.2.***

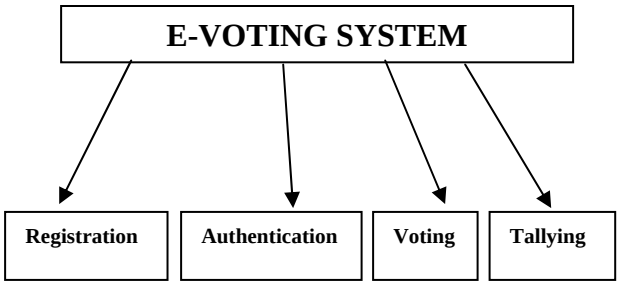

Fig 4.1 Phases of Electronic Voting

In the registration phase, Validator stores the voter's information like Unique Id, Address details, Iris pattern of the voter and the public key (based on RSA 512-bit) information into the smart card. After testing the smart card, Validator issues the smart card to the voter. This step has to be started and completed before the process of election.

The voter authentication is the first step in the process of voting according to this system. In this phase, First the voter inserts the smart card into the smart card reader, the Validator performs authentication by comparing the stored iris pattern and with the live iris pattern. If it is matched, the Validator sends the authenticated message to the Tallier. Tallier checks whether he is already voted or not. If the voter is not, the Tallier send's the candidate details to the voter. Once the voter is selected the candidate, the ballot is encrypted using the public key which is available in the smartcard and the encrypted ballot is transferred to the Tallier. Instead of waiting till the voting ends the Tallier sends a receipt to the voter when his/her ballot has been received and the Tallier strike off the voter's name from the registered list. . This receipt is no more than a confirmation the vote has been transferred to the Tallier correctly. Immediately the encrypted ballot is decrypted by using the corresponding private key which is kept secret by the Tallier.

In the existing protocol, the Tallier has to wait until the voter sends their corresponding private key. So, this proposed protocol completes the entire voting process in one session and completes within a few minutes.

Journal of Theoretical and Applied Information Technology
31st December 2011. Vol. 34 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

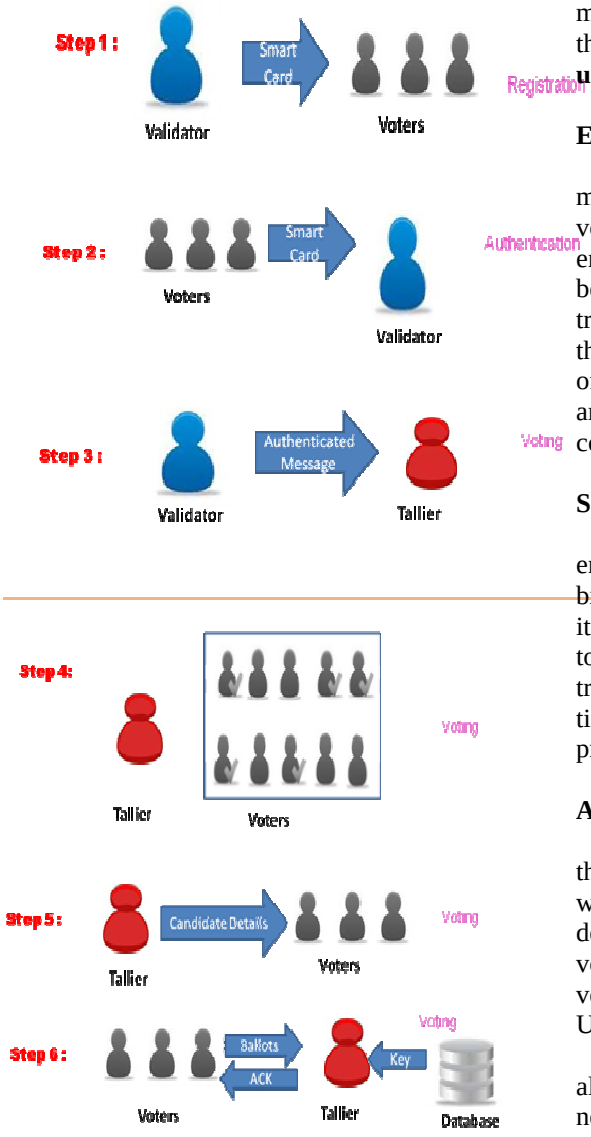

Fig 4.2 Steps involved in the Proposed Protocol

5.0 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.

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 be 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.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In practice, this means that online voting cannot be used in elections or polls where fraud by the sale of votes or coercion is concern, like in political elections.

The following table is the comparison of the various protocols [***Table 1***]:

Property	Simple Protocol	Two Agency Protocol	Blind Signature Protocol	Sensus Protocol	Proposed Protocol
Eligibility	Yes	Yes	Yes	Yes	Yes
Accuracy	No	Medium	Yes	Yes	Yes
Fairness	No	No	Yes	Yes	Yes
Efficiency	No	No	Medium	Medium	High
Privacy	No	No	Yes	Yes	Yes
Security	No	Yes	Yes	Yes	Yes
Uniqueness	No	No	Yes	Yes	Yes
Authentication	No	Medium	Yes	Yes	Yes
Verifiability	No	Yes	Yes	Medium	Medium
Anonymity	No	No	No	No	Yes
Uncoercibility	No	No	No	No	No

Table 1.Comparison of the Various Protocols

6.0 CONCLUSION

Electronic voting can play a really vital role in the democracy of our life. This paper proposed an electronic voting protocol and the new proposed protocol is compared with the various existing protocols. 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 discussed about how the proposed protocol achieves the following requirements such as fairness, uniqueness, accuracy, privacy, anonymous, authentication and un-coercion.

7.0 ACKNOWLEDGEMENT

I am grateful to **SASTRA** University, Thanjavur, Tamilnadu-India for providing the necessary facilities to carry out this work reported in this paper. I sincerely thank the Management for the generous financial support under Innovation Fund.

REFERENCES

[1]. 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. www.informatik.uni-trier.de/~ley/db/c...

[2]. 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. search.ieice.org/bin/summary.php%3Fid

[3]. Kazue Sako. Electronic voting schemes allowing open objection to the tally. In Transactions of IEICE, vol. E77-A No.1, Jan.1994. search.ieice.org/bin/summary.php%3Fid

[4]. 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. www.springerlink.com/index/91cf7ct3b9.

[5]. Markus Jakobsson. A Practical Mix. In Advances in Cryptology | EU-ROCRYPT '98, vol. 1403 of LNCS,pp. 448-461, Springer-Verlag, 1998. http://markus-jakobsson.com/papers/jakobsson-eurocrypt98.pdf

[6]. Masayuki Abe. Mix-networks on permutation networks In Advances in Cryptology |ASIACRYPT '99, vol. 1716 of LNCS, pp. 25-273. Springer-Verlag, 1999. **DOI:** 10.1007/978-3-540-48000-6_21

[7]. 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. **DOI:** 10.1145/195058.195407

[8]. Ronald Cramer, Matthew K. Franklin, Berry Schoenmakers, and Moti Yung. Multi-authority Secret-ballot elections with linear work. In Advances in Cryptology | EUROCRYPT '96, v ol. 1070 of LNCS, pp.72-83.Springer-Verlag, May 1996.**ISBN:**3-540-61186-X

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[9]. Ronald Cramer, Rosario Gennaro, and Berry S choenmakers. A secure and optimally efficient multi-authority election scheme. European Transactions on Telecommunications, 8:481-489, 1997. Preliminary version in Advances in Cryptology | EUROCRYPT '97.
DOI: 10.1007/3-540-69053-0_9

[10]. Kazue Sako and Joe Kilian. Secure voting using partially compatible homomorphisms. In Advances in Cryptology | CRYPTO '94, vol. 839 of LNCS, pp.411-424. Springer-Verlag, 1994.
DOI: 10.1007/3-540-48658-5_37

[11]. Kazue Sako and Joe Kilian. Receipt-free mixtype voting scheme A practical solution to the implementation of a voting booth. In Advances in Cryptology | EUROCRYPT '95, vol. 921 of LNCS, pp. 393{403. Springer-Verlag, 1995. ftp://thebaine.sabotage.org/pub/mirrors/Advances%20in%20Cryptology/HTML/PDF/E95/393.PDF

AUTHOR PROFILES:

Kalaichelvi V received her B.E degree in Computer Science and engineering from Bharathidasan University, Trichy in 1998 and M.E degree in Computer science engineering from Annamalai University, Chidambaram in 2004. She is working as a Assistant Professor in the Department of Computer science engineering from 2004 at SRC- SASTRA university. Currently, she is pursuing her Ph.D (ICE) in the Department of Computer Science engineering, Anna University Tiruchirappalli, Tamil Nadu, India. She has published more than 10 papers in national, international Conferences and 10 papers in Journals. Her research interest includes Cryptography, Network security, smart card applications and Mobile Security.

Dr.RM. Chandraekaran is currently working as a Professor at the Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Tamil Nadu, India. From 1999 to 2001 he worked as a software consultant in Etiam, Inc, California, USA. He received his Ph. D Degree in 2006 from Annamalai University, Chidambaram. He has conducted Workshops and Conferences in the Areas of Multimedia, Business Intelligence and Analysis of algorithms, Data Mining. He has presented and published more than 70 papers in conferences and journals and is the coauthor of the book Numerical Methods with C++ Program (PHI, 2005). His Research interests include Data Mining, Algorithms and Mobile computing. He is Life member of the Computer Society of India, Indian Society for Technical Education, Institute of Engineers, Indian Science Congress Association.