ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 7, July 2013

E-Voting System for on Duty Person Using RSA Algorithm with Kerberos Concept

Ms. Tanzila Afrin[1] , Prof.K.J.Satao[2]

Abstract: An electronic voting (e-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. There are many security challenges associated with the use of Internet voting solutions. Authentication of Voters, Security of voting process, Securing voted data are the main challenge of e-voting. This E-Voting system mainly for those people who are unable to come to the voting booth due to on duty leave or the people who are physically handicapped. In voting system there are many processes. This system having main four processes: firstly, application control process which involves the identification and authentication phases for the applied citizens. Secondly, the voting process which will be done by voter information. In Third section confirmation process, in this system check the image captured in application duration and match the image of voter which is online for giving vote for their identification. Finally the election server, administrator will sort out the final result by decipher the received encrypted information using private key.

Keyword:-Encryption, Decription, KDC, TGS

I.INTRODUCTION

There are two types of voting system: On-line and Offline. On-line, via Internet, and offline, by using a voting machine or an electronic polling booth.

Drawback of Offline voting system:

- In offline voting system physical presence is needed along with identification.
- Offline voting system is broadly divided into paper work.
- Time consuming.
- Take lots of time for declaring result.

Advantage of Online voting system:

- Voter can vote from any ware without going to voting booth. Mainly save votes of those people who are unable to come to the voting booth due to on duty leave, or the people who are physically handicapped.
- Less paper work
- Save time.
- Providing fast voting result.

Usages of new technology in the voting process improve the elections in natural. This new technology refers to electronic voting systems where the election data is recorded, stored and processed primarily as digital information.

The main goal of a secure e-voting is to ensure the privacy of the voters and accuracy of the votes. The authenticating voters and polling data security aspects for e-voting systems are discussed here.

A secure e-voting system is satisfies the following requirements:

- Eligibility: only votes of legitimate voters shall be taken into account;
- Un-reusability: each voter is allowed to cast one vote;
- Anonymity: votes are set secret;
- Accuracy: cast ballot cannot be altered. Therefore, it must not be possible to delete ballots nor to add ballots, once the election has been closed;
- Fairness: partial tabulation is impossible;
- Vote and go: once a voter has casted their vote, no further action prior to the end of the election;
- Public verifiability: anyone should be able to readily check the validity of the whole voting process.

The software engineering challenges:

- Accuracy: It is not possible for a vote to be altered eliminated the invalid vote cannot be counted from the finally tally.
- Democracy: It permits only eligible voters to vote and, it ensures that eligible voters vote only once.
- Privacy: Neither authority nor anyone else can link any ballot to the voter
- Verifiability: Independently verification of that all votes have been counted correctly.
- Resistance: No electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting.
- Availability: The system works properly as long as the poll stands and any voter can have access to it from the beginning to the end of the poll.
- Resume Ability: The system allows any voter to interrupt the voting process to resume it or restart it while the poll stands the existing elections were done in traditional way, using ballot, ink and tallying the votes later.

There are some main modules in an E-Voting system:

- Administration
- Verification
- Control
- Voting

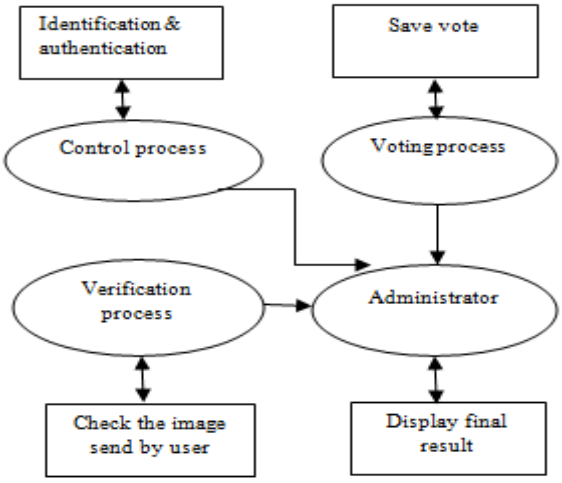

Fig-1:-A simple block diagram of E-Voting system.

II. METHODOLOGY:

II.I Secure information using Cryptography:-

Cryptography is the science of providing security for information. It has been used historically as a means of providing secure communication between individuals, government agencies, and military forces. Today, cryptography is a cornerstone of the modern security technologies used to protect information and resources on both open and closed networks. Public key cryptography [1] is one of the ways to protect data in network.

II.II Network Security & Cryptography

This is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is required to apply effective encryption/decryption methods to enhance data security.

For network authentication here we will use Kerberos concept [4]. Kerberos is a computer network authentication protocol which works on the basis of "tickets" to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed primarily at a client–server model, and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol messages are protected against replay and eavesdropping. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication. The proposed system architecture is shown in fig-2 as follows:

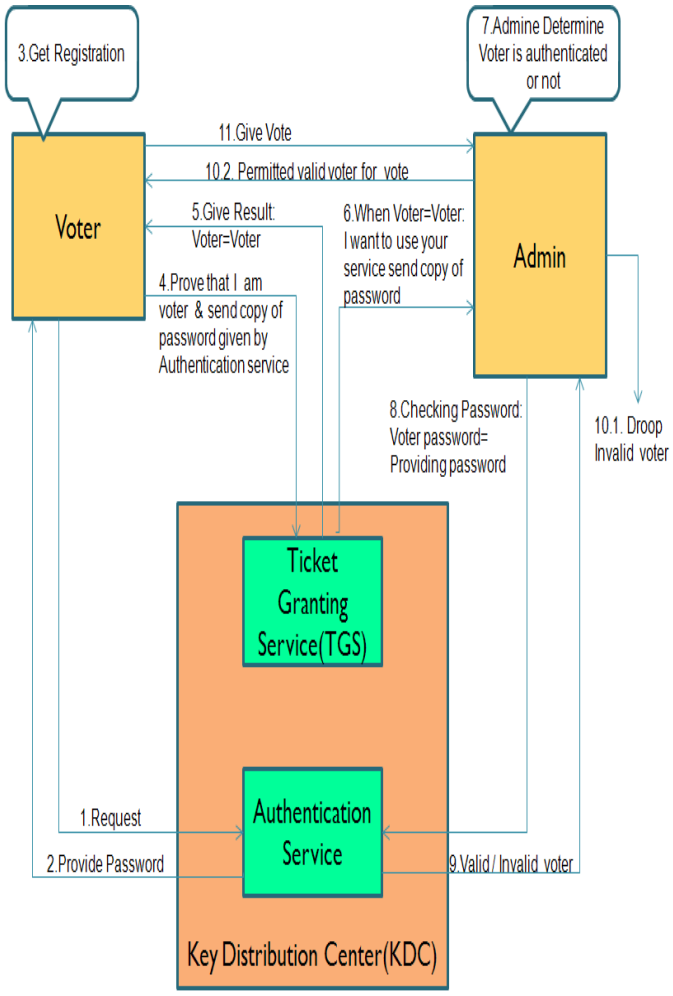

Fig-2:-Proposed system architecture

III. ALGORITHM USED

The public key in this cryptosystem consists of the value n, which is called the modulus, and the value e, which is called the public exponent. The private key consists of the modulus n and the value d, which is called the private exponent.

An RSA public-key / private-key pair can be generated by the following steps:

1. Generate a pair of large, random prime's p and q.
2. Compute the modulus n as n = pq.
3. Select an odd public exponent e between 3 and n-1 that is relatively prime to p-1 and q-1.
4. Compute the private exponent d from e, p and q.
5. Output (n, e) as the public key and (n, d) as the private key.

The encryption operation in the RSA cryptosystem is exponentiation to the e^{th} power modulo n:

$$c = \text{ENCRYPT}(m) = m^e \bmod n .$$

The input m is the message; the output c is the resulting cipher text. In practice, the message m is typically some kind of appropriately formatted key to be shared. The actual message is encrypted with the shared key using a traditional encryption algorithm. This construction makes it possible to encrypt a message of any length with only one exponentiation.

The decryption operation is exponentiation to the d^{th} power modulo n:

$$m = \text{DECRYPT}(c) = c^d \bmod n .$$

The relationship between the exponents e and d ensures that encryption and decryption are inverses, so that the Decryption operation recovers the original message m.Without the private key (n, d) (or equivalently the prime factors p and q), it's difficult because given only n, e, and c, but not the prime factors, it appears to be quite hard to recover the value m. to recover m from c. Consequently, n and e can be made public without compromising security, which is the basic requirement for a public-key cryptosystem.

The fact that the encryption and decryption operations are inverses and operate on the same set of inputs also means that the operations can be employed in reverse order to obtain a voter ID scheme following Diffie and Hellman's model. A message can be digitally signed by applying the decryption operation to it, i.e., by exponentiation it to the d^{th} power:

$$s = \text{VOTERID}(m) = m^d \bmod n .$$

The digital signature can then be verified by applying the encryption operation to it and comparing the result with and/or recovering the message:

$$m = \text{VERIFY}(s) = s^e \bmod n .$$

In practice, the plaintext m is generally some function of the message, for instance a formatted one-way hash of the message. This makes it possible to sign a message of any length with only one exponentiation.

III.I: *"Voter Account Maintenance":-*

When any voter register him/her self for voting process then this system verify voter is valid or not ,if voter is valid then creates an account of that voter and activated his/her account for particular election date, Once any individual passes the authenticity criteria, he/she will be logged into his/her voting account. We can easily restrict a voter from logging into his/her voting account more than once during that elections date. Once a particular voter is login using password given by the TGS, a secure channel will be established between voter and admin after that, he/she will be able to cast the vote. The vote will remain secret in every sense, i.e., it will not be reflected anywhere in the database that which user has voted for whom. Finally, the account will be automatically deactivated and that user will not be able to log back in by any means again. This completes the voting process.

IV. CONCLUSION AND FEATURE

The proposed scheme is an efficient electronic voting scheme that provides basic security requirements and the voter's identity remains hidden. It utilizes the advantages of the threshold cryptography to make the counting votes submit to group of authority. The secure internet voting system should not only allow all voters to verify the voting result but also avoid ballot buying. Therefore the proposed internet voting system uses proposed threshold blind signature to protect the content of the ballot during casting, the proposed internet voting system is verifiable and discourages ballot buying at the same time.

So our scheme is expected to serve as efficient and secure. At the end of the proposed protocol has been provided some of the most important security criteria for the electronic voting systems.

REFERENCES

[1]. Hayam K. Al-Anie," E-VOTING PROTOCOL BASED ON PUBLIC-KEY CRYPTOGRAPHY", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[2]. Gajendra Singh,Gajendra singh, " A Hyper Modern Cryptography Algorithm to Improved Data Security: HMCA" Vishwa Gupta et al, International Journal of Computer Science & Communication Networks,Vol 1(3), 258-263 258 ISSN:2249-5789

[3]. Xin Zhou," Research and Implementation of RSA Algorithm for Encryption and Decryption" 2011 The 6th International Forum on Strategic Technology, 978-1-4577-0399-7/111$26.00 ©20111EEE.

[4]. Rasmi P S et al," An Implementation of a New public key System based on RSA which leads hackers solve multiple hard problems to break the cipher" 12th International Conference on Intelligent Systems Design and Applications (ISDA),2012.

[5]. Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.
[6]. Hussein Khalid Abd-alrazzq1, Mohammad S. Ibrahim2 and Omar Abdul Rahman Dawood 3 "Secure Internet Voting System based on Public Key Kerberos", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012.
[7]. Menezes, A., P. Van Oorschot, and S. Vanstone, (1996), Handbook of Applied Cryptography, CRC Press, pp.4-15, 516.
[8]. I. Branovic, R. Giorgi, E. Martinelli, (2003) "Memory Performance of Public-Key Cryptography Methods in Mobile Environments", ACM SIGARCH Workshop on Memory performance: Dealing with RSA Laboratories, (2007) "What is a Hard Problem. RSA the Security Division of EMC"..
[9]. Jaydeep Howlader, Vivek Nair, Saikat Basu and A. K. Mal," UNCOERCIBILITY IN E-VOTING AND EAUCTIONING MECHANISMS USING DENIABLE ENCRYPTION ", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011..
[10]. Komminist Weldemariam et al," Formal Specification and Analysis of an e-Voting System", 2010 International Conference on Availability, Reliability and Security, DOI 10.1109/ARES.2010.83164,978-0-7695-3965-2/10 $26.00 © 2010 IEEE
[11]. Vishwa Gupta, Gajendra Singh, Ravindra Gupta " A Hyper Modern Cryptography Algorithm to Improved Data Security: HMCA", International Journal of Computer Science & Communication Networks, Vol 1(3), 258-263, ISSN:2249-5789
[12]. Kuldeep Singh, Rajesh Verma, Ritika Chehal," Modified Prime Number Factorization Algorithm (MPFA) For RSA Public Key Encryption", International Journal of Soft Computing and between voter and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012
[13]. C. Karlof, N. Sastry, and D. Wagner, (2005), "Cryptographic voting protocols: A Systems perspective", 14th USENIX Security Symposium, pp. 33-49.
[14]. M. Abo-Rizka, and H. Ghounaim, (2007) " A Novel in E-voting in Egypt", IJCSNS International Journal of Computer Science and Network Security, VOL.7, No.11.

About Authors:

Ms.Tanzila Afrin received the B.E. From Pt. *Ravishankar Shukla University, Raipur* (C.G.), India in Computer Science & Engineering in the year 2008. She is currently pursuing M.Tech. Degree in Computer Science Engineering with specialization in Software Engineering from CSVTU Bhilai (C.G.), India. She is currently working as Assistant Professor with the Department of Computer Science & Engineering in Chhattisgarh institute of Technology, Rajnandgaon (C.G.), and India. Her research areas include Software Engineering, Cryptography etc.

Prof. K. J. Satao is Computer Science & Engineering and Head of Information Technology Department at Rungta College of Engineering & Technology, Bhilai (C.G.),India. He has obtained his M.S. degree in Software Systems from BITS, Pilani(Rajasthan), India in 1991. He has published over 40 Papers in various reputed National & International Journals, Conferences, and Seminars. He is Dean of Computer & Information Technology faculty in Chhattisgarh Swami Vivekanand Technical University, Bhilai, India (A State Government University). He is a member of the Executive Council and the Academic Council of the University. He is a member of CSI and ISTE. He has worked in various Engineering Colleges for over 25 Years and has over 4 Years industrial experience. His area of research includes Operating Systems, Editors & IDEs, Information System Design & Development, Software Engineering, Modeling & Simulation, Operations Research, etc.