IET *Chennai and Dr.MGR University Second International Conference on Sustainable Energy and Intelligent System (SEISCON 2011), Dr. M.G.R. University, Maduravoyal, Chennai, Tamil Nadu, India. July. 20-22, 2011.*

Internet Voting Using Cloud Computing

S. Ramesh[1], **Dr.V. Muralibhaskaran**[2]

[1]Department of ComputerScience, Paavai College of Engineering, Namakkal, Tami Nadu, India
raameshs@gmail.com,
[2]Principal,Paavai College of Enginering, Namakkal, Tamil Nadu, India
murali66@gmail.com

Keywords: Internet Voting, Cloud Computing, Smart cards, Digital signing and encryption.

Abstract

In this paper we propose a novel I-voting scheme that allows voters to cast their vote using cloud computing technology. I-voting process comprises a series of cloud services mapping to the voters needs. This method combines both Internet and cryptographic technique. In this scheme the cloud services promising the voters to cast their vote in a secured way. The democracy, privacy, security are the important criteria for evaluating voting schemes. We propose I-voting use private or community cloud that can satisfy all security requirements. The advantage of this scheme is it consumes less time that results in overall speeding up the voting process and also reduce the expenditure for voting process.

1 Introduction

Voting is an efficient method for the public to show their opinion about a given topic or issue. It is the key of democracy; the constitution grants every citizen the right to vote[1]. Conventional paper based ballot or manual voting is inconvenient for voters it has some drawbacks such as decrease the rate of voting, in accuracy in ballot counting and delayed election results announcement[5]. In electronic voting use computers or computerized equipments to cast votes in elections. With rapid development of computer networks, the Internet has become a necessity for many people. A voter in any geographical area can participate in the election process. The beneficiaries are businessman, military and students who are doing their higher education. The electronic ID card or smart card issued by the governments as electronic document which is used as an authenticated proof for voting[13]. The Internet and cryptographic techniques are used to build the I-voting system is expecting to result with a voting system which confirms that only people with the right to vote are able to cast a vote emphasizing that every cast is counted only once. Requirement of I-voting

The requirement in E-voting are also apply to I-voting, the requirements can expected to be universal, any system must try to apply these requirements

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

Eligibility: Only registered voters are permitted to vote

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

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

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

Accuracy: All valid votes should be counted correctly.

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

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

The remainder of this paper is organized as follows. In section 2 describe I-voting algorithm. In section 3 details of cloud computing and its SAAS services and cloud types for voting. In section 4 we shows the participants and phases used in I-voting scheme. In section 5 and section 6 analyze the main goal and security issues that should satisfy all the requirements described above. Finally we present the conclusion in section 7.

2 I-voting algorithm

1. In the registration site voter fill the registration form that has username and password.
2. Voter input ID no as user name and PIN as password and feed UID details as proof.
3. Compare voter's information with cloud data centers electoral register.
4. Register the eligible voters.
5. Generate voting certificate or tokens to the voters.
6. Distribute the tokens/certificate to the voters either by mail or SMS.
7. Choose the method of voting i.e. E-voting, I-voting, or M-voting.
8. Submit necessary proof for Identification and authentication.
9. To cast his/her vote.
10. Encrypt the voter form and sent to private cloud data center.
11. To decrypt the vote from the cloud center and tally the votes.

3 Cloud Computing

Cloud Computing is evolving as a key computing platform for sharing resources that include infrastructures, software, applications, and business processes. Cloud computing collects all the computing resources and manages them automatically through software. In the process of data analysis, it integrates the history data and present data to make the collected information more accurate and provide more intelligent service for users and enterprises. Cloud Computing can be fused with grid computing, utility computing and autonomic computing.

3.1 Cloud Computing Services in I-voting

In cloud computing environment there exist three different services such as SaaS,PaaS and IaaS.The following SaaS services used in I –Voting are

Validation Service

This service will allow the eligible voters to register their vote. Its primary task is to check the UID number and compare the information present within the UID card with electoral register in the cloud data center. The invalid users are not allowed to do the registration process.

KeyGeneration Service

Key generation Service is to generate the tokens for the voters by using the RSA algorithm for safe communication between the voters machine and data center. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. Finally generated tokens fill the map table for the registered voters in the cloud center.

KeyExchange Service

Key exchange service exchanges the tokens between the voters and cloud data center. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Map Service

This service maps the tokens for the registered voters and fills all entries of the mapping table. The map table format.

Checking Service

During the voting phase checking service allow the registered voters to cast the vote only once. So duplicate voting is avoided by using this service.

Table 1 : Mapping Table

UID	VoterName	Constituency/Percint	Public/Private Keys	Mobile No/Mail Id

Tallying Service

During the counting phase the tallying service decrypt the voter information with the help of the map table and count the vote as per the constituency.

3.2 Cloud Types and Security in I-Voting

In cloud computing environment three existing cloud delivery models are as SaaS, PaaS and IaaS. Cloud deployment models include public, private, community and hybrid clouds[3]. Among these four private cloud are typically suitable with dedicated virtualized resources for I-voting. By using cloud voting services voters can easily access their personal information and make it available to various services access the Internet. An Identity management as a Service(IdaaS) could provide the authenticated voters to manage the voting system in a safer way.

4 Participants and Phases

I-Voting model comprises of five phases and four participants. The five phases are given by Identify, Registration, Authentication or verification, Voting and Counting phase. And then five participants are given by

Voters: People who have eligibility to participate in an election.

Election officers:

(1) Maintain District cloud
(2) Maintain the polling candidate list according to the consistency & registered list.
(3) Maintain the registration phase

Election Commission

Its mission is to conduct free and fair elections in the country. The following are the principle functions of the Election Commission of India

1. Demarcation of Constituencies.
2. Preparation of Electoral Rolls.
3. Recognition of Political parties and allotment of symbols.
4. Scrutiny of nomination papers.
5. Conduct of polls.
6. Scrutiny of election expenses of candidates.

The role of election commission is listed below.

1. Issue voting certificate i.e. token to the registered voters by the use of key generation service
2. By getting help of Key generation service to generate tokens for the voters and use Mapping service to map tokens with voter for encrypt and decrypt the votes.
3. Exchange the tokens to the corresponding voters make use of Key Exchange service for encrypt and decrypt the votes and to maintain state cloud's encrypted votes
4. Use Checking service to avoid duplicate voting.

Polling officer

1. Maintain authentication by use of card reader and also Biometric Device. To compare the thumb impression /Iris

pattern of the voter with the thumb impression/Iris pattern already stored in the UID card.

2. Polling officers maintain one computer for authentication and touch screen PC for voting.
3. The authentication computer does the local checking for the voter and allows the voting computer to cast the vote. Take care of polling is going securely and smooth way.

Counting officers

1. Use counting service to decrypt the encrypted votes and announce the election results.

And then phases are given and the procedures are carried out.

Registration phase

Step1: Voters register their name to the election commission by their UID card using the smart card reader at the registration centers before ten days of the election date.

Step2: All the identity information stored in the UID card will be store at the district cloud's datacenter.

Step3: With the help of UID number and PIN number to encrypt the voter's information and transfer from registration centers to district cloud center.

Step4: The registration confirmation is send to the voters either their mail id or mobile number through the SMS. The registered voters are eligible to cast their vote at the time of election.

Step5: After the deadline period of the registration phase closed no one cannot register their names.

Hence in this registration phase we are encrypted the information by using the secret key.

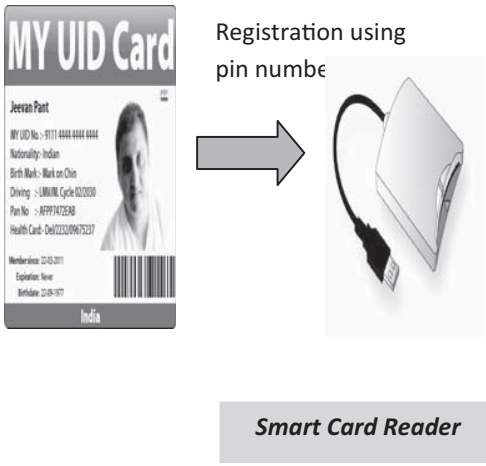

Figure 1 : UID Card

Identity phase

Voter Identify is the process of identifying the voters for voting.

Step1: obtain thumb impression/Iris pattern of the voter using bio metric devices.

Step2: obtain the approved thumb impression/Iris pattern of the voter from UID card.

Step3: Compare the images to know whether they match or not.

Step 4: On matching the voter identification is confirmed.

Step 5: On mismatch the voter is notified and further action to be taken.

Identity management (IDM) assumes an upper and in the whole area of cloud security. Cloud computing is an amalgamation of various technologies to meet the demands of an interdependent maze of software and services. Utilizing a cloud computing service model, there should also be added focus on ensuring that security is properly implemented either in authentication or authorization.

Authentication or Verification Phase

Step1: For registered candidates automatically the tokens will be distributed to the voters for the authentication and verification.

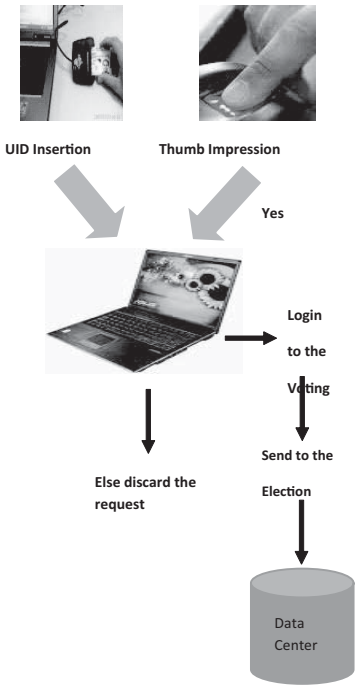

Figure 2 : E-Voting

Step 2: tokens used for not only the verification and also act as the private key for the voting.

Step 3: by using the user name password and tokens we are allowed for voting. The token are encrypted for the secure authentication.

Step 4: polling officers are the authenticate person to give the private key and manage the voters list.

Voting Phase

In a voting phase the step by step process is given by

Step1: Voters insert the UID card in the card reader and take sample of the thumb impression from the bio metric device to verify the voter's information.

Step2: Tthe information gets mapped into the data center which verifies the following information is correct

Step3: Voting page shows the list of candidates. Voter click on candidate icon and click the encrypt button.

Step 4: Input the token for encryption and submit the information to election commission.

Step 5: The encrypted voting information stored in the database. Voting status field in the database is marked. So the same voter will not cast again.

Step 6: From the election commission they send the acknowledgement to the voter that his vote is in the voting database.

Counting Phase

Step 1: When the voting time is up. Center stops the voting process.

Step 2: After getting the private key center decrypts the encrypted vote.

Step 3: Then by using the hashing function count the list.

Step 4: Finally Election Commission publishes the election result and makes the counting result list to the public.

5 Main Goal

The main goal of the secure Internet voting system is to ensure the privacy of the voters and the accuracy of votes.

The requirements of the internet voting as follows.

1. Accuracy
2. Simplicity
3. Democracy
4. Verifiability
5. Privacy

6 Security Issues

- Only eligible people should be able to vote by using validate service.
- It should be possible to use checking service voters vote only once.
- Make sure that voters have a secure, encrypted connection to the data center. Use key generation and key exchange services no one should be able to intercept and decipher voters data.
- The system should ensure correct tallying of votes at all levels(district,constituency and area)

7 Conclusion

In this paper we proposed an internet voting by using cloud computing. It adopts using the digital signing to protect the content of the ballot during casting. By internet voting we believe that it is a secure system and also avoid the ballot buying. With a secure and low cost we can vote without the geographical restrictions. By using the UID card the election process is very easy for the registration and counting also. If the ballot buyer exists but no use of that all the content is stored in the data center and also without the decryption it can't be used.

References

[1] Chun-Ta Li, Min-Shiang Hwang, Yan-Chi Lai. "A verifiable Electronic Voting Scheme over the Internet" IEEE Intl Conf on IT:NG 449-454 , (2009)

[2] ChunyeGong,Jie Liu,Qiang Zhang,Haitao Chen,Zhenghu Gong "The Characteristics of Cloud Computing" IEEE Intl Conf on parallel processing workshops 275-278 , (2010)

[3] Sohan Singh Yadav,Zeng Wen Hua "CLOUD: A Computing Infrastructure on Demand" IEEE Intl Conf on Computer Engineering and Technology" V1-425, (2010)

[4] Hassan Takabi,James B.D.Joshi,Gail-Joon Ahn "Security and Privacy Challenges in cloud computing environments" IEEE Computer and Reliablity pp24-31, (2010).

[5] Kalaichelvi.V, R.M.Chandrasekaran "Secured Single Transaction E-Voting Protocol",Journal of Scientific Research, 51(2), 276-289, (2011).

[6] Jian-Liang Lin,Hhsiu-Feng Lin,Chih-Ying Chen and Chin-Chen Chang "A Multiauthority Electronic Voting Protocol Based upon a Bling Multisignature Scheme",Journal of compter science and Network security", 6(12),266-273, 2006.

[7] Debasish Jena,Sanjay Kumar Jena,Banshidar Majhi "A Novell Untraceable blind signature based on EC discrete Logarithm problem",Journal of compter science and Network security", 7(6),269-274, 2007.

[8] Xiangdong Li,"Security analysis on an elementary E-Voting System" Journal of Computer Science and Network Security" ,1 0(10) 128-131, (2010)

[9] Chia-Hsien Wen,Hei-Ru Shiau,Chen-Yen Wang,Szu-Yen Wang "A SLA based Dynamically integrateing servives SAAS framework", IET ,pp 306-311 (2010)

[10] Gallardo,J.C Belleboni E.P "Use of new Smart Identity card to reinforce e-voting gaurantee" , IEEE Intl conf on internet technology and secured transactions pp1-6,(2009)

[11] Zhenjie Huang; Qunshan Chen; Rufen Huang; Xuanzhi Lin,"Efficient Schnorr Type Identity based Blind signature from bilinear pairings",IEEE Intl conf on Computer Science and Information Engineering,pp 130 -134, (2009).

[12] E. Magkos, P. Kotzanikolaou, C. Douligeris. "Towards Secure Online Elections: Models, Primitives and Open Issues". In: Electronic Government, an International Journal, Inderscience Publishers, Volume 4 - Issue 3, pp. 249-268, 2007

[13] CAO Feng,CAO Zhenfu,"A secure anonymous Internet Electronic voting scheme based on the polynomial",WU Journal for Natural Sciences Vol 11(6) , (2006)