Asian Journal of Information Technology 15 (19): 3826-3834, 2016
ISSN: 1682-3915

An Agent Based Online Voting System in Cloud Using Blind Signature

S. Vijayalakshmi and G.R. Karpagam
PSG college of Technology, 641004 Tamil Nadu, India

Abstract: The concept of cloud is sprinkled on an excess of emerging products. Online voting is preferred by the elector by facing several major issues in traditional voting system including geographically dispersed, time constraint job, disabled and others. Online voting system is publically accessible so there are some issues one of the major issues is security. Our objective is to design and develop a frame work for a secure online voting system in cloud environment by using token based authentication, secure hash algorithm, RSA based blind Signature and encryption algorithms. This proposed system consists of three mangers such as User Administration Manager (UAM), Vote Administration Manager (VAM) and Vote Tallying Manager (VTM). In registration phase the elector interacts with UAM to acquire a certificate. VAM is responsible to authenticate the elector. VTM is in charge for verifying the identity of the elector, validity of his/her certificate and tally the votes. All the managers are implemented as agents because it is a capable of working autonomously and continuously in cloud environment. The assessment of the system is verified using properties called authenticity, verifiability, uniqueness, accuracy and non-coercibility.

Key words: Cloud, online voting, agent, RSA blind signature, RSA encryption algorithm, secure hash algorithm

INTRODUCTION

Cloud computing is an emerging computing paradigm and got wide popularity from both industries as well as academic institutions since 2007. It is employed because of its powerful computing and storage capabilities necessary in a distributed environment (Anbazhagan and Somasundaram, 2014). It is a paradigm that focuses on sharing data and computations over a network of nodes. These nodes include users, computers, data centers and cloud services. It enables both users and developers to utilize computing resources that are virtualized. According to National Institute of Standards and Technology, USA (NIST) cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with less management effort or service provider interaction. Several firms like Google, Amazon, IBM, Microsoft, etc. that offers services for Internet users.

There are different types of voting systems are available in India. It is in need of such a system where elector can vote without any problem and feel secure. Such environment can only be created through some automated system which cannot be deceived by anyone. (Mugunthan and Parameswari, 2013)Voting is as much a responsibility as it is a right. The whole edifice of Indian democracy is built on the foundation of voting. If citizens are not careful about casting their vote or, skip their vote altogether will jeopardize the existence of our democratic Republic. The online voting system using the cloud technology is highly secure voting system in information securityresearch in India. It provides a platform for the elector to elect their candidate and manifest their best choice for who will be governed. The faith of the public in the online voting process is most important (Kohno *et al*., 2004).The online voting system using cloud provide an overall process of election fully coverage of media it is helpful for public and election commission if something is going on wrong. This approach will raise a high level of security in terms of ballot confidentiality, authentication, integrity and faith for electorate. An online-voting system using cloud involves many steps in the setup, elector registration, authentication, verification and tally of encrypted ballots. Online voting using Aadhaar card and cloud computing are well defined concept as an individual so far, there is a considerable amount of space to incorporate the electronic voting with cloud computing to make it success, an integration approach can certainly be proved as an efficient and secure election process.

Key characteristics of cloud computing: Cloud provides several prominent features which are different from Indian traditional system.

Elasticity: Users can rapidly provision computing resources as required, without human interaction. Some time it automatically, to scale up or down.

Corresponding Author: Vijayalakshmi, PSG college of Technology, 641004 Tamil Nadu, India

Shared resource pooling: It allows cloud provider to provide one pool of large scale resources to serve multiple cloud consumers. Different resources will be mutually assigned or reassigned according to the cloud consumer demand (Zhang *et al*., 2010).

Broad network access: Cloud capabilities or services are available over the network and accessed through internet using by heterogeneous platforms (e.g., smart phones, laptops, etc).

Reliability: Reliability improves through the use of multiple replicas at multiple locations which makes cloud computing suitable for business continuity and disaster recovery.

Benefits ff cloud computing in online voting: We are in position to store huge volume vote in data base due to millions of electorate in India, The cloud storage is a more suitable for storing the huge data. Cloud based online voting system provide usability for both election commission of India and electorate because it helps to provide the location independent platform for the communication through internet with efficient and fast computing power so that a user can work at anytime from anywhere and also provide the best services at the time of heavy load by using the number of resources in transparent. Online voting can be speedup using the cloud data centre that provides powerful servers, more memory, CPU and fast storage devices. This study proposes a framework for agent based online voting system to achieve privacy, security and online voting requirements (Jadav *et al*., 2015).

Role of agents in online voting: An agent is a computer system or an instance that is capable of working autonomously and continuously in a particular environment. Agents produce an outcome based on the interactions among individual components. The inherent properties namely self organization, dynamism, conceptual simplicity and scalability have led to prefer and realize various managers as agents.

MATERIALS AND METHODS

Existing work in the area of online voting system: In 2004 online voting systems have been implemented in European parliamentary election. Electorate resident in out of station, i.e., they are temporarily abroad on the election day. In great Britain, remote electronic voting systems were used in the local elections in 2003. In USA; several attempts have been made to use electronic voting systems. In 2001 the voting over the Internet project was used in the general elections in four states. The Internet votes were legally accepted but their amount was very small. (DuRette, 1999). Presents a remote voting scheme that applies the blind signature technique to a elector's ballot so that it is impossible for anyone to trace the ballot back to the elector. It achieves the properties of untraceability, verifiability and privacy. The California internet voting report defines four different Internet voting models such as Internet voting at voter's polling site (location specific), internet voting at any polling site (location not specific to home polling site) and remote internet voting from county computers and, Remote Internet voting through Internet connection. It addresses the issues on design implementation and security issues of each of the four models. (Jambhulkar *et al*., 2014) proposed a novel security for online voting system by using digital signature and multiple encryptions with public key algorithm to provide security for elector and his/her vote. (Pranay *et al*., 2014) proposed an online voting system with android platform. Using this application voter can easily vote for candidate from home itself. It provides security for elector and his/her vote but these was some authentication problem. Electronic voting security study (Mugunthan and Parameswari, 2013) identifies attacks, sources of attack and feasible methods of attack in such voting systems and also finds the security objectives and requirements of an electronic voting system. In (Kaliyamurthie *et al*., 2013) eligible elector can cast their vote through online without going to physical polling station. This system is highly secured and reliable. It is developed and tested to work on ethernet. This system will increase the voting percentage and reduce false votes in India.

Existing work in the area of utilizing cloud infrastructure for e-governance application: In 2011 the government and the ministry of information society and Administration began "open e-services" project which involves more than hundred services and sixty documents based on the public partnership. Using this project it concerns get the opportunities to develop electronic services that are offered by the public institutions to the citizens and to provide fast access to them through Internet. IT companies will make profit from this, citizens and the private sector will have new opportunity for getting electronic services without waiting in queue. By

realization of this project, republic of Macedonia would be the leader in the Europe by electronic services that are offered by the state. Cloud computing for E-governance can reduce IT labor cost by 50%, improve capital utilization by 75%, significantly reducing license costs and provides much scalability than traditional system (Balaji and Srinivasan, 2010).

Existing work in the area of privacy preservation in online voting system: Zwattendorfer *et al.* (2013) Proposed a proxy voting system supporting liquid democracy which improves current systems in terms of security and privacy by using separated servers, public key encryption and digital signature and also reduce the risk of an attack, this system does not store any information on a server that makes reconstruction of votes possible and it relies on a desktop-based client application that must be installed by the user. It does not support sufficient scalability. Fujioka *et al.* (1992) proposed electronic voting protocol is capable of solving the fairness problem by using the bit-commitment function. Here the voting authority, cannot know the intermediate result of the voting. Thus it prohibits the fraud by either the elector or the voting authority. (Shubhangi *et al*., 2013) Proposed online voting systems using homomorphic encryption, votes are verifiable during and after the election. This encryption cannot observe the proper execution of the election, so that a special audit logging is maintained in order to trace the execution process. There are several cryptographic mechanisms are available for online voting systems. Suitability of these varies with condition under with it is to be applied. All these cryptographic protocols satisfy most of the electronic voting requirements however, the blind signature is much more efficient due to their simplicity and less computation complexity (Joaquim *et al*., 2003). Our proposed online voting systems are based on RSA blind signature and Encryption algorithm to satisfy eligibility, privacy, accuracy and individual as well as universal verifiability.

Security properties and techniques of online voting system: Security is the most essential part for elections. There has been a lot of attention to online voting by cryptographers because of the challenging need to achieve many apparently contradictory properties, like authentication, privacy. The most important requirements of online voting are the following:

Eligibility: About 18 year and above registered electorate are only able to cast their vote that is counted in the final tally others are disfranchised.

Uniqueness: Eligible voters are unable to cast more than one vote on the election date.

Correctness: It is possible for auditors/Election commission of India to check whether the final tally is correctly computed.

Privacy: In online voting no one can find out the relationship between a casted vote and a specific elector and the results of voting must be secret until end of voting.

Verifiability: Each elector can view his/her sent encrypted ballot in the result list.

Security techniques: Our proposed system uses some of the most important concepts to enhance the security such as privacy, authentication of the elector and integrity of the vote.

RSA public-key cryptosystem: In 1978, Rivest, Shamir and Adleman proposed RSA public cryptosystem based on factoring problem (Rivest *et al*., 1978). In RSA public cryptosystem, there were two participants, namely, the receiver and the sender, E-Voting employs RSA Public-key encryption algorithm; it uses two different keys to perform encryption and decryption. The public key, the private key is {n,e} and {n,d}. The equation for encryption and decryption are as follows:

$$\text{Encryption: } C = M^e \bmod n$$

$$\text{Decryption: } M = C^d \bmod n$$

Blind signatures: D. Chaum was introduced the blind signature scheme in 1982 (Chaum, 1983). It guarantees the anonymity of the participants. The blind signature scheme contains two parties, namely, the requester R and the signer S. The requester R wishes to obtain the signature from the signer S on the message M for that the following steps are performed:

Step1: Requester R blinds the message M into M^1 and sends M^1 to the signer S.

Step2: Signer S generates the Sg^1 on M^1 and returnsSg^1 to R

Step3: R receives the Sg^1 and unblind Sg^1 into Sg and outputs Sg as the signature on the message M. Here, Requester can protect the content of message; S cannot resolve for whom he/she signed that message. This concept is widely used in online voting systems and electronic money systems.

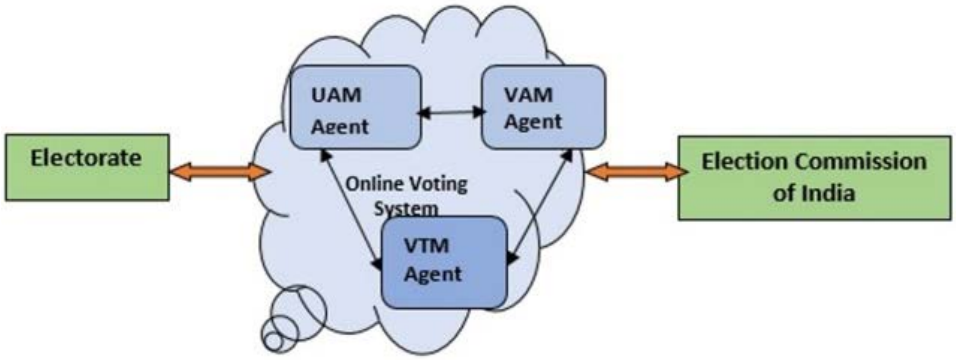

Fig. 1: Cloud based online voting system

The blind signature scheme based on RSA: Was proposed by (Chaum, 1983). There were three participants in this scheme, namely, the requester (Elector), the signer (VAM) and the verifier (VTM). This scheme contains following five phases.

Initialization phase: The signer S randomly chooses two large primes pand qand computes n = p×q and ϕ (n) = (p-1)×(q-1). The S chooses large number eGCD (e;ϕ(n)) = 1 and computes (d = e^{-1}modϕ(n)). Let (e,n) be the be the signer's public key and (d, n) be the signer's private key kept secret. He/she then publishes (e, n) and a one-way hash function h(.).

Blinding phase: The requester has a message m and wants to have it signed by the signer. The requester randomly chooses an integer r as the blinding factor and then computes and sends M^1 = r^eh(m) modnto the signer.

Signing phase: When the signer receives M^1 from the requester, the signer computes S^1 = $(M^1)^{\wedge}$ dmodnand sends $S^1$to the requester.

Unblinding phase: After receiving $S^1$from the signer, the requester computes S = S^1r^{-1} modnand sends the message-signature pair (m; S) to the verifier.

Verifying phase: Verifier receives the message-signature pair (m; S) and use h (.) and (e, n) to verify the legitimacy of the signature by checking whether S^e = h(m) mod n exists.

Proposed system overview: In online voting system the Election Commission of India (ECI) decides the date and the time for starting and ending of the election process. The electorate can vote from anywhere within the decided time period by the election commission of India on election day. Each manger is implemented as agent. Online voting system consists of three agents which interact with one another. For a successful interaction, agents require the ability to cooperate, coordinate and negotiate with each other. Role of each agent in online system as follows.

User Administration Manager (UAM): This agent is responsible for the management of the users. It maintains information about the valid electorate, who should register in the system and also controls the accesses assigned to the electors that create or modify voting processes. In the registration phase the elector requests his/her key pair and certificate by sending his/her identity with the random integer number.

Vote Administration Manager (VAM): Is in charge to authenticate the elector. Verifying whether each Electorate interacted with the user administration manager or not with the help of electorate's certificate issued by UAM. If it is registered then it signs the encrypted vote (without knowing his/her vote) using RSA blind signature.

Vote Tallying Manager (VTM): Receive the votes form electorate and check electorate identity and the validity of his/her certificate. If it is valid, store them in its data base. ECI Tally and publish the result to public after the election date is over. Everyone can publically verify their votes.

The proposed online voting system: The Proposed online voting system consists of five stages, namely Initialization stage, the registration stage, the authentication stage, the voting stage and the tallying stage show in Fig. 1. The detail of the each stage is described as follows.

Initialization stage: Generate the public parameters and public/private keys, as follow. Receiver chooses two large

prime numbers p and q and computes n = p×q and $\phi(n) = (p-1)\times(q-1)$ Then, chooses an integer e such that $1<e<\phi(n)$ and $GCD(e,\phi(n)) = 1$ and computes $d = e^{-1}(\mathrm{mod}\phi(n))$. Obtains two keys, namely, public key (e,n) and private key (d,n) The public keys of user administration manager, vote administration manager and vote tallying manager are known by every electorate and vice versa.

Registration stage:

- Elector sends his/her details such as name, father's name, date of birth, Aadhaar card number, email-id, mobile number, to user administration manager (UAM)
- UAM receives message and send Aadhaar number to Aadhaar card issuing authority. Aadhaar card authority sends elector credential to UAM
- UAM verifies the information provided by both Aadhaar card issuing authority and electorate. After successful verification UAM send acknowledgement, Eid, Password pass to elector through email-id and mobile no
- Upon receiving the message from UAM, electorate choose random integer i and apply SHA-1 hash on election card number (id) and ii.eH(id||i). Encrypted result value i.e Epass[H(id ||i] sends to UAM
- UAM generates key pair such as public key (Pke), Secret key (Ske) and certificate (certe = ESKe[Pke,H(id ||i)), TS,LT and encrypt Epass[Pk_e,Sk_e, certe] and send it to elector and same information is stored in UAM database where TS represent Time stamp and LT represent Life time for a certificate

Authentication stage: Vote administration manager (VAM) is responsible for this stage.

- VAM extract the certificate from VAM by decrypting with its Secret Key (Sk_v) and store it in a database
- After the successful verification process it sends ballot to the electorate
- Electorate choose a candidate and encrypt it with public key of the Tallying manager Pk_ti.e (C =EPk$_t$[M]
- Electorate choose blind factor r and compute $B^1 = r^{pkv*C \mathrm{mod} n}$(Blinding phase) X =H(id ||i) and $X_1 = r^{pkv*x \mathrm{mod} n}$ X_2 = EPK$_v$[H(id ||i)] Encrypt the result with VAM's public key^z = EPK$_v$[X^1||B^1|certe ||X^2] send it to VAM
- VAM receives and decrypt Z using its secret key SK_vi.eDSk$_v$[Z]and extract B^1 and X^1
- Retrieve the electorate's public key from certificate and verify the validity of the key pair, life time and Timestamp values of the certificate
- After the successful verification, VAM sign the blinded ballot and Elector identity without reading the ballot

$$S^1 = (B^1) \wedge Skv \mathrm{mod} n \text{ and}$$
$$W^1 = (X^1)^{\wedge Skv} \mathrm{mod} n \text{ VAM compute}$$
$$Y = EPK_e[S^1 \| W^1] \text{ send it to Elector}$$

Voting stage: Authenticated electorate can cast their vote by decrypts Y using his secret key SK_e i.e., $DSK_e(Y)$ and extract S^1, W^1 and unblind the signature using his blinding factor r:

$$S = S^1 r^{-1 \mathrm{mod} n}$$
$$W = w^1 r^{-1 \mathrm{mod} n}$$

Verify the signed ballot and send Epk$_t$[H(id||i), C, S, W] to vote tallying Manager.

Tallying stage: The vote tallying manager receives it and decrypts using its private key. VTM performs the following process (verification phase) First Check if $S^{Pkv} \mathrm{mod} n$ = C and $W^{PKv} \mathrm{mod} n$ = H(id) || i) if it is matched decrypt the ballot C using its secret key Sk_ti.eM =DSk$_t$[C] and stores M,C and W in its vote database and incrementing the vote count by one.Finally it sends the notification to UAM as Identity of a particular elector voted successfully. Upon receiving it UAM update its data base as H(id||i) is voted. This ensures that an eligible electorate can cast a vote only once. UAM Intern sent acknowledgement to electorate show in Fig. 2.

Prototype implementation

Experimental setup: Eucalyptus 3.4.1 FastStart an open source cloud infrastructure was setup that includes Cloud Controller (CLC), Walrus, Cluster Controller (CC), Storage Controller (SC), Node Controller (NC) configuration, the CLC, Walrus, CC and SC are installed on one machine, called the Frontend. The NC is installed on another machine, called the Node. In our configuration we have one frontend and one node. In the eucalyptus 3.4.1 fast start configuration, all components are installed on one machine. Installing fast start in the cloud-in-a-box configuration requires a minimum of 200 GB of disk space, a minimum of 4 GB of memory and one ethernet NIC. Eucalyptus will assign these IP addresses to VM Instances. Each VM instance represents a Manager in our

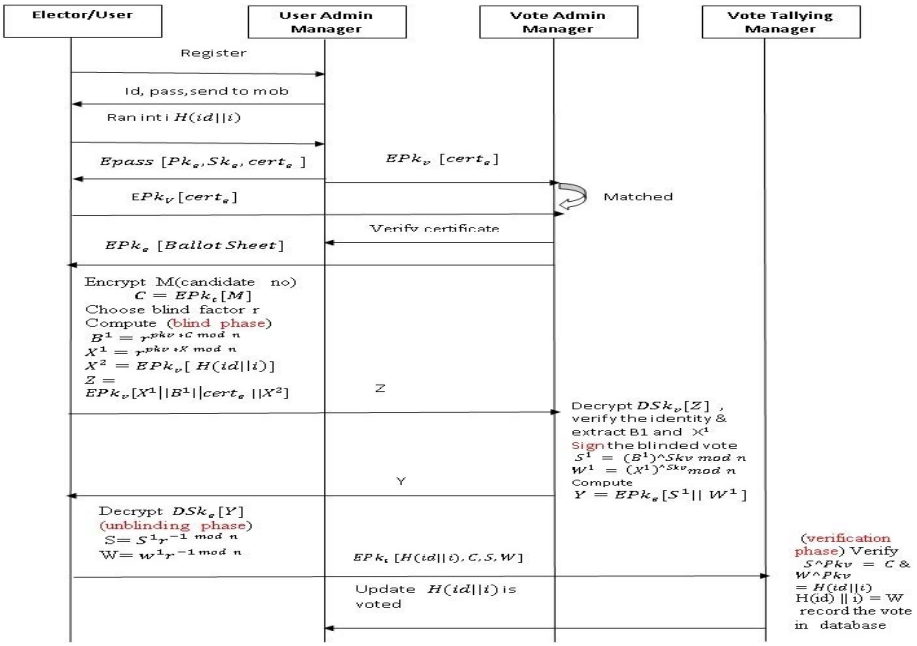

Fig. 2: Sequence diagram for propsed online voting system

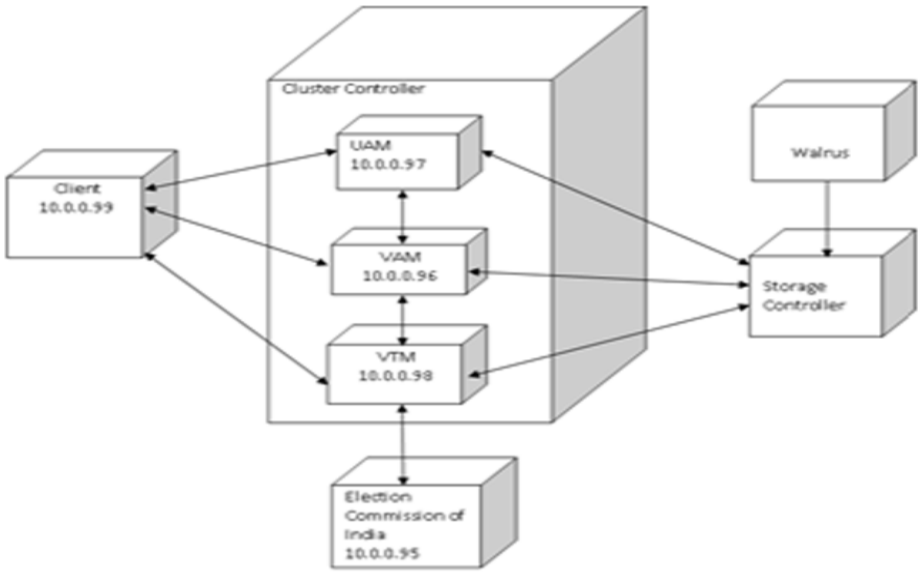

Fig. 3: Deployment diagram showing variou communicating agent of cloud and interaction for online voting system

framework. Elector can communicate with appropriate manager through its corresponding IP address using SSH connection show in Fig. 3. SSH connection provides a secure communication between a browser and the server. The Illustration for the entire agent interaction is attached in Appendix A.

Security analysis: The proposed online voting system is evaluated based on the criteria that qualify to be characteristic for any online voting system. This study shows how security analysis performed for the entire system.

Eligibility: Person having the right to do or satisfying the appropriate conditions.only eligible electorate can take part in voting phase to vote. Each electorate registers their detail in UAM and verified by Aadhaar database before take part in voting.

The details of electorate are placed along with their public key and certificate. In authentication stage the ballot is encrypted ($C = EPK_t [M]$)) with public key of VTM. If an adversary wants to modify the vote he has to decrypt it first, to do this he has to derive the secret key of VTM from the public key but it is very difficult because one needs to solve the factoring problem i.e find the two prime numbers (p and q) from the product $N = p * q$. When the selected prime numbers are very large, the problem is not at all easy. Since the attacker cannot find p and q he/she cannot proceed further to find out d, because d depends on p, q and e.

Uniqueness: One being the only one of its kind; unlike anything else. An elector can vote only once. If eligible electorate tries to vote several times, in the voting stage detected he/she is ineligible because the hashed identity H (id||i) is recorded in VAM database. Online voting system uses SHA-1 algorithm to achieve integrity of the elector identity. The chances of any two message digest being same are one in 2160. If an attacker tries to find out elector original identity he has to perform 2160 bit operations. It consumes more time to break.

Accuracy: The quality or state of being correct or precise. Accuracy is ensured during the tallying stage. Voting systems should record the votes correctly. Each ballot is Encrypted using public key of VTM. So no one can decrypt it except vote tallying Manager. After verifying all the components $S^{PKv} \text{mod} n = C$ and $W^{PKv} \text{mod} n = H(id) || i$) it decrypts the ballot C using its secret key Sk_ti.e$M = DSK_t[C]$ and store M, C and W to its database.

Verifiability: It is possible to verify that votes are correctly counted in the final tally. In online voting system an electorate able to see his/her sent encrypted ballot and can also verify the signature signed by the VAM. Each elector can verify legitimacy of the signature generated by VAM (signer) using VAM's public key (Pkv) i.e$S^{PKv} = C$ and WPKv = H(id)||i). Each electorate can check whether their cast ballot was counted correctly or not.

Non-coercibility: The policy of not forces to others. Voters should not be able to prove how they voted. The identity of all electorate is protected in all of the stages in the proposed system. Each authority unaware of the identity of an electorate, If anyone wants to prove that a specific H(id)||i) represent ID of particular electorate , the random integer i must be known. So the proposed scheme is coercion-resistance.

RESULTS AND DISCUSSION

The proposed secure online voting system simplifies the entire voting process and helps in a wide range of decision-making processes.Advantage of using agent based approach provides more flexibility to elector and any modification in the voting system can be transferred automatically among all agents easily without any human interruption. It uses token based authentication method, using this only registered elector only cast their vote through online. Based on the qualified RSA blind signature and encryption algorithm, this system ensures the privacy of the electorate, accuracy of the votes and also satisfies the online voting requirements such as eligibility, unreusability, verifiability and integrity. Due to encryption and decryption process there is a computational overhead because in the tallying stage every encrypted ballot is decrypted using Tallying manager secret key. If there is N electorate, then this process requires operations which can be acceptable since the decryption takes place in tallying stage. So it does not affect the practicality of online voting process.

CONCLUSION

The proposed secure online voting system simplifies the entire voting process and helps in a wide range of decision-making processes. Advantage of using agent based approach provides more flexibility to elector and any modification in the voting system can be transferred automatically among all agents easily without any human interruption. It uses token based authentication method, using this only registered elector only cast their vote through online. Based on the qualified RSA blind signature and encryption algorithm, this system ensures the privacy of the electorate, accuracy of the votes and also satisfies the online voting requirements such as eligibility, un reusability, verifiability and integrity. Due to encryption and decryption process; there is a computational overhead because in the tallying stage every encrypted ballot is decrypted using Tallying manager secret key. If there is N electorate, then this process requires operations which can be acceptable since the decryption takes place in tallying stage. So it does not affect the practicality of online voting process.

APPENDIX A

Though the original implementation involves complex computing and corresponding values for the sake of readers' simplicity and understandability the example shown here are encoded into decimal numbers (Table 1-7).

Table 1: Required parameters and descriptions

Parameters	Values	Remark
Time stamp value in certificate (TS)	12	TS represent at what time the certificate is issued (12:00:00)
Life time of the certificate (LT)	10	LT represent number (10) days the certificate is valid from date of registration
H (id‖i)	15	Encoded hash value
Elector Public key (Pk_e) and	Pk_e = 11 and	From two large random primes p = 11 and q = 17 public (e) and secret (d) components are
Secret Key (SK_e)	Sk_e = 131	calculated
VAM Public key (Pk_v)	Pk_v = 7 and	
and Secret Key (SK_v)	Sk_t = 23	n = pq and phi =(p-1) (q-1)
VTM Public key (Pk_t) and	Pk_t = 13 and	1<e<phi, stgcd (e, phi) = 1
Secret Key(SK_t)	Sk_t = 37	1<d<phi, sted = 1 (mod phi)

Table 2: Registration stage

Operations with parameters	Values
User Register (name, Father name, Dob,	{name= Aaass , Father name = Esssas,
Aadhaar no, Email-id, mobile no)	dob=15.04.1987, Aadhaar = 1234 3445 7895, email-id = aas@gamail.com,mobile = 9145678924}
UAM-> (Eid,pass)	Eid = '1152', Pass = 10
Elector Calculate SHA -1 (Hid ‖ i)	H(id‖ i) = H(TRQ0837427‖6) = 931ae8b0d7c9007cc67b1b914df797226d975b69
Elector -> UAM : E_{pass}[H(id‖i)]	E_{10}[15] = 25
UAM-> Elector : E_{pass}(Pke,Ske,certe)	E_{10}(11,131,11,15,12,10) = 21,11,21,25,22,20
certe = (Pk_e, H(id‖i)	
Elector decrypt : D_{pass}(Pke,Ske,certe)	(11,131,11,15,12,10)
UAM-> Elector : (certe)	E_{11}(11,11,15,12,10) = (165,26,23,54)
UAM-> VAM: Ep_k (certe)	E_7(11,15,12,10) = (88,93,177,175)

Table 3: Authentication stage

Operations with parameters	Values
Elector -> VAM: EpK_v[$cert_e$]	E_7(11,15,12,10)= (88,93,177,175)
Compare (elector certificate C_e, with	C_e C_{VAM} : (88,93,177,175)
VAM certificate C_{VAM} in its database	= (88,93,177,175)
Send(ballot)	Ballot (A - 0, B - 1, C-2...n)

Table 4: Blinding phase

Operations with parameters	Values
Electorate choose a candidate M and	Pkv =7, Skv=23, n=187,
Encrypt: C = EPK_t[M]	M = G = 6 C=E_{13}[6] = 95
Blind (vote)	Choose r = 12
Choose blind factor r and compute	$B^1 = (12)^{7*}$ 95 mod 187 = >B^1 = 172
$B^1 = r^{pkv*Cmodn}$ $X^1 = r^{pkv*xmodn}$	$X^1 = (12)^{7*}$15 mod 187 =>X^1 = 37
Encrypt X^2 = EPk_v[X] identity	X^2 = E_7[15] = 93
Encrypt z = Epk_v[X^1‖B^1‖ certe‖X^2]	Z=E_7[37‖172 ‖88,93,177,175 ‖ 93]

Table 5: Signing phase

Operations with parameters	Values
VAM Decrypt Z: DSKv[Z]	X^1 = 37, B^1 = 172
extract X^1 and B^1	
Verify the validity of the certificate if matched	Check X^2 = H(id‖i)
Sign blinded ballot: $S^1 = (B^1)\wedge^{Skvmodn}$	93^23 mod 187 = 15
Sign blinded elector's identity: $W^1 = (X^1)^{\wedge SKv}$ modn	It is valid S^1 = (B1)^SKvmodn = (172)^23 mod 187
	S^1 = 145 W^1 = (X1)^SKv mod n = (37)^23 mod 187 = 130
	W^1 = 130
VAM send = Y EPk_e[S^1 ‖w^1]	E_{11}[145 ‖ 130] = [134 ‖ 97]

Table 6: Voting stage

Operations with parameters	Values
Unblind sign	S = 145*12^{-1} mod 187
$S = S^1 r^{-1 \bmod n}$	S = 90
Unblind identity	W= 130* 12^{-1} mod 187
$W = w^1 r^{-1 \bmod}$	W= 42

Table 7: Tallying stage

Operations with parameters	Values
Elector->VTM: EPK_t [H(id) ‖ I), C, S, W]	E_{13} [H(id) ‖ I), C, S, W]= [53,79,173,179]
VAM decrypt	D_{37} [H(id) ‖ i), C, S, W]= [15,95,90,42]

Table 7: Continue

Operations with parameters	Values
(Dsk_t) [H(id ||I)C, S, W]	
Check (SPKv modn = C and WPkv modn = H(id ||i)	SPKv modn = C =>90^7 = H(id) || I) mod 187 = 95 Wpk_v modn = H(id||i) =>42^7 mod 187=15
Decrypt M = DSK_t [C]	Decrypt M = DSk_t[C]95^37 mod 187 = 6
Count= Count +1	After Decoding M = 6 ='G'Now Candidate G count = count +1

REFERENCES

Anbazhagan, S. and K. Somasundaram, 2014. Cloud computing security through symmetric cipher model. Int. J. Comput. Sci. Inf. Technol., 6: 57-66.

Balaji, P.G. and D. Srinivasan, 2010. An Introduction to Multi-Agent Systems: Innovations in Multi-Agent Systems and Applications-1. Springer, Berlin, Germany, pp: 1-27.

Chaum, D., 1983. Blind Signatures for Untraceable Payments. In: Advances in Cryptology. David, C., L.R. Ronald and T.S. Alan (Eds.). Springer, Berlin, Germany, ISBN:978-1-4757-0604-8, pp: 199-203.

DuRette, B.W., 1999. Multiple administrators for electronic voting. BA Thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts.

Fujioka, A., T. Okamoto and K. Ohta, 1992. A Practical Secret Voting Scheme for Large Scale Elections. In: Theory and Application of Cryptographic Techniques. Jennifer, S. and Z. Yuliang (Eds.). Springer, Berlin, Germany, ISBN:978-3-540-57220-6, pp: 244-251.

Jadav, M.B., M.A. Desai, M.F. Patel and M.R. Patel, 2015. Cloud computing E-voting: A technical review. Int. J. Res. Emerg. Sci. Technol., 2: 8-13.

Jambhulkar, S.M., J.B. Chakole and P.R. Pardhi, 2014. A secure approach for web based internet voting system using multiple encryption. Proceedings of the 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC), January 9-11, 2014, IEEE, Nagpur, India, ISBN:978-1-4799-2102-7, pp: 371-375.

Joaquim, R., A. Zuquete and P. Ferreira, 2003. REVS-A robust electronic voting system. IADIS. Int. J. Internet, 1: 47-63.

Kaliyamurthie, K.P., R. Udayakumar, D. Parameswari and S.N. Mugunthan, 2013. Highly secured online voting system over network. Indian J. Sci. Technol., 6: 4831-4836.

Kohno, T., A. Stubblefield, A.D. Rubin and D.S. Wallach, 2004. Analysis of an electronic voting system. Proceedings of the 2004 IEEE Symposium on Security and Privacy, May 12-12, 2004, IEEE, San Diego, California, USA, ISBN:0-7695-2136-3, pp: 27-40.

Mugunthan, S.N. and M.D. Parameswari, 2013. Highly secured online voting system (OVS) over network. Int. J. Commun. Netw. Syst., 02: 146-152.

Pranay, R.P., P.N. Dhiraj, R.K. Mahendra, L.R. Sushil and S.R. Rahul et al., 2014. A remotely secure E-voting and social governance system using android platform. Int. J. Eng. Trends Technol., 9: 671-676.

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM., 21: 120-126.

Shubhangi, S.S., S. Shukla and D.K. Chitre, 2013. Privacy preservation in I-voting using homomorphic technology. Int. J. Comput. Sci. Telecommun., 4: 12-14.

Zhang, Q., L. Cheng and R. Boutaba, 2010. Cloud computing: State-of-the-art and research challenges. J. Internet Serv. Appl., 1: 7-18.

Zwattendorfer, B., C. Hillebold and P. Teufl, 2013. Secure and privacy-preserving proxy voting system. Proceedings of the 2013 IEEE 10th International Conference on E-Business Engineering (ICEBE), September 11-13, 2013, IEEE, Graz, Austria, ISBN:978-0-7695-5111-1, pp: 472-477.