An Implementation of Online Voting System using Okamoto-Uchiyama Encryption Scheme

Ms.Sneha N Patil ,PG student, Department of Computer Engineering, Shah and Anchor College of Engineering,Chembur, Maharashtra,India

Prof. Vidyullata Devmane, Associate Professor, Department of Computer Engineering, Shah and Anchor College of Engineering,Chembur, Maharashtra,India,

ABSTRACT

Electronic voting (e-Voting) has totally replaced the traditional voting system. Due to the rapid growth of computer networks and cloud computing the existing e-Voting system can be replaced with online voting system.When data is on cloud,the major challenge in voting system is confidentiality, security and accuracy. The advances in cryptography can be used to a face these challenges. The presented work implements Okamoto-Uchiyama algorithm with its additive homomorphic property. This work focuses on serving voting system on large scale of voters. Here system is user friendly, faster and meets security aspects.

Keywords:e-Voting, cloud-computing, encryption, Okamoto-Uchiyama, Homomorphic.

Academic discipline and sub-disciplines

Computer Science : Data security , Cryptography

SUBJECT CLASSIFICATION : Security, Integrity

Language: English

Date of Publication: 21-09-2018

DOI: 10.24297/ijct.v17i2.7632

ISSN: 2277 - 3061

Volume: 17 Issue: 02

Journal: International Journal Of Computers & Technology

Website: https://cirworld.com

This work is licensed under a Creative Commons Attribution 4.0 International License.

INTRODUCTION

In the past two decades, various types of electronic voting systems have got considerable attention. Electronic voting promises to make the electoral process simpler and more efficient for political parties, candidates, election administration, and for voters[7].For developing nations like Egypt, many voting schemes are evolving with newer strategies[6].While choosing India as a case study, a framework should be developed with security of the voting data for direct deployment.Cloud computing services provides efficiency and cost saving. Cloud services can be used to perform calculation on voting data.When data is on cloud,security plays major role because data may get accessible for intruders. One of the major challenge in e-Voting system is the voting data manipulation by the entities in the system. We cannot simply put confidential voting data on cloud. To overcome this problem data should be encrypted before sending to server. For encryption of data various algorithms can be used among which Elgamel, Okamoto-uchiyama&Paillier are now-a-days most likely to be used[3][4][5].Okamoto-Uchiyama algorithm is asymmetric cryptographic algorithm. In asymmetric cryptosystem public key is used to encrypt data and private key is required to decrypt the data. The public key is shared among parties. The algorithm shows additive homomorphic properties. Homomorphic encryption allows computation over encrypted data generating encrypted result. The decrypted result matches the result of operations as if they had been performed on plaintext. This property is used to hide the vital voting data form counting system [2].In this work we propose an approach for secure authentication of users in the cloud in online voting system. We use homomorphic encryption for securitypupose. With implementation of the Okamoto-Uchiyama algorithm we analyze the time taken by an algorithm and compare the performance of our system with that of the other existing systems. We check the similarities and differences of existing systems with our system. In the proposed system, we make sure that there will not be violation of user credentials at the authentication stage , We also make sure the vote given by voter will not be tampered as their values are encrypted and as we use algorithm with homomorphic property it will not be revealed at transferring on cloud.Also for meeting integrity constrain message digest is used so that an attempt for tampering of data will be detected.

RELATED WORK

[1]P. Sanyasi Naidu[et al] takes two shares of fingerprint image are created from which one is kept with VIC (Voter's Identification Card) and another with admin. These two shares are used for secure computation. In this paper Confidentiality and authenticity of the data is maintained. Work from this paper can be improvised through multi-factor authentication which can be used to reduce fake voting. As each time two shares of same fingerprint file has to save, large database is required.

[2]RifkiSuwandi [et al] have addressed the system for e-voting using Okamoto-Uchiyama algorithm and its homomorphic property which is used for encryption. Each cipher text is generated with unique value.Tally number generated represents accuracy of the calculation result of the ballots. Here Data confidentiality and security are ensured. Main critics in this is large cipher text is generated. Hence computation power and time required is also high.

[3]SmitaKhairnar[et al] in this paper, system uses PIN, biometric image and steganography for authentication. Non-transferable credential (biometric) is used to make authentication secure. Hash code works as checkpoint for integrity of stego image. In this special purpose pixel selection algorithm is used for non-retrieval of PIN. Encryption of the data is achieved using timestamp and hashing. Drawback of this approach is huge data as huge file size is generated in steganography hence anyone can suspect about it and can attempt to look into it. Hence it is easy to leak the data for an attacker.

[4]ShifaManaruliesyaAnggriane[et al] This research focuses on prove the effectiveness of the Paillier algorithm and its homomorphic property that implemented in an e-voting systemThis system claims the success ratio of the systems as 100%. But results for encrypted text is actually of size of 4 times larger than the plaintext size which takes big computational time for system.

[5]Xuechaoyang[et al] proposes a ranked choice based online voting system which eliminates all hardwired restrictions on the possible assignments of points to different candidates according to the voters' personal preferences. In order to protect the confidentiality of the votes, each cast ballot is encrypted using the exponential ElGamal cryptosystem before submissionwhich validates the votes and maintains confidentiality. Limitation for this research is system needs to assume that at least one authority is honest, since otherwise the system is not secure.

[6]NilamKate[etal], authors proposed an online voting system using visual Cryptography which aims atproviding aflexibility to allow casting of vote from any remote place thorugh web based application. AES encryption scheme is used for encrypting the voting data for its cost-effectiveness and speed of execution. Authenticity measures used in this paper are login and password which if get shared, fake voting can take place.

[7]Pranay R. Pashine[et al], proposes a new cryptographic electronic voting scheme based on public key cryptosystem. The proposed e-voting scheme is based on the conceptof *Prêt à Voter,*a paper ballot e-voting scheme.The proposed scheme uses paper ballots, due to its familiarity among the public, but with strong encryption protocols that provides enhanced level of ballot secrecy, verifiability and voter privacy. The proposed e-voting scheme eliminates the need for anonymous channels and yet provides the same level of security with less system complexity. But as with paper ballot system security of voting data cannot be handled.

SYSTEM DESIGN

System comprises of following steps to carry out for implementation of voting system through Okamoto-Uchiyama algorithm.

Algorithm consist of following steps [2]:

Key Generation

Steps for key generation are as follows :

1. Generate two large primes p, q and set n= p^2q.
2. Choose g $\in \mathbb{Z}^*$
3. Let h = g^n mod n

By following above steps we get a tuple as (n, g, h) forms public key and two primes (p, q) is private key.

Message Encryption

To encrypt a message m which has to be integer $\in \mathbb{Z}^*$

1. Select a random number r $\in \mathbb{Z}^*$
2. Compute a cipher text by C = $g^m h^r$ mod n

Message Decryption

To decrypt the message function is defined as follows,

1. L(x) = (x – 1) /p which is an auxiliary function.
2. Compute decrypted text by,
3. m = L (C^{p-1} mod p^2) / L (g^{p-1} mod p^2) mod n

Homomorphics Process

In case of o-u cryptosystem the encryption function is additively homomorphic. The product of two cipher text decrypts to sum of their corresponding plaintexts.

If of *m0* and *m1* are plain texts, then their respective cipher texts are

$$C_0 = g^{m0}\, h^{r0} \text{ and } C_1 = g^{m1}\, h^{10}$$

As *o-u* possess additive homomorphic property, the end result will be

$$C_0\, C_{1\,=}\, g^{m0+\,m1}\, h^{r0+\,r1} \bmod n$$

This key feature is used in the presented work to count the votes.

MD-5 Algorithm

Md-5 algorithm is used for authentication and integrity of data over the network. This hash function produces checksum of 128 bit on provided plaintext as an input [3].

Replay attack

Replay attack in network counts with malicious activities over data transmission like delaying data transmission fraudulently or retransmission of data,where duplicate data can also be send over network. We,in our proposed work have handled this with formation of secret session key for every voting session,so that no voter can vote twice.

IMPLEMENTATION

The e-voting application is designed to be the advanced simulation of existing e-voting system in general. With graphical user interface (GUI), system design mentioned below will be a web based system implemented using Java language and uses MySQL for its database.[6]

Fig.1 represents the system design proposed in this research

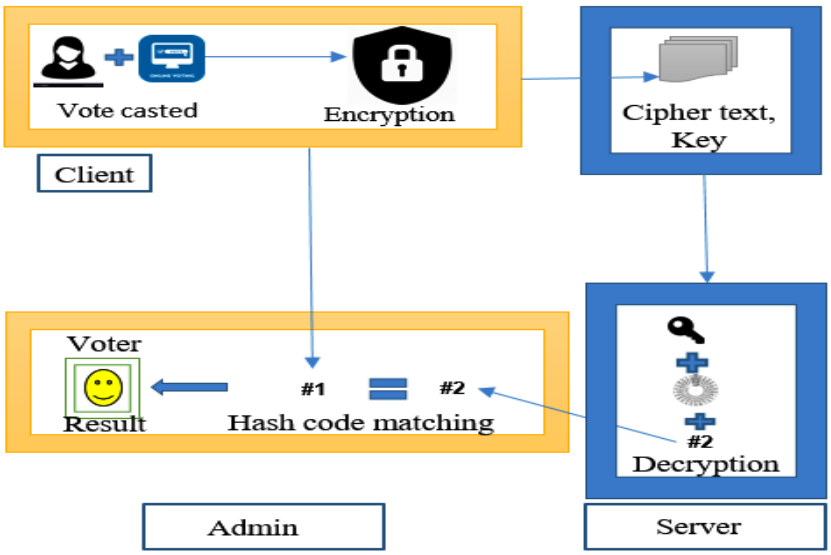

Fig. 1. System Design

System initiates with client-side encryption followed by casting a vote by user. Cipher text with public key will be sent over the network to the server side and hash implemented over the ciphertext will be sent to admin. Decryption will take place at server side and hash will be matched at admin side after implementing it over ciphertext at server side too. Finally the winner will be announced.

Fig.2 shows the GUI developed for making system user friendly.

Fig. 2. Home screen

Figure2.representshome screen who welcomes the user of an application including admin where user can register himself as a voter and can cast vote after logged into the system provided admin can only view the results.

Fig.3 shows the registration screen for voter.

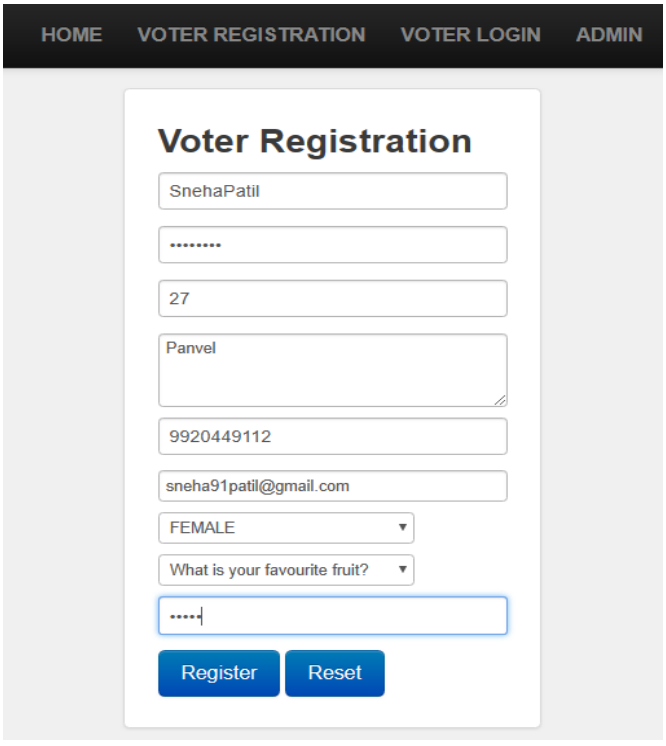

Fig. 3. Registration

Every user has to register himself and has to get validated to the system. The voter who are validated need to log in to the system using login credentials and then he supposed to cast his vote followed by the session key received on his mail. Question captcha is provided for login in case of password failure.Furthermore, user will be able to cast his vote using unique session key received on his e-mail and user's ballot choice will be encrypted by an application using Okamoto-Uchiyama cryptosystem. The ballot's choice after encryption is stored in the database. Each voter's choice will have different cipher text even though they have voted same candidate. We are maintaining another separate database for storing responses of votes to carry out encryption decryption process over the plain text.

Encryption using Okamoto-Uchiyama algorithm as explained above gives advantage of homomorphic property which can obtained results of encryption of two votes by multiplying the votes and decrypting them beforehand.Implementations of hash function over the encrypted data to check data integrity at client and server side. MD-5 hash algorithm is used to generate 128-bit value over cipher text file at client side.

At the server side, a combination of hash value, public key and ciphertext will be sent. Say admin, will implement hash over received ciphertext file and will match that hash value with received client side hash value. If both hash values are matching, the data is not violated while transmission is obtained.

Fig.4 shows the registration screen for voter.

Fig. 4. Candidate selection ballot

Once voter logged in to his account he can view his profile with all credentials he entered, can view profiles of candidates of election altogether and can cast his vote for one candidate.

RESULT ANALYSIS

System is tested over different sizes of plaintext files which contains multiple records. Here representing 5 vote records for 5 parties. Here an attempt is to show plain text and ciphertextgenerated using random number. Where vote for each candidate will be counted in terms of 1's.

TABLE I. VOTE RESPONCES WITH CIPHERTEXT

Voter	***Responses for candidates***					***Vote message to be encrypted***	***Ciphertext***
	1	***2***	***3***	***4***	***5***		
	1	10	100	1000	10000		
1	1					1	8.71E+152
2				1000		1000	4.128E+153
3	1					1	6.388E+153
4	1					1	3.965E+153
5		10				10	3.502E+153

Every response of vote is considered as plain text and is encrypted with calculations with random number and stored in database. Every time the system is refreshed ciphertext will be different for same data. Even though plain text issame, the ciphertext will be different. This operations makes the data unpredictable for network attack. Candidate 1 has got total 3 votes and candidate 2 and 4 are holding second position with 1 vote each.

Furthermore the system is tested over multiple records but testing is not limited to number of records. Different files generated with huge number of records of votes as dummy are used for testing an algorithm over other existing cryptosystems. Referring to existing systems with other encryption schemes, we compared performance of our system with other encryption scheme time[8] and came out with some observations as follows :

Here Table II shows the comparison amongexisting cryptosystems of their encryption and decryption time for different file sizes of plain text.

TABLE II. COMPARISON OF ENCRYPTION & DECRYTPION TIME

File Size	Time (milliseconds)			
	Encryption		***Decryption***	
(KBs)	RSA	OKA	RSA	OKA
50	216	108821	4135	95
100	410	217655	8230	201
200	815	435365	16553	423
400	1620	870767	32743	863
800	3263	1743113	65722	1692
1600	6743	3491806	132154	3385
3200	13124	6992024	265307	6827

Records mentiond above are tested with files having multiple votes in it. E.g. 50 Kb file contains approximate 1600 votes which takes 1.81 minutes for encrytpion under Okamoto-Uchiyama cryptosystem which is noticeably more than RSA.But it takes very less time for decryption of same plain text file compared to other cryptosystems that counts to 0.001 minute.Md-5 hash generates 128-bit hash value over the encrypted file at client as well as server side. We tested this by changing content of plain text manually and it lead to mismatching of hash code and there violation of data is detected.

In cloud environment, Data can be easily tampered through different network loopholes. We analyzed that our system detects the data tampering or suspicious change in data if occurred.Also as the proposed system is more focused towards security of voting data than performance of system in terms of time, we analyze performance of okamotouchiyama in following way for 49 bytes of voting data :

TABLE III. PERFORMANCE OF O-U WITH DIFFERENT KEY SIZES

Key sizes(kbs)	Time(ms)
512	27
1024	62

For same data RSA took more time with same key sizes.Although time may vary at every execution because of batch processes of systems,we have analyzed okamoto performs better than existing cryptosystem.

CONLUSIONS

As voting systems needs security more than fast processing , we have focused on the security aspects under this work such that the effectiveness of Okamoto-Uchiyama algorithm and its homomorphic property is proved in e-voting system. Thus for tackling the Replay attack of under cloud environmentas we tested system for this, we are using secret session key for every voting session which will limit the attempt for vote casting.Hash function provides check for data integrity within a network. This work presents one of the

possible ways to detect suspicious activities in online voting systems. Since it uses cryptography algorithm it is possible to secure the data and using hash function to check tampering of data for unauthorized activities carried if any. The security and performance analyses from in this paper demonstrate that proposed method has achieved significant improvements in comparison with the existing cryptosystems. Finally, we proof that our scheme can detect and prevent some malicious attacks over voting data over the network.

Acknowledgments

We wish to express our profound gratitude to our Principal Dr.Bhavesh Patel for allowing us to go ahead with this project and giving us the opportunity to explore this domain. We would also like to thank our Head of Department Prof.Mr.UdayBhave for our constant encouragement and support towards achieving this goal.

References

[1] P. Sanyasi Naidu ,Reena Kharat, RuchitaTekade, PallaviMendhe, VarshaMagade,"E-voting system using visual cryptography & secured Multi-party computation"in IJCRS,2016

[2] RifkiSuwandi, Surya MichrandiNasution, Fairuz Azmi, "Okamoto-Uchiyama homomorphic encryption algorithm implementation in E-voting system" in IEEE Trans. ISBN 978-1-5090-1648-8, International Conference on Informatics and Computing(ICIC) , 2016

[3] Smita B. Khairnar , P. Sanyasi Naidu, Reena Kharat,"Secure authentication for online voting system" published in IEEE Trans. ISBN 978-1-5090-3291-4, International Conference on Computing Communication Control and automation (ICCUBEA) 2016.

[4] ShifaManaruliesyaAnggriane,SuryaMichrandiNasution, Fairuz AzmiR. Nicole, "Advanced e-voting system using Paillier homomorphic encryption algorithm" in E-voting system" in IEEE Trans. ISBN 978-1-5090-1648-8,International Conference on Informatics and Computing(ICIC) , 2016

[5] Xuechao Yang ,Xun Yi ,Surya Nepal ,Andrei Kelarev ,FenglingHan,"A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption," published under IEEE journal vol.6 March 2018. DOI 10.1109/ACCESS.2018.2817518

[6] NilamKate ,J.v.Katte, "Security of remote voting system based on Visual Cryptography and SHA" published in IEEE Trans. ISBN 978-1-5090-3291-4,International Conference on Computing Communication Control and automation (ICCUBEA) 2016.

[7] Pranay R. Pashine , Dhiraj P. Ninave , Mahendra R. Kelapure , Sushil L. Raut , Rahul S. Rangari , Kamal O. Hajari. "A Remotely Secure E-Voting and Social Governance System Using Android Platform", International Journal of Engineering Trends and Technology (IJETT), V9(13),671-676 March 2014. ISSN:2231-5381

[8] FransiskusPancaJuniawan,Jl. Jend. Sudirman, SelindungBaru. "RSA Implementation for Data Transmission Security in BEM Chairman E-Voting Android Based Application",2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia,978-1-5090-1567-2/16 ©2016 IEEE