Volume 3 Issue 1 | March 2015 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Homomorphic Encryption and Re-Encryption Applied to Voting Data Security

Mukta Bhatele
Head of Department
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: mukta_bhatele@rediffmail.com

Md. Sohel Ansari
M.Tech. Research Scholar
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email:ansarisohel0@gmail.com

Raghvendra Singh Tomar
Assistant Professor
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: raghvendra_tomar@rediffmail.com

B. L. Rai
Assistant Professor
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email:blrai_08_76@yahoo.co.in

Abstract**—***Homomorphic Encryption is a good basis to enhance the security measures of untrusted systems/applications that stores and manipulates sensitive data. This strong protection of data results from the capability, allowed through HES, to perform arithmetic operations over encrypted bits. The homomorphic property of various cryptosystems can be used to create secure voting systems.*

The Idea of the project is create the Web interface for the voters to conduct voting online. However security and integrity of vote count on the data server is a major concern. To secure vote count on data Server to be hacked, the proposed system is to use the homomorphic encryption techniques. Also use of Re-encryption further enhanced Voting Data Security.

Keywords*:— Homomorphic Encryption, Re-encryption, Private Key, Serialization, Vote count, FHE.*

1. INTRODUCTION

Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services, for example a chain of different services from different companies could 1) calculate the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services. A cryptosystem which supports both addition and multiplication (thereby preserving the ring structure of the plaintexts) is known as fully homomorphic encryption (FHE) and is far more powerful. Using such a scheme, any circuit can be homomorphically evaluated, effectively allowing the construction of programs which may be run on encryptions of their inputs to produce an encryption of their output. Since such a program never decrypts its input, it can be run by an untrusted party without revealing its inputs and internal state. The existence of an efficient and fully homomorphic cryptosystem would have great practical implications in the outsourcing of private computations,

Homomorphic Encryption is a good basis to enhance the security measures of untrusted systems/applications that stores and manipulates sensitive data. This strong protection of data results from the capability, allowed through HES, to perform arithmetic operations over encrypted bits.

The homomorphic property of various cryptosystems can be used to create secure voting systems, the Idea of the project is create the Web interface for the voters to conduct voting online. However security and integrity of vote count on the data server is a major concern. To secure vote count on data Server to be hacked, the proposed system is to use the homomorphic encryption techniques. A windows Interface will be provided to the election commissioner that will be used to configure the Election. On configuring Election, the Election commissioner will generated the private Key and it will be serialized on the Computer of the Election commissioner. For all the parties participating in the election, the vote count for each of them will be initialized to Zero and will be stored in the database of the server in the encrypted form encrypted using the generated Private Key by the Election commissioner. On the Election date, the registered voters can login on to the Web Site and can vote for their desired party. When voting is done, one will be added to the encrypted vote count and incremented vote count will be stored on the data server in the encrypted Form.

For enhanced Security, during the voting period, the Election commissioner can use Re-Encryption that is to generate the new Private Key and re-encrypt the previously encrypted data using the newly generated Private Key.

On declaration date, the election commissioner will retrieve the Private Key by DE serializing it. Then the encrypted vote count will be retrieved from Server and using the Private Key will be decrypted and the vote count will be placed on the Server, so that the viewers will be able to view the result. It also provides facility to display the result of Election in graphical format.

2. REQUIREMENT

Requirements for an election vary by country and election type, but there are certain properties that are a starting point for all voting systems.

1. ***Democratic*** – each eligible voter must be able to vote and may vote at most once.
2. ***Private*** – a voter's final ballot must be secret.
3. ***Incoercible*** – a voter cannot prove the contents of her final ballot to anyone.
4. ***Accurate*** – the final tally is the sum of the cast votes.
5. ***Verifiable*** – an individual can prove to herself that her vote was cast as intended and that it was counted, and anyone can prove that the final tally is accurate.
6. ***Robust*** – a small group of people cannot disrupt the election.
7. ***Fair*** – Partial totals should not be known early.

It is also important for an election to be convenient and flexible for the voters and officials. Voters will be less likely to vote if the process is complicated and difficult to understand. Officials are unlikely to adopt a system that cannot support voting practices particular to their districts, such as write-in votes and instant runoff elections.

Paper-based voting systems have been the standard since the mid-19th century, when secret votes became the norm. Electronic systems, often called Direct Recording Electronic (DRE) systems, have become more prominent recently. In a society that is increasingly turning to technology to automate and streamline everyday tasks, it is natural to apply technology to an institution as important as elections. Electronic voting systems have the potential to improve accuracy and security of elections as well as alleviate many of the logistical headaches.

One of the major advantages of DRE systems is the potential for consistent implementation of security policies. A machine does only what it is programmed to do, whereas human behavior is situation-dependent and may bias the election system. Despite this potential, most DRE systems still rely exclusively on the integrity of election officials and training of poll workers to ensure the election maintains the proper security and privacy.

In order to believe her vote was properly recorded and tallied, the voter must trust election officials in her district, the technicians that set up the machines, the programmers that wrote the software, and the engineers that designed the hardware. She needs to trust that the machines were stored in a way that prevents tampering, and that they have been properly monitored since being removed from storage. She needs to trust that they will be securely delivered to the counting location after the polls close.

Since this issue has come to the forefront in 2000, there has been a push to integrate security into voting systems and thereby eliminate the reliance on trusted third parties. In particular, many have focused on the problem of trusting that the voting machine has recorded the proper vote.

The goal of this paper is to provide a voting data security using Homomorphic Encryption and Re-Encryption.

3. HOMOMORPHIC ENCRYPTION

Homomorphic encryption is naturally suited to election schemes. It allows the votes to be tabulated before decryption, improving privacy. For example, in additive Homomorphic encryption, the sum of two cipher texts is a third cipher text that encrypts the sum of the two original plaintexts.

Voting applications may use additive homomorphism to allow tallying to be done before decryption. With other forms of encryption, all the ballots are dissociated from their identifying pieces of information and then decrypted and tallied. If Homomorphic encryption is used, the tallying can be done while the votes are still encrypted, and the final total can then be decrypted. This effectively hides the contents of the original ballots while providing a publicly computable tally.

4. PAILLIER ENCRYPTION

The Paillier cryptosystem, named after and invented by Pascal Paillier in 1999, is a probabilistic asymmetric algorithm for public key cryptography. The problem of computing nth residue classes is believed to be computationally difficult. The decisional composite residuosity assumption is the intractability hypothesis upon which this cryptosystem is based.

The scheme is an additive homomorphic cryptosystem; this means that, given only the public-key and the encryption of m_1 and m_2, one can compute the encryption of $m_1 + m_2$.

Advantages:

1. Voting Simplified.
2. Use of Homomorphic Encryption ensures secured Voting.
3. It prevents unregistered users or unregistered users from using voting.
4. Ensures biased free Voting.
5. It results in time saving as opposed to Electronic Voting.
6. It is going to save time, Efforts and Resources.

5. NEED AND SIGNIFICANCE OF PROPOSED RESEARCH WORK

The main problem with current DRE systems is that they require a large amount of trust from the election officials, who are either elected officials themselves or else appointed by elected officials. However, there has been a significant amount of research on providing cryptographic schemes that reduce this burden of trust.

6. EXPECTED OUTCOME

The system is developed as a Web Site. The developed application will be deployed on a space purchased on a web server. The homomorphic property of various cryptosystems can be used to create secure voting systems,

The Idea of the project is create the Web interface for the voters to conduct voting online. However security and integrity of vote count on the data server is a major concern. To secure vote count on data Server to be hacked, the proposed system is to use the homomorphic encryption techniques. A windows Interface will be provided to the election commissioner that will be used to configure the Election. On configuring Election, the Election commissioner will generated the private Key and it will be serialized on the Computer of the Election commissioner. For all the parties participating in the election, the vote count for each of them will be initialized to Zero and will be stored in the database of the server in the encrypted form encrypted using the generated Private Key by the Election commissioner. On the Election date, the registered voters can login on to the Web Site and can vote for their desired party. When voting is done, one will be added to the encrypted vote count and incremented vote count will be stored on the data server in the encrypted Form.

For enhanced Security, during the voting period, the Election commissioner can use Re-Encryption that is to generate the new Private Key and re-encrypt the previously encrypted data using the newly generated Private Key.

REFERENCES :

[1] Ms. Parin V. Patel#1, Mr. Hitesh D. Patel*2, Pinal J. Patel#3, A Secure Cloud using Homomorphic Encryption Scheme, International Journal of Computer Science Research & Technology (IJCSRT) Vol. 1 Issue 1, June - 2013

[2] Maha Tebaa, Saïd El Hajji, Abdellatif El Ghazi, Homomorphic Encryption Applied to the Cloud Computing Security, Proceedings of the World Congress on Engineering 2012 Vol WCE 2012, July 4 - 6, 2012, London, U.K.