ISSN:0975-9646

Review on: Providing Arithmetic Operations on RSA using Homomorphic Technique

Shiwali[1], Namita kakkar[2]

[1,2] Computer Science & engineering department
Rayat & Bahra Institute of Engineering & Biotechnology, Mohali

Abstract — **Cloud computing is the sending of computing as a service rather than a product; and shared resources, software, and message are given to computers and other devices as a utility over a network. Traditionally departments store and maintain information in their own data centres, over which they had complete control. With the emergence of cloud computing organizations can store data in the cloud provider's data centre, but the security of the data in the cloud is a major concern. Information can be store in the cloud in an encrypted format; but the problem is that while message can be sent to and from a cloud provider's data centre in encrypted form; the servers that power a cloud can't do any work on it that way. To the Homomorphic encryption; a company could encrypt its entire database and upload it to a cloud and it is possible to analyse data without decrypting it. Thus Homomorphic encryption is a type of form of encryption which allows specific types of computations to be carried out on ciphertext and obtain an encrypted result which is the ciphertext of the result of operations performed on the plaintext. To this paper we are describing Homomorphic technique with arithmetic operation on RSA, Improving the Security level without compromising the security of existing technique**

Keywords— **Cloud, RSA, Homomorphic, DES, AES and NTRU**

I. INTRODUCTION

When we use the Internet, we're not always just clicking around and passively taking in information; such as reading news articles or blog posts a great deal of our time online involves sending others our own information. The ordering something over the Internet; whether it's a book; a CD or anything else from an online vendor; or signing up for an online account; requires entering in a good deal of sensitive personal information. And a typical transaction might include not only our names; e-mail addresses and physical address and phone number; but also passwords and personal identification numbers (PINs).

The incredible growth of the Internet has excited businesses and consumers alike with its promise of changing the way we live and work. This is extremely easy to buy and sell goods all over the world while sitting in front of a laptop. Therefore security is a main concern on the Internet; especially when you're using it to send sensitive information between parties.

Information security is provided on computers and over the Internet by a variety of methods. Then the simple but straightforward security method is to only keep sensitive information on removable storage media like portable flash memory drives or external hard drives. And most popular forms of security all rely on encryption; the process of encoding information in such a way that only the person (or computer) with the key can decode it. In this paper; you will learn about encryption and authentication. We will also learn about public-key and symmetric-key systems; as well as hash algorithms.

Encryption is the conversion of data into a form; called a cipher text; that cannot be easily understood by unauthorized people. And decryption is the process of converting encrypted data back into its original form; so it can be understood.

The use of encryption/decryption is as old as the art of communication. In war time; a cipher; often incorrectly called a code; can be employed to keep the enemy from obtaining the contents of transmissions. Therefore simple ciphers contain the substitution of letters for numbers; the rotation of letters in the alphabet; and the "scrambling" of voice signals by inverting the sideband frequencies. Thus more complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal; the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Thus alternatively; computer can be used in an attempt to break the cipher. Then more complex the encryption algorithm; the more difficult it becomes to eavesdrop on the communications without access to the key.

Encryption/decryption is especially important in wireless communications. It is because wireless circuits are easier to tap than their hard-wired counterparts. And nevertheless; encryption/decryption is a good idea when carrying out any kind of sensitive transaction; such as a credit-card purchase online; or the discussion of a company secret between different departments in the organization. Then stronger the cipher that is; the harder it is for unauthorized people to break it the better; in general. Thus however; as the strength of encryption/decryption increases; so does the cost.

II. OVERVEW OF RSA ENCRYPTION SYSTEM

Asymmetric encryption is also known as public-key cryptography. Therefore asymmetric encryption differs from symmetric encryption primarily in that two keys are used: one for encryption and one for decryption. Then most common asymmetric encryption algorithm is RSA. Compared to symmetric encryption; asymmetric encryption imposes a high computational burden; and tends to be much slower. Thus it isn't typically employed to protect payload data. Instead its main strength is its ability to establish a secure channel over a non-secure medium. This is accomplished by the exchange of public keys; which can only be used to encrypt data. Then complementary private key; which is never shared; is used to decrypt.

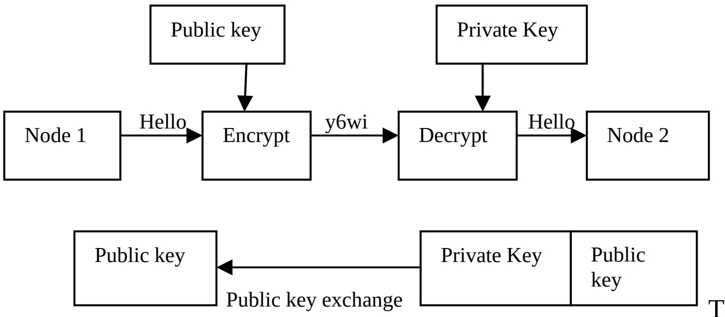

Figure 1: RSA System

Homomorphic encryption is the conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form. The homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. Thus in mathematics; homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets. Then term is derived from the Greek words for ‘same structure’. Due to the data in a homomorphic encryption scheme retains the same structure; identical mathematical operations whether they are performed on encrypted or decrypted data will yield equivalent results. Homomorphic encryption is expected to play an important part in cloud computing; allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider’s analytic services. Here is a very simple example of how a homomorphic encryption scheme might work in cloud computing. To encrypt the data set, Business XYZ multiplies each element in the set by 2; creating a new set whose members are 10 and 20.Business XYZ sends the encrypted VIDS set to the cloud for safe storage. And few months later, the government contacts Business XYZ and requests the sum of VIDS elements. Business XYZ is very busy, so it asks the cloud provider to perform the operation. To encrypt the data set, Business XYZ multiplies each element in the set by 2, creating a new set whose members are 10 and 20.Business XYZ sends the encrypted VIDS set to the cloud for safe storage. A few months later, the government contacts Business XYZ and requests the sum of VIDS elements. Business XYZ is very busy, so it asks the cloud provider to perform the operation. Then cloud provider; who only has access to the encrypted data set, finds the sum of 10 + 20 and returns the answer 30.Business XYZ decrypts the cloud provider’s reply and provides the government with the decrypted answer, 15.

III. DIFFRENT TECHNIQUES OF ENCRYPTION

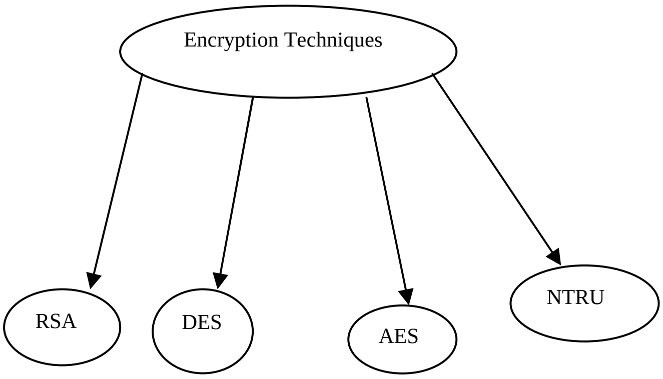

Figure 2: Different technique of encryption

The existing encryption technique includes using various cryptography techniques using RSA, DES, AES, NTRU etc. However it’s been studied that various improvements needed to be analysed before making a further improvement and taking cryptography to another platforms. The encryption along with Arithmetic Operations on RSA shall be a new area of research and wasn’t not been implemented yet and can be a new area of research where a data can be send along the network with more secured side size without compromising its quality.

V. LITERATURE SURVEY

Yang Pan et al. (2013) there lacks of practical homomorphic encryption schemes in cloud computing at present. CESVMC is a scheme supposed to solve the problem. CESVMC ensures that after calculating the user’s encrypted data and returning the cipher result to user by the service provider, the user can decrypt the cipher result and get the right service result. But CESVMC only supports multiplication or division operation once. Meanwhile, to decrypt the ciphertext, user needs to tell which type of operation has been done to the ciphertext. All these constrain the usability of CESVMC in cloud computing. Solve these problems; an improved CESVMC (ICDM) is proposed. Thus encryption algorithm; the information of plaintext and the operation type are hidden in a diagonal matrix. Therefore diagonal matrix is encrypted by using an invertible matrix as secret key. Then in decryption algorithm; ICDM chooses the right encryption method by reading the sign of the operation type without any manual interventions. Security analysis indicates ICDM is IND-CPA. Then experiments proof ICDM can support unlimited times arithmetic operations homomorphically after partly lowering efficiency and adding the ciphertext length. Thus, it can fit privacy-preserving in cloud computing better.

Vishwa Gupata et al. (2012) they have developed a new cryptography algorithm which is based on block cipher concept. In this algorithm they have used logical operation like XOR and shifting operation. And experimental results proof that proposed algorithm is very efficient and secured with better speed.

Zhiqiang Xie et al. (2012) present a problem that Rijndael algorithm can be attacked by Square attacks; an improved Rijndael algorithm method which is based on prefix codes is put forward. Because to the good Characteristics in decoding of prefix codes; the method will change the order of sub-keys through the procedure of decrypting different plaintext inputted by prefix codes; and make the order relate with the plaintext; in other words; it makes the system be variable. To the improvement it has no effect on the efficiency; but it can resist the Square attack fundamentally.

Aman Kumar et al. (2012) this paper is to present the comparison between DES secret key based algorithm and RSA public key based algorithm. The two main features that specify and differentiate one algorithm from another are the ability to secure and protect the data against attacks and speed of encryption and decryption. Performance of different algorithms is different according to data loads.

Amritpal Singh et al. (2013) proposed technique of comparative study between four such widely used encryption algorithms DES; of DES; 3DES; AES and RSA on the basis of their ability to secure and protect data against attacks and speed of encryption and decryption. The two main characteristics that identify and differentiate encryption algorithm from another are their capability to secure the protected data against attacks and their speed and effectiveness in securing the data.

Brittan Paul: This paper describes four lossless data compression algorithms. Lempel-Ziv 77 (LZ77) and Lempel-Ziv-Welch (LZW) which are based on the dictionary methods, Prediction with Partial Match (PPM) which is based on the statistical methods and Burrows-Wheeler Transform (BWT) which was found to be inadequate since the algorithm does not compress the data, it only optimizes it for compression. After comparison of the algorithms using benchmark testing, it was found that using Lempel-Ziv (LZ77) was the optimal algorithm because of its speed and low memory usage.

P.Saveetha et al. (2013) The Network Security means to protect data during their transmission over channel of networks similarly Internet security also to protect data during their transmission over a collection of interconnected networks in all over the world. Cryptography is the way of hiding information during transmission over a cannel. There are lots of cryptographic algorithms available to protect our data from intruders.RSA also one of effective the public key cryptographic algorithm which needs time and memory. Many research papers submitted on this cryptographic algorithm.

VI. Conclusions

Security of cloud computing based on fully Homomorphic encryption is a new concept of security which is enable to provide the results of calculations on encrypted data without knowing the raw entries on which the calculation was carried out respecting the confidentiality of data. And our work is based on the application of fully Homomorphic encryption to the security of Cloud Computing:

a) Analyze and improve the existing cryptosystem to allow servers to perform various operations requested by the client.

b) To modify the complexity of the Homomorphic encryption algorithms and study the response time to requests according to the length of the public key.

Acknowledgment

I would like to thank my guide Mrs. Namita kakkar, Assistant professor in department of computer science and engineering at RBIEBT (Mohali), Punjab, India and all my professors.

References

[1.] Yang Pan, Gui Xiaolin, Yao Jing, Lin Jiancai, Tian Feng; “ICDM: An encryption that supports unlimited times Homomorphic arithmetic operations on encrypted data, IEEE, pp-1220-1225, 2013.

[2.] Gupta Vishwa, Singh Gajendra, Gupta Ravindra; “Advance Cryptography algorithm for improving data security”, IJARCSSE, Volume 2, Issue 1, January 2012.

[3.] Kumar Aman, Jakhar Sudesh, Makkar Sunil; “Comparative analysis between DES and RSA algortihm’s”, IJARCSSE, Volume 2, Issue 7, July 2012.

[4.] Xie Zhiqiang, Gao Pengfei, He Yujing, Yang Jing; “Study on Improved Rijndael Encryption algorithm based on Prefix code, Advances in computer science and information Technology, Volume 2, pp- 485-491, 2012.

[5.] Singh Amritpal, Marwaha Mohit, Singh Baljinder, Singh Sandeep; “Comparative study of DES, 3DES, AES and RSA”, International journal of computers and technology, Volume 9 No.3, pp-1164-1170, july 25, 2013.

[6.] Brittan Paul, “Evaluating lossless data compression algorithms for use on mobile devices”, Literature Synthesis.

[7.] Tebaa Maha, Haji El Said, Ghazi El Abdellatif, “Homomorphic encryption method applied to cloud computing”, IEEE, pp- 86-89, April 2012.

[8.] Saveetha P., Arumugam S., “Study on improvement in RSA Algorithm and its implementation”, International journal of computer and communication technology, Volume 3, Issue 6,7,8, 2012.