Global Journal of Advance Engineering Technologies and Sciences

A GENERAL STUDY OF HOMOMORPHIC ENCRYPTION ALOGORITHM WITH CLOUD COMPUTING

V.Sangeetha[1], V.Jaganraja[2], T.Gnanaprakasam[3]

[1]M.E Computer Science and Engineering
[2]M.E Computer Science and Engineering with Specializations in Networks
[3]Head of department/Computer Science and Engineering,
The Kavery Engineering College, Mecheri
sangee1992@gmail.com

ABSTRACT

In Cloud computing, instead of all the computer hardware and software we are using our desktop, or somewhere inside our company's network, it's provided as a service by another company and accessed through the internet, usually in a completely consistent way. It gives various benefits to users but the fact most of users consider is their data security. Security is the most prioritized aspect for any form of computing, the obvious expectation that security issues are very crucial for cloud environment. As the cloud computing approach could be associated with having users data stored at both clients end as well as in cloud servers, identity management and authentication are very crucial in cloud computing. This paper shows how we secure the cloud security, privacy and reliability when an unauthorized is processing sensitive data. In this paper, we have discussed security risks and concerns in cloud computing and instructed steps that an enterprise can take to reduce security risks and protect their resources and about the study of homomorphic encryption algorithm.

INTRODUCTION

Cloud computing is a model for allocating compute and storage resources on demand. Cloud computing provide new ways to provide services to change the cost structure using those services. The technical and pricing opportunities drive changes in the way businesses operate. Cloud computing is a unique combination of capabilities which include:

- Highly scalable
- Dynamic infrastructure
- Universal access
- Fine-grained usage controls and pricing
- Standardized operating system
- Support services for management

Cloud computing security is the set of policies and control-based technologies designed to adhere the compliance rules and protect information, data applications and infrastructure accompanied with the use of cloud computing.

Using of cloud computing in more organizations and their cloud providers for data functions, the security in these and other potentially vulnerable areas are the priority for organizations contracting with a cloud computing provider.

Cloud computing security processes should address the security controls the cloud provider that will applied to maintain the customer data security, privacy and compliance with necessary regulations. The processes will also likely include a business continuity and data back-up plan in the case of a cloud security breach.

CLOUD SERVICES

Cloud Services can be dived into 3 stacks:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Infrastructure As A Service

- Cloud computing providers maintain the storage, database and hosting environment for the clients.
- The clients are allowed to use the infrastructure provided as a service for which they pay as per usage as agreed by the cloud computing providers.
- Iaas acts as the base layer for the cloud stack.
- For their execution it serves as a base for other two layers. Virtualization is the keyword behind this stack.
- In Amazon EC2 (Elastic Compute Cloud) the application executed on a virtual computer.
- We can select the optimal virtual computer in the configuration of CPU, memory and storage for the application.
- The whole cloud infrastructure viz. hardware based load-balancing, servers, routers, storage, firewalls and other network equipments are provided by the IaaS provider.

Platform As A Service

- Cloud computing providers manage the platform on the cloud infrastructure.
- PaaS model delivers computing platform as service.
- It helps the users to develop and display applications without the need to purchase the required hardware and software.
- Now you don't need to invest millions of dollars to get that development foundation ready for your developers.
- The PaaS provider will deliver the operating system on the web, and in most of the cases you can consume the platform using your browser, so we no need to download any software.
- It has definitely empowered small and mid-size companies and to even an individual developer to launch their own SaaS leveraging the power of these platform providers, without PaaS Layers:
  - Cloud OS
  - Cloud Middleware

Software As A Service

- The cloud computing provides install, manage and maintain the software.
- Cloud computing provides own the physical infrastructure on which software is running.
- User access the services to which they have subscribed and pay as per the agreement between them and the cloud computing provider.
- The licenses for the applications that are used by the cloud users are handled by the cloud computing providers.

HOMOMORPHIC ENCRYPTION

What Is Homomorphic Encryption?

Homomorphism - a transformation of one set into another that preserves in the second set the relations between elements of the first. The systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data. It is operation performed on a set of cipher texts such that decrypting the result of the operation is the same as the result of some operation performed on the plaintexts. Consider a cryptosystem that has encryption function ε, plaintext x_n, ciphertext c_n such that

$$\varepsilon(x_n) = c_n$$

Fully Homomorphic Encryption (FHE) Scheme is the mostly used encryption scheme which is used to encrypt the data to be sent or stored into the cloud. Homomorphic is the property which defines the concept of encrypting the cipher data text before its decryption. FHE is a scheme which enables user to do computations on that data which has been encrypted without decrypt it. It enables user to perform the numeric calculations or some of simple aggregations on the encrypted data and it enables user for the computation of some functions on the encrypted data. FHE scheme is based on the concept of asymmetric key encryption scheme which is used to secure the data from a diverse set of tasks. The plain as well as cipher text both are considered with the same algebraic function. In FHE scheme, a user can perform an operation on encrypted data without having the knowledge regarding the actual data. In FHE scheme, the plaintext is changes to encrypted data and after the encryption the services of cloud comes into practice to provide the safe and secure storage of data.

The flow of encryption and decryption of data in FHE and protection of data is explained as follows:

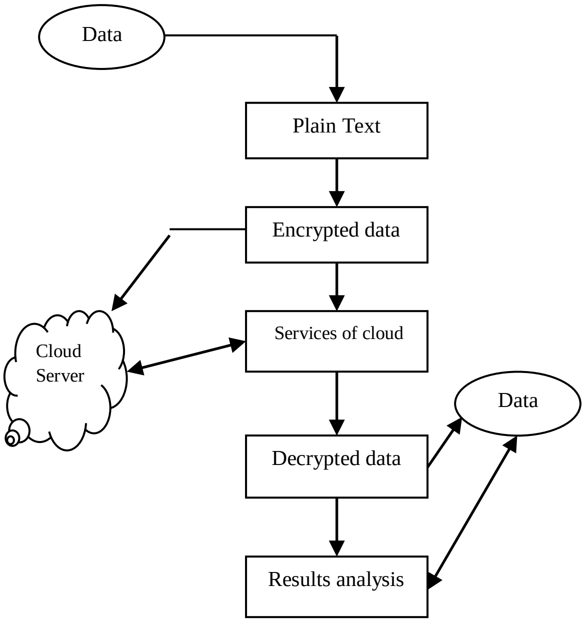

Fig 1.1 Data flow diagram

ENCRYPTION METHOD

For the analysis of Homomorphic Encryption cryptosystems behaviour, we develop the each encryption algorithm in this module. The Homomorphic encryption has two properties; they are Partial Homomorphic Encryption and Fully Homomorphic Encryption. The algorithms Multiplier Homomorphic Encryption (RSA cryptosystem), Additive Homomorphic Encryption (Paillier cryptosystem), Elgamal cryptosystem are partial encryption algorithms.

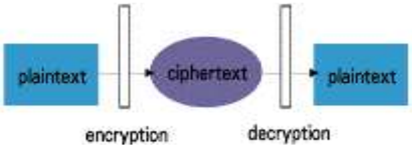

Fig.1.2 Basic encryption and decryption process

An encryption scheme is “homomorphic” if it is possible to perform implicit operation on the plaintext by processing the ciphertext only. Homomorphic encryption is the encryption technique on the already encrypted data rather than on the original data that provide the result as it is done on the plain text. The complex mathematical operations can be performed on the cipher text without changing the nature of the encryption

Homomorphic Encryption H is a set of four functions: H = {Key Generation, Encryption, Decryption, Evaluation}

1. Key generation: client will generate pair of keys public key (pk) and secret key (sk) for encryption of plaintext.
2. Encryption: Using secret key (sk) client encrypt the plain text (PT) and generate Esk (PT) and along with public key (pk) this cipher text (CT) will be sent to the server.
3. Evaluation: Server has a function f for doing evaluation of ciphertext (CT) and performed this as per the required function using pk.
4. Decryption: Generated Eval(f(PT)) will be decrypted by client using its sk and it gets the original result.

RSA exhibits multiplicative homomorphism. By multiplying two (or more) RSA ciphertexts together, the decrypted result is equivalent to the multiplication of the two (or more) plaintext values.RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product. The homomorphism is: Suppose there are two plaintexts P1 and P2. Then

$$\begin{aligned} ek(P1)\ ek(P2) &= P1^{b}\ P2^{b} \bmod n \\ &= (P1P2)^{b} \bmod n \\ &= ek(P1P2). \end{aligned}$$

Paillier follows additive homomorphic encryption. By multiplying each component of multiple ciphertexts with their corresponding respective components, the decrypted result is equivalent to the addition of the plaintext values. The Homomorphic: Suppose x1 and x2 are plaintext. Then,

$$\begin{aligned} Ek(x1,r1).ek(x2,r2) &= gx1\ r1^{m}\ gx2\ r2^{m} \bmod n^{2} \\ &= gx1 + x2(r1\ r2)^{m} \bmod n^{2} \\ &= ek(x1 + x2,\ r1\ r2) \end{aligned}$$

ElGamal exhibits multiplicative homomorphism. By multiplying each component of multiple ciphertexts with their corresponding respective components, the decrypted result is equivalent to the multiplication of the plaintext values. ElGamal also has a multiplicative homomorphic property. Given ciphertexts (c1, c2) and (d1, d2) that are encryptions of m1 and m2, using random values XB1and XB2, respectively, then

$$\begin{aligned} (c1d1,\ c2d2) &= (g^{x}B1\ g^{x}B2,\ (m1.S1)\ (m2.S2)) \\ &= (g^{x}B1^{+x}B2,\ m1m2.S1+S2) \end{aligned}$$

A cryptosystem which supports both addition and multiplication is known as Fully Homomorphic Encryption (FHE) and is far more powerful. Using such a scheme, any circuit can be evaluated homomorphically, and 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 will have great practical implications in the outsourcing of private computations, especially, in the context of cloud computing.

FUTURE WORK

Cloud computing is an emerging technology for the next generation of IT applications. The barrier toward the rapid growth of cloud computing are data security and privacy issues. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. In this paper we have discussed some key data security issues and also different techniques to provide data security. In this paper we have given some fully homomorphic encryption scheme developed by researchers which allow us to perform computation on encrypted data without using secret key of client.

REFERENCES

1. Nishigandha LavkumarDhotre, Rahul Ashok Chavan(2015), “Homomorphic Encryption- a Consolidate Element for Data Security in Cloud Computing”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 5.
2. Maha TEBAA, Said EL HAJII(2013),”Secure Cloud Computing through Homomorphic Encryption”, International Journal of Advancements in Computing Technology(IJACT) Volume5, Number16.
3. Craig Gentry (2009),“Fully Homomorphic Encryption Scheme”.
4. D. Boneh and al(2004) Public key encryption with keyword search, proceedings of Eurocrypt 2004, LNCS 3027, pp. 506-522.
5. K.RevanaSuresh(2014) “Ensuring Data Security Using Homomorphic Encryption In Cloud”.
6. Louay Karadsheh(2012), “Applying security policies and service level agreement to IaaS service model to enhance security and transition”.
7. Peter Mell, Timothy Grance(2011), “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145.
8. Reem Alattas(2014), “Cloud Computing Algebraic Homomorphic Encryption Scheme”.
9. Sean Marston and al.(2011) “Cloud computing — The business perspective”, Volume 51, Issue 1, Pages 176–189, http://www.sciencedirect.com.

10. Sean Carlin, Kevin Curran(2012), “Cloud Computing Technologies”, International Journal of Cloud Computing and Services Science (IJ-CLOSER), Vol.1, No.2, pp. 59~65.