ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

A Comparative Study of Encryption Techniques in Cloud Computing

Yesha N B, Dr Ashwini Kodipalli

B.E. Student, Dept. of ISE, New Horizon College of Engineering, Bangalore, Karnataka, India.

Assistant Professor, Dept. of ISE, New Horizon College of Engineering, Bangalore, Karnataka, India.

ABSTRACT: Security is one of the most critical aspect we need to focus on before moving the data to cloud. In the current trends cloud computing is at the verge of revolutionizing computing. According to Gartner, by 2020 an organization without cloud will be as rare as life without internet today. This widespread innovation has also led to concern over security and privacy. Encryption is one of the most important ways for secure transmission of data over the network. It is one of the sturdiest techniques which is developed and is evolving to include capabilities that ensure increase in user's trust on security. Encryption is a technique used to hide the original data by transforming it into other form by means of complex algorithms using encryption keys. Many encryption techniques and algorithms have been designed and developed overtime which facilitate secure transmission of data between the cloud customer and the Cloud Service Provider(CSP).This paper focuses on various Encryption techniques such as Homomorphic Encryption, Public key Encryption(PKE) and Identity Based Encryption(IBE), explaining capabilities of each of these as well as drawbacks and possible solutions of each of these techniques.

KEYWORDS: Cloud computing, Cloud, Security, Homomorphic Encryption, Identity Based Encryption (IBE).

I. INTRODUCTION

Cloud computingmeans storing the data and programs over the internet rather than on your own desktop computer.Cloud computing is a model that facilitates access to shared pool of computing resources over the internet with minimal consumer effort or service provider interaction. It allows access to massively scalable inexpensive, on demand computing resources[3]. The Cloud computing architecture is composed of various characteristics, service models, and deployment models which are the major business drivers[1].

The defining characteristics of Cloud computing are: 1)On-demand self-service 2) Broadnetworkaccess 3) Location-independent resource pooling 4) Scalability 4) Measured services[1].

Cloud computing offers services through three service models which are 1) Software as a Service(SaaS) where software is provided as a service to the customer 2) Platform as a Service(PaaS) where application platform that provides developers with quick deployment is provided as a service over the web[2] and 3)Infrastructure as a Service(IaaS) is model that enables on-demand access to cloud computing infrastructure such as server, network, storage, operating system etc.

To make better use of computing resources and controlling growth, various cloud computing models are deployed they are Public cloud, Private cloud , Community cloud and Hybrid cloud each of which offers specific functionality.

Cloud computing has gained popularity over past few years which led to increase in number of cloud providers and the number of organizations using cloud services to store and access their massive amount of data. Many big companies like Google, Amazon, and Microsoft are offering cloud services. This widespread innovation has also led to concern over security and privacy.

When it comes to security the owner of the data should consider the following; How does the Cloud Service Provider(CSP) ensures you that your data will not be lost or reused by other users? What if the datacentre is attacked or sever is hacked? How to hide the original data from the other user or even the CSP?[7].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

So users should encrypt the data before they could send it to the cloud provider. And the calculations are performed on the encrypted data at the CSP. And results are sent back to the user who decrypts the encrypted result and uses it.
Our discussion will start with the problem statement followed by defining encryption and describing the various encryption techniques with algorithms and drawbacks and possible solutions for each.

II. RELATED WORK

Problem Statement: Security is one of the main challenges today's cloud computing is facing. Cloud customers are less likely to entrust about the security techniques used in cloud computing. So we need to have some robust techniques to achieve this. Eventually many techniques and algorithms have been developed of which encryption is one of the sturdiest technique which is developed and is evolving to include more capabilities that increases users trust on security of cloud computing.
Encryption: Is a technique which hides the original data by transforming it into some other form using various algorithms. For secure communication between the customers and the users in the presence of cloud service provider. Users must encrypt their data before they could send it to the cloud therefore maintaining privacy of the data[9]. There are various cryptographic techniques used for encrypting the datasuch as Homomorphic Encryption, Public-Key Encryption and Identity Based Encryption.

1) Public-Key Encryption(PKE): PKE makes use of two keys 1). Public key: This is shared with everyone. 2). Private Key: this key is known only to the recipient of the data i.e. the CSP[12]. The customer encrypts the data using the public key and sends this encrypted data over the network to the cloud provider[4]. The cloud provider upon receiving decrypts using a private key. In PKE the public key and private key are generated by the a Trusted Third Party(TTP). TTP generates the public key to each user uniquely along with the corresponding private key, this is termed as assertion. This assertion which is given by the TTP is called certificate and the TTP is called Certificate Authority(CA)[4]. The generation of public keys to each user uniquely with corresponding private keys by CA is very difficult which involves many complexities. In order to certify the authenticity of public keys additional Public Key Infrastructure(PKI) is required which leads to difficult key management. There is large proportion of overhead involved in key management infrastructure settings as well. PKE becomes expensive to maintain if revocation infrastructure(infrastructure required for withdrawal of keys by users) of has to be incorporated in the system. And the sufficient hardware required for key management is also expensive. This drawback can be avoided using a sophisticated techniques like Homomorphic Encryption and Identity Based Encryption(IBE).

2) Identity Based Encryption (IBE): IBE is an alternative to PKE as it simplifies the public-key and certificate management at the Public Key Infrastructure(PKI)[12].In IBE, there are two types of keys involved. They are: Public key:- known to everyone and Private key:- known only to the data receiver. The public key should be unique for each user. The public key can be generated based on users unique identification strings such as email or IP addresses and the corresponding private keys are created automatically using a public key by trusted third party authority or Trusted Authority (TA)[4]. As such must overhead is reduced involved generating the public key to each user uniquely. The user will encrypt the data using public key and sends it to the CSP. The CSP upon receiving the encrypted message can decrypt it by using the private key provided by Trusted Authority (TA). IBE is more advantages than any other encryption algorithms due to the following motives.

- The sender can provide expiration date along with the encrypted data. So that the receiver need to decrypt the data before specified time period using private key. Hence more secure.
- Since the public key is generated using unique identification strings, thereby reducing the complexity in storing the public keys securely.

Drawbacks and possible solutions of Identity Based Encryption:

- Even though IBE has many advantages, this technique is unacceptable by many users and in many application scenarios like closed military, government etc. These organizations do not prefer IBE as they want secure communication between their employees. So they don't want TA to know their private key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

In order to overcome this drawback, Goyal in 2007 proposed a concept called Accountable Authority IBE where user obtains the private key using a secure key generating protocol, such that the TA has no knowledge of key obtained by the user[4].

- There is a problem when it comes to withdrawal of a particular user identity which results in overhead computation at the private key generator[6].

This can be overcome by introducing an entity called Key-Update Cloud Service Provider(KU-CSP) which does the operations related to key generation such as key issuing and key update processes. Thus reducing the overload on PKG leaving it to perform simple operations[6].

- Sometimes in IBE private keys maybe compromised which lead to access of data by unauthorized users.

In cases whenever private key of any user is compromised then that particular users identity must be cancelled from the system. The user need to regenerate their private keys periodically often in order not to compromise their private keys. The user must contact PKG periodically to prove their identities and update new private key. All the operations on PKG are carried out online and requires a secure network to maintain all transactions[6].

3)Homomorphic Encryption:

Homomorphic Encryption is the effective technique among all where the user can hide the original data even from the CSP (cloud service provider) by allowing the CSP to perform computations on the encrypted data. Even in case the server is hacked your original data is still safe and secure from hackers[11].

A) Problem statement: The users will encrypt the sensitive data and sends it to the cloud. The CSP will be provided with the secrete key for accessing the original data on cloud. Whenever the user wants to perform some manipulations on the data stored in cloud, he requests the CSP to perform the operation of his behalf. CSP usesthe secrete key decrypts the data and perform computations as requested by the user and returns the result. Ideally, at this stage the hacker might get a chance to hack the data in decrypted form. The above situation can be prevented by using Homomorphic encryption algorithm.

Homomorphic encryption is the technique where the operations such as addition or multiplication are carried on the encrypted data without the need for decryption for performing the computations on the data.

B) Algorithm

Homomorphic encryption algorithm has four functions:

1) Generation of public key(p) and secrete key(s):
Output: p, s.

The user generates a pair of keys a) Public key (p) - used by the cloud provider for processing encrypted data.
b) Secrete key(s)-used by the user for encrypting and decrypting the Original Data (OD).

2) Encryption: Input: OD(original data), s, p.
Output: Encrypted Data(ED).

The user will encrypt the Original Data (OD) using secrete key s and generates the Encrypted Data(ED). And then the user sends ED along with the public key p to the CSP.

3) Computation: Input: ED, p.
Output: Encrypted Result(ER).

The cloud provider uses public key p and performs computations on Encrypted Data(ED) as requested by the user and send the result of computation i.e. Encrypted Result(ER) to the user.

4) Decryption: Input: ER, s.
Output: Original Result (OR).

The user decrypts the Encrypted Results(ER) by using secrete key s and gets the Original Result(OR).

There are three types of Homomorphic Encryption

- *Partially Homomorphic Encryption(PHE)*- On the encrypted data either addition or multiplication can be performed at any instance of time. Simultaneously both addition and multiplication cannot be performed[8].
- *SomeWhat Homomorphic Encryption(SWHE)*- On the encrypted data both addition and multiplication can be performed simultaneously but offers only limited number of operations[5].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

- *Fully Homomorphic Encryption(FHE)*- On encrypted data any number of operations can be performed simultaneously and therefore it is fully flexible[5].

D) RSA and Homomorphic Encryption Algorithm

RSA is one of the first practical encryption algorithm used to encrypt the data before transmission[9]. It is asymmetric as it uses two different keys a public key and a private key. These two keys are used for encrypting and decrypting the data[10]. RSA is often called Public key encryption algorithm as the public key is known to everyone[9].
Homomorphic encryption can perform two operations on the data. They are:
Additive homomorphic encryption –
$Encr(X1 \oplus X2) = Encr(X1) \oplus Encr(X2)$
Multiplication homomorphic encryption –
$Encr(X1 \otimes X2) = Encr(P1) \otimes Encr(X2)$

i) RSA Algorithm as Multiplication Homomorphic Encryption:

The public key is generated by two large prime numbers by a user. This public key can the given to everyone. The prime number must be secret.
RSA Encryption Algorithm:

Start

Step 1) Choose two large primes number p and q.
Step 2) n=>p*q
Step 3) $\pi(n)$=>(p-1)(q-1)
Step 4) Select e where $1<e<\pi(n)$ and e,n are co-prime
Step 5) compute d=>$((d*e) \bmod \pi(n)) = 1$
Step 6) public key(e,n), private key (d,n)
Step 7) encryption of the plaintext P=> C=> P mod(n)
Step 8) decryption of cipher text(encrypted text) C=>P=> mod(n)
Step 9) RSA follows the homomorphic property by-
Step 10) Encr(X1)*Encr(X2)=Encr(X1*X2).

Finish

III. CONCLUSION AND FUTURE WORK

Cloud computing is becoming an attractive business standard in the current IT world. Advancement is expanding at rates never experienced and will keep on doing so.The up and coming era of cloud computing have to concentrate on developing new and efficient techniques to secure their data and abstracting encryption technologies and the functional procedures that are supportive in securing the data. Cloud computing is a new technology and still in initial stages. But as many people have gotten hands into it, it has evolved and changed[3]. More evolution is taking place in cloud computing in order to fulfil the user needs with maximum performance and efficiency with best possible encryption techniques. Many encryption techniques are evolving which are more robust in nature that ensures users security. Development of encryption techniques for optimal performance on relatively large data sets and efficient key management are taking place. Researchers are trying to implement different versions of encryption algorithms such as fully and partial Homomorphic algorithms[8].

REFERENCES

1. Barrie Sosinsky,‘ Cloud Computing Bible’, pp. 4-22, ed. 2011.
2. GurudattKulkarni, JayantGambhir, RajnikantPalwe, ‘Cloud Computing-Software as Service’, International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol. No.1, pp. 11-16, March 2012.
3. Nitin Kumar Upadhyay, Dr Ashok Bhansali, Manish Kumar Upadhyay, ‘Security Issues in Cloud Computing’, International Journal of Technical Research and Applications, Vol. No.2, pp. 143-148, 2014.
4. SriramkrishnanSrinivasan,’Identity Based Encryption:Progress and Challenges’, Elsevier- Information Security Technical Report, pp. 33-40, 2010.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

5. GarimaRastogi, Rama Sushil, 'Cloud computing Security and Homomorphic Encryption', The IUP Journal of Computer Science, Vol IX, No.3, pp-48-57, 2015.
6. Payal.V.Parmar, ShraddhaB,Padhar, ShafikaN.Patel, Nityateel. Bhatt and Rutvij H. Jhaveri, 'Survey of various Homomorphic Encryption algorithms and schemes', International Journal of Computer Science, Vol91, No.8, pp-26-30, April 2014.
7. MahaTebaa, Said el Hajji, Abdellatif el Ghazi, 'Homomorphic Encryption Applied to Cloud Computing Security', Proceedings of the World Congress on Engineering,VolNo.1, pp-536-539, 2012.
8. SanghpriyaR.Bangar, S.M.Bansode, 'Homomorphic Encryption:Security for Cloud Computing', International Journal of Innovative Research in Computer and Communication Engineering(IJIRCCE), Vol. 4, pp. 14217-14222, July 2016.
9. https://simple.wikipedia.org/wiki/RSA_(algorithm), 5Jan 2017.
10. https://en.wikipedia.org/wiki/RSA_(cryptosystem) , 22 Jan 2017.
11. Iram Ahmad, ArchanaKhandekar, 'Homomorphic Encryption Method Applied to Cloud computing', International Journal of Information and Computation Technology(IJICT), Vol No. 4, pp. 1519-1530, 2014.
12. Girish, Phaneendra H.D, ' Identity Based Cryptography and Comparison with traditional Public key Encryption: A Survey', International Journal of Computer Science and Information Technologies(IJCSIT), Vol No.5, pp. 5521-5525, 2014.