ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud

Rishav Chatterjee[1], Sharmistha Roy[2]
UG Scholar[1], Assistant Professor[2]
School of Computer Engineering
KIIT Bhubaneswar, India

Abstract:
Cloud computing is an Internet-based computing model which provides several resources through Cloud Service Providers (CSP) to Cloud Users (CU) on demand basis without buying the underlying infrastructure and follows pay-per-use basis. It supports virtualization of physical resources in order to improve efficiency and accomplishment of multiple tasks at the same time. Cloud Computing Environment (CCE) provides several deployment models to represent several categories of cloud owned by organization or institutes. However, CCE provide resources to Cloud Users through several services like PaaS, SaaS, IaaS. Cloud Computing is a notion based on the concept of summing up physical resources and displaying them as an unacknowledged resource. It is a model for producing resources, for sorting out applications, and for manifesto-independent user access to services. Cloud can come in different types, and the services and the applications that possibly run on clouds may or may not be provided by a cloud service provider. There are two unique group of models namely deployment models and service models. Service models consists of IaaS , SaaS, PaaS . The Deployment or deployment model consists of Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud .Cloud Computing has lots of distinct properties that make it very important. privacy seems to be an unique concern in cloud .Various types of service models under cloud computing facilitate various levels of privacy services. We will get the minimum security in IaaS (Infastructure as a Service) and most with a SaaS provider. In this paper, we will focus upon the reviewing and understanding cloud security issues by proposing crypto algorithms and effective measures so as to ensure the data security in cloud. Along with this, we will elucidate a bit more about some security aspects of cryptography by showcasing some privacy issues of current cloud computing surroundings.

Keywords: Cloud Computing, Cryptography, Security Issues Privacy, Security Algorithms, Encryption, Decryption.

1. Introduction

Cloud computing is one of the popular topics of the current world. Internet has started driving all these new technologies. Internet was designed firstly to be strong, but not completely safe. Distributed applications like these is much prone to attacks. Cloud Computing has all the feebleness associated with these internet utilization and the extra threats arise from the combined, Virtualized and redistributed resources. There are many data privacy concerns in cloud computing. Incorrect revelation of a data used in businesses in cloud to third parties is one of the major issues that has been found. **[4]**Encryption should be properly used and the crypto algorithms include AES, RSA, DES and 3 DES .In this paper, we describe about using crypto algorithms so as to increase security concern. Cloud Security can be ensured by data integrity, Secured data transfer and by Cryptography. There are varieties of cryptographic algorithms which can be implemented so as to ensure security in the cloud. The two types of algorithms are Symmetric and Asymmetric encryption key algorithms. Symmetric contains algorithms like DES, AES, 3 DES and Blowfish algorithm. Asymmetric contains algorithms like RSA, Diffie- Hellman Key Exchange. Symmetric key and asymmetric key algorithms is used to encrypt and decrypt the data in cloud.

2. Related Works

a. In the paper [1] the authors deal with the problem of security of data during data transmission. The main thing to fear about this paper is the encryption of data so that confidentiality and privacy can be easily achieved. The algorithm used here is Rijndael Encryption Algorithm along with EAP-CHAP.

b. This paper[2] presents a protocol or set of instructions that uses the services of a third party auditor or checker not only to verify and authenticate the integrity of data stored at remote servers but also in retrieving and getting the data back as soon as possible in intact form. The main advantage of this scheme is the use of digital signature to assure the integrity of local data. However, the overall process is quite problematic and complex as the keys and data are also encrypted and decrypted respectively

3. Cryptography: Security principles & Algorithms

Cryptography can help dawning integration of Cloud Computing by increased number of privacy related companies. The primary level of privacy where cryptography can help Cloud computing is safe and secure storage. Cryptography is the science of storing messages securely by converting the raw data into forms which is not readable **[7]**. In today's world,

cryptography is considered as a collection of three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms and Hashing [**6**]. In Cloud computing, the main problems are related to problem in data security, backup data, network traffic, file storage system, and security of host, and cryptography alone can solve these issues to extents. For a safe and secure communication between the guest domain and the host domain, or from hosts to management systems, encryption technologies, such as Secure HTTP, encrypted VPNs, TLS, Secure Shell, and so on should be used. Encryption will help us prevent such exploits like man-in-the-middle, spoofed attacks, and session hijacking. Cloud computing provides clients with a computing facilities or infrastructure on top of which they can store data and run applications. While the advantages of cloud computing are pretty clear, it introduces new security challenges as cloud operators are supposed to manipulate data for clients without necessarily being fully trusted. We will be trying to design cryptographic primitives and protocols which are tailored to the setting of cloud computing, attempting to strike a balance between security, efficiency and functionality. Cloud data storage enhances the risk of leakage of data and does not give access to unauthorized users. Cloud data management cannot be fully trusted by data owners. Cloud data process and computation could expose the privacy of users, owning the data or related entities to parities which does not have unauthorized access. For overcoming the above problems, cryptography has been widely applied to ensure data security, privacy and trust in cloud computing.

3.1 Symmetric key algorithms

Symmetric uses single key, which works for both encryption and decryption. The symmetric systems provide a two channel system to their users. It ensures authentication and authorization. Symmetric-key algorithms are those algorithms which uses only one and only key for both. The key is kept as secret. Symmetric algorithms have the advantage of not taking in too much of computation power and it works with very high speed in encryption. Symmetric-key algorithms are divided into two types: Block cipher and Stream cipher. In bock cipher input is taken as a block of plaintext of fixed size depending on the type of symmetric encryption algorithm, key of fixed size is applied on to block of plain text and then the output block of the same size as the block of plaintext is obtained. In Case of stream cipher one bit is encrypted at a particular time. Some popular Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES).

a) Advanced Encryption Standard (AES)

In cryptography, the Advanced Encryption Standard **[3]** is type of symmetric-key encryption algorithm . Each of the ciphers has a 128-bit block size and having key sizes of 128, 192 and 256 bits, respectively. AES algorithm assures that the hash code is encrypted in a secure manner. AES has a block size of 128 bits . Its algorithm is as follows: Key Expansion, Initial Round - Round Keys are added. Rounds, Sub Bytes—a non-uniform substitution step where each byte is substituted with another according to a table. Rows are shifted—a transposition step where each row of the state is shifted cyclically a certain number of steps. Columns are mixed—a mixing operation which operates on the columns of the state, combining the four bytes in each column 8. Add Round Key—each byte of that particular state is combined with the round key; each round key is derived from the given cipher key using a key schedule. Final Round, Sub Bytes, Shift Rows, Add Round Key. The DES algorithm was finally broken in 1998 using a system that costs about $250,000.Triple DES turned out to be too slow for efficiency as the DES algorithm was developed for mid-1970's hardware and did not produce efficient and effective software code. Triple DES has three times as many rounds as DES and is correspondingly slower

b) Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a block cipher and comes under symmetric key cryptography. found in January 1977 by the National Institute of Standards and Technology, named as NIST. At the encryption site, DES simply takes a 64-bit plaintext and creates a 64-bit cipher text, at the decryption process, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made using two permutations (P-boxes), which we call initial and final permutation, and sixteen Fiestel rounds. Each round uses a different sort of 48-bit round key which is generated from the cipher key according to a predefined algorithm.

c) Blowfish Algorithm

Blowfish also comes under symmetric block cipher that can be used as a substitute for DES. It takes a variable-length key, starting from from 32 bits to 448 bits, making it considerably better for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a free, fast substiute to existing encryption algorithms. Since then it has been verified considerably, and it is gradually gaining popularity as a strong encryption algorithm. Blowfish is unpatented and license-free, and is available free for all uses.

3.2 Asymmetric Key Algorithms

It is relatively a new concept unlike symmetric cryptosystem. Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme. Each receiver possesses a decryption key of its own, generally referred to as his private key. Receiver needs to generate an encryption key, referred to as his public key. Generally, this type of cryptosystem involves trusted third party which officially declares that a particular public key belongs to a specific person or entity only.

a) RSA Cryptosystem

This cryptosystem is one the initial systems and oldest of asymmetric cryptosystem. It remains most employed and used cryptosystem even now. The system was invented by three scholars named Ron Rivest, Adi Shamir, and Len

Adleman and hence, it is termed as RSA cryptosystem. This algorithm is used for public-key cryptography and not private key crptofra. It is the first and still most commonly used asymmetric algorithm. It involves two keys namely a public key and a private key. The public key is used for encrypting messages and is known to everyone. Messages encrypted with the use of public key can be decrypted only by using the private key. In this verification process, the server implements public key authentication by signing a unique message with its private key, which is called as digital signature. The signature is then returned to the client. Then it verifies using the server's known public key.

b) Diffie-Hellman Key Exchange

Whitfield Diffie and Martin Hellman introduced a key exchange protocol with the help of the discrete logarithm problem in 1976. In this key exchange protocol sender and receiver will manage to set up a secret key to their symmetric key system, using an unsafe channel. To set up a key Alice chooses a random integer aE[1; n] computes ga, similarly Bob computes gb for random bE[1; n] and sends it to Alice. The secret key is gab, which Alice computes by computing (gb)a and Bob by computing (ga)b. The important concepts on which the security of the Diffie-Hellman Protocols defend upon DDH, DHP, DLP like etc

3.3 Hashing Algorithms

a) MD5- (Message-Digest algorithm 5)

A widely used hash function algorithm in cryptography with a 128-bit hash value and possesses a variable length message into a fixed-length output of 128 bits. First the input message is divides up into lump of 512- bit blocks then the message is padded so that its total length is divisible by 512. The sender of the data uses the public key to encrypt the message and the receiver uses its private key to decrypt the message.

4. Security Problems Faced By Cloud Computing

When it comes to privacy and security, cloud is greatly affected by the threat of that. The people such as the vendors must make sure that the people using cloud does not face any problem such as data loss or theft of data. There is a chance where a malicious user or hacker can get into the cloud by impersonating a legitimate user, there by affecting the entire cloud thus affecting many people who are using the infected or affected cloud. Some of the problem which is faced by the Cloud computing are:

i. Data theft
ii. Integrity of data
iii. Privacy problems
iv. Loss of data
v. Infected Applications
vi. Exact location of data
vii. Vendor level Security
viii. User level Security

The current generation of cloud computing facilities does not provide any privacy against untrusted cloud operators and hence they are not supposed to store important information such as medical records, financial records or high impact business data. To address this we are pursuing various research projects that range from theory to practice. The main use of encryption is to provide privacy through abstraction of all useful information about the plaintext. Encryption modifies data useless in the sense that one does not get to access it. We will be making algorithms for cryptosystems that will help to perform a variety of computations on encrypted raw data, starting from normal purpose of computation to the special purpose computations in order to eradicate this problem. Research on homomorphic cryptography includes work on fully-homomorphic encryption, searchable encryption, structured encryption, functional encryption.

a. **Proofs of storage.** A client can verify whether the cloud operator has tampered with its data using proof of storage. Particularly, this is done without the client storing a copy of the data and without it having to store back any of the data. In fact, the work for the client is negligible no matter how large the data is.
b. **Secure Storage system.** We are trying to design cloud storage systems that provide privacy, security, integrity of client data against an malicious cloud provider. Systems will provide privacy without any loss of efficiency and better functioning will have to be taken care of by making use of new cryptographic encryption techniques like homomorphic encryption, searchable encryption, verifiable computation and proofs of storage and many others.

5. Conclusion and Future Scope

Cloud computing is growing as a new thing and it is the new trend indeed and many of the organizations and big companies are moving toward the cloud but lagging behind because of some security problems. Cloud security is an ultimate concept which will crush the drawbacks the acceptance of the cloud by the big MNCs, companies and organizations. There are a lot of security algorithms which may be implemented to the cloud. DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithms. DES and AES are mostly used symmetric algorithms as they are relatively more secure. DES is quite simple to implement than AES. RSA and Diffie-Hellman Key Exchange is the asymmetric algorithm. RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms in cloud. But the security algorithms which allow linear searching on decrypted data are required for cloud computing, which will take care about the safety of the data.

There is a large scope of improvement in this field of research. **[5]**We can use cryptography in numerous places in order security in cloud. For example, Cryptography can be used for maintaining cloud data access control, cloud data trust management, verifiable computing, cloud data authorization and authentication and secure data storage. Apart from all these, Lattice based Cryptography and ID based Cryptography are the two important sectors which is ensuring cloud data security in present world. Still there is a lot of research to be done in this field.

6. References

1. Sanjoli Singla, Jasmeet Singh ,"Cloud computing security using encryption technique**",** IJARCET, vol.2, ISSUE 7.

2. R. Bala Chandar, M. S. Kavitha , K. Seenivasan," A proficient model for high end security in cloud computing", International Journal of Emerging Research in Management &Technology, Vol.5, Issue 10.

3. Bokefode Jayant.D, Ubale Swapnaja A, Pingale Subhash V., Karane Kailash J. , Apate Sulabha S. ,"Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role bases Access Control Model", International Journal of Computer Applications, Volume 118-No.12, May2015

4. Karun Handa, Uma Singh," Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing", Vol.4 Issue.5, May-2015, pg.786-791

5. M.Vijayapriya,"security algorithm in cloud computing: overview", International Journal of Computer Science & Engineering Technology (IJCSET), Vol.4, ISSN: 2229-3345.

6. Rashmi Nigoti, Manoj Jhuria, Dr. Shailendra Singh, "A survey of Cryptographic algorithms for cloud computing", International Journal of Emerging Technologies in Computational and Applied Sciences, March 2013, ISSN (online)-2279-0055.

7. Douglas R. Stinson," Cryptography: Theory& Practice", Chapman and Hall Publications.