



Cloud Computing: A step towards CryptoCloud

Er. Sharanjit Singh, Er. Rasneet Kaur Chauhan

Department of CSE

Guru Nanak Dev University RC Gurdaspur, Punjab, INDIA

Abstract: Cloud Computing has become one of the most talked about technologies in the recent times and has thus got a lot of attention from media, organizations, and analysts because of a large number of opportunities it is offering to all. Other ways would be the security services such as computing hash of data and hence integrity of data is verified, encryption and decryption service as provided by the same cloud storage provider, hence the data compromise could not be ruled out because same provider has access to both the security services as well as storage. Divide and rule technique can also be one of the techniques which means dividing the various responsibilities amongst different cloud services providers could benefit the clients too. A trusted third party cloud provider can be used to provide security services, or cloud provider can be data storage provider. A trusted 3rd party security service provider does not store data at its side, and hence confined to provide the security service. The application or software will provide data integrity verification by using hashing algorithm, provide encryption and decryption with the help of symmetric and asymmetric algorithms, and also a group of people who can have access to the shared data securely can be achieved by defining an access list.

Keywords: Cloud Computing; Security; Service Models; Cryptography.

I. INTRODUCTION

Cloud Computing is the name given to the recent trend in computing service provision. This trend has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely and en masse, by third-party service providers. Cloud Computing is a used to describe both type of application and platform. As a platform it supplies, configures and reconfigures servers and some resources. These servers can be some physical machines or some kind of virtual machines. On the other side, Cloud Computing also describes some applications that can be extended to be accessible through internet and thus for this purpose, powerful servers and data centers are used to host the web services and web applications.

The cloud is a metaphor for the Internet. It is also an abstraction for the complex infrastructure it conceals. There are some points in the definition that needs to be discussed regarding Cloud Computing. Cloud Computing is different from traditional computing paradigms because it is scalable, can be easily encapsulated as an abstract entity and thus provides different level of services to clients, might be related to economies of scale or other services that can be dynamically configurable.

Various definitions and interpretations of “cloud computing” and / or “clouds” exist. With respect to the various aspects and usage scopes the term is employed to, a *representative* (as opposed to complete) set of definitions as taking into consideration towards future usage in the cloud computing related research space. This definition does not claim to be complete with this respect, but tries to capture the maximum and gives an abstract term in a way that best represents the technological aspects and issues related to it.

In its broadest form, we can define

a 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service).

In other words, clouds as we understand them are primarily platforms that allow execution of various applications in various forms across multiple resources on various servers. The main characteristics are also discussed. Several different *types* of cloud have been discussed, all of which directly or indirectly have in common that they can enhance resources and various services with additional capabilities related to manageability, elasticity, and the system platform independency.

II. CRYPTOGRAPHIC ALGORITHMS

To protect the data on the storage of cloud can use methods to access the control for encrypting the data. The access control consists of both authorization and authentication. Some service providers also make use of a weak authentication mechanism and hence the authorization control is not very granular and in most cases the access control does not even give much protection. With the help of the mechanisms, data which is plain text can be very vulnerable to many types of attacks. These mechanisms are thus applied to data and hence give the best solution for the data protection.

This means that the customer must also encrypt data locally as well before uploading it to the cloud. The

indexing and also the searching of the data would not be done and hence neither the processing. To search the data the user must thus download all data locally as well, then decrypt and hence do the searching of the cloud would decrypt data before searching it but it must also have the decryption key which is not suitable. The major issue for adopting the cloud is security. The data stored in the cloud get increased day by day and thus we need some kind of mechanisms to make sure that the data is stored in a secured manner without any illegal unauthorized access to data. Thus security of the data stored in cloud is an important issue. Also providing integrity to data that is distributed over cloud has also been a challenging one. The main solution to deal with this type of difficult situation is make use of the cryptographic methods in cloud. Thus, we will describe several different cryptographic techniques that are used to protect the data that is used in the cloud and thus prevent data and information from being leaked and also to ensure that the privacy has been maintained. These cryptographic methods are used to provide the security for the Confidentiality as its main characteristics.

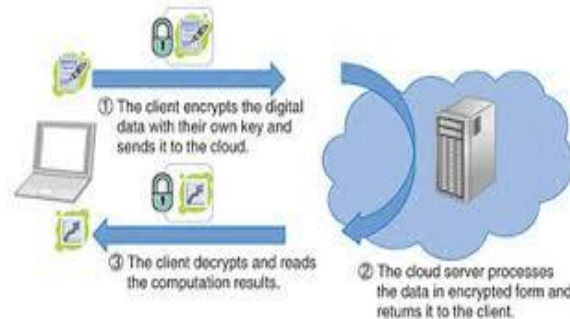


Fig. 1. Cryptography

III. CRYPTOGRAPHY GOALS

Here we explain the main five goals that are behind the use of Cryptography. Every security system should provide numerous security functions that makes sure the secrecy of the system. These functions are mostly referred to as the goals of a security system. These goals are divided into following five main categories:

- **Authentication:** it means that before sending data or receiving it using the system, the receiver and sender identity must be verified.
- **Secrecy or Confidentiality:** mostly this function or feature is on how most of the people identify some secure system. This also means that only the authorized and only authenticated people must be able to interpret the message content and no one else.
- **Integrity:** this means that the content of the data transmitted must assured to be free from all types of modification between the end points i.e. the sender side and receiver side. The basic form of this integrity is called the packet check sum in IPv4 packets.
- **Non-Repudiation:** it implies that the sender and the receiver both cannot falsely deny that they have sent a specific message.
- **Service Reliability and Availability:** as secure systems mostly get attacked by intruders, that might affect its availability and the type of the service to users. Such systems also provide some way to grant their users some quality of service that they expect.

IV. MODE OF OPERATIONS

The most common modes of operations in Block Cipher encryption-ECB and CBC.

There are many types of block cipher, where different techniques are used to secure and strengthen the security of the system. The most commonly used methods are: ECB i.e. Electronic Codebook Mode, CBC also called as Chain Block Chaining Mode, and OFB also called as Output Feedback Mode. ECB mode is a type of CBC mode that uses the cipher block from the last step of the encryption in the current one and forms a chain like encryption process. OFB also operates on plain text in similar way to the stream cipher, where the encryption key is used in every step that depends on the encryption key from the last step.

There are several other modes such as CTR (counter), CFB (Cipher Feedback), and 3DES specific modes also.

V. ENCRYPTION TECHNIQUES

• Symmetric Encryption

The symmetric cryptography techniques hence use the same key or single key for both the encryption and the decryption of data. Due to the single key encryption and decryption is fast but the security risks are more here. Thus there is less resource and also less time consumption but the integrity lost problem as the key can be easily guessed by the attackers. Due to the same key these are not much secure. The different Symmetric key algorithms include DES, Blowfish, RC4, AES, and RC5. The concern behind this type of encryption is that how to share the secret key securely between the peers. If key gets known to some attackers any reason, the whole system could also collapse. Thus the key management for this type of encryption can be very troublesome, if

there is only unique secret key that might be used for each connection, thus the total number of the secret keys to be managed and saved for n -nodes will be $n(n-1)/2$.

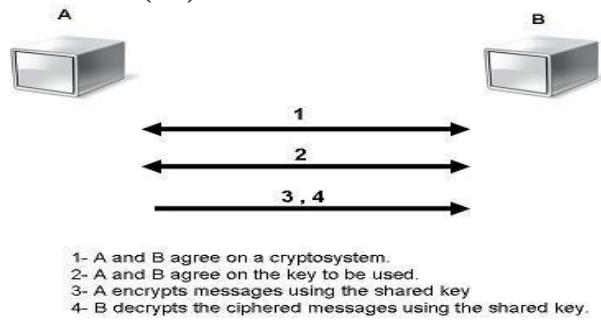


Fig. 2. Symmetric Encryption

- **Asymmetric Encryption**

Asymmetric encryption is another type of encryption where two keys are used. In this technique two keys are used, the one is private key that is kept secret and not shared and the other is a public key that is shared. The private key is used for only decryption and the public key is used for the encryption process. This capability hence creates the symmetric encryption problem of managing the secret keys. But on the other hand, this unique feature of the public key encryption also makes it more prone to attacks. However, asymmetric encryption techniques are almost 1000 times slower than the symmetric techniques, as they require more computational processing power. The various asymmetric key algorithms are: RSA, DSA, Elliptic curve, Diffie Hellman's key exchange,

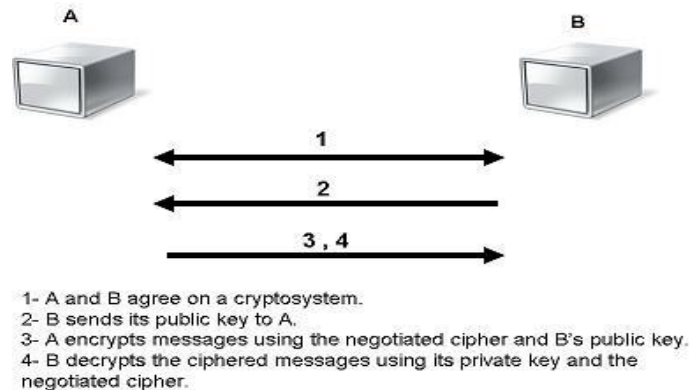


Fig. 3 Asymmetric Encryption

- **Hash Function Cryptography**

The hash function cryptography or One way cryptography offers a different way of creating some fixed-size blocks of data by making use of entry data with a variable length. It is also called as taking of digital fingerprint of the data, and exit data are called as the message digest or a one-way encryption. If the data is modified after a hash function was generated, then the second value of the hash function of data will not be same. Even a slightest alteration in the data like addition of a comma to a text, will thus create a huge difference between the hash values. The hash values resolve the problem of integrity of the messages. The mostly used hash function cryptography techniques are SHA1 and MD5.

VI. CRYPTOGRAPHIC ALGORITHMS

- **Data Encryption Standard (DES)**

This encryption process is thus made of two permutations i.e. P-boxes, which are also called as initial and final permutation, and the sixteen Feistel rounds. It thus makes use of block cipher. Same key and algorithm are used for the encryption and the decryption. Key is mostly 56 bits long. The position of 8, 16, 24, 32, 40, 48, 56 and 64 are discarded.

DES is based upon two different fundamental attributes of cryptography i.e. Diffusion (Substitution) and the Confusion (Permutation) that consist of 16 rounds. In each of the round key and data bits are shifted, then permuted, hence XORed and finally sent through a 8 s-box.

- **Advanced Encryption Standard (AES)**

Advanced Encryption Standard is a symmetric key block cipher technique. This is a non-Feistel cipher. It encrypts the data with a block size of 128-bits. It encrypts the data with a 128-bits block size. It thus makes use

of 10 and 12, or fourteen rounds. Hence depending on number of rounds, the key size could be 128, 192, or 256 bits as shown in figure. It operates on 4×4 column major order matrix of bytes also known as the state.

- **Triple-DES**

In this, triple iteration of DES encryption on each and every block is done. In 3-DES the triple iteration is done to increase the encryption level and also average time. Common method of 3-DES is the Minus Encrypt-Decrypt-Encrypt (-EDE). Each iteration in 3DES that uses – EDE will thus encrypt a block by using a 56-bit key. After the encryption, it uses a different 56-bit key to decrypt that block. On the last pass, again a 56-bit key is used for encrypting the data again. This is also equivalent to using a 168-bit encryption key method which is also called as Minus Encryption- Encryption – Encryption (-EEE). All the three keys can be different or identical or the first and the third key can be same.

- **RSA**

In this algorithm, a sender signs the messages with its own private key, a receiver in return verifies the signed message with that of sender's public key. This is how authentication service is guaranteed by a RSA-based signature algorithm. In business sectors secure and an efficient data transfer is very important and essential.

- **Blowfish**

It has a 16-round Feistel cipher and makes use of a large key-dependent S-boxes. Its structure resembles the CAST-128, which makes use of fixed S-boxes. Each line thus represents 32 bits. The algorithm thus keeps two sub key arrays i.e. a 18-entry P-array and four 256-entry S-boxes. The S-boxes thus accepts 8-bit input and hence produce 32-bit output. One entry of a P-array uses every round, and then after the final round, and each half of a data block is XOR-ed with any one remaining unused P-entry.

VII. PERFORMANCE ANALYSISPARAMETERS

The data will be encrypted using the cryptographic algorithms such as, AES, DES, RSA, Blowfish and 3-DES. By using these algorithms, the speed-up ratio and the mean processing time for different inputs is calculated.

Speed-Up ratio is defined as the difference between the mean processing time of a single system and the cloud network. Speed-up ratio tells us how fast the data have been encrypted. It gives an idea about the speed of encryption.

Mean processing time is defined as the difference between the starting time that is taken to encrypt the data and its ending time. It is also evaluated on both the single system and on the cloud network. It is difference between time that is taken to encrypt the data. As the size of input increases, the time taken to encrypt the data will increase and hence with the increase in time the speed-up ratio decreases.

Input	AES	AES CLOUD	DES	DES CLOUD	BLOW FISH	BLOW FISH CLOUD	RSA	RSA CLOUD	3-DES	3-DES CLOUD
11	11	1.	7.9	2.4	4.8	2.4	241	275	107	62.6
Kb	.6	6						.25		
15	14	2.2	12	2.9	4.9	2.4	328	332	256.	79.
Kb	.9						.95	.5	67	67
36	20	3.5	31.	6.4	8.7	2.9	359	354	290.	87.
Kb			3		5	5	.5	.7	8	6
58	25	3.	50.	9.5	15.	3.3	498	417	319.	100.5
kb	.5	95	85	5	9		.25	.25	45	

Mean processing time is calculated in ms i.e. milliseconds.

Table 1. Comparison of the Mean processing time of algorithms on the local system and on cloud network

INPUT	AES	DES	BLOWFISH	RSA	3DES
11 KB	7.9	3.89	2.3	0.96	1.9
15 KB	7.6	4.2	2.6	1.01	2
36 KB	7	4.98	3.4	1.07	2.2
58 KB	6.8	5.88	5.85	1.23	2.5

Table 2: Comparison of speed-up ratio of the algorithms for different inputs.

Among all these algorithms RSA, an asymmetric encryption algorithm is the average most time consuming AES which is a symmetric encryption algorithm, the speed-up ratio falls sharply with an increase in the input size. AES algorithm also has the highest speed-up ratio and then comes DES. Speed up ratio of DES, RSA and BLOWFISH remains almost constant. There is a very slight change in the speed-up ratio for DES, RSA and BLOWFISH. Thus, AES is the fastest symmetric technique since it has the scalability based on different hardware, as well as it can be implemented very easily and simply. After then, the symmetric techniques can be ordered as DES, 3-DES and finally the Blowfish.

VIII. CONCLUSION

Because of the magnitude of both benefits and risks it brings, cloud computing continues to be one of the most actively discussed, criticized and researched technologies in IT. Both the current and the prospective cloud users are very well aware of the existing risks and threats, still the majority of them believe that cloud computing is reasonably secure for both the mission-critical and non-critical application deployments. Due to the nature of the technology and architecture it is based on, cloud computing do requires some preventative measures and a broader security perimeter compared to the traditional and on-premise application and data hosting. Moreover cloud computing, if properly planned and deployed, will also bring positive functional, economic, and for some organizations some additional security benefits too. The aim of this paper is to clearly identify various current security risks of cloud computing, and to measure how these risks can be handled by various cloud security models and with the help of cryptography resulting in cryptocloud that affects its adoption decision.

REFERENCES

- [1] OoiBeng Chin, —Cloud Data Management Systems: Opportunities and Challengesl, 2009 Fifth International Conference on Semantics, Knowledge and Grid @2009 IEEE
- [2] RAN Shuanglin, —Data Security Policy In The Cloud Computingl, Digital Media Department of Communication
- [3] School, Guizhou University for Nationalities, Guiyang, China, The 7th International Conference on Computer Science & Education (ICCSE 2012) July 14-17, 2012. Melbourne, Australia, @ 2012 IEEE
- [4] Uma Somani, Kanika Lakhani, Manish Mundra,—Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computingl, 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010), @2010 IEEE
- [5] Zhang Xin, Lai Song-qing, Liu Nai-wen , —Research onCloud Computing Data Security Model Based on Multi-dimensionl , International Symposium On Information Technology In Medicine And Education, @2012 IEEE
- [6] Xing Zhou, Xiaofei Tang 2011, Research and Implementation of RSA Algorithm for Encryption and Decryption, Department of Computer Science andTechnology Harbin, china.
- [7] Jansen, Wayne &Grance, Timothy. *Guidelines on Security and Privacy in Public Cloud Computing*. National Institute of Standards and Technology, 2011.
- [8] M.Shand and J.Vuillemin, “Fast Implementation of RSA Cryptography”, Pro c.1 1th IEEE Symp. Computer Arithmetic, E.E.Swartzlander, M.J.
- [9] Liu, P. You, Y. Peng, “Security Issues and Solutions in Cloud Computing”, IEEE-computer society, 2012.
- [10] R. Padhy, M. Patra and S. Satapathy, “Cloud Computing: Security Issues and Research Challenges”, IJCSITS, Vol. 1, No. 2, December 2011.
- [11] M.Walloschek, B.Grobauer, E.Stöcker,“Understanding of Cloud Computing Vulnerabilities”, IEEE Computer and Reliability Society, 2011.