SURVEY ON EFFICIENCY OF ENCRYPTION ALGORITHMS FOR CLOUD DATA SECURITY

Ms. Jalashree D. Trivedi[1], Prof. Amita V. Shah[2]

[1] *Student ,Computer Engineering Department, L.D College of Engineering,Ahmedabad, Gujarat, India*
[2] *Professor, Computer Engineering Department, L.D College of Engineering,Ahmedabad, Gujarat, India*

ABSTRACT

Cloud computing is technology where the clients" can use high end services in form of software that reside on different servers and access data from all over the world. With a promising technology like this, it certainly abandons clients" privacy, management of data and services, putting new security threats towards the assurance of data in cloud. However, there are some security concerns when clients handle and share data in the cloud-computing environment. The security threats such as maintenance of data integrity, data hiding and data safety dominate clients concerns when the issues of cloud security come up. The big data and time-consuming encryption calculations related to applying any encryption method have proved as a hindrance in this field. Cryptography is knowledge of protecting the information for providing encryption techniques. In this paper we survey different security issues to cloud and different cryptographic algorithms adoptable to provide better security for the cloud.

Keywords : - *cloud computing,cryptographic algorithms, security issues*

1. Introduction

Cloud computing is the emerging field in the modern era. Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. It conveys everything as a service over the internet based on user demand, for instance operating system, network hardware, storage, resources, and software. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed Encryption. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms.

Fig-1: Cloud Computing

2. Security Issues in The Cloud

The security requirements of a cloud and non-cloud data center are fairly similar. The Cloud Security Alliance's initial report contains a different sort of taxonomy based on different security domains and processes that need to be followed in general cloud deployment. Some privacy and security-related issues that are believed to have long-term significance for cloud computing are:

A. Governance Governance implies management and oversight by the organization over procedures, standards and policies for application development and data technology service acquirement, also because the style, implementation, testing, use, and watching of deployed or engaged services.

B. Compliance

Compliance refers to an association's responsibility to work in agreement with established laws, specifications and standards. One with all the foremost common compliance problems facing a company is an information location means storage of data or information.

C. Malicious Insiders

This threat is well known to most organizations. 'Malicious insiders' impact on the organization is considerable. Malicious insiders are the threat which has access to the data or information about the organization being a member of the organization. As cloud consumers application data is stored on cloud storage provided by cloud provider which also has the access to that data.

D. Account or service Hijacking

This threat occurs due to phishing, fraud and software vulnerabilities. In this type attacker can get access to critical areas onto the cloud from where he can take permit and steeling important information leading to compromise of the availability, integrity, and also confidentiality to the services.

E. Hypervisor vulnerabilities

The Hypervisor is the main software component of Virtualization. There known security vulnerabilities for hypervisors and solutions are still limited and often proprietary [4].

F. Insecure APIs

Anonymous access, reusable tokens or password, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring, and logging capabilities etc security threats may occur to organizations if the weak set of interfaces and APIs are used.

Table – 1: Data Security Threats

Problems	Public Cloud	Private Cloud
Data leakage	✓	✓
Unknown data physical location	✓	
Lack of guarantee of total data destruction	✓	
Insecure Applications	✓	
Account or service hijacking	✓	✓
Inability to access data	✓	✓
Data lock-in	✓	
Malicious insiders	✓	✓
Common shared infrastructure	✓	
Data loss/Leakage	✓	✓
Sniffer attacks	✓	✓

3. Literature Survey

Our aim is device an efficient encryption scheme over data sharing in cloud computing so here we discuss most of the related work in this field.

Hongwei Li, Dongxiao Liu, Yuanshun Dai,Tom H. Luan and Xuemin(Sherman) Shen [3] This paper propose a multi-keyword ranked search scheme to enable accurate, efficient and secure search over encrypted mobile cloud data. Security analysis have demonstrated that this scheme can effectively achieve confidentiality of documents and index, trapdoor privacy, trapdoor unlinkability, and concealing access pattern of the search user. Extensive performance evaluation has shown that this scheme can achieve better efficiency in terms of the functionality and computation overhead. Still authentication and access control issues need to be investigated.

Mathew Green, Susan Hohenberger and Brent Waters [11] This paper is about outsourcing the decryption of ABE Ciphertexts, a new paradigm for ABE that largely eliminates the overhead of complexity of access formula for users. If ABE ciphertexts are stored in the cloud, this paper shows how a user can provide the cloud with a single transformation key that allows the cloud to translate any ABE ciphertexts satisfied by the user attribute into a (constant size) EI Gamal-style ciphertext, without the cloud being able to read any part of the users message. Moreover this approach has a minimal impact on performance.

YerraguntaHarshada, K.Janardhan [12] presents a ranking based share authority privacy preserving authentication protocol, in this protocol a ranking at the admin level assign to file on the basis of how frequently that file accessed. In this access control mechanism incognito access request matching is provided without disclosing user's information. User can access their data by the feature based access control process. Universal composability model is used to provide security for the data when different protocols are used during the process. A ranking is assign at the admin level to mention that how many time that file accessed. User can see that in their dashboard. That enhances the security of the system and provides knowledge about the vulnerability of the file.

Jianyongchen, Yang Wang [10] presents an on-demand security architecture for cloud computing. In this architecture three layers are there one is input layer, second is policy layer, and third layer is security mechanism layer. In input layer three checks is performed first is security level, in this only authorized user can be allowed to access the service unauthorized user doesn't have permission to access data. Second is type of service, in this, what type of service user want to access is checked because different type of service needs different security. Access network risk, in this the risk when service passes through the server is checked. Security policy in this layer data is checked and security parameters are implemented on the basis of security level,. Third layer is security mechanism layer, in this each domain provides different security mechanism, like encryption/decryption in storage domain, IP security in the network domain, honey pot in service do.

S Sankareswari, S Hemanth [9] presents an access control mechanism for shared data over cloud. This technique a decentralize access control mechanism is used, in that there are several no of key distribution centers KDCs to share key among the user. In existing technique a centralized key distribution mechanism is used, which sometimes leads to the problem of single point failure. To prevent replay attacks which used to performed to get access for the user's data. In this if a user once restricted by the protocol then he cannot back stale their information. Identity of the user is also not disclosed to the cloud server during the whole process. In this a SHA based encryption is used to hide the information of the user. In this information of the user not disclosed to the cloud server but cloud server knows the access mechanism for each data that stored in the cloud server.

Neelam S. Khan, Dr. C. Rama Krishna and Anu Khurana [14] In this paper an attempt was made to improve the data discovery and user searching experience by supporting secure ranked fuzzy multi-keyword search. In RFMS the time to generate the index at the DO reduced to a great extent. Also the overhead of generating the trapdoor for each query sent by Du is eliminated on DO. The DU directly queries the cloud server C. In future this searching scheme can be made more efficient by reducing the searching time as much as possible. An efficient ranking algorithm can also be made that will rank files first on the basis of multi-keyword match and then for the files with same rank it will calculate relevance score on the basis of frequency of each keyword in the file.

Chang Liu, Chi Yang, Xuyun Zhang and Jinjun Chen [15] In this paper a novel authenticated key exchange scheme namely Cloud Computing Background key Exchange (CCBKE), which aimed at efficient security-aware scheduling of scientific applications in hybrid computing environments such as cloud computing. This scheme has been designed based on commonly used Internet Key Exchange (IKE) scheme and randomness reuse strategy. In future, further investigation on new strategies to improve the efficiency of symmetric key encryption can be carry out.

4. CRYPTOGRAPHY

Cryptography can help emergent acceptance of Cloud Computing by more security concerned companies. The first level of security where cryptography can help Cloud computing is secure storage. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms. Now a day's cryptography is considered as a combination of three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, and Hashing. In Cloud computing, the main problems are related to data security, backups, network traffic, file system, and security of host [2], and cryptography can resolve these issues to some extents. Consider an example, In the cloud consumer can protect its confidential data, then he has to encrypt his information before storing in the cloud storage, and it is advised not to save an encryption key on the same server where you have stored your encrypted data. This will helps us in reduction of Virtualization vulnerability. For secure communication between the host domain and the guest domain, or from hosts to management systems, encryption technologies, such as Secure HTTP (HTTPS), encrypted Virtual Private Networks (VPNs), Transport Layer Security (TLS), Secure Shell (SSH), and so on should be used. Encryption will help prevent such exploits as man-in-the-middle (MITM), spoofed attacks, and session hijacking [5].

A. Symmetric-key algorithms

The most important type of the encryption is the symmetric key encryption. Symmetric-key algorithms are those algorithms which use the same key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption [1]. Symmetric-key algorithms are divided into two types: Block cipher and Stream cipher. In block cipher input is taken as a block of plaintext of fixed size depending on the type of a 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 at a time is encrypted. Some popular Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES).

1. Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit ciphertext, at the decryption site, it takes a 64-bit ciphertext and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm as shown in figure 1. The function f is made up of four sections:

- Expansion P-box
- A whitener (that adds key)
- A group of S-boxes
- A straight P-box.

2. Advanced Encryption Standard (AES)

Advanced Encryption Standard is a symmetric- key block cipher published as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). AES is a non-Feistel cipher. AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits as shown in figure 3. AES operates on a 4×4 column-major order matrix of bytes, known as the state.

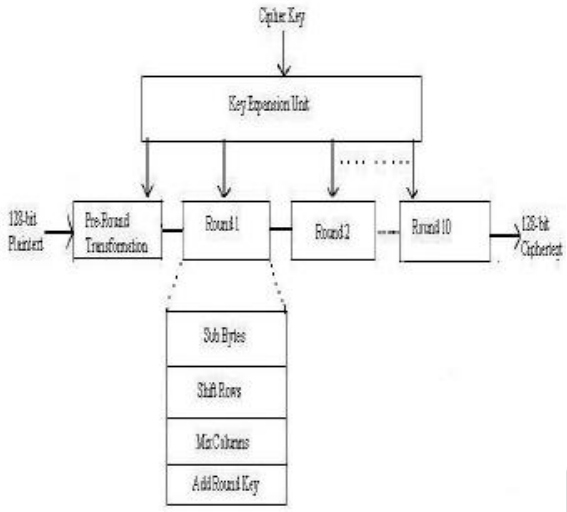

Fig-2 : Encryption with AES

3.Triple-DES

A quite simple way of increasing, the key size of DES is to use Triple DES, to guard it against attacks without the need to design a completely new block cipher algorithm. DES itself can be adapted and reused in a more secure scheme. Many former DES users can use Triple DES (TDES) which was described and analyzed by one of DES's patentees. It involves applying DES three times with two (2TDES) or three (3TDES) different keys as shown in figure 3. TDES is quite slow but regarded as adequately secure.

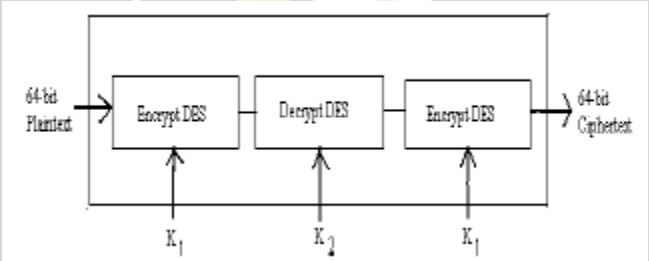

Fig-3 : Encryption with Triple-DES

4.Blowfish Algorithm

Blowfish is a symmetric block cipher algorithm. It uses the same secret key to both encryption and decryption of messages. The block size for Blowfish is 64 bits; messages that aren't a multiple of 64-bits in size have to be padded. It uses a variable –length key, from 32 bits to 448 bits. It is appropriate for applications where the key is not changed frequently. It is considerably faster than most encryption algorithms when executed in 32-bit microprocessors with huge data caches.

B. Asymmetric-key algorithms

Asymmetric-key algorithms are those algorithms that use different keys for encryption and decryption. The two keys are: Private Key and Public Key. The Public key is used by the sender for encryption and the private key is used for decryption of data by the receiver. In cloud computing asymmetric-key algorithms are used to generate keys for encryption. The most common asymmetric-key algorithms for cloud are: RSA, IKE, Diffie-Helman Key Exchange.

1. Homomorphic Encryption

Cloud consumer encrypts its data before sending to the Cloud provider, But, each time he has to work on that will have to decrypt that data. The consumer will require giving the private key to the server to decrypt the data before to perform the calculations required, which might influence the confidentiality of data stored in the Cloud.
Homomorphic Encryption systems are needed to perform operations on encrypted data without decryption (without

knowing the private key); only the consumer will have the secret key. When we decrypt the result of any operation, it is the same as if we had performed the calculation on the plaintext (or original data). The Homomorphic encryption is distinguishing, according to the operations that are performed on raw data [13].

- Additive Homomorphic encryption: additions of the raw data.
- Multiplicative Homomorphic encryption: products for raw data.

2. *RSA*

RSA cryptosystem realize the properties of the multiplicative Homomorphic encryption [13]. Ronald Rivest, Adi Shamir and Leonard Adleman have invented the RSA algorithm and named after its inventors. RSA uses modular exponential for encryption and decryption. RSA uses two exponents, a and b, where a is public and b is private. Let the plaintext is P and C is ciphertext, then at encryption ,C = Pa mod n

And at decryption side ,P = Cb mod n.

n is a very large number, created during key generation process. The process is shown in figure 4.

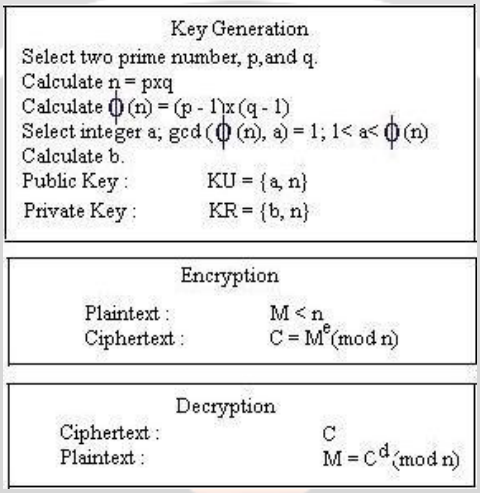

Fig-4 : RSA Algorithm[8]

3. ECC

Elliptic Curve cryptography (ECC) is a cryptographic plan that uses the properties of elliptic curve to create cryptographic calculations. In the 1980s Koblitz and Miller proposed utilizing the gathering focuses on elliptic curve cryptography. Over a limited field in discrete logarithmic cryptosystems. An elliptic curve is the arrangement set over a non-particular cubic polynomial mathematical statement with two questions over a field F. In short terms it is a discretized set of answers for a curve that is in the structure:

$$y2 = x3 + ax + b \text{---------- (1)}$$

If P1 and P2 are points which on the curve E, P3 = P1 + P2 Both clients consents to some publicly aware of information items.

1. The elliptic curve mathematical statement
2. Estimation of a and b
3. prime, p
4. The elliptical curve figure gathered from the elliptic curve equation
5. A base point, B, taken from the elliptic gathering.

Key generation:

1. A choose a whole number dA. this is A‘s private key.
2. A then produce a public key PA= dA*B
3. B correspondingly chooses a private key dB and process an public key PB= dB *B
4. A produces a security key K= dA *PB. B produces the security key K= dB *PA.

Signature Generation: For marking a message m by A, utilizing A‘s private key dA

1. Compute e=HASH (m), where HASH means cryptographic hash function, such as SHA-1
2. Select a arbitrary whole number k from [1, n − 1]

3. Compute r=x1(mod n), where(x1, y1) =k*B. If r=0, go to step 2
4. Computes=k−1(e+dAr)(mod n).Ifs=0,gotostep2
5. The signature is the couple of (r, s).
6. Send signature (r, s) to B client.

Encryption algorithm: Suppose A wants to send to B an encrypted message.
1. A takes plaintext message M, and encodes it onto a point, PM, from the elliptic gathering.
2. A picks another arbitrary whole number, k from the interval [1, p-1]
3. The cipher text is a couple of points.
4. PC = [(kB), (PM + kPB)]
5. Send cipher text PC to client B.

Decryption algorithm: Client B will take the following steps to decrypt cipher text PC.
1. B computes the result of the principal point from PC and his private key, dB dB * (kB)
2. B then takes this item and subtracts it from the second

5. Performance Evaluation

Table-2: Encryption time comparison

Sr. No	Algorithm	Drawbacks	Description
1	**AES**	1. Too Simple algebraic structure. 2. Problem in sharing keys. 3. Encryption process is slow	AES is based on substitution and permutation network, it is fast in both hardware and software. It has a fixed block size of 128 bits and key size of 128, 192 and256 bits. If the key size is 128 bits AES perform 10 rounds, if the key size is 192 bits it performs 12 rounds and if the key size is 256 rounds it performs 14 rounds.
2	**RSA**	1. Public keys should/must be authenticated 2. public key encryption is slow compared to symmetric encryption 3. loss of private key may be irreparable	RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system
3	**DES**	1. Two chosen input to an S-box can create the same output. 2. The purpose of initial and final permutation is not clear.	The DES function is made up of P and S-boxes. Pboxes transpose bits and S-boxes substitute bits to generate a cipher.
4	**ECC**	1. ECC algorithm is more complex and more difficult to implement. 2. Main disadvantages of ECC is that it increases the size of the encrypted message	Elliptical curve cryptography is a method of encoding data files so that only specific individuals can decode them.

5.1 Encryption Time

Comparison between symmetric and asymmetric algorithms such as between AES, RSA and ECC are shown below. This compares the time taken to encrypt using these algorithms. This analysis shows that ECC is comparatively better than AES and RSA.

Table-3: Encryption time comparison

Key Size	Time Taken to encrypt in microsec		
	AES	RSA	ECC
6	1000	800	400
25	850	500	250
48	1100	720	300
102	2500	1200	650
128	250	120	70

6. Conclusion

When compared to symmetric algorithms such as AES and Blow fish, asymmetric algorithms such as RSA and ECC are secure as they maintain two keys where one is secret and the other is shared. They can be used for authentication, confidentiality, key exchange. ECC is better than RSA as this provides equal security at smaller key length. This can be implemented in any applications that requires security such as Image Encryption, banking applications, online exchanges, e-commerce.

7. REFERENCES

[1] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, Pp.3033-3037.
[2] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, 2012, pp. 316-321.
[3] Hongwei Li, Dongxiao Liu, Yuanshun Dai,Tom H. Luan and Xuemin(Sherman) Shen "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage",March 2015
[4] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund and Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing",Springer Journal of Cloud Computing: Advances, Systems and Applications 2012.
[5] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing Wiley Publishing, Inc. Indianapolis, Indiana 2010.
[6] M. Naveed, M. Prabhakaran, and C. A. Gunter. "Dynamic searchable encryption via blind storage," in Proc, IEEE Symp. Sector: Privacy May 2014.
[7] Y. Harshada, K. Janardhan, "Ranking Based Shared Authority Privacy Preserving Authentication protocol in cloud computing" IJIRCCE, May 2015.
[8] Akhil Behl "Emerging Security Challenges in Cloud Computing ", IEEE World Congress on Information and Communication Technologies, 2011 pp.217-222.
[9] S. Sankareswari, S. Hemanth "Attribute Based encryption with privacy preserving using asymmetric key in cloud computing" IJCSIT, 2014.
[10] Jianyongchen, Y. Wang, X. Wang, "On-demand Security Architecture for cloud computing" IEEE, 2012.
[11] Mathew Green (Johns Hopkins University), Susan Hohenberger (Johns Hopkins University), Brent Waters (University of Texas at Austin), "Outsourcing the decryption of ABE Ciphertexts".
[12] Y. Harshada, K. Janardhan, "Ranking Based Shared Authority Privacy Preserving Authentication protocol in cloud computing" IJIRCCE, May 2015.
[13] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering Volume I, July 4 - 6, 2012, London, U.K. ISBN: 978-988-19251-3-8, ISSN: 2078-0958 (Print); ISSN: 2078- 0966 (Online).
[14] Neelam S. Khan, Dr. C. Rama Krishna and Anu Khurana, " Secure Ranked Fuzzy Multi-Keyword Search over Outsourced Encrypted Cloud Data",2015 5th International Conference on computer and communication technology.
[15] Chang Liu, Chi Yang, Xuyun Zhang and Jinjun Chen, "CCBKE-Session key negotiation for fast and secure scheduling of scientific applications in cloud computing".