ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

Analysis of Security Algorithms for Data Sharing in Cloud Computing

K. Lakshmi Sirisha[1], Sk. Mahboob Basha[2]

PG Scholar, Department of CSE, QIS College of Engineering and Technology, Ongole, India[1]

Assistant Professor, Department of CSE, QIS College of Engineering and Technology, Ongole, India[2]

Abstract: Cloud computing is the fastest growing technology. This technology has changed the face of traditional computing technologies and offers many benefits to the field of IT enterprises, even though it has to overcome many challenges to satisfy its maturity level. Cloud computing provides a adaptable, flexible and convenient way for sharing the data that brings plethora of benefits for both the industry and community. But often there is a natural resistance for individual users/industry to directly outsource the data to be shared on to the cloud server as the data often might contain sensitive information. Encryption is the one of the most secured way to prevent unauthorized access. This paper discusses the major security challenges of cloud computing and also highlights the importance of various cryptographic encryption algorithms as it is the major solution that can be considered for the security challenge. Due to increasing demand for more clouds and data are stored in an open environment several security issues like confidentiality, integrity and authentication may arise. This paper discusses various algorithms that ensure security in the cloud environment.

Keywords: Encryption, confidentiality, computing, integrity and authentication

I. INTRODUCTION

Cloud computing is the fastest growing technology, offers various services over the internet. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. It can serve many facilities to the business such as resources, infrastructure, platform etc by paying amount on demand basis over network with the functionality of increase or decrease the requirements. It can serves most of the hardware and software facilities required for companies for storing, creating, managing, running consumer applications on cloud in lease or rent basis, it provides resources as a service to multiple consumers by virtualization. This technology helps many IT organizations to start up business without huge economical barriers, slowly move to leading organization in the industry. According to NIST, Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Various cloud service providers are Amazon, Google, IBM, Microsoft, and Salesforce.com, offer their cloud infrastructure for services.

It can serve facilities irrespective of the size of organizations. These services gave new face to the computing technology. However, it also suffers from several security threats, which are the primary concerns of cloud users [7]. Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data.

Security is the major issue in the adoption of cloud computing. Many cryptographic algorithms are available to solve data security issue in cloud. Algorithms hide data from unauthorized users. Encryption Algorithms have vital role in the data security of cloud computing. Examples of algorithms are AES, DES, RSA, Homomorphic, etc. Two operations performed by these algorithms are encryption and decryption. Encryption is the process of converting data into scrambled form and Decryption is the process of converting data from scrambled form to human readable form. Symmetric algorithms use one key for encryption and decryption while Asymmetric algorithms use two keys for encryption and decryption.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

With respect to Cloud computing, the major security concerns [4] are end user data security, network traffic, file systems, and host machine security. There are various security issues that arise in the Cloud:

- Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end user control of where the resources are hosted.
- Ensuring Secure Interface: integrity of information during transfer, storage and retrieval needs to be ensured over the unsecure internet.
- Have Separation of data: privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.
- Secure Stored Data: question mark on controlling the encryption and decryption by either the end user or the Cloud Service provider.
- User Access Control: for web based transactions (PCI DSS), web data logs need to be provided to compliance auditors and security managers.

II. BENEFITS OF CLOUD COMPUTING

1. Reduced Cost: Cloud computing provide facility to start an IT company with less effort and initial cost. Cloud computing services are shared by multiple consumers in the world. It reduces the cost of service due to large number consumers. It charges amount depending upon the usage of infrastructure, platform and other services, this helps consumers to reduce the cost by specifying the exact requirements. Companies can easily increase or decrease their demand for services according to the performance of their company in market.

2. Scalability and Flexibility: Cloud computing can assist companies to start with a small set up and grow to a large condition fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands. Moreover cloud computing is ready to meet any peak time requirement by setting up with high capacity servers, storages etc. This facility helps consumers to meet any type of requirement irrespective of the size of project.

3. Backup and Recovery: Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device [4]. Also it has many techniques to recover it from any type of disaster; most efficient and new techniques are adopting by most cloud service providers to meet any type of disaster. Cloud Providers can get any type of technical and other support very fast than any individually set up organizations irrespective of their geographical limitations.

4. Broad network Access: Cloud services are delivered through open network (Internet), it can be accessible at any time anywhere in the world. These facilities can be accessed by various devices such as mobile phones, laptops, PDAs etc with different platforms. Consumers can access their files and other applications anytime from anywhere by using their mobiles. This has increased the rate of adopting cloud computing technology.

5. Multi-sharing: Cloud Computing offers services by sharing of architecture and other applications over Internet for single and multiple users by using virtualization and multi-tenancy. With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure [5].

6. Collaboration: Major projects or applications are delivering by the effort of multiple group of people working together. Cloud computing provide a convenient way to work group of people together on a common project or applications in an effective manner.

7. **Deliver New Services:** Cloud services are provided by multi-national companies like Amazon, Google, IBM, Microsoft, Salesforce.com, etc. These organizations can easily deliver any new application/product at the release time itself.

III. SECURITY ALGORITHMS

Encryption Algorithms for Cloud Security Encryption algorithms have vital role in the field of cloud security. Many algorithms are available for cloud security. Most useful algorithms for cloud security are discussed below.

1.Data Encryption Standard (DES): The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). It uses single key (secret key) for both encryption and decryption. It operates on 64-bit blocks of data with 56 bits key. The round key size is 48 bits.

Entire plaintext is divided into blocks of 64bit size; last block is padded if necessary. Multiple permutations and substitutions are used throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. DES

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

algorithm consists of two permutations (P-boxes) and sixteen Feistel rounds. Entire operation can divided into three phase. First phase is Initial permutation and last phase is the final permutations.

1. Initial permutation rearranges the bits of 64-bit plaintext. It is not using any keys, working in a predefined form.
2. There are 16 fiestel rounds in second phase. Each round uses a different 48-bit round key applies to the plaintext bits to produce a 64-bit output, generated according to a predefined algorithm. The round-key generator generates sixteen 48-bit keys out of a 56-bit cipher key.
3. Finally last phase perform Final permutation, reverse operation of initial permutation and the output is 64-bit cipher text.

2. Advanced Encryption Standard (AES): AES is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). Most adopted symmetric encryption is AES. It operates computation on bytes rather than bits, treats 128 bits of plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. It operates on entire data block by using substitutions and permutations. The key size used for an AES cipher specifies the number of transformation rounds used in the encryption process[8][9].Possible keys and number of rounds are as following:

- 10 rounds for 128-bit keys.
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

Major advantages of AES over DES are

1. Data block size is 128 bits.
2. Key size 128/192/256 bits depending on version.
3. Most CPUs now include hardware AES support making it very fast.
4. It uses substitution and permutations.
5. Possible keys are 2128 , 2192 and 2256 [10]
6. More secure than DES.
7. Most adopted symmetric encryption algorithm.

3. Rivest-Shamir-Adleman (RSA): RSA is a public key cipher developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is most popular asymmetric key cryptographic algorithm. This algorithm uses various data block size and various size keys. It has asymmetric keys for both encryption and decryption. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose [11]. This algorithm can be broadly classified in to three stages; key generation by using two prime numbers, encryption and decryption.

RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data[12]. This algorithm is mainly used for secure communication and authentication upon an open communication channel. While comparing the performance of RSA algorithm with DES and DES, When we use small values of p & q(prime numbers) are selected for the designing of key, then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES[12]. Operation speed of RSA Encryption algorithms is slow compare to symmetric algorithms, moreover it is not secure than DES.

4 Multi-Authority Ciphertext-Policy-Attribute Based Encryption (CP-ABE): In Attribute-Based Access Control only one system is responsible for the production and distribution of public keys and private keys respectively. In this type all the burden of creating and sending the different keys lies on a single system. This may cause some delay in transmitting the keys to different users. In order to reduce the load to the single system multi-authority CP-ABE was introduced. A party can act as an authority by creating public key and distributing the private keys to different users that reflect their attributes.

In multi-authority CP-ABE system for cloud computing consists of five types of entities: the Certificate Authority (CA), the Attribute Authorities (AAs), the data owners (owners), the data consumers (users) and the cloud server. The figure1 illustrates the model of multi authority system and depicts the communication between different entities like cloud service provider, AA, user, data owner and CA.

5 Message Digest Algorithm: Message Digest Algorithm (MDA) uses public key encryption, symmetric encryption and standard hashing algorithm in the registration process, authentication process and generating the message digests

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

respectively. As MDA does not have any specification for algorithms, any standard combinations of encryption algorithms and hashing algorithms could be used in the operations of MDA [8].

Message digest function, also known as hash function is used to generate Digital Signature of the information. The digital signature produced by the hash function is known as message digest. MD5 algorithm is used to implement integrity of the message and it produces message digest of size 128 bits. There are mathematical functions that process data to produce different message digest for each different message. Message digest algorithm has two advantages. The first advantage is that identical messages always generate the same message digest and even if any changes occur in the message bit, it produce different message digest for that message. The second advantage is that message digests are much shorter than the document from which message digests are generated. It processes the message and generates 128 bits message digest. The algorithm contains the following steps:

1. Appending the padding bits
2. Appending the length
3. Initializing a MD buffer
4. Processing message in 512 bit blocks
5.Generating output

6.Revocable Identity Based Encryption: The concept of revocable identity-based encryption (RIBE) might be a promising approach that fullfills the aforementioned security requirements for data sharing. RIBE features a mechanism that enables a sender to append the current time period to the cipher text such that the receiver can decrypt the cipher text only under the condition that he/she is not revoked at that time period. A RIBE-based data sharing system works as follows:

Step 1: The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the cipher text of the shared data to the cloud server.

Step 2: When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding Cipher text. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.

Step 3: In some cases, e.g., Alice's authorization gets expired; David can download the cipher text of the shared data, and then decrypt-then-re-encrypt the shared data such that Alice is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

Obviously, such a data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks.

In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the cipher text periodically by using secret key. Another challenge comes from efficiency. To update the cipher text of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-re encrypt-upload. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage.

One method to avoid this problem is to require the cloud server to directly re-encrypt the cipher text of the shared data. However, this may introduce cipher text extension, namely, the size of the cipher text of the shared data is linear in the number of times the shared data have been updated. In addition, the technique of proxy re-encryption can also be used to conquer the aforementioned problem of efficiency. Unfortunately, it also requires users to interact with the cloud server in order to update the cipher text of the shared data.

IV. COMPARISION OF SECURITY ALGORITHMS

The Multi-authority attribute-based encryption algorithm provides collusion resistance against any number of colluding users. Each authority's attribute set must be disjoint. To overcome this problem, a separate copy of each attribute for each clause may be created. The CA can decrypt every cipher text so that the user privacy and confidentiality of the data is less in this system. The system structure of RSA algorithm is based on the number theory. It is the most security system in the key systems. A third party cannot break the private key because of factorization of larger numbers. If you want to break the information, you need to decompose a large number. In order to make the RSA safety, it must choose a large value for x and y. Users' usually choice more than 100 decimal digits, so that the attacker cannot decompose the N in polynomial time effective internal. The RSA encryption and decryption algorithm need a lot of calculation and the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

speed is slow when compared with the symmetric cryptographic algorithm. Size of the key is inversely proportional to security. In order to increase the level of security the size of the key should be greater.

If the size is long the computational speed will be greater. Message digest functions are faster than the traditional symmetric key cryptographic algorithms. The recently used message digest algorithms have no pattern restrictions. MACs based on message digests provide the "cryptographic" security for most of the Internet's routing protocols. Message digest functions appear to provide an excellent means of spreading the randomness from an input among all of the function's output bits.

IBE eradicates the need for providing a public key infrastructure (PKI). Regardless of the setting of IBE or PKI, there must be an approach to revoke users from the system when necessary, e.g., the authority of some user is expired or the secret key of some user is disclosed.

In the traditional PKI setting, the problem of revocation has been well studied [15], [16], [17], [18], [19], and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates. However, there are only a few studies on revocation in the setting of IBE. Boneh and Franklin [14] first proposed a natural revocation way for IBE. They appended the current time period to the cipher text, and non-revoked users periodically received private keys for each time period from the key authority.

Unfortunately, such a solution is not scalable, since it requires the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys. To conquer this problem, Boldyreva, Goyal and Kumar [20] introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users.

Inspired by the above work and [25], Liang et al. [26] introduced a cloud-based revocable identity-based proxy re-encryption that supports user revocation and cipher text update. To reduce the complexity of revocation, they utilized a broadcast encryption scheme [27] to encrypt the cipher text of the update key, which is independent of users, such that only non-revoked users can decrypt the update key. However, this kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non revoked users can share the update key with those revoked users.

The performance of the algorithm has been analysed by considering the parameters like block size, key size and the application of the algorithm, and is summarized in table 1

Table 1:Performace of algorithms

Algorithm	Block Size	Key Size	Security
DES	Variant	56 bits	Secure for data
Multi-authority CP-ABE	Variant	512 to 4096 bits	Secure for Man applications
RSA	Variant	512-2048bits	Secure for large amount of data
Message Digest	Variant	>160 bits	Secure for internet routing protocol
Revocable Identity Based Encryption	Variant	56 bits	Secure for large amount of data

CONCLUSION

Cloud computing appears very useful service for many people; every third person is using cloud in different ways. Due to its flexibility, many persons are transferring their data to cloud. Cloud computing prove a very successful application for organisations. Because organisations have large amount of data to store and cloud provides that space to its user and also allows its user to access their data from anywhere anytime easily. As people are saving their personal and important data to clouds, so it becomes a major issue to store that data safely. Many algorithms exist for the data security like DES, AES, and Triple DES. These are symmetric key algorithms in which a single key is used for encryption and decryption whereas RSA, Diffie-Hellman Key Exchange and Homomorphic equations are asymmetric, in which two different keys are used for encryption and decryption. These algorithms are not secure, there is need to enhance the security of algorithms. The identity based encryption algorithm is the algorithm that provides security for a cloud based environment for shared data access in a efficient manner.

REFERENCES

[1]. Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , Cloud Computing System Based on Trusted Computing Platform, International Conference on` Intelligent Computation Technology and Automation, Volume 1, May 2010, On page(s): 942-945.

[2]. Pearson, S., Benameur, A., Privacy, Security and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference 2010, On page(s): 693-702.
[3]. Rohit Bhadauria and Sugata Sanyal, A Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, Volume 47- Number 18, June 2012, On page(s): 47-66.
[4]. Mohammed, E.M, Ambelkadar, H.S, Enhanced Data Security Model on Cloud Computing, 8 th International Conference on IEEE publication 2012, On page(s): cc-12- cc-17
[5]. Sang Ho. Na, Jun-Young Park, Eui- Nam Huh, Personal Cloud Computing Security Framework, Service Computing Conference (APSSC), Dec 2010 IEEE, On page(s): 671- 675.
[6]. Wang, J.K.; Xinpei Jia, Data Security and Authentication in hybrid cloud computing model, Global High Tech Congress on Electronics (GHTCE), 2012 IEEE, On page(s): 117-120.
[7]. Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, January 2011.
[8]. Iankoulova, I.; Daneya, M., Cloud computing security requirements: A systematic review, Research Challenges in Information Science (RCIS), Sixth International Conference on, 2012, On page(s): 1 - 7.
[9]. Cloud Security Alliance, Top Threats to Cloud ComputingV1.0,http://www.cloudsecurityall iance.org/topthreats.
[10]. Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao, Cheng Fu, Xi He, Andrew Younge, Cloud Computing: A Perspective Study, New Generation ComputingAdvances of Distributed Information Processing, Volume 28, Issue 2, April 2010, On page(s): 137-146.
[11]. Puneet Jai Kaur, Sakshi Kaushal, Security Concerns in Cloud Computing, Communication in Computer and Information Science Volume 169 in 2011, On page(s): 103-112.
[12]. Shui Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, Cloud Computing Research and Development Trend, Second International Conference on Future Networks (ICFN), IEEE Publications, January 2010, On page(s): 93-97.
[13]. Pearson, S., Benameur, A., Privacy, Security and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference,2010.
[14]. Leena Khanna, Anant Jaiswal, "Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them", IJARCSSE 2013.
[15]. G Devi, Pramod Kumar "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" IJCTT 2012.
[16]. Simarjeet Kaur "Cryptography and Encryption in Cloud Computing", VSRD International Journal of CS and IT, 2012.
[17]. Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing", Springer 2012.
[18]. Ronald Krutz, Russell Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing" Wiley Publishing 2010.
[19]. Behrouz Forouzan, "Cryptography and Network Security", McGraw-Hill Special Indian Edition 2007.
[20]. Wayne Jansen, Timothy Grance "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology 2011.
[21]. Akhil Behl "Emerging Security Challenges in Cloud Computing", IEEE 2011.
[22]. Maha Tebba, Saïd Haji Abdellatif Ghazi, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering 2012.
[23]. Cloud Security Alliance (CSA), "Security Guidance for critical Areas of Focus in cloud computing V3.0" CSA 2015.
[24]. Ayan Mahalanobis, "Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups." 2005.
[25]. Neha Jain, Gurpreet Kaur, 'Implementing DES Algorithm in Cloud for Data Security", VSRD International Journal of CS and IT, 2012.
[26]. Mandeep Kaur, Manish Mahajan, "Implementing Various Encryption Algorithms to Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology 2012.
[27]. Jeeva, Dr. Palanisamy, Kanagaram, "Comparative Analysis of Performance Efficiency and Security Measures of some Encryption Algorithms", IJERA ISSN: 2248-9622 Vol. 2, Issue 3, 2012.
[28]. Dr. Sarbari Gupta, "Securely management crypgraphic keys used within acloud environment", NIST Cryptographic Key management workshop, 2012.
[29]. Dr. R. Chandramouli "Key Management Issues in the Cloud Infrastructure", Workshop on Cloud Computing, 2013.
[30]. Sandro Rafaeli, "Survey of key management for secure communication", ACM Computing Surveys, 2013.
[31]. S. Anahita Mortazavi, Alireza Nemaney Pour, Toshihiko Kato, "An Efficient Distributed Group Key Management using Hierarchical Approach with Diffie-Hellman and Symmetric Algorithm: DHSA",CNDS Feb 2011.[19]
[32]. ENISA, "Algorithms, Key Sizes and Parameters Report, 2013", recommendations version 1.0 – October 2013.
[33]. Y. Fan, L. Xiao-ping, D. Qing-kuan and L. Yan-ming, "A Dynamic Layering Scheme of Multicast Key Management," IEEE 5th International Conference on Infomration Assurance and Security, Xian 2009.

BIOGRAPHIES

K. Lakshmi Sirisha is a PG Scholar in Computer Science and Engineering Department, QIS College of Engineering and Technology. Her Interest includes Networking, Cloud computing.

Sk. Mahboob Basha is working as Assistant Professor in Computer Science and Engineering Department, QIS College of Engineering and Technology. His field of Interest is Networking and has published several papers.