Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cloud Security Using Encryption Techniques

Diksha Gupta*, Partha Sarathi Chakraborty, Pragya Rajput
CSE Department, SRM University
India

Abstract— Cloud Computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms. However, a major barrier for cloud adoption is real and perceived lack of security. A large number of cryptographic schemes are available to encrypt the sensitive information and to protect data. Even though it protects the data but it limits the functionality of the cloud storage. In this paper we survey different security issues to cloud and different cryptographic algorithms adoptable to better security for the cloud.

Keywords— Confidentiality, Deployment models, Cloud security, DES, MD5, Blowfish.

I. INTRODUCTION

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. [1] 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.

Cloud Service Models

a) Software-as-a-Service (SaaS). The SaaS service model offers the services as applications to the consumer, using standardized interfaces. The services run on top of a cloud infrastructure, which is invisible for the consumer. The cloud provider is responsible for the management the application, operating systems and underlying infrastructure. The consumer can only control some of the user-specific application configuration settings. Example: Yahoo!, Gmail, Google Docs, etc.

b) Platform-as-a-Service (PaaS). The PaaS service model offers the services as operation and development platforms to the consumer. The consumer can use the platform to develop and run his own applications, supported by a cloud-based infrastructure. "The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations". Example: Google Aps, SQL Azure, etc.

c) Infrastructure-as-a-Service (IaaS). The IaaS service model is the lowest service model in the technology stack, offering infrastructure resources as a service, such as raw data storage, processing power and network capacity. The consumer can the use IaaS based service offerings to deploy his own operating systems and applications, offering a wider variety of deployment possibilities for a consumer than the PaaS and SaaS models. "The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)". Example: Amazon (S3, EC2), Windows Azure, etc.

Cloud Deployment Models

Regardless of which delivery model is utilized, cloud offerings can be deployed in four primary ways, each with their own characteristics. [2] The characteristics to describe the deployment models are;

(i) who owns the infrastructure;
(ii) who manages the infrastructure;
(iii) where is the infrastructure located;
(iv) and who accesses the cloud services.

A. Public Clouds

Public cloud computing is based on massive scale offerings to the general public. The infrastructure is located on the premises of the provider, who also owns and manages the cloud infrastructure. Public cloud users are considered to be untrusted, which means they are not tied to the organization as employees and that the user has no contractual agreements with the provider.

B. Private clouds

Private clouds run in service of a single organization, where resources are not shared by other entities. "The physical infrastructure may be owned by and/or physically located in the organization‟s datacenters (on-premise) or that of a designated service provider (off-premise) with an extension of management and security control planes controlled by the organization or designated service provider respectively".[3] Private cloud users are considered as trusted by the organization, in which they are either employees, or have contractual agreements with the organization.

C. Community clouds

Community clouds run in service of a community of organizations, having the same deployment characteristics as private clouds. Community users are also considered as trusted by the organizations that are part of the community.

D. Hybrid clouds

Hybrid clouds are a combination of public, private, and community clouds. Hybrid clouds leverage the capabilities of each cloud deployment model. Each part of a hybrid cloud is connected to the other by a gateway, controlling the applications and data that flow from each part to the other.

The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud .This leads to affects many customers who are sharing the infected cloud.

There are five types of issues raise while discussing security of a cloud. [4]

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues
5. Trust Issues

Various Characteristics of Cloud Computing[5]

1) On Demand Self-Service: Cloud providers provide services such as email, applications, network or server services on demand of user.

2) Broad Network Access: Cloud services are delivered over network which can be accessed from anywhere such as laptops, mobile phones, etc.

3) Resource Pooling: To provide services to the multiple users the resources are pooled together.

4) Rapid Elasticity: Cloud services are provisioned with elasticity. Services are quickly scale out and scale in as per user demand.

5) Measured Service: Resource usage can be monitored by providing transparency for both the provider and user of the utilized service. Services are charged per usage units – as pay-per-use. There more the utilization the higher user have to pay.

II. RELATED WORK

Wei-Tek Tsai et al. [6] described the current cloud architecture and issues related to its implementation. They proposed a Service-Oriented Cloud Computing Architecture (SOCCA) for interoperability with each other and to better support multi-tenancy.

Gangolu Sreedevi et al.[7] have presented new way of security ICCC for small organizations in cloud where data storage transparency can be minimized. They are not encrypting the whole message. Rather than encrypting whole message, they encrypt the some bits in each block. For data correctness, they have generated the Meta data which is used to verify the data for alteration or deletion by unauthenticated party. Through this technique, they achieve the correctness of data of owner at low cost and computational part is also free from overhead.

Mohammad Sajid et al. [8] presented challenging issues related to various aspects of cloud computing.

Kalpana Batra et al.[9] have tried to achieve the security of data in distributed storage system by applying the file distribution technic to provide the redundancy. For correctness of the data they have generated the token pre computation technic and stored at servers in cloud for the verification purpose. They have shown that their scheme is efficient and reliable to detect the misbehaving servers and correct the data in particular servers and avoid colluding attacks of server modification by unauthorized users.

Sherif El-etriby et al. [10] had presented an evaluation of modern encryption techniques at two independent platforms. A randomness testing using NIST statistical testing in cloud computing environment has been performed on those encryption algorithms to determine most suitable encryption technique among them and analyze their performance.

Chao Yang et al. [11] proposed the data security in cloud data storage. For that a novel triple encryption scheme is presented, which combines HDFS files encryption using DEA and the data key encryption with RSA, and then encrypts the user's RSA private key using IDEA. They implemented the triple encryption scheme in Hadoop-based cloud data storage.

GaidaaSaeed Mahdi, [12] proposed to develop a simple, stronger and safer cryptographic algorithm which would not only be a secure one, but also reduces total time taken for encryption and decryption. The modified algorithm MTEA is a new secret-key block cipher of 64 bit that uses good features of Tiny Encryption Algorithm (TEA) and RC6 algorithms.

III. SECURITY SOLUTION APPROACH

In cloud computing environment there is need of security technologies that are required for providing protection to the resources and virtual machines or virtual servers. Following technologies are used for providing privacy and security in cloud: [13]

A. Firewall

To decrease the attack surface of virtualized servers in cloud computing environments, a firewall [17] is deployed on individual virtual machine that controls incoming and outgoing network traffic based on applied rules to prevent unauthorized access to a cloud computing system. It acts as a barrier between secure internal networks to outside network that is not secure.

B. Intrusion Detection System

Applying intrusion detection and prevention on virtual machines and Operating system (OS) that detects malicious activity in computer systems and conducts forensic analysis once attack is over.It monitors network resources to detect intrusions or attacks.

C. Third Party Auditor

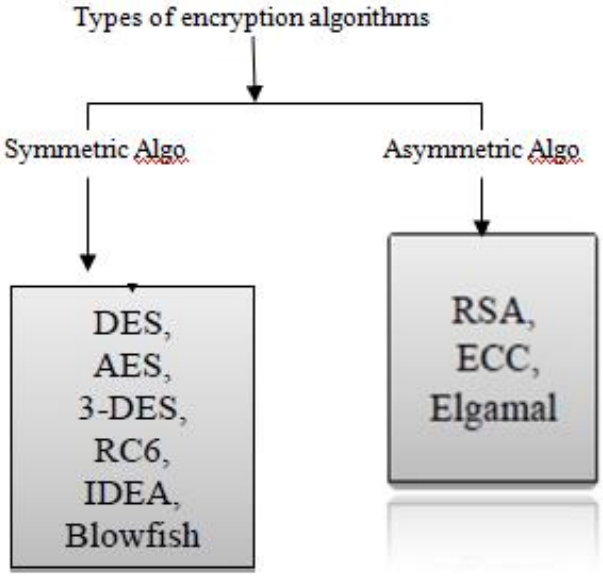
Checks the integrity of data stored at the cloud server and insures cloud user that their data are secure in cloud.

D. Cryptography

Using cryptography we can protect the sensitive data in the cloud. In cryptography the sensitive data of the user are encrypted in cipher text which adds a security level over the data.

IV. CRYPTOGRAPHIC SECURITY TECHNIQUES

There are two main categories of encryptions used in cryptography to achieve data confidentiality, integrity, availability, authentication. There are symmetric and asymmetric encryption algorithms.



• Symmetric Encryption

In this algorithm, encryption and decryption requires that the same algorithm and key are used to both encipher and decipher the message.[14] There is a private key that is used to encrypt and decrypt the message at both ends. Symmetric encryption algorithm provides confidentiality, integrity and availability but it fails to provide authenticity.

i. Data Encryption Standard (DES)

One of the first widely popular symmetric cryptography algorithm that uses block cipher and encrypts 64 bit blocks. Drawback is that it has been cracked back in 1977.

ii. Triple Data Encryption Standard (3DES)

This algorithm has been designed to replace DES algorithm. It uses 3 rounds of encryption instead of one and uses 16 iterations within each round.

iii. Advanced Encryption Standard (AES)

This algorithm has been approved by NIST in the late 2000 as a replacement for DES algorithm. [15] It performs 3 steps on every 128 bit block of plaintext. Within 2 steps, multiple rounds are performed depending upon the key size. Drawback is AES algorithm has been theoretically broken.

iv. BLOWFISH: Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption.

v. RC5: It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow.

• Asymmetric Encryption

Asymmetric encryption algorithm uses two keys instead of one. One is a private key only known to the recipient of the message and the other is a public key known to everyone and can be freely distributed. Either key can be used to encrypt and decrypt the message. Asymmetric algorithms are slower than symmetric algorithms. But it has better key distribution than symmetric algorithm. It has better scalability and also provides authenticity.

i. RSA

It is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. [16] Messages encrypted with the public key can only be decrypted using the private key. user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission.

ii. Elliptic curve cryptography (ECC)

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key.

iii. EI Gamal

In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. ElGamal encryption can be defined over any cyclic group . Its security depends upon the difficulty of a certain problem in related to computing discrete logarithms

V. CONCLUSIONS

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the 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 algorithm. DES and AES are mostly used symmetric algorithms.DES is quite simple to implement then AES.

RSA and Diffie-Hellman Key Exchange is the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms.

But the security algorithms which allow operations (like searching) on decrypted data are required for cloud computing, which will maintain the confidentiality of the data..

REFERENCES

[1] Mohiuddin Ahmed , Abu Sina Md. Raju Chowdhury , Mustaq Ahmed , Md. Mahmudul Hasan Rafee , "An Advanced Survey on Cloud Computing and State-of-the-art Research Issues", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012 ISSN (Online): 1694-0814.

[2] Jason, "Defining Cloud Deployment Models":" http://bizcloudnetwork.com/defining-cloud-deployment-models", Last modified on AUGUST 4, 2010.

[3] Ang Li, Xiaowei Yang, Srikanth Kandula and Ming Zhang, "Comparing Public Cloud Providers",IEEE Internet Computing, Vol. 15, no. 2, pp. 50-53, 2011.

[4] Lori M. Kaufman, "Data Security in the World of Cloud Computing", IEEE Security & Privacy, vol. 7, no. 4, pp. 61 -64, 2009.

[5] Yogita Gunjal, Prof. J.Rethna Virjil Jeny, "Data Security and Integrity of Cloud Storage in Cloud Computing", in the year of April 2013.

[6] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya, "Service-Oriented Cloud Computing Architecture", Seventh International Conference on Information Technology, IEEE 2010.

[7] Gangolu Sreedevi, Prof. C. Rajendra," ICCC: Information Correctness to the Customers in Cloud Data Storage", in the year of June 2012.

[8] Mohammad Sajid, Zahid Raza, "Cloud Computing: Issues & Challenges", International Conference on Cloud, Big Data and Trust 2013, RGPV.

[9] Kalpana Batra, Ch. Sunitha, Sushil Kumar," An Effective Data Storage Security Scheme for Cloud Computing", in the year of June 2013.

[10] Sherif El-etriby, Eman M. Mohamed, "Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing", ICCIT 2012.

[11] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing".

[12] GaidaaSaeed Mahdi, "A Modification of TEA Block Cipher Algorithm for Data Security (MTEA)", Engg.& tech. Journal, vol 29, No.5, 2011.

[13] Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[14] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[15] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[16] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

