Obtaining Data Security using Cloud Computing and Cryptographic Algorithms

Deepthy S[1] Vidya Vijayan[2]
[1,2]Mount Zion College of Engineering, Kadammanitta, India

Abstract— Cloud storage involves stashing data on hardware in a remote physical location, which can be accessed from any device via the internet. Clients send files to a data server maintained by a cloud provider instead of storing it on their own hard drives. It is readily manageable by the Internet, a cloud infrastructure can be accessed by enterprises easily and quickly. The data can be accessed from anywhere and anytime. In this paper we aim to provide a set of technology protection designed to protect resources from leakage, theft, or data loss. AES and RSA which are from symmetric, asymmetric cryptographic algorithm. We propose a combination of AES, RSA and SHA-1 algorithm for optimum cloud security. Our approach ensures the security and privacy of client sensitive information by storing data across single cloud, using AES, RSA and SHA-1 algorithm.

Keywords: AES, RSA and SHA-1 algorithm, Cloud Computing, Cryptographic Algorithms

I. INTRODUCTION

Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or delete information. Because of cloud simplicity everyone is moving data and application software to cloud data centers. The Cloud service provider (CSP) should ensure integrity, availability, privacy and confidentiality but CSP is not providing reliable data services to customer and to stored customer data.

Cryptography is the protecting technique of data from the unauthorized party by converting into the non-readable form. The main purpose of cryptography is maintaining the security of the data from third party. There are following two types of algorithms such as: (i) symmetric key based algorithm, sometimes known as conventional key algorithm and (ii) asymmetric key based algorithm, also known as public-key algorithm. In this paper, we will focus on the security of cloud by proposing crypto algorithms and effective measures so as to ensure the data security in cloud.

II. CLOUD COMPUTING

Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized Service- Level Agreements.

A definition of cloud computing must recognize the fundamental characteristics that make cloud computing services valuable and distinguishable. The NIST pointed out most of the characteristics that are widely used among the cloud computing community and these characteristics include:

- On-demand self-service. Cloud computing resources (e. g. CPU, storage, software) are provided as needed and scheduled without requiring human interactions with a service provider. The key points of this feature are time saving, cost effectiveness, usability and the range of services provided.
- Broad network access. Cloud services are accessed through a widely accessible network, mainly the internet, which uses standard protocols and mechanisms to support various types of devices and platforms e.g., smart phones, thin clients, and PDAs.
- Resource pooling. The physical cloud resources, based on virtualization technology, are shared among cloud users, depending on their consumption demands. The users are not aware of the physical limitations of resources as they are virtually provisioned and de-provisioned automatically according to demand.
- Measured service. As the service is provided under the pay-as-you-use business model, the usage of services and resources can be metered and automatically billed for each particular user session.
- Rapid elasticity. The provisioning and de-provisioning of cloud services and resources are done rapidly and elastically for each cloud user in real time.
- Location independence. The cloud resources can be located physically at any geographical location as long as the communication capability is available. Also the cloud users can reach the service from anywhere with the same condition.
- Privacy and integrity are important requirements for various applications such as e- government and EHR (Electronic Health Record). Cloud computing customers are not only worried about the compromising of privacy and integrity of their data from possible attackers, but also from potential curious cloud providers. Unfortunately, security breaches counted in 2011 and show that big companies such as Google, EMC/ RSA, Sony, UK National Healthcare System (NHS) and Amazon EC2 all experienced security incidents. In cloud computing, customers' data are outsourced to cloud providers which can be either trusted or un- trusted. The term un-trusted may be used to indicate that the cloud providers cannot be fully trusted. For instance, un-trusted cloud providers may not alter users' data but they can passively compromise data privacy or stealthily change the protocols for their financial benefit. In other words, a cloud provider server can be considered as a honest-but-curious server. Hence, it is trustworthy in providing the services, in terms of data availability, enforcing basic security control requirements and processing honestly authorized queries on stored data and returning the correct results. Nevertheless, possible malicious actions from inside the cloud can be carried out from a malicious administrator or employee.

The utility of this cloud and its services are not restricted to a domain or any premises. All the users are allowed to use this data whenever needed. This paper has cloud that is accessible to all, a database to store all data and information, website for users to login to the cloud. The cloud can be accessed through internet from anywhere. The users have to login to the cloud and provide details to access the data from database. The cloud will also provide security to all the data stored at our server.

Companies and organizations need to take a data-centric approach to protecting their sensitive information in order to guard against advanced threats in the complex and evolving environments of virtualization, cloud services, and mobility. Companies should implement data security solutions that provide consistent protection of sensitive data, including cloud data protection through encryption and cryptographic key management. A comprehensive platform for cloud security and encryption also should deliver robust access controls and key management capabilities that enable organizations to practically, cost effectively, and comprehensively leverage encryption to address security objectives.

III. USE OF CRYPTOGRAPHY

AES algorithm uses a round function that is composed of four different byte-oriented transformations:

1) byte substitution using a substitution table (S-box),
2) shifting rows of the State array by different offsets,
3) mixing the data within each column of the State array, and
4) adding a Round Key to the State.

In AES the main architecture is centrally controlled by both hardware and software. Decryption of this system is depending upon the designing rule which is called Substitution Permutation Networking. Advanced Encryption standard has standard blocks with fixed length of 128 bits and their allowed key size is 128,192 or it can be 256 bits, new research has evolved that multiple key size can be allocated to the block it could be 32 bits with the least capacity of 128 bits and its key size may be extended no fixed length is announced. Its operations are based on the 4X4 matrix of the bytes with finite field calculations especially designed for the purpose of calculations. AES specifies the repetition numbers for converting the input to the normal readable text. An input provided by the user undergoes several steps of processing according to the encryption key provided. These steps are categorized as rounds and for converting the text back to the encrypted form same rounds are repeated with the same key which was used for decryption.

The cipher consists of a basic operation called round which is repeated a number of times. In this case, AES is based in a design principle called Substitution-Permutation Networks which means that the cipher is composed of a series of substitutions and permutations one after each other . The number of rounds (R) in AES depends on the key length: 10 rounds for 128, 12 rounds for 192 and 14 rounds for 256 bits. AES works on a structure known as the AES state, which is simply an arrangement of the block in a 4x4 matrix. Furthermore, most AES operations can be described as operations in the GF (28) finite field. This gives AES a quite neat algebraic description.

RSA is widely used Public-Key algorithm. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data.

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

A. Key generation

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:

1) Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2) Compute n = a * b.
3) Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
4) Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.
5) Now determine d as follows: $d = e^{-1} \pmod{Ø(n)}$ i.e., d is multiplicate inverse of e mod Ø(n).
6) d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7) The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8) The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

B. Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps:

1) Cloud service provider should give or transmit the Public- Key (n, e) to the user who want to store the data with him or her.
2) User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3) Data is encrypted and the resultant cipher text(data) C is
$$C = m^e \pmod{n}.$$
4) This cipher text or encrypted data is now stored with the Cloud service provider.

C. Decryption:

Decryption is the process of converting the cipher text(data) to the original plain text(data).

Steps:

1) The cloud user requests the Cloud service provider for the data.
2) Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e, C.
3) The Cloud user then decrypts the data by computing,
$$m = C^d \pmod{n}.$$
4) Once m is obtained, the user can get back the original data by reversing the padding scheme.

IV. CONCLUSION

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.

Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing RSA algorithm.

V. REFERENCES

[1] Philip Wik, "Thunderclouds: Managing SOA-Cloud Risk".Service Technology Magazine. 2011
[2] Aderemi A. Atayero, Oluwaseyi Feyisetan,"Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", In Journal of Emerging Trends in Computing and Information Sciences, Vol-2,No.10, pp.546-552, October 2011
[3] Pengfei You, Yuxing Peng, Weidong Liu, Shoufu Xue, "Security Issues and Solutions in Cloud Computing".
[4] Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.
[5] Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011
[6] P Naik, S Sanyal, "Increasing Security in Cloud Environment" arXiv: 1301.0315 [cs.CR], 2013
[7] "Cloud Security Front and Center". Forrester Research.2009-11-18. http://blogs.forrester.com/srm/2009/11/cloudsecurity-front-and-center.html. Retrieved 2010-01-25.
[8] Dr. L. Arockiam, S. Monikandan, Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013. [5].

