A Review of Data Security Algorithms in Cloud Computing Environment

Venkatesh H[1] and Dr.G.N.K.Suresh Babu[2]

[1]Lecturer, Department of MCA, Acharya Institute of Technology, Bangalore- 560107
[2]Associate Professor, Department of MCA, Acharya Institute of Technology, Bangalore – 560107

Abstract - The main goal of this paper is how we can provide secure data in a cloud computing environment. Cloud Computing is an emerging computing paradigm. It aims to share data, calculations, and service transparently over a scalable network of nodes. Today many organizations using the business model with the help of cloud computing technology. But the threat in cloud computing technology is security of data. Data security refers to the security of data on the storage media. So, Security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud. Data must not be stolen by the third party so authentication of client becomes a mandatory task. In this paper, we discuss a number of existing methodologies through cryptographic algorithms used to provide data security in the field of cloud computing and the proposed solutions for secured data.

Keywords : Cloud, Security, Privacy, DES, RSA

I INTRODUCTION

Cloud is nothing but the group of servers and datacenters that are placed at different places and these severs and datacenters are responsible for providing on demand service to its users with help of internet. The service provided by cloud is not present on user's computer. User has to access these services with help of internet connection through subscribing them. The main advantage of Cloud computing is that it eliminates the need for user to be in same location where hardware software and storage space is physically present. Cloud makes it possible to store and access your data from anywhere anytime without worrying about maintenance of hardware software and storage space. All these services are provided to user at low cost. User has to pay according to storage space he is using. Due to this flexibility everyone is transferring his data on cloud. Security becomes big issue when any one stores its important information to a platform which is not directly controlled by the user and which is far away. While sending of data and during storage data is under threat because any unauthorised user can access it, modify it, so there is need to secure data. A data is secure, if it fulfils three conditions (i) Confidentiality (ii) Integrity (iii) Availability. Confidentiality means the data is understandable to the receiver only for all others it would be waste; it helps in preventing the unauthorised disclosure of sensitive information. Integrity means data received by receiver should be in the same form, the sender sends it; integrity helps in preventing modification from unauthorised user. Availability refers to assurance that user has access to information anytime and to any network. In the cloud confidentiality is obtained by cryptography.

II CLOUD TYPES

Public Clouds

A public cloud encompasses the traditional concept of cloud computing, having the opportunity to use computing resources from anywhere in the world.

Private Clouds

Private clouds are normally datacenters that are used in a private network and can therefore restrict the unwanted public to access the data that is used by the company. It is obvious that this way has a more secure background than the traditional public clouds. However, managers still have to worry about the purchase, building and maintenance of the system.

Hybrid Clouds

As the name already reveals, a hybrid cloud is a mixture of both a private and public cloud. This can involve work load being processed by an enterprise data center while other activities are provided by the public cloud. Fig. 1 represents the how the user can access the data through cloud computing environment.

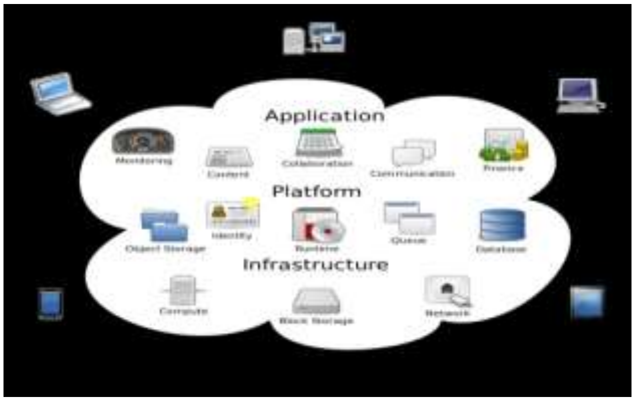

Fig.1 – Overview of Cloud Computing Paradigm

III CLOUD COMPUTING SERVICES

Cloud Computing encompasses different types of services. There are 3 classes of technology capabilities that are being offered as a service and which will be introduced in the following:

Infrastructure as a Service

Statistically proven figures show that 80% of the computing power is not efficiently used, neither is 65% of the storage of servers. Hence there is a huge potential to share resources in order to use them in a cost efficient way rather than underutilizing them.

Platform as a Service

Platform as a service provides the facility to support the development lifecycle from design, implementation, debugging, testing, deployment, operation and support of rich internet applications (RIA) and online services. Here mostly the internet browser will be used for the development).

Software as a Service

Companies can use software that is made available online on a rental or usage basis rather than buying the whole software package locally without being sure whether or not the investment will pay off on a long-term basis. No maintenance or updates are involved; this will all be handled by the software provider.

IV CLOUD COMPUTING CHARACTERISTICS

There are several characteristics of cloud computing, which are described below-

 Virtualization: Through Cloud computing, user is able to get service anywhere through any kind of terminal. User can attain or share it safely anytime.

 High Reliability: Cloud uses data fault tolerant to ensure the high reliability of the service.

 Versatility: Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.

 On Demand Service: Cloud is a large resource pool that a user can buy according to his/her need; cloud is just like running water, and gas that can be charged by the amount that user used.

 Extremely Inexpensive: The centered management of cloud make the enterprise needn't undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully take advantage of low cost.

Some advantages are listed below-

 Cloud computing do not need high quality equipment for user and it is easy to use.

 Cloud computing can realize data sharing between different equipments.

 Cloud computing provides dependable and secure data storage center. You don't worry the problems such as data loss or virus.

Figure 2 represents the organization of data security and privacy in cloud computing environment.

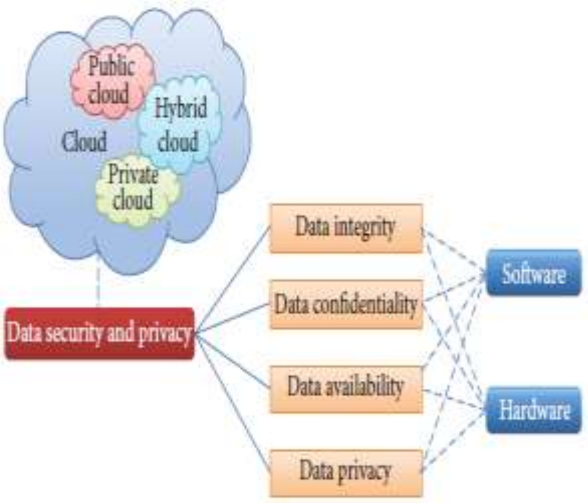

Fig. 2 Organisation of Data Security and Privacy in Cloud Computing Environment

V CHALLENGES OF CLOUD COMPUTING

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages.

• **Security and Privacy** — Perhaps two of the more "hot button" issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust and a Hybrid cloud could support such a deployment.

• **Lack of Standards** — Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an

Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable.

• **Continuously Evolving** — User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving.

VI CLOUD COMPUTING SECURITY MEASURES

Security of data has become a major concern. When data mobility is at a high level then the risks and issues increase many folds especially when data is transferred to another country with different regulatory framework. High levels of data relocation have negative implications for data security and data protection as well as data availability. Thus the main concern with reference to security of data residing in the Cloud is: how to ensure security of data that is *at rest*. Although, consumers know the location of data and there in no data mobility, there are questions relating to its security and confidentiality of it. No doubt the Cloud Computing area has become larger because of its broad network access and flexibility. But reliability in terms of a safe and secure environment for the personal data and info of the user is still required. The following security measures may be taken in view of the potential threats to the security in cloud computing:

 The cloud consumer privacy bill of rights with private protection is focused on the administration of personnel data and maintain its status of accuracy and its utilization on user demand basis.

 Need to design new data centers and sources, devices, services and applications for "THREAD DETECTION" related to outsourcing a top co-operate risk.

 Focus to design personal clouds that move gravity centre from application centric to personnel centric models so that users will retake the control over personal data. Focus on mechanism based on the operational transparency rather than information technology. So that Internet crime decreases and security increase.

 Provide transparency towards data handling techniques by cloud service provider during internet monitoring and cloud service provider must use strong encryption algorithms with strong encryption keys like RC2, RC4, 128-bit RC4, DESX, 128-bit AES, 192-bit AES, and 256-bit AES.

 Need to reduce the CTERA-Bridges gap between cloud and the local storage in CTERA network that provide ONLINE CTERA solution portfolio & also manage service provider base in US.

 Replace all existing applications with the "CIPHERCLOUD" environment that helps to provide new interaction with cloud based security services & data loss prevention (DLP) environment so cloud service MONITORING will become easy.

Need to design various new key cloud issues related to latency, bandwidth and various security standards.

 Challenge towards new designed methodologies based on data leakage, cloud credentials, snooping, key management and performance efficiency.

 Need to design a new procedure to secure dormant virtual machines in offline mode still available to any application that can access the virtual machine storage over the network & therefore susceptible to malware infection.

VII DATA SECURITY ALGORITHMS

To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption; two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption.

1. RSA

This algorithm is used for public-key cryptography. It is the first and still most commonly used asymmetric algorithm. It involves two keys- a public key and a private key. The public key is used for encrypting messages and known to all. Messages encrypted with the use of public key can only be decrypted by using the private key. In this authentication scheme, the server implements public key authentication by signing a unique message with its private key, thus creating what is called digital signature. The signature is then returned to the client. Then it verifies using the server's known public key.

2. MD5- (Message-Digest algorithm 5)

A widely used cryptographic hash function algorithm with a 128-bit hash value and processes a variable length message into a fixed-length output of 128 bits. First the input message is broken up into chunks of 512-bit blocks then the message is padded so that its total length is divisible by 512. In this, the sender of the data use the public key to encrypt the message and the receiver uses its private key to decrypt the message.

3. AES- Advanced Encryption Standard (AES)

It is a symmetric-key encryption standard. It uses 10, 12, or 14 rounds. Each of the ciphers has a 128-bit block size, with the key sizes of 128, 192 and 256 bits, respectively. It ensures that the hash code is encrypted in a highly secure manner. Its algorithm steps are as follows:

1. Key Expansion
2. Initial round
3. Add Round Key
4. Rounds
5. Sub Bytes
6. Shift Rows
7. Mix Columns
8. Add Round Key
9. Final Round
10. Sub Bytes
11. Shift Rows
12. Add Round Key.

VIII GOALS OF PROPOSED SYSTEM

1. To develop a system that will Provide Security and Privacy to Cloud Storage.
2. To Establish an Encryption Based System for protecting Sensitive data on the cloud and Structure how owner and storage Service Provider to operate on encrypted Data.
3. To Create a System where the user store its data on the cloud the data is sent and stored on the cloud in encrypted form As in normal cases in cloud computing when a user login to the cloud and they store data on cloud storage device the data stored on the server cloud is not much secure as it can be readable to anyone which have permission to access and leaving data vulnerable.
4. To Develop a retrieval System in which the data is retrieved by the user in encrypted form and is decrypted by the user at its own site using a public and private key encryption both the keys working at the user level.

PROPOSED SOLUTION

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

Key Generation

- Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.
- Encryption is the process of converting original plain text (data) into cipher text (data).
- Decryption is the process of converting the cipher text(data) to the original plain text(data).
- Secure inter-host communication channel
- Encrypt data in transit
- Secure key store
- Protect encryption keys
- Ensure encryption is based on industry/govt standards.
- No proprietary standard
- Limit access to key stores

Fig.3 represents the process of encryption and decryption.

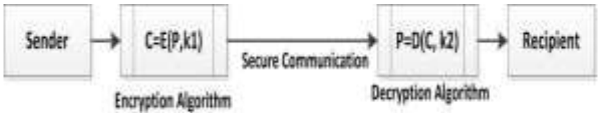

Fig.3 Encryption – Decryption Process

A framework or software is developed to enhance security while storing multimedia files which includes role base access control, encryption, signature verification**.** The framework would include a premium and normal user concept in which a normal user would get a normal speed where as the premium user would get more speed. To encrypt large messages a hybrid approach is used in which the messages are actually encrypted using symmetric schemes (TDES) and the key is transported using asymmetric schemes (Diffie Hellman Key Exchange). The combination of encryption algorithms encrypt the data files before storage on cloud. In our proposed architecture, firstly Diffie Hellman algorithm is used to generate keys for key exchange step. Then TDES encryption algorithm is used to encrypt or decrypt user's data file. All this is implemented to provide trusted environment. The signature is used for authentication, would be an image file. If the image file of the uploaded signature would match with the image file uploaded at run time, only then the data would be downloaded.

IX CONCLUSION

The strength of cloud computing is the ability to manage risks in particular to security issues. Security algorithms mentioned for encryption and decryption can be implementing in future to enhance security over the network. In the future, we will extend our research by providing algorithm implementations and producing results to justify our concepts of security for cloud computing. 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. Cloud computing opens several new trends, like using software that are not present on your computer, accessing data from anywhere. One of the big advantage of cloud computing is virtualization, but we can use cloud computing properly only if it provide reliable security. 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. Our research indicates that that Security and Privacy are the major issues that are needed to be countered, efforts are being made to develop many efficient System That can Provide Security and privacy at the user level and maintain the trust and intellectual property rights of the user. Our method States Encryption is one such method that can provide peace of mind to user and if the user have control over encryption and decryptions of data that will boost consumer confidence and attract more people to cloud platform.

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. Our goal is achieved through implementing encryption and decryption algorithm to provide more secured data to the organizations.

REFERENCES

[1] Caceres, Lindner, Vaquero, “A break in the clouds:towards a cloud definition”, [2008].

[2]Keahey, Fortes, Freeman, “Science Clouds:Early Experiences in Cloud Computing for scientific applications” [2008].

[3] Sachdev Abha Thakral, and Mohit Bhansali. "Addressing the Cloud Computing Security Menace." IJRET, Volume 2, Issue 2, pp. 126-130, Feb 2013.

[4] Chen, Yao, and Radu Sion. "On securing untrusted clouds with cryptography. “Proceedings of the 9th annual ACM workshop on Privacy in the electronic society. ACM, 2010.

[5] Shakeeba S. Khan and Prof. R.R. Tuteja, ‘Security in Cloud Computin Using Cryptographic Algorithms’, International Journal of Innovative Research in Computer and Communication Engineering. January 1, **(2015)** ISSN (online): 2320-9801, (Print): 2320-9798 Vol. 3, Issue.

[6] Maha TEBAA, Said EL HAJJI and Abdellatif EL GHAJI, ‘Homomorphic Encryption Applied to the Cloud Computing Security’, World Congress on Engineering. July 4 **(2012)** Vol. 1, London U.K. ISBN: 978-988-19251-3-8, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (online).

[7] Manzoor Hussain Dar, Pardeep Mittal and Vinod Kumar, ‘A Comparative Study of Cryptographic Algorithms’, International Journal of Computer Science and Network. June **(2014)** ISSN(Online): 2277-5420, Volume 3, Issue 3.

[8] Kashish Goyal, Supriya Kinger” Modified Caesar Cipher for Better Security Enhancement” International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013.

[9] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,”Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures” IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[10] 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.

[11] Tharam Dillon, Chen Wu, Elizabeth Chang, 2010 24th IEEE International Conference on Advanced Information Networkingand Applications ,“Cloud computing: issues and challenges”.

[12] Simarjeet Kaur, “Cryptography and Encryption in Cloud Computing”, VSRD International Journal of Computer Science and Information Technology, Vol.2(3), 242-249, 2012.

[13] Birendra Goswani, Dr.S.N.Singh, “Enhancing Security in Cloud computing using Public Key Cryptography with Matrices”, International Journal of Engineering Research and Applications, Vol 2, Issue 4, 339-344, July-Aug 2012.

[14] William Stallings, “Network Security Essentials Applications and Standards”, Third Edition, Pearson Education, 2007

[15] Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao, Cheng Fu, Xi He, Andrew Younge, Cloud Computing: A Perspective Study, New Generation Computing- Advances of Distributed Information Processing, Volume 28, Issue 2, April 2010, On page(s): 137-146.

[16] 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.