RESEARCH ARTICLE OPEN ACCESS

Privacy Protection in Cloud Using Rsa Algorithm

Amandeep Kaur*, Manpreet Kaur**
* (Department of Computer Science, MMEC, Mullana, Ambala)
** (Department of Computer Science, MMEC, Mullana, Ambala)

ABSTRACT
The cloud computing architecture has been on high demand nowadays. The cloud has been successful over grid and distributed environment due to its cost and high reliability along with high security. However in the area of research it is observed that cloud computing still has some issues in security regarding privacy. The cloud broker provide services of cloud to general public and ensures that data is protected however they sometimes lag security and privacy. Thus in this work of research an architecture is developed to preserve the security in two phases that is by RSA algorithm and auto-backup policy.
Keywords:- cloud computing security, Privacy protection, RSA algorithm, encryption, decryption.

I. INTRODUCTION

Cloud Computing

Cloud computing is a general term that delivers hosted services over internet. It connects multiple users to a single computer processor through dumb terminals, which have a keyboard and a monitor, but the computing is done by central machine. We don't need to keep our music, photos and important documents in our computer's hard drive. Cloud computing provides more space to store our all digital property. Cloud computing works on pay-per-use basis. User can use as much data as required and at any time. User only needs personal computer and internet access.

Data security is an important aspect of quality of service. So, security must be imposed on data by using some encryption schemes so as to achieve secured data storage and access. Because of opaque nature of cloud, it is still having some security issues. Since the data are not stored in the client area, implementing security measures cannot be applied directly. In this work of research we will implement RSA algorithm before storing the sensitive data in the cloud. When the authorized user request for the data then data is decrypted and provided to the user.

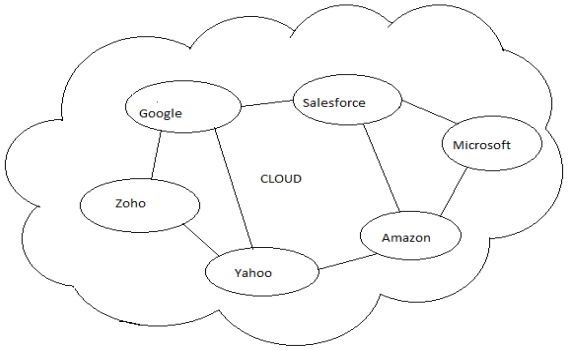

Figure 1: Cloud computing environment

Characteristics

Characteristics	Description
Scalability	Ability to meet higher demand without degrading the system
Manageability	Ability to manage system with minimum requirements
Control	Ability to control system in terms of cost, performance, scalability etc
Multi-tenancy	Ability to support multiple users at a time
Data availability	Ability of system's uptime
Elastic	Ability to adjust readily to different conditions
Pay-per-use	User pays according to his usage of data

Table 1: Characteristics of Cloud

Types of cloud

Cloud can be categorized as follows [1]

– Public clouds sells services to anyone on internet. Here all the resources like applications and documents are available to general public.

– Private clouds are internal clouds. These type of clouds can be accessed and used by individuals inside the organizations. It is only available to limited number of people.

– Hybrid clouds bring together public and private clouds, resulting in hybrid clouds. It shows the characteristics of both public and private clouds maintaining scalability and cost effectiveness. Here some data is stored in public cloud and other in private cloud according to requirements.

Categories

Basically there are three types of cloud services: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [2].

IaaS provides computing infrastructure. It delivers computer infrastructure like physical or virtual machines. Some other resources are virtual-machine disk image library, networking technology, firewalls, data center spaces etc. Examples Amazon, GoGrid, Rackspace.

PaaS (Platform as a service) provides computing platforms which includes everything needed by developers to build and run application. Like operating system and programming language execution environment. Examples Microsoft Azure, Heroku, Salesforce, Google App Engine.

Saas (Software as a service) model are provided with access to application softwares. Theses softwares are hosted by cloud providers. These are also referred as on demand softwares. Service provider will do installation and setup work. You just need to pay and use it. Examples Google Apps, Netsuite,CRM.

Compared with traditional It model, cloud computing has many advantages but from consumers' prospective, security of cloud computing remain a major barrier for adaptation of cloud computing. In our work of research we will encrypt the data in cloud with help of RSA algorithm and provide backup of our data. This will help retain the users level of trust on cloud storage providers and thus gives the new shape to further research on mobile cloud computing as well as general cloud computing.

This paper describes data security and privacy protection issues in cloud. In this paper Section II gives brief introduction of data security issues in cloud. Section III describes current security solutions for data security and privacy protection. Section IV explains purposed work Section V describes RSA algorithm that helps in providing privacy protection in cloud and Section VI summarizes the contents of this paper and Section.

II. SECURITY ISSUES IN CLOUD

Privacy and confidentiality:

Once the data is hosted to cloud, there should be no unauthorized access to data. Unauthorized access to data pose potential threat to cloud data. It should assure data safety and confidentiality.

***Data integrity*:**

Integrity of data should be maintained in cloud. It should be able to tell what happened to particular dataset and at what time. Input and output of data should not vary to ensure that data is not modified, origin and custody of data or information must be maintained.

Data availability:

In cloud computing availability of uninterruptable and seamless provision of data becomes an important issue. Here data is stored on different servers and locations, therefore data availability should be assured.

Backup and recovery:

Once data is hosted to cloud, cloud providers should be able to provide backup services that help in serious hardware failure. User can roll back to earlier stage to prevent data loss. Cloud provider should also assure adequate data storage system [2].

Data location and relocation:

Data is highly mobile in cloud computing. If consumer wants to know location of his data, there should be agreement between consumer and cloud provider. Data can also be moved from one location to another, therefore cloud provider should ensure security of information [3].

III. CURRENT SECURITY SOLUTIONS FOR DATA PRIVACY PROTECTION

IBM developed homomorphic encryption scheme in 2009. It allows data to be processed without decryption. Roy I and Ramadan HE applied differential privacy protection technology in data generation calculation stages in cloud and purposed airvat [4]. It prevents privacy leakage without authorization. Main problem is key management for data encryption in cloud computing. Users need enough expertise to manage their keys and on the other hand cloud service providers need to maintain large number of keys. The Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP) is trying to solve this problem [5].

In case of data integrity verification, user cannot first download data then verify its correctness and again upload data. Data is dynamic in cloud therefore traditional data integrity solutions cannot be used. NEC Labs's provable data integrity (PDI) solution can help in data integrity verification [6]. Cong Wang proposed a mathematical way to verify the integrity of data dynamically stored in the cloud [7]. Randike Gajanayake developed a privacy protection framework based on information accountability (IA) components [8]. The IA agent can identify the users who are accessing information and what type of information they are using. When any inappropriate misuse is detected, then agent defines a set of methods that can hold the users responsible for misuse of data.

Cloud storage solutions come in all sizes and shapes. Dropbox is very simple to use. It creates

a folder on hard drive that is linked to web. To upload files we can simply drag them to folder. Windows Live Skydrive make it easy to view and edit office documents in cloud. Amazon's Cloud Drive gives 5 gigabytes of storage and a Web interface for uploading files. Other services like SugarSync and Mozy, focus on automatically backing up important data and storing it, rather than make it easily accessible online[1].Smartest way to backup your data is to not rely on one service. Store the files that are accessed more frequently in Dropbox and back up more data in Amazon Cloud Drive service which is free and keep a local backup on some secondary hard drive.

IV. PURPOSED WORK

Security of data is of primary concern in cloud computing. To provide security of data in cloud computing we can use RSA, DES, homomorphic or AES algorithm [9] . In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the authorized user can access it. By securing the data, we are preventing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When data is required, Cloud provider first authenticates the user and then delivers the data.

The following table shows characteristics of existing algorithms.

Characteristics	**DES Algorithm**	**RSA Algorithm**	**Homomorphic Encryption**
Platform	Cloud computing	Cloud computing	Cloud computing
Keys Used	Same key used for both encryption and decryption	Different keys are used for encryption and decryption .	private key is used without decryption
Scalability	It is scalable algorithm due to the varying key and block sizes	Not scalable	scalable decryption
Security applied to	Both providers and client side	Client side only	Cloud providers only
Authentication Type	Message authentication used	Robust authentication implemented	Authentication never used

Table 2: characteristics of existing algorithms

V. RSA ALGORITHM

RSA is Public-Key algorithm. It has been developed by Ron Rivest, Adi Shamir and Len Adleman in 1977[3]. We use RSA algorithm to encrypt the data so that no unauthorized user access it. It provides security of data in cloud. User data is first encrypted and then it is stored in the Cloud. When data is required by user Cloud provider authenticates the user and then delivers the data. RSA is like a block cipher, where every message is mapped to an integer. It consists of Public-Key and Private-Key. Pubic-Key is known to all, but Private-Key is known only to the user who owns the data. Therefore, encryption is done by Cloud service provider and decryption is done by the Cloud user. When the data is encrypted with help of Public-Key, it can only be decrypted with the corresponding Private-Key.

RSA algorithm involves three stages:

1. Key Generation
2. Encryption
3. Decryption

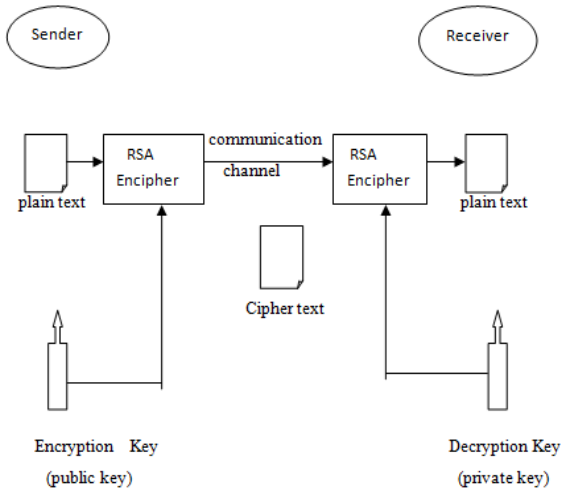

Figure 2: Overview of RSA Algorithm

VI. CONCLUSION

Cloud Computing is still an evolving paradigm where computing is on-demand service. Once the organization moves to the cloud, it faces many security issues. Thus, the amount of protection needed to secure data in cloud is directly proportional to the value of the data stored. Security of the Cloud can be improved by trusted computing and cryptography. Thus, in our proposed work, we used RSA algorithm to provide security where only the authorized user can access the data. Even if some unauthorized user gets the data accidentally or intentionally and he captures it, he cannot decrypt it and get back the original data from it. Therefore, data security is provided by implementing RSA algorithm.

REFERENCES

[1] Rupali Sachin Vairagade, Nitin Ashokrao Vairagade "Cloud Computing Data Storage and Security Enhancement," International journal of Advanced Research in computer engineering & technology, Vol. 1, august 2012

[2] Prof.Rupali Bagate, Prof.Archana Chaugule "Cloud architecture and security measures". International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 1, No. 2, November 2012.

[3] Parsi kalpana, sudha singaraju " Data security in cloud computing using RSA algorithm," International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[4] Roy I, Ramadan HE, Setty STV, Kilzer A, Shmatikov V, Witchel E. "Airavat: Security and privacy for MapReduce," In: Castro M, eds. Proc. of the 7th Usenix Symp. on Networked Systems Design and Implementation. San Jose: USENIX Association, 2010.

[5] Subhash Sankuratripati, Saikat Saha, Robert Lockhart **"**OASIS Key Management Interoperability Protocol (KMIP)," Advancing open standards for the information society,2012.

[6] Zeng K, "Publicly verifiable remote data integrity," In: Chen LQ, Ryan MD, Wang GL, eds. LNCS 5308. Birmingham: Springer-Verlag, 2008.

[7] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," in Proceedings of the 17th International Workshop on Quality of Service,2009.

[8] Randike Gajanayake, Renato Iannella, and Tony Sahama, "Sharing with Care An Information Accountability Perspective," Internet Computing, IEEE, vol. 15, pp. 31-38, July-Aug, 2011.

[9] Dr.A.Padmapriya, P.Subharshi "Cloud Computing: Security Challenges & Encryption Practices," International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, March 2013.