International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.4, April 2013 DOI:10.15693/ijaist/2013.v2i4.39-42

# Enhancing Cloud Storage Security and Privacy

Mohit Marwaha
Department of CSE
PTU, Jalandhar, India

Rajeev Bedi
Assistant Professor/Department of CSE
PTU, Jalandhar, India

Dr. S.K. Gupta
Associate Professor/ Department of CSE
PTU, Jalandhar, India

***Abstract***— **The Cloud computing is blend of conventional computing technology and network technology like grid computing distributed computing, parallel computing, web hosting and so on. It tries to develop a powerful computing platform at relatively low cost by using the advanced business models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to hand out the powerful computing capability to the user. Cloud computing provides a new model for IT service delivery and it typically involves over-a-network, on-demand, self-service access, which is dynamically scalable and elastic, utilizing pools of often virtualized resources making cloud computing the next big thing after internet. But question Questions about cloud data protection, data privacy and other Security issues may continue to linger and are cited as the most substantial roadblock for cloud computing uptake. We are trying to develop an encryption based system to contour these problems [17].**

***Index Term- Cloud Computing, Privacy, Cloud Computing Security, Encryption.***

## I. INTRODUCTION

In short interval of time cloud Computing has emerged as promising business concept to one of the fastest growing segments of the IT industry. Cloud computing is an evolutionary form of grid computing, utility computing, Distributed Computing and Business Computing. It Represents a Development trend of the IT industry that started with commencement of hardware to software, software to service, Distributed services to centralized services. Cloud Computing provides the user with the business centric view of technology where applications and Services are provided through purchase, rental or even development at the will of the user. Cloud Computing provides a Service Oriented architecture Infrastructure with rapid provisioning of IT resources, massive scaling, Dynamic service management and Energy saving via auto workload distribution. It is basically an application that provides users to log in to a web based service which hosts all the programs required by the user to accomplish his job through a simple internet connection there by reducing the Processing burden on the user's terminal end. Even though cloud computing has many advantages but it came down to its major disadvantage that is its Security that is a major Area of Concern for people to shift to cloud computing.

## II. Major Concerns

Security, Privacy and Intellectual property put the major threats on growth of cloud computing that are needed to be worked upon. Basically, a cloud storage system can be considered to be a network of distributed datacenters which typically uses cloud computing technologies like virtualization, and over some kind of interface for storing data. To increase the availability of the data, it may be redundantly stored at different locations. In general, all of this is not visible to the user. As Cloud storage is fast becoming the tool for file sharing the security of data on these cloud facilities become more important the authorization and authentication of user and threats of hacking and cracking are also areas of major concerns [9].

In a recent survey by website www.computerworld.com they quoted "that cloud user chose "security concerns" (40%) as their top issue. Storage capacity limits was second with (25%) people choosing it; file synchronization limitations was third with (15%); slow responses, fourth with (10%) and "other" (5%). As of June 2012, about 7% of personal data was stored in the cloud, but that number is expected to climb to 36% by 2016, according to market research firm Gartner [15]."

Recent issue reported by Dropbox a leading cloud storage service provider were hacking of accounts, problems with privacy policies as opening of account without passwords has demoralised cloud service provider. Similarly users of Google drive also reported incidents like losing folders and password hacking.

All in all these issues with public cloud Storage Facilities are not helping user sentiments and causing doubts in the mind of user who wants to use these services. The nervousness of someone else controlling your data is still in the mind of the user that is needed to be removed. As cloud storage service providers provider exciting features like pay-as-you-go model where you don't need to buy equipment in sense of future planning as your requirement increase you can just demand for more resources by paying a fraction of amount for the services as compared to buying a whole new equipment to support your operations. But for all this you have to trust your vendor and according to many security experts the word of advice is to proceed with caution. And resent attacks on cloud storage providers has fuelled this argument.

## III. Possible Solution

There are five parameters for security requirement that can make cloud safe these parameters and their objectives are (i) Registration and Login, to protect against incrimination, information gathering and to enforce usage of strong passwords. (ii) Transport Security, to secure communication between client and server. (iii) Encryption, to disable the provider to examine stored data. (iv) Secure File Sharing, to protect documents shared by a closed group, optionally including non-subscribers. (v) Secure De-duplication, to avoid privacy problems when using de-duplication [15].

Out of five parameter we have choose encryption as the method to work upon as we can use Cryptographic techniques to address the issues of security and privacy , encryption of data can be used to ensure Data confidentiality. The security vulnerabilities, external attack and internal attacks within the cloud storage service provider it is necessary to save data from these successful security attacks and maintain the confidentiality of data. The solution to this problem is to store data in encrypted form. There are several cryptographic techniques but some cloud service provider generally encrypt there data using their company's key which is only known by them to save data from external attacks but does not protect the data from the threats within the cloud service provider.

So if user is provided with facility to encrypt his own data and there are two different keys to encrypt data one is the public key and the other is the private key that is only known to the user it will take care of many security issues like in case of external attacks because data being encrypted it will be of no use for the attacker and in same way in case of internal attack because the private key is available with the user internal personnel may not be able to misuse the data of the user. We have specifically used RSA algorithm for this as it is the only algorithm with two keys a public key to encrypt the data and private key to decrypt the data. The user himself has the privilege to encrypt his data and decrypt the data that he wants to upload on cloud. The user gets the private key of the data he wants to encrypt on his e-mail. Thus making it secure for the user maintaining privacy as well as intellectual property rights. Cloud Computing Provides a service oriented architecture infrastructure, rapid provisioning of IT resources, massive scaling, Dynamic service management, Energy saving via auto workload distribution. Cloud computing enables an economic paradigm of data service outsourcing, where individuals and enterprise customers can avoid committing large capital outlays in the purchase and management of both software and hardware that was all laid down by few issues and once we will be able to resolve most of the issues Cloud Computing will become a massive billion Dollar industry that will change computing completely.

## IV. System Objectives

1. To develop a system that wills Provide Security and Privacy to the data stored on Cloud.

2. To Establish an Encryption Based System for protecting Sensitive data on the cloud and Structure how data owner and storage Service Provider to operate on encrypted Data

3. To develop a retrieval System in which the data is retrieved by the user 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 [17].

## V. Simulation Setup

We have developed web Application using ASP.NET that works as the front end of our cloud system and Windows Azure Microsoft cloud platform to provide infrastructure as a service for the storage. We have used two services of Windows Azure SQL Datacenter and its storage Facility. To provide Security and privacy we have applied RSA and DES encryption algorithm for data security and privacy in cloud Storage by giving user rights to encrypt and decrypt his own data. Ant colony optimization (ACO) technique has been used so that the servers that are communicating with each other, no one server out of them has complete information about the data. As the information about data is distributed among different servers it makes system even more secure from threats of Hackers and Crackers.

RSA is an algorithm for public-key cryptography is used for encryption that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. We have specifically used RSA algorithm for the reason being it's the only asymmetrical encryption algorithm [1]. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. But limitation with RSA algorithm was it was suitable to encrypt the text data but with audio and video files it was very difficult and inconvenient. So to solve this problem we have used DES (Data encryption Standard) to encrypt Audio and video files. DES is the archetypal block ciphers its uses symmetric key to encrypt the data although DES is not a very strong encryption standard we have meshed it with RSA to make it stronger. All the information about the data that we enter is encrypted by RSA. Audio and Video files are encrypted by DES so even if we want to download a audio or video file we have to give the private key only then we are able to download so even though DES is not a strong cryptographic technique but to make it stronger we have merger it with RSA encryption technique thus providing stronger encryption thus better protection to user.

## VI. Results

1. Through our system we are able to provide Security and Privacy to Cloud Storage.

2. The RSA and DES Encryption Based System protects sensitive data of user on the cloud and provides owner with privilege to encrypt and decrypt data on his will.

3. In our System the user can store its data on the cloud the data in encrypted form, An Email containing the decryption key is sent by the system regarding the file he has saved and when the user want to decrypt the data he has to uses that decryption key in the system and file will be loaded on his system.

4. Our system was able to overcome problems of Data Security, Privacy, Trust and Intellectual Property Rights

## VII. CONCLUSION

Cloud computing enables an economic paradigm of data service outsourcing, where individuals and enterprise customers can avoid committing large capital outlays in the purchase and management of both software and hardware that was all laid down by few issues and once we will be able to resolve most of the issues Cloud Computing will become a massive billion Dollar industry that will change computing completely. The Data storage on un-trusted cloud makes data security and privacy a challenging issue. To make data more secure and private, a data access policy and confidentiality of sensitive data should be enforced on Cloud storage service providers. Cryptographic techniques are applied to address this issue, encrypted data are stored on storage servers while secret key(s) are retained by data owner; access to the user is granted by issuing the corresponding data decryption keys. In this thesis we have discussed an important issue of data storage security and privacy on cloud storage facility. We investigated the challenges pertained to this problem and proposed an idea of using RSA encryption algorithm to provide cryptographically enforced data access control for providing a complete cryptographic basis for data storage on un-trusted cloud storage facility [12] .

In this paper we have tried to build a system that will provide security and privacy to cloud data storage. We have used RSA algorithm for this as it is the only algorithm with two keys a public key to encrypt the data and private key to decrypt the data. The user himself has the privilege to encrypt his data and decrypt the data that he wants to upload on cloud. The user gets the private key of the data he wants to encrypt on his e-mail. Thus making it secure for the user maintaining privacy as well as intellectual property rights. DES data encryption standard is used to encrypt the multimedia content as RSA was not suitable for this job with this we have used ACO Ant colony optimization for solving computational problem it is used to store data in an optimum form so that awareness of placement of data is not known to anybody not even the service provider. We have used Windows Azure which is the Microsoft's application platform for public cloud and have used Azure to build a Cloud application that runs and stores its data in Microsoft datacenters. ASP.Net platform is used to develop the application that interacts with Windows Azure and together they work as cloud application. Our results show that our proposed scheme is securer as compared to standard cryptographic models. And we were able to achieve our objectives.
In future work, there are different paths in which we can peruse for secure data sharing and Performance enhancement:
Decentralised Access Control: we know that in this dissertation there is a owner who acts as the only authority in every cryptosystem. If a user wants to access data, there is a particular secret key for each cryptosystem. But if we see this system in large scale, there is need of decentralized access control. With the help of this, a user can access multiple cryptosystem using a single secret key and in the same way, we allow the existence of multiple authorities in an application and encryption of data using public keys assigned by multiple authorities. The solution for this problem is the concept of decentralization. So it is necessary to enhance decentralized and hence provide decentralized data access control for un-trusted storage [10].

**Operation on Encrypted Data:** As encryption provides data confidentiality but also creates problem for flexibility of data operation. For this issue, we need to incorporate searchable encryption, private information retrieval and homomorphic encryption to enable computation on encrypted data without decrypting the data. Another future work would be taking into account information theoretic techniques from the areas such as database privacy.

**Combining with secure computation:** Advanced architecture that allows parallel processing of user data, providing a mechanism for users who don't believe in the third party service and allowing user to define the hotspots in the data. These features can be implemented with our approach and can provide user with a better working and a user friendly environment.

Provable Data possession: This model can ensure can ensure that possession of file on un-trusted cloud storage this system can make it mandatory for service provider to provide the user with an authenticated list of his files in case of missing or alteration in files the service provider can be held responsible.

**Dynamic data computation:** Our approach work on static data that is when data is not needed to change frequently and frequent computations are not needed on the data but for the data that needs constant updates and that is dynamically changing we need a dynamic data computation facility that provides security and privacy with less overheads.

**Performance of cloud:** While working with cloud the major hurdle experienced by us was unpredictability of cloud mainly its performance that depends on various factor the major being the speed of our internet connection and load on the system also played a major role so future work we would like to propose a structure that makes user aware about the lapse time and show the performance of the system on a monitor dashboard so the user is aware about the capability and performance of the cloud. As service level agreement should be there with user and the cloud service provider **[14].**

## References

[1].http://en.wikipedia.org/wiki/Cloud_computing.

[2]. Rich Maggiani, solari communication. “Cloud computing is changing how we communicate”.

[3]. Randolph Barr, Qualys Inc, “How to gain comfort in losing control to the cloud”.

[4]. Greg Boss, Padma Malladi, Dennis Quan, Linda Legregni, HaroldHallHiPODS,www.ibm.com/developerworks/webspere/zones/hipds.

[5]. http://www.roughtype.com.

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

[7].http://server.zol.com.cn/183/1830464.html.

[8]. Elinor Mills, January 27, 2009. “Cloud computing security forecast: clear skies”.

[9]. Jianchun Jiang, Weiping Wen, “Information security issues inCloudcomputingenvironment,NetinfoSecurity,doi:10.3969/j.issn.16711122.2010.02.026.

[10]. Jianchun Jiang, Weiping Wen, “Information security issues in cloud computing environment”, Net info Security,doi:10.3969/j.issn.1671- 1122.2010.02.026. Of virtual machines” In Proc. Of NSDI’05, pages 273-286, Berkeley CA, USA, 2005. USENIX Association.

[11]. Eucalyptus Completes Amazon Web Services Specs with Latest Release.

[12]. Open Cloud Consortium.org.

[13]. July 27, 2009. Available from http://fx.caixun.com/.

[14]. Jack Schofield. Wednesday 17 June 2009 22.00 BST, http://www.guardian.co.uk/technology/2009/jun/17/cloud- computing jack- schofield.

[15]. Gartner. “Seven cloud-computing security risks”.

[16]. Ranjita Mishra “A Privacy Preserving Repository for Securing Data across the Cloud”.

[17] Mohit Marwaha “Designing Data Storage Security and Privacy in Cloud Computing” International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682 Vol.8, No.8, December 2012.

## Authors Profile

**Mohit Marwaha** received the **B.Tech.** degree in Information Technology from the Beant College of Engineering and Technology, Gurdaspur, Punjab Technical University, Jalandhar, India, in 2008. Currently pursuing **M.Tech.** in Computer Science engineering (cloud computing) in Punjab Technical University, Jalandhar, India. My research interest includes Cloud Computing, Distributed computing and Network security

**Rajeev Bedi** received the **B.Tech.** degree in Computer Science and Engineering from Punjab Technical University, Jalandhar, in 2000 and completed **M.Tech.** in Computer Science engineering from Punjab Technical University, Jalandhar, in 2008. Currently doing PhD from CMJ University Shillong. My research interest includes Cloud Computing and Distributed computing.

**Dr. S.K.Gupta** has done B.E. in Computer Science Engineering from M.M.M. Engineering College, Gorakhpur, India in 1988. He completed postgraduation in Engineering from BITS, Pilani in 1992 and got Ph.D. in 2011. He has 24 years of teching experience. He has served in many reputed Engineering Colleges like R.E.C., Hamirpur (Presently NIT, hamirpur). At present, he is working as Associate Professor and Head of department, Computer Science & Engg. in Beant College of Engineering and Technology, Gurdaspur, Punjab. He has several research publications to his credit. His area of interest are distributed systems, mobile computing, database management systems, mobile adhoc networks.