ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Review towards Preserving Data Security and Integrity in Cloud Environment by using RSA Partial Homomorphic and MD5 Cryptography Algorithm

Rushvi Rajkumar Jaiswal, Prof. Vijay B. Gadicha

M.E Student, Dept. of CSE, P.R.Pote (Patil) College of Engineering and Management, Amravati, India

HOD, Dept. of CSE, P.R.Pote (Patil) College of Engineering and Management, Amravati, India

ABSTRACT: As the usage and storage of data is growing on increasing along with the use of internet. So, this will required the flexibility of storing unlimited data without any worry about storage limitations. Along with storage this data should be available to all and required the freedom to use it whenever required. This makes cloud computing the most preferred technology & platform to store and transfer data. Currently, lots of organizations and individual users are very much comfortable to store their important data and software on the cloud servers and make themselves free from all the concerns of storage and access. But at the same time, there is a threat of user's privacy, data confidentiality & integrity. Among all of these, the secure transfer of data from organization's premises to the cloud servers and from cloud server to authenticated users is of upmost importance. For this purpose, here, the proper encryption and cryptographic techniques based on RSA Homomorphic encryption and MD5 Hashing techniques are proposed. This stores data securely from the client's to server, with the Cloud Service provider (CSP). We have used a combined approach of encryption and cryptography because it will provide a two way security to the data that is being transmitted on the network. At the reverse side, Cloud Service Provider (CSP) perform the authentication and authorization of the user who is going to access any document from the cloud storage.

KEYWORDS: Cloud Computing; RSA encryption, MD5 cryptography, Data Security & Integrity.

I. INTRODUCTION

The Cloud computing is becoming future of the next generation architecture of IT solutions. It defines a framework for delivering IT as a service in most efficient and the fastest way possible, without actually purchasing that resources [1]. The Cloud computing is also called as a type of computing that relies on sharing computing resources rather than having local servers to personal devices that handle applications. Here, different services are offered such as data storage, application storage, Software services, etc. that are delivered to an organization's computers and devices through the Internet [2]. Cloud computing technology apply super-computing or high-performance computing power to perform tens of trillions of computations per second. This computations are mostly effective in consumer-oriented applications such as financial portfolios, delivering personalized information, provide data storage or to power large, immersive online computer games, etc. So, cloud computing technology serves effective and important in all the areas of software technology [3].

Despite of all the advantages of the cloud there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public environment and shared in cloud environments. The security threats consist of data breaches and actual loss of data, traffic hijacking, insecure APIs, malicious insiders, and many others [4]. By exploiting vulnerabilities in Cloud, an adversary can launch many attacks that definitely effects on the data, applications, software's, user authentication information and in many other ways.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

To ensure the cloud computing data security, we usually use Encryption methods as a central technology. Here for the purpose of strong security, as the cloud contains most important data and software's, a new approach is defined in which firstly the data is encrypted by RSA Partial Homomorphic algorithm and then it is uploaded on cloud servers [5]. In this approach each client can generate their public and private key. In which public key is known to all and private key is only known to the client or authorized users. One another feature added here is, after the encrypted data is securely uploaded to cloud server its back up is also get generated. This is done by calculating the hash value of the file stored by using MD5 algorithm and its secure back up is sent to the data owner in terms of hash value.

So, as the cloud computing is the necessity of all the application areas, this paper performs the study of literature consisting the work done by different researchers in the field of cloud computing. Different methods applied by them to securely store and maintain the data in the public cloud environment. This paper also collects the information regarding different cloud service providers and proposed his own model of building and using cloud servers. The remaining paper is organized as Section II gives The Literature Survey containing related work done by different authors and gives the information about different drivers of cloud computing environment. Section IIIgives the proposed methodologycontaining basic idea for developing our system and designing of working system. Finally, Section IV concludes the paper.

A. MOTIVATION:

As the cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort and service provider interaction. Then at the same time it is necessary to know the different security techniques being used to protect privacy on cloud for its different services. The leading Cloud Computing providers, to prevent active and passive attacks when the data is being transferred between the Cloud and a local network? It is necessary to learn the various security techniques being used to prevent unauthorized access to data within the Cloud? What are the major security challenges we expect in future Cloud Computing andHow to handle these challenges? For that here, a prototype is mention that perform identification of security challenges and mitigation techniques in large number of services of Cloud Computing with the help of encryption and cryptographic techniques.

B. OBJECTIVES:

The idea behind this system is dedicated to achieve some of the following objectives.

- To implement a mechanism which incur the techniques for data security and integrity in cloud computing environment.
- To identify the major security threats and their corresponding remedial solution in cloud computing environment.
- To maintain data integrity to restrict data duplication or updation.
- To establish a secure mechanism for accessing and sharing of data from CSP.

C. SCOPE:

Cloud is a computing model that refers to provide services as pay per use basis. It provide large platform for providing applications, software's, databases and many more on the basis of services. And one can use them whenever required. Here the main focus is of data i.e. Database-as-services. If it is stored in cloud in secure manner and available to access whenever required to only authorized persons, it has large scope of applications. Data for the banks - for maintaining customer's information, balance, pin number, transaction, data. For Governmental organizations – Housing department papers, Agriculture departments, Municipal Corporation related data, and all sectors of government required secure storage for large amount of data. In private sectors also, all companies requires their documents like employee information, their projects related data, customers related data and all transaction details required secure storage. This show that the scope of the secure data storage cloud is much large and can say must for many of the online service provider.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

II. LITERATURE SURVEY

A. HISTORICAL BACKGROUND:

Cloud Computing is rapidly being accepted as a universal access appliance on the Internet. Cloud computing is an emerging technology in the field of networking. It is gaining popularity in all areas. The National Institute of Standards and Technology (NIST)[6] defines cloud computing as a model for enabling ubiquitous ,convenient, on demand network access to a shared pool of configurable computing resources. In simple words cloud computing is a computing model in which resources are provided to the users based on their demand. In cloud computing resources are provided by the cloud service provider known as CSP [7]. Even though, the virtualization and Cloud Computing delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud which makes the users to resist themselves in adopting the technology of Cloud Computing.

B. RELATED WORK:

The authors in [2] has proposed a system by first highlighting the cloud types, its characteristics, background of cloud environment and also addresses some of cloud issues and challenges that are faced nowadays. Bearing in mind all these things author discuss symmetric and asymmetric encryption algorithms and then proposed a system that forms a cipher cloud to which user will not need any of the resources or software to encrypt the data. Keys are generated instantly and choice of encryption algorithm is also provided to the user to which they want. This makes the cloud environment more efficient.

The authors in this paper [3], propose fully homomorphic encryption auditing system for the data storage security in the cloud computing. They have integrated the fully homomorphic encryption in TPA auditing system. Proposed scheme of fully homomorphic provides auditing technique which not only preserves privacy but also provide authenticator that allow an unbounded number of verification. But this system also has to verify its approach practically and to add experimental analysis to derive some conclusion from it. The proposed scheme is being theoretically approached. After implementating this scheme author id intended to add experimental analysis and derive some more experimental validation and conclusion in future.

The authors in [6] perform the detailed study of advantages and disadvantages of storing data on cloud. Then work on the existing scenarios of security and what are their drawbacks and concluded that, Data security has become the most important issue of cloud computing security. They find out that the FHE Fully Homomorphic Encryption represents a big step in modern cryptography and opens new challenges to cryptology researchers and also it helps the new IT technologies to be faster adopted. It is a new view of data security solution with encryption, which is important and can be used as reference for designing the complete security solution. But authors have to work further on the application of traditional and fully Homomorphic encryption schemes to a Cloud environment, Analyze and improve the existing cryptosystem to allow servers to perform various operations requested by the client using openstack cloud.

The authors in this paper [7] said that to secure cloud data storage it is a good practice toapply a third party auditing schemes. A client willleave the work of public audibility to third partyauditor but sometimes they may also be unreliableand it is possible that they do not verify the client'sdata periodically. In this system, authors have proposedsimultaneous audibility with data dynamics for datastored in remote cloud computing storage. They tried to resolve both issues of publicaudibility and dynamicity of remote data.Efficiency is another major concern for this scheme, for making the scheme more efficient authors use theMerkel hash algorithm for tagging blocks forauthentication. Here, the scheme with Third party authenticator i.e. (TPA) is used for the purpose of efficiency. This scheme can be connect with mobile gateway so that aTPA can immediately generate the reports to ourmobile phone. Along with this, the newscheme suggested here can further supports secure and efficientdynamic operations on data blocks stored in the cloud, including: data update, delete and append.

The authors in this paper [8]find out that, earlier algorithms are implemented on local processor system, but now encryption and decryption techniques are implemented on cloud network too. It clearly indicates the need of more resilient algorithms for cloud network. Homomorphic cryptosystems have also added new challenges towards the secure and fast execution of programs on cloud. The results are obtained on the basis of Speed-Up Ratio and Total Execution Time parameter on varying input sizes. All the algorithms are applied on both the cloud network and local system. Comparative analysis of all the different cryptographic algorithms reveals many facts about cryptographic algorithms execution on cloud network. Some of these algorithms, like homomorphic algorithms, have to pass a long

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

way before their actual implementation on cloud. My further research work is to test more homomorphic schemes which may be used as zero knowledge proof algorithms on cloud network.

The authors in this paper [9] find out that, amajor hurdle to the adoption of cloud-based services is security. They have address the construction of an efficient PDP scheme for distributed cloud storage to support the data security and integrity, in which author consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. They presents a Cooperative Provable Data Possession(CPDP) scheme based on Homomorphic verifiable response and hash index hierarchy. Their proposed system provides security for data and integrity by using fully homomorphic encryption in a multi cloud environment by using Depsky model. Depsky model which is virtual storage cloud system that consists combination of different clouds to build a cloud of cloud. They are providing a scheme which could audit data integrity without decrypting it. After this implementation they have concluded that proposed fully homomorphic encryption auditing system for the data security and integrity in the multi cloud provide better security. Authors have integrated the fully homomorphic encryption in TPA auditing system. Proposed scheme of fully homomorphic provides auditing technique which not only preserves privacy but also provide authenticator that allow an unbounded number of verifications.

The authors in this paper [10] suggest that, Cloud computing is an emerging technology that will receivemore attention in the future from industry and academia.The cost of this technology is more attractive when it iscompared to building the infrastructure. However, there aremany security issues coming with this technology as happenswhen every technology matures. Those issues include issuesrelated to the previous issues of the internet, network issues,application issues, and storage issues. Storing data in a remoteserver leads to some security issues. Those issues arerelated to confidentiality of data from unauthorized people inremote sites, integrity of stored data in remote servers and theavailability of the data when it is needed. Also, sharing data incloud when the cloud service provider is mistrusted is an issue. Authors have mentioned some techniques that protect data seenby the cloud service provider while it is shared among manyusers.Many studies have been conducted to discover the issuesthat affect confidentiality, integrity, and availability of data tofind a solution for them. Those solutions will lead to moresecure cloud storage, which will also lead to more acceptancefrom the people and the trust on the cloud will increase.

The authors in [11] suggested thatSecurity is the key for the success of the cloud environment. In order to avail the benefits of cloud, one has to ensure the security of data being transferred between the client and user. New attacks have been appearing day by day and we need some strong mechanism to handle with all the types of attacks. In this work authorshave proposed a new security solution by using the hybrid combination of encryption algorithms link AES and RSA. They have used, the MD5 hashing algorithm along with some other encryption algorithms for the verification process.

The authors in [12] studied and finds the results of the technique may show the improvement in providing the security with feasible operations on cipher using partially homomorphic cryptosystems that is most suitable for outsourced cloud environment. This improved encryption is faster and less computational overhead is involved. It provides the high end reliability towards the new orientation of the system. The third party mechanism deals with continuous monitoring of user record. This monitoring along with improved throughput and efficiency is achieved. Out of these methods an enhanced secure scenarios is generated through our proposed TPA-HE. At the initial level authors identified that this scheme is has benefits asimproved security solution with less operational overheads and retains reliability on novel encryptions, unauthorized access is blocked, Continuous monitoring gives the user behavior measurements and analyzes the affection of such novel cryptosystem on other services. But for the implementing it on large scale server platform one has to work further.

C. DRIVERS OF CLOUD COMPUTING SERVICES:

Cloud Computing is rapidly growing sector in the Computer Science and Information Technology field security space because the use of Cloud architectures are increasing by all over. The major companies present in the market that provide this important cloud services are Amazon, Microsoft, Google, IBM, Oracle, Eucalyptus, VMware, Eucalyptus, Citrix, Salesforce, Rackspace and there are many different vendors offering different Cloud services. Along with this the cloud providers are have different forms to provide their services as [13]:

- Amazon: Amazon Web Services including the Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), etc. Thisprovides a highly scalable computing platform to the customer with high flexibility and availability to build a wide range of applications.
- Google: Google App Engine
  - This is one of the most familiar service provider. It supports application programming interfaces(APIs) for the data store, image manipulation, Google accounts and e-mail services.
- Microsoft: Windows Azure Platform
  - This is mainly associated with Windows operating system users. This Windows Azure platform is a group of Cloud technologies which provides a specific set of services to application developers.
- Eucalyptus: Eucalyptus is an open source software infrastructure to create private Cloud architecture on existing enterprise.
- IBM: Lotus Live (Platform as a Service)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

- Salesforce: (Software as a Service)
- Rackspace Cloud: (formerly Mosso)
- VMware: Provide Virtualization infrastructure

All the above are cloud service providers and provides their services depends on users' needs that is differ from organizations and developers point of view. Users have to take the services according to pay-per-use basis.Some of the venders are free service providers, some offers free trials of some duration for developers point of view and some are taken by paying their necessary fees according to demand.

IV. PROPOSED WORK

A. BASIC IDEA:

The basic idea behind developing this project is, the users that are using this system should be authorized and authenticated at all the time they are using this system. For performing user's security check, MD5 algorithm is proposed. Now, for building personal system as cloud server, one has to take support of the driver that provide cloud computing services. And after building cloud server to our system, the platform should be build for securely storing our data files in the cloud server. For providing security to data file RSA partial homomorphic algorithm is proposed. With this file gets encrypted and securely stored on cloud platform. This file are make available securely to any user with the help of cloud service provider (CSP). After checking its authentication CSP sends file to that user.

B. Data Flow Diagram:

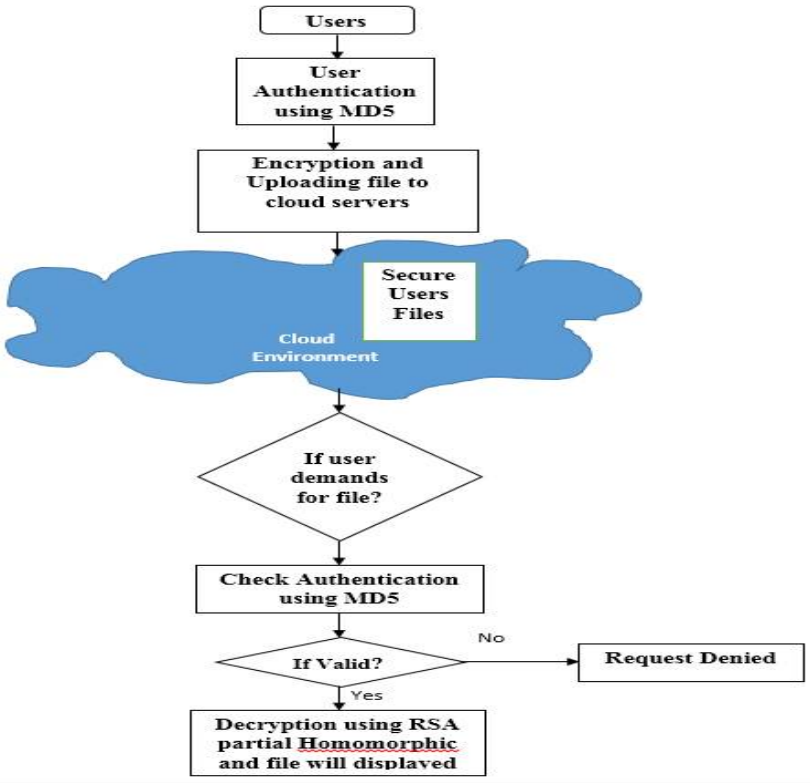

Fig. 1: Workflow of the proposed system

C. Stepwise Working of Proposed System:

- As the system is designed for secure data storage and access, all the users of the system are authenticated with their id and password that can be protected with hash value generation using MD5 algorithm.
- Then these authenticated user can upload files to cloud server designed

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

- Now for keeping the data/files secure these data is encrypted with the RSA homomorphic algorithm.
- The public and private key related with file is generated.
- After encryptions are performed file is uploaded on cloud servers.
- After uploading Data owner gets its general detail like uploading time, date, storage information.
- In this approach for maintaining data security access permission to the specified file is defined.
- Specified user get the file in encrypted form which can be decrypted by a private key which was generated at the time of encryption and provided to only authorize users.
- If anyone wants to access any data from cloud platform, this will be make available by cloud service provider which will first of all check the authorization of the demanding person
- If the person is authorized then, this file makes available to him by securely sending in encrypted format, and authorized person have key to decrypt it and open.

V. CONCLUSION

This research paper consisting of the idea about preserving data security and maintaining integrity of data in cloud computing services. As we know that, cloud computing environment are having numerous application in all over industry as well as for academic for providing computational services. Therefore this research paper gives an idea about implementation of cloud server on the personal system. After building the cloud for storing and accessing the data securely RSA and MD5 algorithms are proposed and studied. By using this security algorithms and developing the platform for cloud storage data confidentiality and integrity is achieved.

REFERENCES

[1] Priyanka Ora, Dr.P.R.Pal, "Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography", *IEEE International Conference on Computer, Communication and Control* (IC4-2015).
[2] R.Ramya, S.Mehervani, SK.khadarbibi& R.Vinodhkumar, "Fully Homomorphic Encrypted Auditing System for Data Security and Integrity in Multicloud", *Imperial Journal of Interdisciplinary Research (IJIR,)* Vol-2, Issue-5, 2016. ISSN: 2454-1362.
[3] Vineet Kumar Singh, Dr. Maitreyee Dutta, " Analyzing cryptographic algorithms for secure cloud network", *International Journal of advanced studies in Computer Science and Engineering IJASCSE*, Volume 3, Issue 6, 2014.
[4] P.Mell and T.Grance, "The NIST Definition of Cloud Computing", *National Institute of Standards and Technology*, Vol.53, no.6, p.50, 2009.[Online]. Available:http://csrc.nist.gov/groups/SNS/cloud computing/clouddefv15.doc.
[5] Dr. Nedhal A. Al-Saiyd, Nada Sail, "Data Integrity In Cloud Computing Security", *Journal of Theoretical and Applied Information Technology*, 31st December 2013. Vol. 58 No.3 © 2005 – 2013
[6] Shivani Gambhir, Ajay Rawat, Rama Sushil, "Cloud Auditing: Privacy Preserving using Fully Homomorphic Encryption in TPA", *International Journal of Computer Applications (0975 – 8887)* Volume 80 – No 14, October 2013.
[7] Gaurav Pachauri, Subhash Chand Gupta, "Ensuring Data Integrity In Cloud Data Storage", *IJISET - International Journal of Innovative Science, Engineering & Technology*, Vol. 1 Issue 3, May 2014. Available at: www.ijiset.com
[8] Sultan Aldossary, William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 4, 2016.
[9] Mandeep Kaur, Manish Mahajan, "Using encryption Algorithms to enhance the Data Security in Cloud Computing," In International Journal of Communication and Computer Technologies, Vol 01, No. 12, 2013.
[10] Pankaj Kamboj, Er. Lovnish Bansal, "A Review Paper on 3 Step Mechanism Using RSA, AES and MD5 to Improve the Security in Cloud Environment", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 6, Issue 7, July 2016 ISSN: 2277 128X. Available online at: www.ijarcsse.com
[11] Ibtihal Mouhib, El Ouadghiri Driss, "ENHANCED DATA SECURITY APPROACH FOR CLOUD ENVIRONMENT BASED ON VARIOUS ENCRYPTION TECHNIQUES", *Journal of Theoretical and Applied Information Technology* 31st October 2015. Vol.80. No.3, © 2005 - 2015 JATIT & LLS.
[12] Ramiz Shaikh, Ankit Dongre, "Fastest Access of Secured Data in Cloud storage by using Attribute-based Encryption", *International Journal of Computer Applications (0975 – 8887)*, Volume 127 – No.1, October 2015.
[13] D.K. Mishra., 'Tutorial: Secure Multiparty Computation for Cloud Computing Paradigm by Durgesh Kumar Mishra', Second International Conference on Computational Intelligence, Modelling and Simulation, xxiv-xxv (Sept.2010).