International Journal of Contemporary Technology and Management
Volume V, Issue XII, December 2016 ISSN (Online) 2278-8034

A Survey on Cloud Data Security In Third Party Auditor's Environment

Arpit Sohani
Computer Science Department
Jagadguru Dattatry College of Technology,
Indore (India)
Rajiv Gandhi Proudyogiki Vishwavidyalaya
(State Technological University of State Madhya Pradesh, India)
arpit.sohani@gmail.com

Kuntal Barua (Asst. Prof.)
Computer Science Department
Jagadguru Dattatry College of Technology,
Indore (India)
Rajiv Gandhi Proudyogiki Vishwavidyalaya
(State Technological University of State Madhya Pradesh, India)
kuntal.barua@gmail.com

Abstract–**now in these days for enhancing the service quality the data and services are offered through the cloud. The cloud is known for better and scalable computing and the storage solutions. In this context the client of the cloud servers are worried not about the performance of the cloud they worried about the security and privacy concern of the data. In this presented work a survey on the cloud security is performed and some key issues in cloud storage are addressed. In addition of that a new model for improving the security in cloud is also proposed using the cryptographic technique. In addition of the future extension of the work is also provided.**

Keywords: *cloud computing, cloud storage, data security, third party auditor, secure communication*

I. INTRODUCTION

Cloud computing has been envisioned as the next generation architecture of the IT enterprise due to its long list of unprecedented advantages in IT: on demand self-service, ubiquitous network access, location-independent resource pooling, rapid resource elasticity, usage-based pricing, and transference of risk [1]. One fundamental aspect of this new computing model is that data is being centralized or outsourced into the cloud. From the data owners' perspective, including both individuals and IT enterprises, storing data remotely in a cloud in a flexible on-demand manner brings appealing benefits: relief of the burden of storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, personnel maintenance, and so on [2].

Cloud storage provides scalable and Quality of service guaranteed resources for storage, users can store and compute their data from any location at any time by a device which can be connected with Internet to visit that cloud. Besides these powerful advantages of cloud Storage, however, many people and companies is still feel hesitant to store their data in cloud. The reason behind this hesitancy is the fear of people and companies regarding loss of control on their data because there are some incidents of data loss and data leakage which make people to think about it [3].

The key aim of the proposed work is to develop a secure and trusted environment for data storage and their security services. Therefore the following tasks are included in the entire study.

I. **To Investigate Data Storage Services in Cloud:** In this phase basics of cloud computing and data storage techniques are studied. Additionally how the data is stored and retrieved from storage is also studied.

II. **To Investigate Security in Data Outsourcing, Access and Security Techniques:** In this phase data outsourcing and service distribution technique is studied, and issues of privacy, security and trust is addressed.

III. **To Implement Privacy Preserving System for Data Security (PSDS):** In this phase we simulate data security using trusted security Framework to ensure end user Privacy in addition of the data access, public auditing and demonstrate system utility.

IV. **To Evaluate the Performance of Proposed Security Technique:** In this phase the performance of system is evaluated in terms of their resource utilization (i.e. time and space complexity) for improving data security policy.

In this presented paper the first two goals of the proposed study are presented additionally a new technique for improving the security in cloud storage is also reported. In the next section the basics of the cloud computing and their storage technology is provided for study.

II. BACKGROUND

In this section the background technology and the proposed cryptographic technique's overview is provided. Therefore the basics of cloud computing and there issues are reported in this section.

A. Cloud Computing

Cloud computing is a computing paradigm, where a big pool of systems are associated in confidential or public networks, to provide dynamically scalable infrastructure for purpose, data and file storage. With the arrival of this technology, the cost of computation, application hosting, content storage and release is reduced considerably. Cloud computing is a practical approach to experience direct cost remuneration and it has the impending to convert a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very primary major of, reusability of IT capabilities'. The difference that cloud computing carry compared to conventional concepts of “grid computing”, “distributed computing”, “utility computing”, or “autonomic computing” is to widen horizon across governmental boundaries. Forrester defines cloud computing as [2].

“A pool of distracted, highly scalable, and managed compute communications capable of hosting end customer applications and payable by consumption.”

B. Cloud Computing: A Significant View

Cloud Computing is nothing but using and accessing applications through internet. In addition to configuration and manipulation of applications we can also store data online. Usually in cloud computing you do not need to install any software for any application to run or work in your PC, this is what makes a difference which avoids platform dependency issues. This is how Cloud computing is making applications mobile and collaborative.

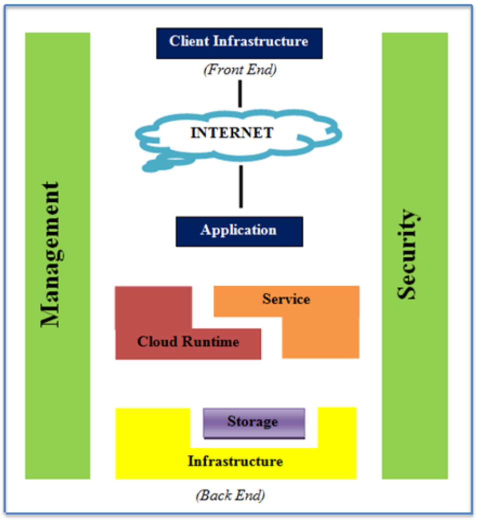

Figure 1 Overview of Cloud Computing [3]

Figure 1 depicts the architecture of the cloud computing. It consists of two parts referred as front end and back end. Front end refers to client side components such as web browser or FTP client or TELNET application etc. [3].

1. **Front End:** The front end is the client part. It consists of interfaces and applications which are necessary to access other applications. The front end is connected to back end via internet. For example web browsers are front ends.

2. **Back End:** It is the cloud by itself containing huge data storage, security, deployment models, service, servers, cloud infrastructure, management etc.

C. Cloud Computing Models

Cloud computing is able to provide a variety of services at the moment but main three services are Infrastructure As-A-Service, Platform-As-A-Service and Software-As-A Service also called as service model of Cloud computing [4].

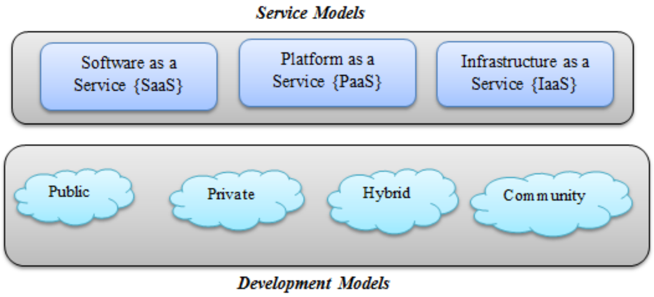
Service Models
Software as a Service {SaaS}
Platform as a Service {PaaS}
Infrastructure as a Service {IaaS}
Public
Private
Hybrid
Community
Development Models

Figure 2 Cloud Services and Development Models

1. **Software as a Service (SaaS):** In this model, a complete application is presented to the customer, as a provision on require. A single instance of the service runs on the cloud &various end users are serviced. On the customers‟ side, there is no need for upfront investment in servers or software licenses, though for the contributor, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is presented by companies such as Google, Salesforce, Microsoft, Zoho, etc.

2. **Platform as a Service (PaaS):** Here, a layer of software, or development surroundings is summarize & existing as a service, upon which other higher levels of provision can be built. The customer has the freedom to build his own applications, which run on the provider’s infrastructure. To convene manageability and scalability needs of the applications, PaaS providers offer a predefined combination of OS and request servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google’s App Engine, Force.com, etc are some of the conventional PaaS examples.

3. **Infrastructure as a Service (IaaS):** IaaS provides basic storage and computing aptitude as consistent services over the network. Servers, storage systems,

networking apparatus, data centre space etc. are collective and made offered to handle workloads. The customer would typically deploy his possess software on the communications. Some common examples are Amazon, GoGrid, 3 Tera, etc.

D. Deployment Models

Enterprises can decide to organize applications on community, Private or Hybrid clouds. Cloud Integrators can play a vital part in formative the right cloud path for each association [5].

Public Cloud

Public clouds are owned and operated by third parties; they deliver more economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each person client an attractive low-cost, "Pay-as-you-go" model. All customers share the same communications pool with incomplete organization, security protections, and availability variances. These are managed and supported by the cloud contributor. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus given that the ability to scale flawlessly, on demand.

Private Cloud

Private clouds are built exclusively for a single venture. They aim to address apprehension on data security and offer greater control, which is typically lacking in a public cloud. There are two differences to a private cloud:

On-premise Private Cloud: On-premise private clouds, furthermore recognized as inside clouds are hosted within one's own data center. This model provides a more standardized process and defence, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and effective costs for the physical income. This is best suited for applications which need absolute control and configurability of the communications and security.

Externally hosted Private Cloud: This type of private cloud is hosted superficially with a cloud supplier, where the contributor facilitates an exclusive cloud environment with full guarantee of privacy. This is best appropriate for enterprise that doesn't rather a public cloud due to sharing of physical income.

Hybrid Cloud

Hybrid Clouds merge both public and private cloud models. With a Hybrid Cloud, service providers can exploit 3rd party Cloud Providers in an occupied or partial method thus increasing the flexibility of computing. The Hybrid cloud situation is competent of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the income of a public cloud can be used to manage any unexpected surges in workload.

Community Cloud

Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns. The cloud community forms into a degree of economic scalability and democratic equilibrium. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community [6].

III. LITERATURE SURVEY

The given section provides the understanding about the Privacy Preserving concepts that are recently contributing in cloud environment therefore a number of research articles and research papers are included in this section.

Cloud storage is one of the service provided by Cloud computing in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). The user is concerned about the integrity of data stored in the cloud as the user's data can be attacked or modified by outside attacker. Therefore, a new concept called data auditing is introduced which check the integrity of data with the help of an entity called Third Party Auditor (TPA). In this work ***Swapnali S. More et al[7]*** purpose work is to develop an auditing scheme which is secure, efficient to use and possess the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. Thus the new auditing scheme has been developed by considering all these requirements. It consists of three entities: data owner, TPA and cloud server. The data owner performs various operations such as splitting the file to blocks, encrypting them, generating a hash value for each, concatenating it and generating a signature on it. The TPA performs the main role of data integrity check. It performs activities like generating hash value for encrypted blocks received from cloud server, concatenating them and generates signature on it. It later compares both the signatures to verify whether the data stored on cloud is tampered or not. It verifies the integrity of data on demand of the users. Thus no additional burden is provided on the cloud server. It is used only to save the encrypted blocks of data. The entire task for the scheme is performed by the TPA and data owner. This proposed auditing scheme makes use of AES algorithm for encryption, SHA-2 for integrity check and RSA signature for digital signature calculation.

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, ***Cong Wang et al[8]*** propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homo-morphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, ***Cong Wang et al [9]*** utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, authors further explore the technique of bilinear aggregate signature to extend this main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. Cloud computing is the vast computing utility, where users can remotely store their data into the cloud so to have the benefit of the on-demand availability of huge and different applications and services from a shared pool of configurable computing resources. Cloud-based outsourced storage space reduces the patron load of storage management. It also reduces the maintenance load of customer by providing a comparably low-cost, scalable, location-independent platform. This new model of data hosting service commence a new security challenges, which requires an independent auditing service which audit the data integrity of cloud. There are different existing auditing services available in cloud which audit data integrity remotely in static motion but these are not applicable whenever data is dynamically updated in cloud. Since it require efficient and secure dynamic auditing method for data owner. However in cloud, the clients no have direct physical possession of data. It shows client faces different formidable risk like missing or corruption of data. To keep away from the security and integrity risk of data, audit services are essential to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing. Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an untrusted server, can be used to realize audit services. In this paper, ***Marshal et al [10]*** shows profiting from the interactive proof system, we address the construction of an interactive PDP protocol to prevent the fraudulence of prove and the leakage of verified data (zero-knowledge property).

Storage outsourcing is a rising trend which prompts a number of interesting security issues, many of which have been extensively investigated in the past. However, Provable Data Possession (PDP) is a topic that has only recently appeared in the research literature. The main issue is how to frequently, efficiently and securely verify that a storage server is faithfully storing its client's (potentially very large) outsourced data. The storage server is assumed to be untrusted in terms of both security and reliability. (In other words, it might maliciously or accidentally erase hosted data; it might also relegate it to slow or off-line storage.) The problem is exacerbated by the client being a small computing device with limited resources. Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form. In this paper, ***Ateniese et al [11]*** construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption. Also, in contrast with its predecessors, this PDP technique allows outsourcing of dynamic data, i.e. it efficiently supports operations, such as block modification, deletion and append.

IV. PROPOSED WORK

The cloud environment provides support for efficient computing and enables to provide the efficient computing and storage solutions at the remote end. In this presented work the main aim to address the following issues in the existing cloud storage:

A. **Data security:** The data is placed on the cloud which is not much secured due to third party access and treads therefore the data security in cloud storage is required

B. **Data owner and client privacy management:** The data owner and client in not distinguishable using the data additionally the privacy on such data is access is required.

C. **Searchable data space:** The cryptographic manner of data security converts the formats and not a bit of data recovered during the information retrieval.

In order to provide end to end solution for the cloud storage the following solution steps are included.

Authentication Management: In authentication management the system and user attributes are recovered additionally the one time password is included to manage the secure authentication.

Cryptographic Data Security: In this phase the MD5 and AES based hybrid cryptographic algorithm is consumed for providing the security.

Providing The Search Solution Over The Encrypted Data: The keyword based search system is provided for identifying the user and their data during different data retrieval operations

3.3.1 Methodology

For the advancement of the current security scenario here we present a proposed PSDS scheme for ensure security and privacy enhancement of the system using figure 3.1.

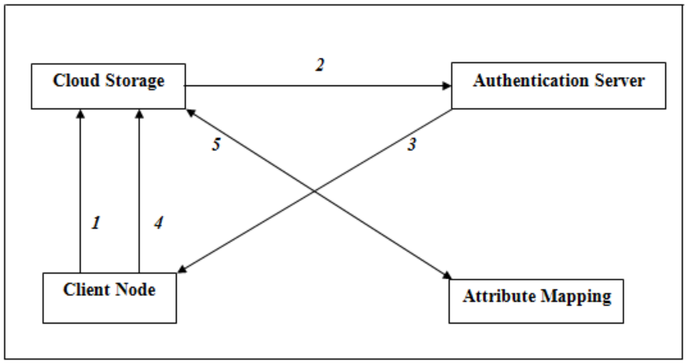

Figure 3.1 Security Management

According to the given figure the proposed security technique involve the following steps of authentication and data preserving technique.

a) Client node is an end client system who wants to store or retrieve the data from the secure server. In this step the end client initiate the authentication by making the request from the server.

b) In this phase the server system trigger the authentication server for finding the user credentials and data attributes and ask for the security questions, in this phase the OTP is applied to make secure the communication between client and server.

c) After authenticating the user access the system ask for user id, password and OTP again here the OTP works as the salt for the encryption and validation.

d) In this step user initiate the communication and data request from the server, during this the MD5 and AES algorithm is organized for encrypting the data additionally the following information is preserved into the attribute MAP. MAP data for finding the user targeted information from search space.

i. User ID

ii. Password

iii. Session key

iv. Text file features as frequent token

v. Original file name

vi. Mapped file name

V. CONCLUSION

The proposed work is intended to provide the secure technique for improving the security of cloud storage. Therefore a basic overview on the cloud technology and their different aspects are prepared. In further recently develop techniques and methods for securing cloud is also studied in this work. Finally a new model for secure communication between server and client is provided. In near future the proposed model is implemented and their performance is analyzed for finding the additional overheads and security issues.

REFERENCE

[1] P. Mell and T. Grance, “Draft NIST Working Definition of Cloud Computing,” 2009; http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

[2] M. Armbrust et al., “Above the Clouds: A Berkeley View of Cloud Computing,” Univ. California, Berkeley, Tech. Rep. UCBEECS-2009-28, Feb. 2009.

[3] Rajeev Bedi, MohitMarwaha and Tajinder Singh, “Analysis of Different Privacy Preserving Cloud Storage Frameworks”, International Journal of Computer Science & Information Technology (IJCSIT), Volume 3, No 6, Dec 2011.

[4] Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." IEEE Transactions on computers 62.2 (2013): 362-375.

[5] “Cloud computing tutorial” available online at: http://www.rfwireless-world.com/Tutorials/cloud-computing-tutorial.html

[6] Torryharris, “CLOUD COMPUTING – An Overview”, http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf

[7] Swapnali S. More and SangitaChaudhari, “Privacy Preserving Third Party Public Auditing Scheme for Secure Cloud Storage”, International Journal of Computer Applications (IJCA), International Conference on Communication, Computing and Virtualization, PP. 23-28,

[8] Wang, Cong, et al. "Toward secure and dependable storage services in cloud computing" IEEE transactions on Services Computing 5.2, PP. 220-232, 2012.

[9] Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing" INFOCOM, 2010 Proceedings IEEE, 2010.

[10] Marshal, ShingareVidya. "Secure audit service by using TPA for data integrity in cloud system." Int. J. Innovat. Technol. Exp. Eng 3 (2013): 2278-3075.