ISSN 2229-5518

Investigation of TPA (Third Party Auditor Role) for Cloud Data Security

Dr. Pradeep K. Deshmukh, Mrs. Vrushali R. Desale, Prof. Rushali A. Deshmukh

Abstract—Cloud computing provides folks the different ways to share distributed resources and services that belong to totally different organizations or sites. As we know that cloud computing sharing the distributed resources via the network within the open atmosphere, therefore it makes security issues necessary for us to develop the cloud computing application. During this paper, we have a tendency to listen to the protection needs in cloud computing atmosphere. We have a tendency to present a technique to create a trustworthy computing atmosphere for cloud computing system by group action the trustworthy computing platform into cloud computing system. We have a tendency to investigate a model system within which cloud computing system is combined with trustworthy third party computing platform with trustworthy platform module. During this model, some necessary security services, together with authentication, confidentiality and integrity, area unit provided in cloud computing system.

In Cloud, application computer code and services move to the centralized massive knowledge center and management of this knowledge and services might not be trustworthy. To manage this knowledge we have a approach to use third party auditor (TPA). It will check the reliability of information; however it will increase the information integrity risk of information owner. Since TPA not only scans the information however additionally he will modify the information, so a mechanism we need to have mechanism which resolves this problem. We investigated one algorithm to overcome this problem. Additionally we are presenting the literature review over cloud computing frameworks and security issues.

Index Terms-Third party Auditor, Integrity, Cloud Service Provider, Cloud Computing.

1 INTRODUCTION

CLOUD computing is net ("cloud") based mostly development and use of engineering ("computing"). It's associate rising computing technology that uses the web and central remote servers to keep up information and applications. Cloud computing permits shoppers and business to use applications while not installation and access their personal files at any laptop with net access. This technology permits for far more economical computing by centripetal storage, memory, and process and information measure [2].

A definition for cloud computing is given as associate rising laptop paradigm wherever information and services reside in massively ascendable information centers within the cloud and might be accessed from any connected devices over the web. The simplest example of cloud computing is Google Apps wherever any application is accessed employing a browser and it is deployed on thousands of laptop through the web. Cloud computing is that the next natural step within the evolution of on-demand info technology services and merchandise. To an outsized extent cloud computing are supported virtualized resources [3].

- *Author Dr. Pradeep. K. Deshmukh PhD in Computer Science & Engineering. His key research interest include Cloud computing,Network Security, ANN. He is currently working as Professor in Rajarshi Shahu College of Engineering, Pune India Department of Computer Engg with the total experience of about 20 years.*
- *Co-Author Mrs. Vrushali R. Desale is currently pursuing masters degree program in computer engineering from University of pune (India)*
- *Co-Author Prof. Rushali A. Deshmukh is currently working as Professor in Rajarshi Shahu College of Engineering, Pune, India, Department of Computer Engg*

The concept of cloud computing is predicated on a really elementary principal of reusability of IT capabilities. Computing is delineated as any activity of victimization and/or developing hardware and software package. It includes everything that sits within the bottom layer, i.e. everything from raw work out power to storage capabilities [4]. Cloud computing ties along of these entities and delivers them as one integrated entity beneath its own subtle management.

Although unreal as a promising service platform for the web, this new information storage paradigm in "Cloud" brings regarding several difficult style problems that have pro-found influence on the protection and performance of the system. One amongst the largest considerations in cloud information storage is information integrity verification at entrusted servers. What is additional serious is that for saving cash and cupboard space the service supplier may neglect to stay or deliberately delete seldom accessed knowledge files that belong to a normal consumer [6][7][8].

TPA is that the third party auditor who can audit the information of knowledge owner or consumer so it'll exempt the burden of management of knowledge of knowledge owner. TPA eliminates the involvement of the consumer through the auditing of whether or not his knowledge keep within the cloud square measure so intact, which might be necessary in achieving economies of scale for Cloud Computing. The discharged audit report wouldn't solely facilitate house owners to gauge the chance of their signed cloud knowledge services, however even be helpful for the cloud service supplier to enhance their cloud based mostly service platform [5]. This public auditor can

facilitate the information owner that his data square measure safe in cloud. With the utilization of TPA, management of information are simple and fewer burdening to data owner however while not encoding of knowledge, however information owner can make sure that his information square measure in a very safe hand. In this research paper we are investigating use of such TPA for cloud data security [9].

2 Literature Review

2.1 How Cloud Works?

A cloud user desires a shopper device like a portable computer or personal computer or any computing resource with an internet browser (or alternative approved access route) to access a cloud system via the globe Wide internet. Generally the user can log into the cloud at a service supplier or personal company, like their leader. Cloud computing is works on a client-server basis. The cloud provides server-based applications and everyone information services to the user, with output displayed on the shopper device [2].

If the user desires to make a document employing an applications programmer, for instance, the cloud provides an appropriate application running on the server that shows work done by the user on the shopper browser display. Memory allotted to the shopper system's browser is employed to form the applying information seem on the shopper system show, however all computations and changes are recorded by the server, and final results together with files created or altered are for good keep on the cloud servers.

Cloud services work on multiple platforms, together with UNIX system, Macintosh, and Windows computers. Smartphone's, pads and pill devices with net and World Wide internet access conjointly give cloud services to work and mobile users. A service supplier could pool the process power of multiple remote computers in an exceedingly cloud to attain routine tasks like backing from massive amounts of information, data processing, or computationally intensive work. These tasks would possibly commonly be tough, time overwhelming, or costly for a personal user or a little company to accomplish, particularly with restricted computing resources and funds.

With cloud computing, shoppers need solely a straightforward laptop, like net-books, designed with cloud computing in mind, or perhaps a Smartphone, with an association to the net, or an organization network, so as to form requests to and receive information from the cloud, therefore the term "software as a service" (SaaS). Computation and storage is split among the remote computers so as to handle massive volumes of each, so the shopper needn't purchase costly hardware or computer code to handle the task. The result of the process task is come back to the shopper over the network, enthusiastic about the speed of the net association.

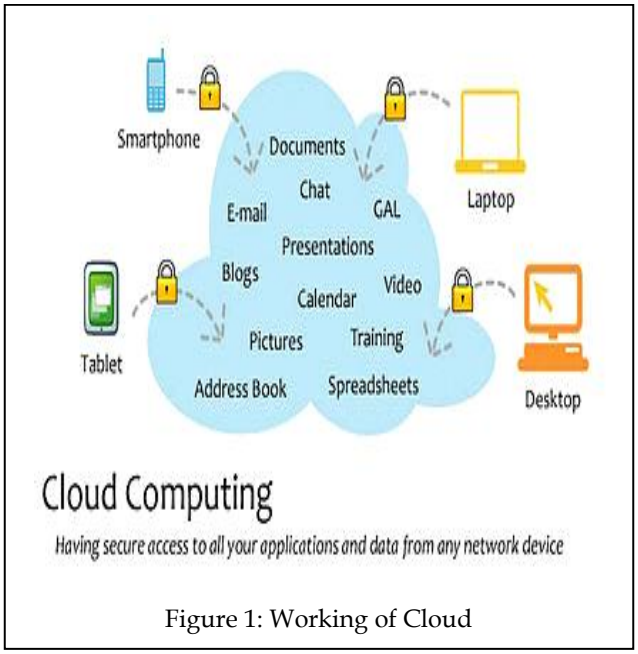

Figure 1: Working of Cloud

2.2 Architecture of Cloud

Cloud systems design of the software package systems concerned within the delivery of cloud computing contains hardware and software package designed by a cloud designer who generally works for a cloud integrator. It generally involves multiple cloud elements communication with one another over application programming interfaces, sometimes internet services.

This closely resembles the UNIX philosophy of getting multiple programs doing one issue well and dealing along over universal interfaces. Quality is controlled and therefore the ensuing systems area unit a lot of manageable than their monolithic counterparts.

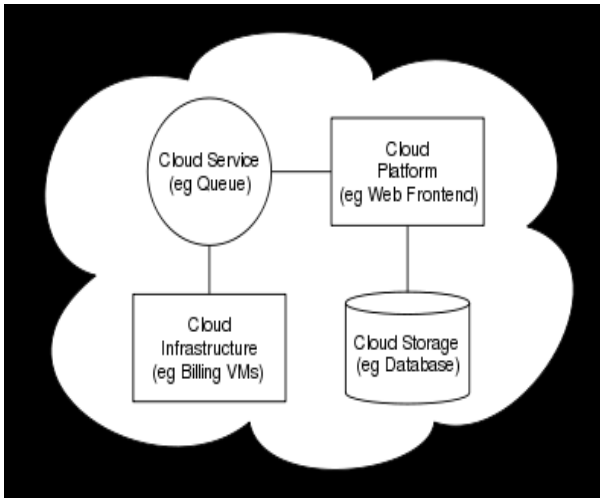

Figure 2: Cloud Framework

Cloud design extends to the consumer, wherever internet browsers and/or software package applications access cloud applications. Cloud storage design is loosely coupled, wherever data operations area unit centralized sanctioning the info nodes to scale into the lots of, every severally delivering information to applications or users. Figure 2 shows the architecture of cloud [5].

2.3 Services of Cloud Computing

The cloud computing services generally divided into 3 categories:

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Infrastructure-as-a-Service provides virtual server instances with distinctive IP addresses and blocks of storage on demand. Customers use the suppliers computer program interface to begin, stop, access and set up their virtual servers and storage. within the enterprise, cloud computing permits a corporation to procure solely the maximum amount capability as is required, and produce a lot of on-line as before long as needed. Platform-as-a-service within the cloud is outlined as a group of computer code and merchandise development tools hosted on the provider's infrastructure. Developers produce applications on the provider's platform over the net.

In the software-as-a-service cloud model, the seller provides the hardware infrastructure, the wares and interacts with the user through a front-end portal. Despite the fact that cloud computing could be a pretty new technology, there square measure several firms giving the higher than mentioned cloud computing services [11].

Different firms like Amazon, Google, Yahoo, IBM and Microsoft square measure all players within the cloud computing services business. However Amazon is that the pioneer within the cloud computing business with services like EC2 (Elastic reckon Cloud) and S3 (Simple Storage Service) dominating the business. Microsoft has sensible data of the basics of cloud science and is building large knowledge centers. IBM, the king of business computing and ancient supercomputers, groups up with Google to urge an edge within the clouds. Google is much and away the leader in cloud computing with the corporate itself engineered from the bottom informed hardware.

2.4 Cloud Computing Implementation

All of the subjects fields of study of knowledge and structure concerns mentioned herein are usually apply to all or any implementations of a cloud infrastructure. As we tend to specialize in building the cloud, variety of models are developed for deploying a cloud infrastructure.

2.4.1 Personal Clouds

In a personal cloud, the infrastructure for implementing the cloud is controlled utterly by the enterprise. Typically, personal clouds are enforced within the information center of the enterprise and managed by internal resources.

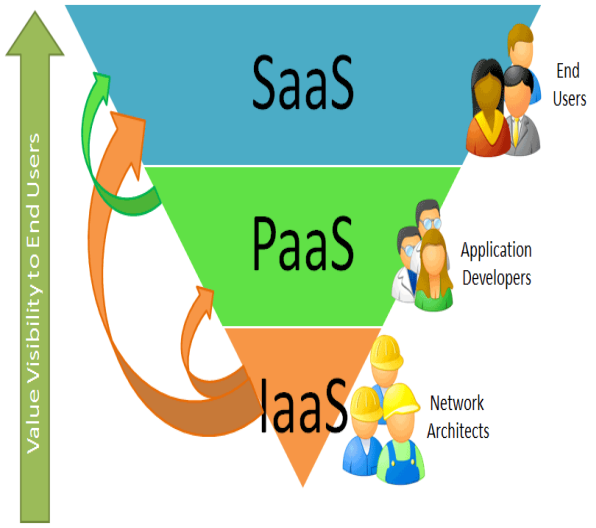

Figure 3: Services of Cloud

A private cloud maintains all company information in resources below the management of the legal and written agreement umbrella of the organization. This eliminates the regulative, legal and security considerations related to info being processed on third party computing resources. The personal cloud can even be utilized by existing IT departments to dramatically cut back their prices and as a chance to shift from a price center to a worth center within the eyes of the business.

2.4.2 Public Clouds

In a public cloud, external organizations give the infrastructure and management needed to implement the cloud. Public clouds dramatically change implementation and square measure generally beaked supported usage. This transfers the value from a cost to Associate in nursing operational expense and might quickly be scaled to fulfill the organization's wants. Temporary applications or applications with burst resource necessities generally get pleasure from the general public cloud's ability to ratchet up resources once required then scale them back once they are not any longer required.

Additionally, as most public clouds leverage a worldwide network of knowledge centers, it's troublesome to document the physical location of knowledge at any explicit moment. These problems end in potential regulative compliance problems that embody the utilization of public clouds sure enough organizations or business applications. Not all public cloud primarily based applications will give the mandatory flexibility and practicality required by business users. Ultimately, many purchasers might decide that the personal cloud offers a lot of flexibility and develop new applications themselves.

2.4.3 Hybrid Clouds

To meet the advantages of each approach, newer execution models are developed to mix public and personal clouds into a unified answer. An application with important legal, regulative or service level considerations for info is directed to a personal cloud. Different applications with less rigorous regulative or service level necessities will leverage a public cloud infrastructure. Implementation of a hybrid model needs extra coordination between the personal and public service management system. These generally involves a federate policy management tool, seamless hybrid integration, federate security, info quality management, coordinated provisioning management, and unified observation systems. Hybrid clouds mix each public and personal cloud models. This is often most frequently seen with the utilization of storage clouds to support Web 2.0 applications [10].

2.5 Security Plan of Cloud Computing

Cloud computing has distinctive security risks. Security risks, threats, and breaches will are available in such a large amount of forms and from such a large amount of places that several corporations take a comprehensive approach to security management across IT and also the business. The subsequent points helpful for making cloud computing security arrange.

• In most circumstances, approach cloud security from a risk-management perspective. Make certain to involve your organization's risk-management specialists within the coming up with.

• The price of security might be a problem. Bear in mind of what similar organizations spend on that security and be ready to pay an identical quantity. It additionally helps to trace time lost attributable to any reasonably attack—as a measure of price that you simply is also ready to scale back.

• Identity management is essential. Offer priority to rising identity management if your current capability is poor.

• Try to form general awareness of security risks by educating and warning workers members regarding specific dangers. It's straightforward to become self-satisfied, particularly if you're employing a cloud service supplier. However, most security breaches as created within the network.

• Use external IT security consultants to often check your company's security policy and network, likewise as those of your cloud service suppliers.

• Determine specific IT security policies for amendment management and patch management, and confirm that policies are well understood by your workers and your cloud service supplier.

• Stay informed news regarding IT security breaches in alternative corporations and also the causes of these breaches.

• Review backup and disaster-recovery systems in lightweight of IT security. Except anything, IT security breaches will need complete application recovery.

3 TPA Base Security Scheme

3.1 TPA Based Cloud Model

In the figure 4 below we tend to prepared a model in which consumer, CSP and TPA are shown. The consumer asks the CSP to produce service where CSP authenticate the consumer and supply a virtual machine by means that of code as a service. During this Virtual Machine (VM), RSA formulas are used wherever consumer encode and decode the file. In this VM, SHA-512 algorithms additionally there which build the message digest and check the integrity of information.

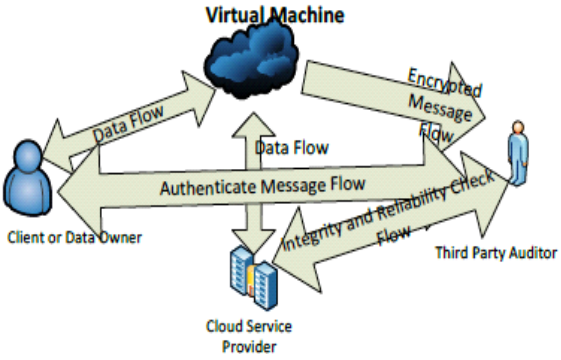

Figure 4: Architecture for Client, Third Party auditor and Cloud Service Provider

3.2 User Level Cryptography

After performing file operation it'll send the information to CSP and TPA. This CSP and TPA can keep our information not solely safe but additionally offer integrity but how it does not make sure that we are going to full trust on TPA. He will send data's of information owner to unauthorized user. If we remove the TPA even it will not solve the matter as a result of CSP may also send the information to unauthorized user and also data owner doesn't get a bonus of TPA. Therefore cryptography is needed at user level. In this scheme encoding and decipherment is completed with the assistance of RSA formula [7].

3.3 Mechanism for Data Check Integrity

As data owners no longer physically possess the storage of their data, cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading the file for its integrity verification is not a practical solution due to the high cost of input/output (I/O) and transmission cost across the network. Also it is not easy to check the data thoroughly and compare with our data. Even the loss of data and

recovery of data is also not easy. Considering the large size of the outsourced data and the owner's con-strained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for data owners. Hence, to fully ensure data security and save data owners' computation resources, we propose to enable publicly auditable cloud storage services, where data owners can resort to an external third party auditor (TPA) to verify the outsourced data when needed.

4 Work Done

The practical works done over this proposed approaches to check their effectiveness. Here we will take example of data dynamics in terms of files and their conversion. During the practical work, at first we created one CSP, data owner and TPA. Data owner gave right to change the data to 10 users with keys and identity number. This identity number he sends to CSP and TPA. This user initially generated the file according to above sections 3.1 and 3.2. TPA found all 10 files in appropriate form. To achieve constant bandwidth cost we took a file range from 100 to 1000 KB. All results were obtained after taking of 10 trials. In our observation we find that after getting digital signature of client and encrypted file the message digest takes less time to convert the data as shown in figure 5. The time required to run our scheme can be consider as negligible. After taking negligible time we can enhance the security of data.

We additionally notice that our theme observe error likelihood concerning 99. The information protective from TPA and CSP is verified by the simulation, as we have a tendency to have converted the file into encrypted kind.

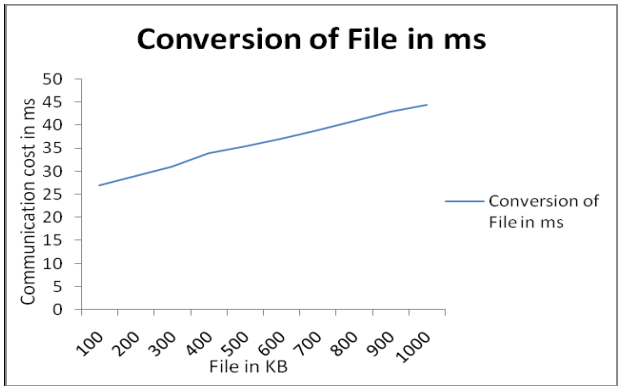

Figure 5: Communication cost Vs. File Conversion

5 Conclusion and Future Work

Cloud Computing is a huge topic and also the higher than report doesn't provides a high level introduction thereto. It's not at all doable within the restricted area of a report back to do justice to those technologies. In this investigation study, we first presented the detailed study over the cloud computing, its infrastructure, and security plans. Further we investigated proposed TPA based security plan and its cloud model.

There are many schemes for security using TPA are proposed by various researchers, however every scheme having their own advantages and disadvantages. For the future work, we will present the current problem statement using the TPA for cloud data security and present new approach to overcome it.

6 References

[1] Cong Wang and KuiRen, Wenjing Lou, Jin Li, Toward Publicly Auditable Secure Cloud Data Storage Services in IEEE Network July/August 2010

[2] G.Ateniese et al., —Provable Data Possession at Untrusted Stores, Proc. ACM CCS _07, Oct. 2007, pp. 598–609.

[3] M. A. Shah et al., —Auditing to keep Online Storage Services Honest, Proc.USENIXHotOS _07, May 2007.

[4] G. Ateniese et al., —Scalable and Efficient Provable Data Possession, Proc. SecureComm _08, Sept. 2008.

[5] H. Shacham and B. Waters, —Compact Proofs of Retrievability, Proc. Asia- Crypt _08, LNCS, vol. 5350, Dec. 2008, pp. 90–107.

[6] E.-C. Chang and J. Xu, "Remote integrity check with dishonest storage server," in Proc. of ESORICS'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.

[7] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[8] A. Oprea, M. K. Reiter, and K. Yang, "Space-efficient block storage integrity," in Proc. of NDSS'05, 2005.

[9] T. Schwarz and E. L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage," in Proc. of ICDCS'06, 2006.

[10] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and secure sensor data storage with dynamic integrity assurance," in Proc. of IEEE INFOCOM'09, Riode Janeiro, Brazil, Appril 2009.

[11] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of SecureComm'08, 2008.

[12] C. Wang, K. Ren, and W. Lou, "Towards secure cloud data storage," Proc. of IEEE GLOBECOM'09, submitted on March 2009.