2018 International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2018

Transparency Service Model For Data Security In Cloud Computing

Salman Ashraf
Department of Computer Science, University of Lahore
Sargodha, Pakistan
salmanashraf.12@gmail.com

Muqaddas Gull
Department of Computer Science, University of Lahore
Sargodha, Pakistan
Muqaddas.gull@sgd.uol.edu.pk

Tanzila Kehkashan
Department of Computer Science, University of Lahore
Sargodha, Pakistan
tanzila.kehkashan@cs.uol.edu.pk

Saira Moin u Din
Department of Computer Science, University of Lahore
Sargodha, Pakistan
saira.moin@cs.uol.edu.pk

Abstract— **Cloud computing is hot innovation in Computer world today and data Security and Privacy are the real issues. Since the main party that has physical access to data storage is the supplier and to monitor where information is put away for specific clients. The suppliers keep meta-data in their own databases where sometimes it leads towards security and data protection issue. If meta-data is compromised than unapproved access to client data is possible. For the protection of client data, we have presented a Transparency Service Model in this research paper. TSM provides a mechanism where cloud provider configures the service on the cloud by giving the service information about the cloud storage devices that would exist the data. It is then responsibility of the TSM to store data on those devices and cloud providers no longer direct access to data storage on those devices.**

Keywords*— *SaaS (Software as a Service), PaaS(Platform as a Service), IaaS (Infrastructure as a service), TSM (Transparency Service Model).

I. Introduction

Cloud computing has increased its importance throughout the years. With expanded client base and accessibility of different applications cloud computing is leading the pack in Computer sciences and it has reinforced its claim to being a standout amongst the most auspicious technology in the Computer World today. Cloud computing is broadly utilized by singular clients and additionally small, medium and extensive associations. Administrations like CDN (Content Distribution Network) gave by cloud systems are utilized by of all shapes and sizes associations alike. Cloud Systems offer a few rewards to its clients some of which are profoundly refreshing, for example, on request self-benefit, access to network and other resources, adaptability and some other basic Services [1].

NIST made the broadly utilized meaning of cloud computing model, which is as "Cloud computing is a model for enabling suitable, on-request network access to a shared pool of adaptive computing means (e.g., networks, storage, servers, applications, and services) that can be quickly provisioned and released with minimum administration endeavor or service provider cooperation. This cloud model promotes the availability and is composed of three service models, five essential characteristics and four deployment models" [12].

Service models characterize the level of abstractedness at which a User's interfaces a Cloud Computing environment. These are the (SaaS) show, the (PaaS) demonstrate, and the (IaaS) model. Some unique models are there for execution of administrations of the cloud systems, and the user chooses how clients would be interfacing with the cloud systems. There are three fundamental services models for the cloud systems which incorporate (SaaS), (PaaS) and (IaaS). SaaS gives application administrations to its clients and that clients of the SaaS cloud do not influence the hidden equipment and programming running on the cloud case can be Microsoft Office 360. In PaaS stage is given by the cloud and applications are produced by the clients that keep running in the cloud this is usually done through API case of such cloud can be Microsoft Azure and Google AppEngine. IaaS gives ultimate control to its clients; it gives Processing Power, Network and capacity case of such cloud is Amazon EC2 [1].

Regular Cloud systems are two essential sorts, Centralized Clouds and Federated Clouds. Brought together Centralized Clouds are commonly utilized for scientific operations, data mining and web services. Federated Clouds give every one of the abilities of the centralized cloud with an additional ability of improved reliability. This is accomplished by graphically distributing the cloud and providing services through the closest dissemination of the cloud upgrading reaction time and reliability

With all the great things said in regards to cloud computing there are a few angles that ruin this service. One such perspective is data security and privacy. When a client stores data on the cloud he has no physical access to the foundation putting away the information or data. He might be given affirmation by the cloud specialist co-ops that data is secure

978-1-5386-1370-2/18/$31.00 ©2018 IEEE

however those confirmations are not physically verifiable. This is a noteworthy worry since most business and clients dislike their data to be helpless against any data security and protection issues. This inquires about proposes another Transparency benefit display for data security and privacy. Model intends to dazzle the service provider so he can't tell where data of the certain client is located. It makes a Transparency layer that spares information or data along these lines blinding supplier's perspective of data. Solving the issue of data security and improving the data security.

II. Traditional Cloud System

Cloud computing is the new modern expression in Computer Science and IT and is relied upon to develop rapidly. It is also expected that it would change the lives of individuals. In this style of registering versatile and, productive resources give services to its clients through the internet. It additionally takes out the need to gain substantial assets this enables clients to exploit the adaptability gave by the cloud rapidly. Because of these reasons technology is hot on the market and it has all the abilities to provide services for little and medium business associations and also home clients. According to one of the gauge, 20 percent of large companies will be conducted the email seats by advertising with the help of Cloud. Another gauge, as a Service Software is a system to have yearly rate of 17 percent for development in 2011 for ERP, SCM and CRM exhibition in the section of SMB. Like this, the investors are examining the conceivable results to adopt this technology. It is essential for these investors to fundamentally estimate the practicality of this reform for their appropriate companies.

A. *Typical Characteristic of This Technology*

System or the resources utilized as a part of making the cloud are generally not owned by the clients. They are claimed by the specialist co-ops who lease those gear or assets to the customers. The duty of Quality of service (QoS) lies with the expert service providers [14]. It is the obligation of the specialist service provider to guarantee 100 percent up time and furthermore ensure that there is no issue with introduced equipment and software. Clients of the cloud computing devour resources as a service, this enables them to pay for just for the service that they have utilized. While a few organizations apply the utility registering model for the installment of the services they render which resembles current utility service like electricity or Landline, clients are charged for the measure of the power expended. Numerous others charge on the membership premise.

B. *Model of Service of Cloud*

Computational power is delivered in cloud computing model using networks. The name "cloud" basically remains for the reflection for the essential equipment, infrastructure and softwares. There are three primary sorts of service models: SaaS, PaaS, and IaaS [1].

In software as a service, distinctive applications like databases and so forth are given to the clients of the cloud. The cloud service providers oversee the infrastructure that has the applications. SaaS is for the most part valued as pay by utilizing basis, and it is likewise known as demand software. SaaS causes the business to altogether cut IT operational costs by utilizing the equipment and software of the service providers on the lease basis. This likewise encourages them to lessen specialized staff on their payroll [10].

1) *Software as a Service*

A product delivery system is known as "Software-as a-Service" which introduces software in the cloud structure, and its related information is also put away in the cloud [1]. Utilizing a web program, SaaS is gotten to by clients. Today numerous business applications utilize SaaS as a typical delivery model including bookkeeping, joint effort, Customer Relationship Management (CRM) and service desk management. In 2010, SaaS deals achieved 10 billion dollars and expanded to 12.1 billion dollars in 2011 i.e. 20.7 percent up from 2010. By 2015 SaaS income will be more than two times from 2010, and may reach up to 21.3 billion dollars. Customer Relationship Management (CRM) prompts be the biggest market for SaaS. SaaS income inside CRM advertised figure to achieve 3.8 billion dollars in 2011, up from 3.2 billion dollars in 2010. The term Software as a Service is thought to be the piece of the classification of cloud computing, alongside (SaaS) and (BaaS).

2) *Platform as Service*

Another service model of cloud computing is PaaS, which gives a computing stage and method (SaaS). In (PaaS) demonstrate client makes a product utilizing apparatuses or libraries from the service providers. Client additionally controls deployment of software and setup settings. The point of the service providers is to give servers, storage, systems and different services. It offers implementation of software by diminishing the cost and multifaceted nature of purchasing and keeping up software and equipment additionally provisioning facilitating abilities. Many sorts of PaaS sellers offer application facilitating and an arrangement domain alongside different incorporated services. The service provides adaptability and support.

3) *Infrastructure as Service*

The infrastructure is the base of cloud computing. IaaS gives delivery of computing as a common service decreasing the speculation cost, maintenance and operation of equipment. Infrastructure ought to be reliable and adaptable for usage and services of applications, resources delivery, for example, servers, storage and system segments as a service brings down the total cost of possession. Full versatility takes out the requirement for management and up keeping of equipment. Enterprise level infrastructure for all endorsers. Framework as Service cloud offers assets, for example, pictures in virtual-machine crude, picture-library and document - based capacity, load balancing, firewalls, IP addresses, local virtual systems and software bundles. Cases of IaaS suppliers are Amazon cloud development, Amazon EC2, Google figure motor, HP cloud, Joyent, iland and Oracle systems as services and Rackspace cloud.

C. *Cloud Types from Service Providers Point of View*

From the perspective of service providers, Clouds depend on common computing clusters: Cloud service providers put critical hardware into massive data centers; each of data centers is centrally managed. Building and working a Cloud data center is costly, so just huge organizations can bear the cost of such an enormous investment. Be that as it may, the current incorporated way to deal with Cloud computing is not by any means the only probability and now and again won't not be the ideal choice.

1) *Centralized Cloud*

Centralized cloud is established on central data center these clouds are based on the single data center to provide the services of the cloud. Amazon E2C is an example of such cloud.

2) *Federated Cloud*

In federalized clouds, datacenters are expended on the globe and cloud services are given by the geographically closest datacenter to clients. Combined cloud provide genuinely necessary and enhanced response time and encase of fiascos, for example, marine web cable link cuts the cloud keep on providing services to its clients in their geographical area.

D. *Advantages of the Cloud systems*

Some significant benefits of the cloud computing includes:

- On Demand resources and service Availability.
- Accessibility of data and resources on the cloud from anywhere using the internet.
- Minimum software installation and licensing issues.
- Cost reduction.
- Less technical staff requirement.

E. *Disadvantages of the cloud systems*

As it is proved that technology always the main reason behind every revolution in the human history, and we cannot deny this fact. In spite of reality, huge range of element are there in cloud computing, expecting another skyline; some basic elements which are not ignorable. Some of them are given below:

- "pinnacle" usage, instead of "greatest" usage. Internet service provider companies generally worked in multiple of 5 to 1, in which companies offer 5 times extra than they have in the package, accepting clients will not use extra resources, but 20 percent of their assigned resources. This works, but a prevalent YouTube video about blackouts, bringing everybody to see in the meantime. Cloud computing is more helpless against the peak usage problem than web transmission.
- Attacks of denial of services, as of now normal, wind up noticeably simpler. What's more, it's become harder to follow, as compromised "cloud assets" can be utilized to dispatch the attacks, instead of bargained "singular pc". Cloud computing is helpless against monstrous security damages. At present, when a system is damaged, only the data of that system are compromised. The damage caused by a security rupture are increased in cloud computing.
- With the help of centralized services, cloud computing improves the probability that a system failure progresses toward becoming "catastrophic", instead of "isolated". Till date, to control the uncontrolled elements, no political approach has been made to take the service to lines of trust and proprietor dispatch.

F. *Security Problems in the cloud Systems*

Few security issues related with customary could systems are there. Cloud Computing depends on the current use of the computing resources and information over the web, so it additionally acquires a portion of the regular security problems of internet, for example, the availability of data, security of data, accessibility of data and data respectability. Cloud computing has its own safety issues like where data would be put away who might manage data i.e. if data is stored outside the nation from where it began and numerous all the more such issues

1) *Privacy and Security of Data*

The base of Data Security implies that the data must be put away in a way where it is guaranteed and that its uprightness is not traded off and it is accessible on request when needed. When you store data in the cloud, it is put away and shared on the web in an area obscure to its clients the greater part of the things, and is put away in a situation that is not under the control of the client who is putting away data on the cloud. Since the end client has no hold on the physical condition data assurance and privacy is never ensured [11]. Since the data is put away in the remote area, data accessibility is another issue regardless of how high the service provider is 100 percent up time is never ensured. This is because of elements, for example, data transmission productivity inaccessibility of part of the cloud and so on. One such example case is Microsoft cloud services Azure confronted enormous corruption for almost 22 hours because of a few issues regarding up gradation of the network [4]. Another problem with Cloud system is that identified with what is called Data disinfection it imply that when data is erased by client from the cloud it must be for all time cleared since the resources are shared on the cloud it is conceivable that a document deleted by a client can be gotten to by another client by mostly utilizing some recuperation tools on the mutual resource [8]. As new threats appear, the taxonomy may be referred to particular problem areas and its value is obtained. The taxonomy is generalized genre-based and therefore gives a perception of the nature of subsisting and new threats in the Cloud environment, just like other taxonomies that lead toward particular problem or application areas. For example, the taxonomy has been implemented to the modeling and design of shared application architecture to provide security functions in a Cloud Computing environment [13]. In cloud computing the most significant interest is theft information. According to the Breach Level Index website [14], entirely 3989114567 records were missed since 2013. Around 554 million records were stolen in 2016, with biggest lost in October that is (around 472 million stolen records). Even the technology titans were not left out; main name is Microsoft, with the eight recorded data breaches in period 2013 – 2015 [14]. Source of the gap for each of them was malicious outsider, and all of them are with hard and catastrophic risk score.

2) *Security Threats*

Regarding cloud system there are many security threats and risks. Some of those risks inherited from traditional distributed systems. Examples of such attacks are TCP-IP hijacking, spoofing, password guessing, attack of service denial, attack of middle man, and so on [7].

- Malware Injection with this threat the exploiters try to inject malicious programs, code or services in the cloud [5].
- Spoofing is another type of attack mainly used to spoof Meta data information so that a more deadly Malware injection or other kind of attack can be carried out [6].
- Service Hijacking in this thread the hackers can hack into a web service hosted on the cloud and install malicious software to get valuable user data and information [2].
- Threat from Insiders Cloud provider's employees with bad intentions can also be a security risk for cloud system.
- Shared Resource Problems can also become a security risk since resources are shared by users on the cloud. Malicious users can gain access to data of the other users on the cloud [2].
- Vulnerabilities in the applications installed on the cloud can also cause serious threats to the cloud systems and users data [2].
- Access Control can also be a problem on the cloud as many corporate users of the cloud have their own applications that are installed on the cloud and if the Access Control for those applications is not good users can gain access to parts of the data that they are not authorized to use [2].

III. Related Work

To overcome the cloud computing and data security issues, there are different approaches have been suggested one such approach was suggested by Cong Wang [9]. In this approach a third party auditing mechanism is created to insure data security and privacy. It uses random masking and holomorphic authenticator to insure that the unrelated party will not learn regarding the data and also insures that data is not compromised. Major issue with this technique is that most users of the cloud systems would not understand encryption concepts and keeping lists of public and private keys. It may suite for advance users but for general public it's difficult to use.

Another Approach to make sure that this accuracy of data and privacy of data in the cloud is suggested by experts [3]. This approach uses agents to insure data privacy and security. In this model when user needs to store data he needs to first negotiate a mechanism for security with Trust Agent (TA). Then data is sent by the user and TA verifies credentials of the sender. If TA is able to verify data it sends data to storage layer for storage. When data is requested same procedure is applied.

There is yet another approach called PasS (Privacy as a Service) discussed in [4]. The PasS is basically a combination of some rules which make sure the data security in the cloud system and maintain the secrecy of data by using encrypted coprocessors to strengthen proof of the stored information or data in the cloud. It provides maximum control to the user in managing data on the cloud for this purpose it provides user configurable software protection for the data. It also provides a mechanism to give feedback to user about the potential risks that can harm confidentiality of user data.

Generally, the approaches used to provide data security and privacy is mostly based on encryption. Most methodologies try to implement ways and methods to temper proof data in order to ensure security and privacy [3, 4, 5, 7]. But most of these approaches neglect the basic issue with cloud storage that is meta-data. To properly ensure that data privacy is not compromised there needs to be a way that the providers of the cloud service have not control over the storage of data and that they should not be aware where the data of certain user resides. Since providers have physical access to hardware or infrastructure if they know where the data of certain user resides they can make copies of the data and do all kinds of misuse of the data. Transparency Service Model of data provides one such solution that blinds providers from viewing the user data.

IV. Transperancy Service Model

Transparency Service Model (TSM) is a service that needs to be configured on the cloud system and that would be used by the customers of the cloud to store data on the cloud in a transparent manner. It provides a mechanism where cloud provider configures the service on the cloud by giving the service information about the cloud storage devices that would hold data. It is then responsibility of the TSM to store data on those devices and cloud providers no longer direct access to data storage on those devices.

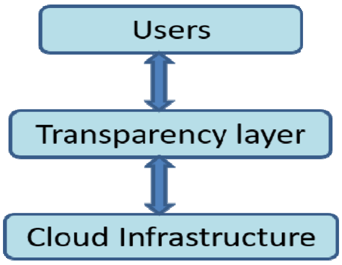

Fig. 1.Transparency Model

A. Design & Service Architecture

Service architecture is simple the TSM has been implemented as a layer between the cloud infrastructure and the user. Whenever user needs to save or retrieve a data item from cloud infrastructure he must interact with the TSM.TSM acts as interface between the cloud and the user. Fig. 1 tries to provide an overview of the architecture of the TSM.As cleared by the Fig. 1 whenever user needs to interact with the cloud infrastructure for saving or retrieving files he must interface with the TSM. Now it's the responsibility of the TSM to ensure data storage and retrieval for users and it must ensure security and integrity of the data. Fig.2 shows some of the main functions of TSM.

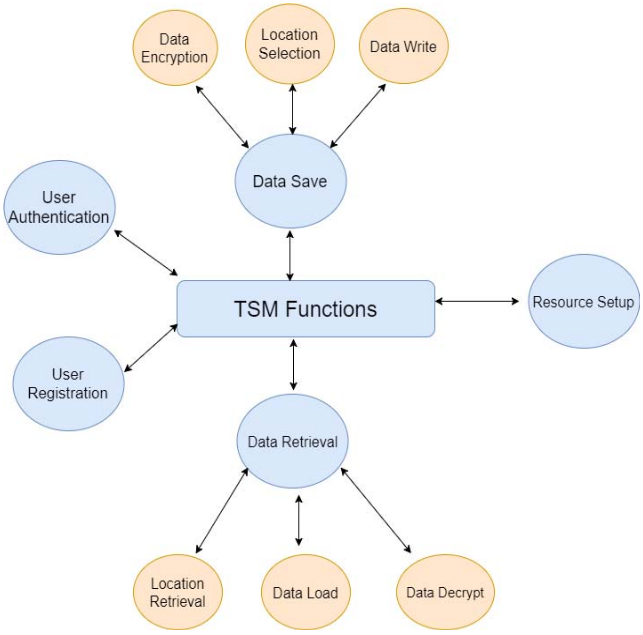

Fig. 2. TSM Functions

1) TSM Functions

There are five major functions of the TSM

a) User Registration - Used to register users with service this is done first time the user tries to save data on the cloud it is asked to create a user profile and create password to securely save data.

b) User Authentication - Is used to verify user credentials with user information provided in the registration process. It is used whenever user needs to save or load data from the cloud..

c) Data Save - Is used to save data.Data possible for transfer, but not feasible for computation, data bases.

d) Data Retrieval - Is used to retrieve the saved data on the resources.

e) Resource Setup - Is used to setup resources on the provider side. Using this function service provider can add all the underlying resources, used by the service for data storing and recovering.

These five functions perform all the work required to ensure data security and privacy. First four functions are related to users of the cloud and are used by them. Last one is used by the cloud providers to add resources in the pool of available resources for the service. This is also used to update and remove any resource whenever needed.

B. How TSM Ensures Data Security and Privacy

There are two aspects to ensuring data security and privacy. TSM will use for outsider and insider's access to data. To block all outsiders access to data TSM uses password authentication it is on top of the original cloud security provided by the cloud provider. So if some outsider needs to hack into data he must first get into cloud by compromising the cloud security and then somehow compromise the security offered by the TSM. To block insider access to data no one knows on which drive you have data for which user. Since data is encrypted using standard encryption techniques it would take years to decrypt. TSM chooses resources randomly from the cloud resources for data save operations. TSM Cloud computing solutions provide powerful authentication and authorization layers. TSM can determine the existence of effective and robust security controls, assuring companies their information is properly secured against unauthorized access, change and destruction.

V. Conclustion

In this paper we have proposed a model to solve the problem of data security and privacy in cloud computing by hiding information from the cloud providers and their employees. Basic purpose of the model was to take over the responsibility of saving and retrieving data from the cloud and doing it in such a way that only the model knows where data of certain user resides and that it can only be accessed by using security mechanism provided in the model. In future we are considering implementing this model as working prototype and after that we would like to create a variant of this model for Peer to Peer Cloud Systems.

References.

[1] Neal Leavitt, " Is cloud computing really ready for prime time?," in IEEE Computer Socciety, 2009.

[2] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," in 44th Hawaii International Conference on System Sciences, pp. 1–10, Koloa, Hawaii, January 2011.

[3] W. Itani, A Kayssi, and A Chehab, "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures, " in IEEE

conference on Dependable, Autonomic and Secure Computing, DASC ’09, pp 711–716, December 2009.

[4] M. Jensen, J. Schwenk, N. Gruschka, and L.L. Iacono, “On technical security issues in cloud computing,” in IEEE International Conference on Cloud Computing, CLOUD ’09, pp. 109–116, September 2009.

[5] Meiko Jensen, Nils Gruschka, and Ralph HerkenhÃner. A, “ A survey of attacks on web services,” in Journal of Computer Science - Research and Development, pp. 185–197, 2009.

[6] Ronald L. Krutz and Russell Dean Vines, “Cloud Security: A Comprehensive Guide to Secure Cloud Computing,” Wiley Publishing, 2010.

[7] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin Shen, “Secure provenance: The essential of bread and butter of data forensics in cloud computing, “ in Proceedings of 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS ’10, pp. 282–292, 2010 Peter Mell and Timothy Grance. The nist definition of cloud computing. Technical Report 800-145, National Institute of Standards and Technology (NIST), Gaithersburg, MD, September 2011.

[8] S. Subashini and V. Kavitha, “ Review: A survey on security issues in service delivery models of cloud computing, “ in Journal of Network and Computer Applications,pp. 1–11, January 2011.

[9] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, “ Ensuring data storage security in cloud computing,” in 17th Internation Workshop on Quality of Service, IWQoS, pp 1–9, July 2009.

[10] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in Proceedings IEEE INFOCOM, pp 1–9, March 2010.

[11] Ardagna, Danilo, Giuliano Casale, Michele Ciavotta, Juan F Perez and Weikun Wang, Quality-of-service in cloud computing:modeling techniquesand their applications,” in Journal of Internet Services and Applications, 2014.

[12] Alan T Litchfield and Jacqui Althouse, “A systematic review of cloud computing, big data and databases on the cloud,” in Proceedings of the Americas Conference on Information Systems, pp 1–19, 2014.

[13] Monjur Ahmed, Alan T Litchfield and Chandan Sharma, “A distributed security model for cloud computing,” in Proceedings of the Americas Conference on Information Systems, 2016.

[14] Z. Masetic, K. Hajdarevic, N. Dogru. Cloud Computing Threats Classification Model Based on the Detection Feasibility of Machine Learning Algorithms,” in 40th International Conference on Information and Technology, Electronics and Microelectronics, 2017.