International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.3, No.5, October 2014, pp. 264~270
ISSN: 2089-3337

Ensuring Data Security And Privacy In Cloud Computing Through Transparency as Service Model

Ahmad Afzaal*, Abbas Younis*, Kamran Komal*, Zafar Amina*, Yasir Nida**
*Student of Departement of Computer Science, University Of Lahore Pakistan
**Lecturer of Departement of Computer Science, University Of Lahore Pakistan

Article Info

Article history:

Received Aug 18th, 2014
Revised Sep 21th, 2014
Accepted Oct 26th, 2014

Keyword:

SaaS
Transparency Service
Cloud Computing
Cloud Security
Cloud Privacy

ABSTRACT

Cloud Computing is hot technology in computer world today. Its getting popular because its inexpensive, provides on demand access when and where needed. It also removes technical staff requirements for maintaining the infrastructure because that is done on the provider side thus significantly reducing organizational costs. It also provides opportunity for scientists to use powerful computing resources for research purposes which are very expensive on rent bases which they normally would not have been able to use due to cost factors.But with these features it has certain problems that discredit the service one of major problems is Data Security and Privacy.Since the only party that has physical access to data storage is provider and to keep track of where data is stored for certain users the providers keep meta-data in their own databases it creates a security and data privacy issue.If meta-data is compromised than unauthorized access to user data is possible.This paper proposes a Transparency Service Model to insure security and privacy of the user data.

Corresponding Author:

Nida Yasir,
Lecturer of Departement of Computer Science, University Of Lahore Pakistan.
Email: nida.yasir@yahoo.com

1. INTRODUCTION

Cloud computing has gained significant importance over the years. With increased user base and availability of diverse applications cloud computing is taking the lead in computer sciences and it has strengthen its claim of being one of the most promising technologies in computer world today. Cloud computing is being widely used by individual users as well as small,medium and large organizations. Services like CDN (Content Distribution Network) provided by cloud systems are used by big and small organizations alike. Cloud Systems provide several advantages to its users some of which are highly appreciated such as on demand self-service, Network Access, Resource Pooling, flexibility and Measured Service.[1]

Concerning definition of cloud computing model, the most widely used one is made by NIST as "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models". [13]

Service models define the level of abstraction at which a Users interfaces a Cloud Computing environment. These are the "Software as a Service" (SaaS) model, the "Platform as a Service" (PaaS) model, and the Infrastructure as a Service" (IaaS) model.There are different models for implementation of services of the cloud systems and the implementation decides how users would be interfacing with the cloud systems. There are three main services models for the cloud systems which include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). SaaS provides application services to its

users and that users of the SaaS cloud have no control over the underlying hardware and software running on the cloud example can be Microsoft Office 360. In PaaS platform is provided by the cloud and applications are developed by the users that run on the cloud this is done typically through API example of such cloud can be Microsoft Azure and Google AppEngine. IaaS gives ultimate control to its users it provides Processing Power, Network and storage example of such cloud is Amazon EC2.[1]

Conventional Cloud systems are of two basic types Centralized Clouds and Federated Clouds. Centralized clouds are mainly used for data mining, web services and scientific computations. Federated clouds provide all the capabilities of the centralized cloud with an added advantage of enhanced reliability. This is achieved by distributing the cloud geographically and providing services through nearest distribution of the cloud enhancing response time and reliability.

With all the good things said about cloud computing their are some aspects that discredit this service.One such aspect is data security and privacy.when a user stores information on the cloud he has no physical access to the infrastructure storing the information.He may be given assurance by the cloud service providers that data is secure but those assurances are not physically verifiable.This is a major concern since most business and users would not like their data to be vulnerable to any kind of data security and privacy issues.This research proposes a new Transparency service model for data security and privacy.Model aims to blind the provider so that he cannot tell where data of certain user is located.It creates a Transparency layer that saves data thus blinding providers view of data.Solving the issue of data privacy and enhancing the data security.

2. TRADITIONAL CLOUD SYSTEM

Cloud computing is the new buzzword in computer science and IT and is expected to grow rapidly.It is also expected that it would transform the lives of people. In this style of computing scalable and dynamic resources provide services to its users through internet. It also eliminates the need to acquire heavy resources this allows users to quickly take advantage of the scalability provided by the cloud. Due to these reasons technology is hot in the market and it has all the capabilities to deliver services for small and medium business organizations as well as home users. As per one of the estimate 20 percent of enterprise market e-mail seats will be delivered via Cloud. [4] As per another estimate from Software as a Service is forecast to have a compound annual growth rate of 17 percent through 2011 for CRM, ERP and SCM markets in SMB segment. Therefore the enterprises are exploring the possibilities to adopte this technology. It is imperative for these enterprises to critically evaluate the feasibility of this technology for their specific businesses.

2.1. Typical Characteristic of This Technology

Infrastructure or the resources used in creating the cloud are generally not own by the users or customers of the platform.They are owned by the service providers who rent those equipment or resources to the customers.The responsibility of Quality of service (QOS) lies with the service provider [15] . It is the responsibility of the service provider to ensure 100 percent up time and also make sure that there is no problem with installed hardware and software. Users of the cloud computing consume resources as a service, this allows them to pay for only for the services that they have used. While some companies apply the utility computing model for payment of the services they render which is like traditional utility services like electricity users are only billed for the amount of the electricity consumed. Many others bill on the subscription basis. [17]

2.2. Model of Service of Cloud

Cloud computing is a model in which computational power is delivered through the use of networks. The name 'cloud' simply stands for the abstraction for the underlying hardware and software and infrastructure. There are three main types of service models: [1]

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

In software as a service different applications like databases etc are given to the users of the cloud. The infrastructure that hosts the applications is managed by the cloud service provider. Saas is mostly priced as pay by use basis and it as also known and on demand software. Saas helps the business to significantly cut IT operational expenses by using the hardware and software of the service providers on rent basis. This also helps them reduce technical staff on their payroll [14].

2.2.1. Software as a Service

On demand software generally called as Software-asa-Service is a software delivery model in which software is installed on the cloud infrastructure and its related data is also stored on the cloud [1]. Using a

web browser SaaS is accessed by users. Now a days many business applications use SaaS as a common delivery model including accounting, collaboration, Customer Relationship Management (CRM) and service desk management. In 2010, SaaS sales reached 10 billion dollars and increased to 12.1 billion dollar in 2011 i.e. 20.7 percent up from 2010. By 2015 SaaS revenue will be more than double from 2010, and may reach upto 21.3 billion dollars. [4] Customer Relationship Management (CRM) leads to be the largest market for SaaS. SaaS revenue within CRM market was forecast to reach 3.8 billion dollar in 2011, up from 3.2 billion dollars in 2010. The term Software as a Service is considered to be the part of the nomenclature of cloud computing, along with platform as a service and infrastructure as a service and Backend as a service (BaaS).

2.2.2. Platform as Service

It is another type of service model of cloud computing which provides a computing platform and solution stack as a service.In this model user or consumers creates a software using tools or libraries from the providers. Consumer also controls software deployment and configuration settings. Main aim of provider is to provide networks, servers, storage and other services. PaaS offers deployment of applications by reducing the cost and complexity of buying and maintaining hardware and software and provisioning hosting capabilities. There are various types of PaaS vendors which offer application hosting and a deployment environment along with various integrated services. The service offers scalability and maintenance.

2.2.3. Infrastructure as Service

Infrastructure is the foundation of cloud computing. It provides delivery of computing as a shared service reducing the investment cost, operational and maintenance of hardware. Infrastructure should be reliable and flexible for easy implementation and operations of applications, delivery of resources such as servers, storage and network components as a service lowers total cost of ownership. Full scalability eliminates the need for administration and maintenance of hardware. Enterprise grades infrastructure for all subscribers. IaaS cloud offers resources such as images in a virtual-machine image -library, raw and file -based storage, firewalls, load balancers, IP addresses, virtual local networks and software bundles. Examples of IaaS providers are Amazon cloud formation, amazon EC2, google compute engine, HP cloud, iland, joyent and oracle infrastructure as a service and rackspace cloud.

2.3. Cloud Types from Service Providers Point of View

From the service provider point of view, Clouds are based on conventional computing clusters: Cloud providers invest significant resources into large datacenters, each of which is centrally managed. Building and operating a Cloud datacenter is expensive so only large companies can afford such a huge investment. However, the current centralized approach to Cloud computing is not the only possibility and in some cases might not even be the optimal choice.

2.3.1. Centralized Cloud

Centeralized cloud is cloud that is based on central datacenter these are based based on single datacenter to provide the services of the cloud. Example of such cloud is Amazon E2C.

2.3.2. Federated Cloud

In Federated clouds datacenters are scattered on the globe and cloud services are provided by the nearest geographical datacenter to users. Federated cloud provide much needed and improved response time and encase of disasters such as marine internet cable cuts the cloud continue to provide services to its users in their own geographical location.

2.4. Advantages of the Cloud systems

Major Advantages of the cloud systems include:

- On Demand Service Availability
- Data and resources on the cloud accessible from any where you can have internet accessibility.
- Minimal software licenses and software installation issues.
- Reduction of the cost
- Need of less technical professionals

2.5. Disadvantages of the cloud systems

As any technology is a boon for an evaluation as the history is evidence, there are disadvantages too which cannot be ignored. Despite a fact cloud computing has so many features which can be awaiting a new horizon there are also key factors which cannot be ignored. Few have been summed up below:

- Lack of connectivity causes 100 percent downtime, whereas with traditional applications, lack of connectivity allows for some local function to continue until connectivity is restored.
- The lack of industry-wide standards means that a usage surge can easily overwhelm capacity without the ability to push that usage to another provider. Companies providing computing services will over-sell these services similar to how bandwidth is over-sold based on average or "peak" usage, instead of "maximum" usage. ISP's typically operate at multiples of 5 to 1, where they sell 5 times more than they have in capacity, assuming users will not use more than 20 percent of their allotted resources. This works, until there is a popular YouTube video that everyone wants to see at the same time resulting in outages. Cloud computing is even more vulnerable to the peak-usage problem than internet bandwidth.
- "Denial of service" attacks, currently common, become easier. What's more they become harder to trace, as compromised "cloud resources" can be leveraged to launch the attacks, rather than compromised "individual pc". Cloud computing is vulnerable to massive security exploits. Currently, when a system is broken into, only the resources of that system are compromised. With cloud computing, the damages caused by a security breach are multiplied exponentially.
- By "centralizing" services, cloud computing increases the likelihood that a systems failure becomes "catastrophic", rather than "isolated". No political approach has been made till date to control the uncontrolled factors to bring the service under the boundary lines of trust and owner ship, as these services are beyond country lines.

2.6. Security Issues in the cloud Systems

There are several security issues associated with traditional could systems.Cloud Computing is based on the modern usage of the computing resources and data over the internet so it also inherits some of the conventional security issues associated with internet such as secrecy of data, security of data, availability of the data and integrity of the data.Cloud has its own security issues as well like where data would be stored who would regulate data i.e if data is stored outside the country from where it originated and many more such issues.

2.6.1. Privacy and Security of Data

The essence of Data Privacy Security means that data must be stored in a manner where it is protected and that its integrity is not compromised and it is available on demand when needed.When you store data on cloud it is stored and shared on the internet on a location unknown to its users most of the times and is stored in an environment that is not under the control of the user who is storing data. Since the end user has no control on the physical environment data protection and confidentiality is never guaranteed [15]. Since data is stored in remote location data availability is another issue no matter how good the service provider is 100 percent up time is never guaranteed. This is due to factors such as bandwidth efficiency unavailability of part of cloud etc. One such is example is microsoft cloud services Azure faced tremendous degradation for nearly 22 hours due to some problems related to network upgrade [8]. Another problem with Cloud systems is that related to what is called Data sanitization it mean that when data is deleted by user from the cloud it must be permanently deleted since the resources are shared on the cloud it is possible that a file deleted by a user can be accessed by another user by simply using some recovery mechanism on the shared resource [12].

2.6.2. Security Risks and Threats

There are number of security risks and threats associated with cloud systems and some of those risks inherited from traditional distributed systems.Examples of such attacks are TCP-IP hijacking, spoofing, password guessing, Man in the middle attack, denial of service attack and so on [11] .

- Malware Injection with this threat the exploiters try to inject malicious programs, code or services in the cloud [9].
- 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 [10].
- 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 others 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].

2.7. Related Work

To overcome the problems of data security and privacy in cloud computing number of different approaches have been suggested one such approach was suggested by Cong Wang [16]. In this approach a third party auditing mechanism is created to insure data security and privacy.It uses random masking and homomorphic authenticator to insure third party auditor would not learn any thing about the data being stored 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 its difficult to use.

Another Approach to insure data security and privacy in the cloud is proposed by M R Islam and M Habiba [6].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) by Wassim Itani [7]. The PasS is basically a set of protocols for ensuring the privacy and security of the data in the cloud it uses cryptographic coprocessors to temper proof the data stored in the cloud.It tries to provide the user maximum control 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 are mostly based on encryption.Most methodologies try to implement ways and methods to temper proof data in order to ensure security and privacy [7, 6, 3, 5].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.

3. TRANPERANCY 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.

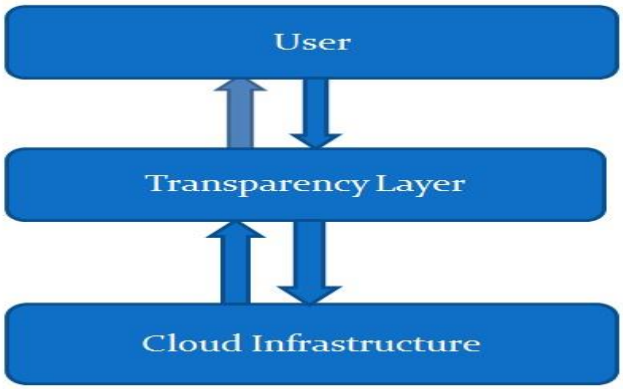

Figure 1. TSM Architecture

3.1. Service Architecture and Design

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.Figure 1 tries to provide an overview of the architecture of the TSM.As cleared by the figure whenever user needs to interact with the cloud infrastructure for saving or retrieving files he must interface with the TSM.Now its the responsibility of the TSM to ensure data storage and retrieval for users and it must ensure security and integrity of the data.

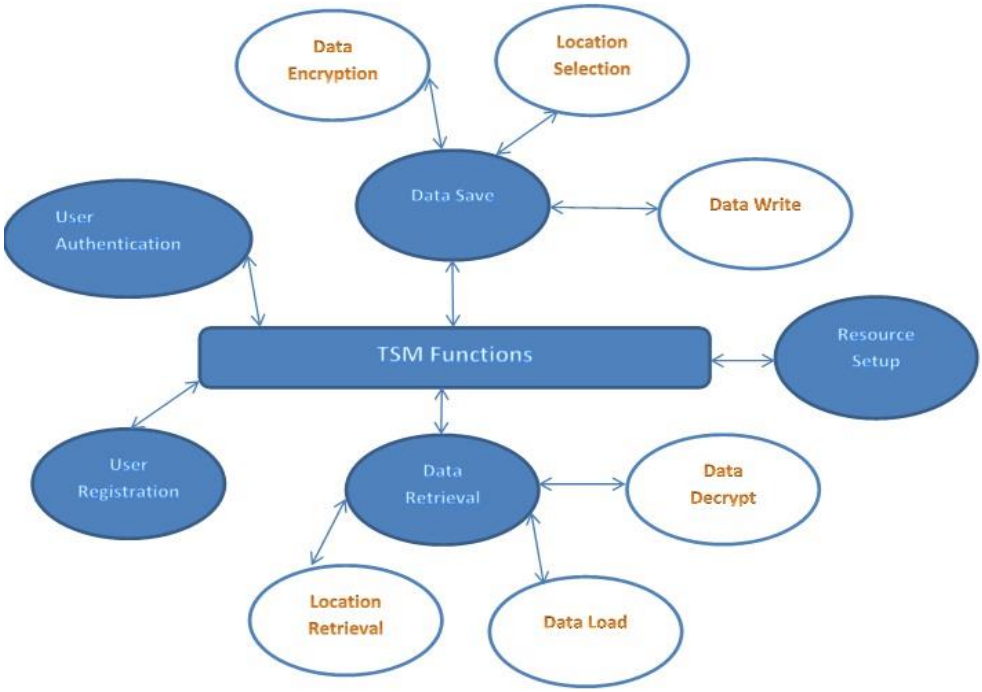

Figure 2. TSM Functions

3.1.1. TSM Functions

There are five major functions of the TSM

- 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.
- 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.
- Data Save - Is used to save data.
- Data Retrieval - Is used to retrieve the saved data on the resources.
- Resource Setup - Is used to setup resources on the provider side.Using this function service provider can add all the underlying resources that can be used by the service to store and retrieve data.

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.

3.1.2. How TSM Ensures Data Security and Privacy

There are two aspects to ensuring data security and privacy.Outsider access to data and insiders 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.

4. CONCLUSION

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] Ozalp Babaoglu, Moreno Marzolla, and Michele Tamburini. Design and implementation of a p2p cloud system. In Proceedings of the 27th Annual ACM Symposium on Applied Computing, SAC '12, pages 412–417, New York, NY, USA, 2012. ACM.

[2] M. Sutton D. Hubbard. Top threats to cloud computing v1. 0, June 2009.

[3] Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, Guangtao Xue, and Minglu Li. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. Computers & Security, 42:151–164, 2014.

[4] Gartner. Estimates.

[5] M.S. Guru Prasad, H.R. Nagesh, and L. Dharmanna. Ensuring data storage in cloud computing for distributed using high security password. In Research Technology in the Coming Decades (CRT 2013), National Conference on Challenges in, pages 1–4, Sept 2013.

[6] M.R. Islam and M. Habiba. Agent based framework for providing security to data storage in cloud. In Computer and Information Technology (ICCIT), 2012 15th International Conference on, pages 446–451, Dec 2012.

[7] W. Itani, A Kayssi, and A Chehab. Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures. In Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on, pages 711–716, Dec 2009.

[8] Wayne A. Jansen. Cloud hooks: Security and privacy issues in cloud computing. In Proceedings of the 2011 44th Hawaii International Conference on System Sciences, HICSS '11, pages 1–10, Washington, DC, USA, 2011. IEEE Computer Society.

[9] M. Jensen, J. Schwenk, N. Gruschka, and L.L. Iacono. On technical security issues in cloud computing. In Cloud Computing, 2009. CLOUD '09. IEEE International Conference on, pages 109–116, Sept 2009.

[10] Meiko Jensen, Nils Gruschka, and Ralph HerkenhÃ¶ner. AÂ survey of attacks on web services. Computer Science - Research and Development, 24(4):185–197, 2009.

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

[12] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen. Secure provenance: The essential of bread and butter of data forensics in cloud computing. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS '10, pages 282–292, New York, NY, USA, 2010. ACM.

[13] 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.

[14] S. Subashini and V. Kavitha. Review: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl., 34(1):1–11, January 2011.

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

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

[17] Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. Future Gener. Comput. Syst., 28(3):583–592, March 2012.