Security Issues and Solutions Using Multifactors Trust Evaluation among Client and Outsourcing Service in Cloud Computing

Priyanka motwani¹, PriyaSaxena²

¹M.Tech scholar, ²Asst. Professor, Sanghavi Innovative Academy, Indore, India

Abstract—the cloud is infrastructure store a huge amount of data from organizations and individuals. Thus security and privacy of data and data owner both are essential area of concern in cloud. The presented paper provides their contribution in two key phases first preparing the survey on different existing security schemes for cloud security and second proposal of an enhanced security technique which provide confidentiality and integrity on data.

Keywords—cloud computing, security, confidentiality, data security, multifactor trust, third party auditor,

I. INTRODUCTION

The term "cloud" refers to the computing power that is available across the Internet. In a sense, the cloud is rapidly transforming a worldwide network into largest "virtual" computing machine in the world.

"Cloud computing come to computing on the Internet, as opposed to computing so on a desktop".

Cloud computing is technology that provides the different services at low cost. The different client stores data on Cloud storage. Cloud computing provides storage for information and provides security for that information. Cloud service models are infrastructure as a service, platform as a service and software as a service.

The term "cloud" means to the computing power that is available across the Internet or cyberspace. In a sense, the cloud is rapidly transforming a worldwide network into largest "virtual" computing machine in the world.

Cloud storage is a network of online storage, contended by third parties. On cloud data is stored in virtualized pools of storage. Hosting companies operate large data centres and lease their storage. Companies, organizations and institutes, hosted their data by buy or lease storage from hosting companies. The storage operator virtualizes the resources as per the requirements of client. The resource may physically span across multiple servers and data may be stored at different places. The advantage of cloud storage over dedicated storage is that, the storage is delivered on demand.

For avoiding the disadvantage of storing all data on a client, data can be split into chunks and distributed among multiple data clusters.

The distributed environment represents different data clusters that placed on different places. Different data cluster store the client’s information after encryption, replication.

Applications

- Clients would be able to access their applications and data from anywhere and any time. They could access computing system using remote computer linked to Internet. Data wouldn’t be kept on a hard drive or even a corporation's internal network.
- Cloud computing would reduce need for advanced hardware on client side. Need not to buy fastest computer, because cloud system take care needs of user. Instead, buy an expensive computer terminal.
- Corporations that work on traditional computers need to choose correct software. The companies don't have to buy a software licenses for employee. Instead, the company could pay a metered fee to a cloud operating company.
- Some companies rent physical space to store files and databases because they don't have it available on site. Cloud computing provide the option of storing data.
- Corporations might save money on IT support.
This section provides the overview of the cloud infrastructure the next section discusses the issues and challenges of cloud computing.

II. CLOUD ADAPTATION CHALLENGES

This section includes the issues and challenges that are in front of new generation technology, some of them are related to the technology cognizance and some of them from the security aspects.

A. Technology awareness

Data Storing Techniques: When data mobility via at a high level then the risks and issues increase many folds especially when data is transferred to another country with different regulatory framework. Users cannot control cloud infrastructure managing their data, which causes threats to the data.

Data Location: Cloud computing offers a high degree of data mobility. Consumers do not always know the location of their data. In most cases, this does not matter. For examples, e-mails and photographs uploaded to facebook can reside anywhere in the world and facebook members are not generally concerned.

Data Relocation: Another issue is the movement of data from one location to another. Data is initially stored at an advantageous location decide by the cloud providers. However, it is often moved from one place to another. Cloud suppliers have contacts with each other and they use each other’s resources. Consumers do not know this and often it does not matter [4].

B. Security attacks in Cloud

Cloud computing offers numerous advantages. Various attacks such as social engineering approach, XML signature wrapping attack, malware injection, and other attacks poses risk clouding systems. Some of them are discussed in this section.

XML Signature Wrapping Attack: Wrapping attacks aim to shoot a faked element into messagebody, by which a valid signature covers unmodified element while the faked one is processed by the application logic. As result, an attacker can perform an arbitrary Web Service request while authenticating as a lawful user.

Malware Injection: In a malware-injection attack an adversary attempts to inject malicious code into a system. This attack can appear in the form of code, scripts, active content, and/or other software. When an instance of a legitimate user is ready to run in the cloud server, the respective service assume the representative for reckoning in the cloud. The only checking done is to determine if the instance matches a logical existing service. However, the unity of the instance is not checked.

Social Engineering Attack: A social engineering attack is an intrusion that relies heavily on human interaction and often tricking other people to break normal protection procedures.

Account Hijacking: Account hijacking is usually carried out with stolen certification. Using the stolen credentials, attackers can access sensitive information and compromise the confidentiality, unity, and availability of the services offered. Example of such attacks includes eavesdropping on transactions/sensitive activities, handling changes of data, returning falsified information, and redirection to unlawful sites.

Traffic Flooding: Traffic flooding attacks bring a network or service down by flooding it with large amounts of traffic. Traffic flooding attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests it cannot process genuine association requests. Eventually, the host’s memory fender becomes full and no further connections can be made, and the result is a Denial of Service.

C. Security Reasons

Security is defined as assurance that sensitive information is not disclosed to unauthorized persons, processes, or devices. Hence, must make sure that users' confidential data, which users do not want to be accessed by service providers, is not disclosed to service providers. It is noted that users’ confidential data is revealed to a service provider only if all of the following three conditions are satisfied at the point:

1. The service provider knows where the users' confidential data is located in the cloud computing systems.
2. The service provider has the perquisite to access and collect the user’s secret data in the cloud computation systems.
3. The service provider can understand the meaning of the users' data. This is due to the following reasons: In order to collect users' data, the service provider must know the position of the data in cloud computing systems and have the privilege to access the data. Even if the service provider can collect users' data with success, the service provider may not be able to understand the meaning of the data unless the service provider has at least some of the following information:
   i) types of data
   ii) functionalities and user interface of the application using the data
   iii) Format of the data
III. CURRENT CLOUD COMPUTING ARCHITECTURES

The current cloud computing system consists of three layers: software layer, platform layer, and infrastructure layer, as shown in Figure 2. The software layer provides interfaces for users to use service provider's applications. The platform layer provides the operating environment for software to run using system resources. The infrastructure layer provides the hardware resources for computation, repositing, and networks. The following are the major problems of current cloud computing systems:

- Each service provider has its own software, platform, and infrastructure layer. When a user uses a cloud application, the user is forced to use platform and infrastructure provided by the same service provider. Hence the service provider knows where the users' data is located and has full access privileges to data.
- The users' data has to be in a fixed data format specified by the service provider, and hence the service provider knows all the information required for understanding users' data.[5]

Therefore, we cannot prevent service providers from satisfying all of the above conditions.

In further discussion, we report some essential security models that are currently being used by different cloud providers.

A. MODEL 1

The available secure architecture defined using Figure 3 includes the following processes:

- **Step1**: Client sends data to cloud provider for storing.
- **Step2**: Cloud provider receives data and performs encryption.
- **Step3**: Full copy of encrypted data stores on data warehouse.
- **Step4**: After backup, performing replication and divide the data in parts according to the availability of data marts (in our system use three data marts: S1, S2, S3)
- **Step5**: Storing the different part of entropy (information) on different data mart.
- **Step6**: Repeat Steps as per storing request.

Advantages of this architecture:

1. Software failure: In case of software failure data mart loses the information of particular node. But data mart takes a backup copy from storage warehouse. It increases the availability of information.
2. Hardware failure: The data mart is in a dash or down also impact on the availability. This system also removes that drawback. If any data mart is crashed then client’s request also able to extract data from backup warehouse.

B. MODEL 2

The security program includes developing design models to describe the minimum acceptable recommended practices to be used in constructing a secure system as shown in Figure 3 according to the given model the model includes the following essential components.

A. Network Segments

The network consists of a series of logical and physical layers divided into network segments to simplify the approach for designing secure network architecture. The network segments can be further classified as follows:

1. Enterprise Network Segment consisting of enterprise computer systems
2. Process Information Network Segment consisting of Manufacturing Execution System computers
3. Control network Segment consisting of controllers and Human Machine Interface devices
4. Field network Segment consisting of sensors and actuators
5. Process Segment consisting of pipes, valves, and transportation belts.[6]

B. Access Control Model

The recommended practices for access and Control can be further sub-divided into the following steps:

a) User Access Management
b) User responsibilities
c) Network Access Control
d) Operating System Access Control
e) Application Access Control
f) Monitoring System Access and Use

User access is regulated by RBAC addresses the problem of traditional model by basing access on user’s job responsibilities rather than customizing access for each individual.

C. MODEL 3

In further a different security model is discussed that is given using figure 5. According to the system design that model works on the basis of the following steps.

1. Integrity protection problem in clouds, sketches a novel Architecture and Transparent Cloud Protection System (TCPS) for improved security of cloud.
2. This claim that the integrity problem in clouds a system named as Transparent Cloud Protection System (TCPS) for increased security of cloud resources.
3. SWsAccording to them their proposed system, TCPS can be used to observe the guests integration and keeping the transparency and virtualization. The strength of their work is their proposed tool which provides improved security, transparency and intrusion detection mechanism.
4. It mainly focuses public clouds that needs significant consideration and presents to make data security decisions. Key security issues reported are end user trust, Insider Access, Visibility, Risk Management, Client-Side Protection, host-Side Protection, Admittance Control and Individuality management. The strengths of work are recognition and discussion on cloud security issues and private risks associated with cloud services. The weakness is that they haven’t proposed any tool or framework to address identifies issues.
5. The filters of the system first finds malicious stuff and in next sensitive information like countersign etc are removed. cradle tracking and access control enable publishers to decide which images are available to which users. Users are able to find their required images. The prelude results showed that filters are working correctly and similarities among images are accurate.
6. The strength of system which provides image filters and scanners to detect malicious images. The weakness is filters are not exact and sometimes lawful images may also be detected as malicious and their virus scanner is also not effective [6].

D. MODEL 4

The Cloud Multiple-Tenancy Model of NIST is given using figure 6 where the different components of the system are reported.

Multiple-tenancy is an important functional characteristic of cloud computing that allows multiple applications to currently running in a physical server. This physical server partitions and processes different customer demands with virtualization. Virtualization possesses good capability of sharing. By running multiple virtual machines in a physical machine, enables to share computing resource such as processor, memory, storage, and I/O, additionally improves the utilization of cloud resources by hosting different customer’s applications into different virtual machines.
The technology difficulties of multiple-tenancy model include data isolation, architecture extension, configuration self-definition, and performance customization. Architecture extension means that multiple-tenancy should provide a basic framework to implement high flexibility and scalability. Performance customization means that cloud computing should assure different customer’s demands on performance of multiple-occupancy platform under different workload. The impact of multiple-tenancy model is different corresponding to different cloud deployment models.

Figure 6 Multiple-Tenancy Model of NIST

E. MODEL 5

The Cloud Risk Accrueement Model of CSA is described using figure 7. Understanding the layer dependency of cloud service models is very critical to analyse the security risks of cloud computing. So there is an inherited relation between service capability of different layers in cloud computing. Similar to inheritance of cloud service capability, security risks of cloud computing is also come into between different service layers. IaaS holds little security functions and capabilities except for the infrastructure’s own security functions and capabilities. IaaS demands that customers take charge of the security of operating systems, software applications and contents etc. Similarly, the intrinsic security function and capability of PaaS are not complete, but customers possess more flexibility to implement additional security.

One critical feature of cloud security architecture is that the lower service layer that a cloud service provider lies in, the more management duties and security capabilities that a customer is in charge of. In SaaS, cloud service providers need to satisfy the demands on SLA, security, monitor, compliance and duty expectation etc. In PaaS and IaaS, the above demands are charged by customers, and cloud service provider is only responsible for the availability and security of elementary services such as infrastructure component and underlying platform.[11]

Figure 7 the Cloud Risk Accumulation Model of CSA

IV. PROPOSED WORK

We have studied research papers related to security and privacy threats in distributed computing. In a few papers, tools and models are proposed to address security and privacy. After analysis of these contributions security and privacy issues are identified and reported.

A. Issues

The key area of the presented work for improving security is discussed as:

- **Issue-I**: Traditional security usages encryption standards which cannot be directly adopted by normal users. There is also a loss of control occurs over data towards cloud providers. Thus a new verification mechanism required to use without measuring the concerned issues for data.
- **Issue-II**: As the cloud faces continuous exchanges of data by users thus user needs to be authenticated for performing the operations on data. Thus, both cloud & user had to be verified for such operations.
- **Issue-III**: Since all the existing security mechanism focuses on the single server interaction environment. But as the interaction is increasing integration of security becomes difficult & complex. Thus a new mechanism required to develop which reduces the user efforts.
- **Issue-IV**: Botnets, huge volumes of spam or launching Distributed Denial of Service (DDoS) attacks on hosts are also some common issues.

B. Solution

Thus in order to provide solution client systems and their behavior elements are used as a key for encoding. This can be achieved by a known key cryptography method named as public key infrastructure with attribute values of user and data. It also added an additional padding bit with modified hash function to make the cloud more secure & reliable.
The proposed architecture is shown in the figure 8. It shows that when a user wants to access his data, he had to give request to a third party server, which verifies its integrity from its databases & having a specified trust value in case of each user with given authorization parameters like credentials, Role, Network properties etc. Then the third party auditor replies the user with its tenant ID having a unique kind of token to access the data. When a user demands an access to cloud this token gets verified and the permission is given. The petition for data storage from user had to go through an encryption service in which the user’s behaviour based key is used.

After this step cloud doesn’t know the type of data stored in storage. After this the cloud provides access ID for a data storage session to users to interact directly with storage. After applying such mechanism the problem related to data isolation & incorrect data display to the user is also solved.

C. Architecture & its Components

In order to provide the secure framework for the data outsourcing and data exchange in first step a data outsourcing system is developed according to given in figure 1. The given system development is divide in two modules first the primary server that have the data storage capability and the secondary server that utilizes the storage from the primary server.

The involved data exchange process and access of data provides the demonstration of security and identity management. The involved components of the system are described as:

Primary server: It is used as storage service provider which provides the hosting service for the outsourced data from the secondary server or other servers. Additionally that implements the data storage, off sourcing and outsourcing services to their clients.

User management: that is responsibility of primary server to keep in track the user or data owner who are going to host their own personal data or their organizational data. Therefore needs to create their membership with that server by which the privacy in data is maintained according to their membership policy.

User data manager: that is a personalize service provided to the client where the user host their data and keep in track their data according to their needs. In order to perform this user can alter, modify and perform other operations on the data which is either stored in primary server or secondary server.

Application and data: In addition of that a utility manager is available which support the data upload, download, share and exchange data to the third party under the directions of data owner.

Secondary server: In order to simulate the security management the secondary server is also established with the similar functions. Additionally other servers can also use the services of the primary server for deploying the similar functionality for clients. The users of secondary server send request to the primary server for data storage and on-demand data access. The data owner’s need their own data too access therefore some processes are implemented to upload, download and sharing of the data hosted in primary server. During this process of data request and management the security techniques are initiated to manage the personalization and authentication for data thus a trust computation technique is used to secure authentication and for providing the security in channel the cryptographic data exchange technique is included with the system.

C. Architecture & its Components

In order to provide the secure framework for the data outsourcing and data exchange in first step a data outsourcing system is developed according to given in figure 1. The given system development is divide in two modules first the primary server that have the data storage capability and the secondary server that utilizes the storage from the primary server.

The involved data exchange process and access of data provides the demonstration of security and identity management. The involved components of the system are described as:

Primary server: It is used as storage service provider which provides the hosting service for the outsourced data from the secondary server or other servers. Additionally that implements the data storage, off sourcing and outsourcing services to their clients.

User management: that is responsibility of primary server to keep in track the user or data owner who are going to host their own personal data or their organizational data. Therefore needs to create their membership with that server by which the privacy in data is maintained according to their membership policy.

User data manager: that is a personalize service provided to the client where the user host their data and keep in track their data according to their needs. In order to perform this user can alter, modify and perform other operations on the data which is either stored in primary server or secondary server.

Application and data: In addition of that a utility manager is available which support the data upload, download, share and exchange data to the third party under the directions of data owner.

Cryptographic Data exchange: in order to keep in track the security and privacy management for data exchange among both the parties (i.e. primary server and secondary server), the data exchange service is implemented that contains two sub-components in the system.

Trust manager: this component used to compute the trust among both the parties, if the computed trust value found adoptable then access to the system or data is provided to exchange the data.

Decision making: For making decision for authentic source of request or authenticated client a threshold (threshold values is point of trust rating which is statically fixed to the .75 and can be varies between 0-1) is computed. If the trust values are higher than the fixed threshold then the data outsourced or off sourced. In order to compute the trust the following formula is used:

\[ \text{Trust} = \frac{\text{Authentication Value}}{\text{Threshold Value}} \]

After this step cloud doesn’t know the type of data stored in storage. After this the cloud provides access ID for a data storage session to users to interact directly with storage. After applying such mechanism the problem related to data isolation & incorrect data display to the user is also solved.

C. Architecture & its Components

In order to provide the secure framework for the data outsourcing and data exchange in first step a data outsourcing system is developed according to given in figure 1. The given system development is divide in two modules first the primary server that have the data storage capability and the secondary server that utilizes the storage from the primary server.

The involved data exchange process and access of data provides the demonstration of security and identity management. The involved components of the system are described as:

Primary server: It is used as storage service provider which provides the hosting service for the outsourced data from the secondary server or other servers. Additionally that implements the data storage, off sourcing and outsourcing services to their clients.

User management: that is responsibility of primary server to keep in track the user or data owner who are going to host their own personal data or their organizational data. Therefore needs to create their membership with that server by which the privacy in data is maintained according to their membership policy.

User data manager: that is a personalize service provided to the client where the user host their data and keep in track their data according to their needs. In order to perform this user can alter, modify and perform other operations on the data which is either stored in primary server or secondary server.

Application and data: In addition of that a utility manager is available which support the data upload, download, share and exchange data to the third party under the directions of data owner.
V. CONCLUSION AND FUTURE WORK

Cloud computing is a kind of computing paradigm that can access conveniently in a dynamic and configurable public set of computing resources. In this environment the security of data and privacy during access of cloud is a primary concern. To contribute some effort to improve security of cloud a survey of existing security models of cloud computing is presented. Additionally the main security risks of cloud computing is also reported.

In the future, we will implement the proposed security strategies that involve different areas and issues of cloud security. Using the available cloud techniques required to demonstrate the effectiveness of the presented model of security and risk management.

REFERENCES


