Security Analysis of Cloud Computing: A Survey

Kamaljeet Pakhré1, Navdeep Singh2, Sanket Mani Tiwari3

1,2,3 Research Scholar, M. Tech. (CSE), Galgotias University, Greater Noida, India.

Abstract—Now these days is golden days of computing the internet has changed the computing world in a drastic way. Now computer service is fast with the help of parallel computing, distributed computing grid computing and a new technique is cloud computing. And it is very beneficial for computing. The user wants to access internet to anywhere to any time with respect of time consuming, cost consuming and fast service. The user uses the computer resources with the help of cloud computing and expect to maintain security form the server side. His/her information cannot access any unauthorized person. The basic model of cloud computing is providing the variety of computer resources over the internet. The main role play of cloud computing to make easy access of computer service. There are three types of service that provide cloud computing is software as a service (SaaS), platform as a service (PaaS) and the last one is infrastructure as a service (IaaS), which provide software for service and provide a platform to run any application and provide network and storage capacity for data defined as a computing. The main advantage of cloud computing is that customers do not have to pay for infrastructure, its installation, required manpower to handle such infrastructure and maintenance. In this paper, we will discuss cloud computing and new technique for data integrity.

Keywords—Cloud security, Data storage, Integrity verification, IaaS, PaaS, SaaS, PDP.

I. INTRODUCTION

Cloud computing provides the variety of resources over the internet and the definition is produced by U.S National institute of standards and technology (NIST). It define there are five key terms and four deployment models and three services and cloud computing we can define other words “Cloud computing is an on-demand network access to a shared pool of computing resources (e. g. Network, servers stage application and service). Which is an internet based technology consider the large size of outsource capacity. The objective of the study is to analyze the security requirement and highlight the existing threats in cloud computing effective security policies for cloud computing systems. It will help the researchers to identify security requirements at multiple levels to recognize the threads in the various cloud computing models posed by both internal and external users and thus will help to clarify cloud security policies that ensure the security of the cloud environment.

A. Resources of Cloud Computing

- Clint
- Server

- Platform
- Software
- Infrastructure

B. Deployment Model

Deployment models we can define easily it may be hosted by third party and it make the service effectively. With the help of deployment model we can access service easily and make good relationship between customer and service provider. There are several types the public cloud is a collection of computer resources and private cloud is a limited number of computer resources and hybrid cloud is a combination of public and private cloud. It is called deployment models.

1. Public Cloud

Public cloud is based on mainstream and we can say cloud resources shard outside there are no restrictions anyone can use it.

2. Private Cloud

The private cloud is that there are limited no of resources to use for people and it is used in any organization.

3. Hybrid Cloud

The concept of hybrid cloud is a collection of public and private cloud. Hybrid cloud like a private cloud linked to one or more services.

4. Community Cloud

The community cloud is a different type of cloud More than one community shares a cloud to share and reduce the cost of computing system. And is costly and time consuming.

C. Service Model

A service model is another type of model in cloud computing. The main work of service model has provided service to customers. The service model provides a toolkit for customer use and build software and develop software for future use. The platform as a service is provide a platform to run any type of software and application and also provide programming language for customer use. The infrastructure as a service is providing a network access and storage capacity for the user who want to store his data on the server end and it handles by cloud service providers. The service model plays a main role in cloud computing. There are mainly three types SaaS, PaaS and the last one is IaaS.
1. SaaS

SaaS model offers the as service as an application to the consumer using standard interfaces. These services run on top of cloud infrastructure and consumer cannot see. The software as a service which provides software and application, and manages on demand user software requirement for need application run. And cloud provider manages all thinks application, operating system and infrastructure. SaaS provides the services according to user requirement.

2. PaaS

Platform as a service which provide a platform for any type of application and it, Platform as a Service (PaaS) brings the benefits that SaaS bought for applications, the platform as a service offers the service as an an operational development platform for consumer. And but over to the software development world. PaaS can be defined as a computing platform that allows the creation of web applications quickly and easily and without the complexity of buying and maintaining the software and infrastructure underneath it. Clients are provided platforms access, which enables them to put their own customized software’s and other applications on the clouds.

3. IaaS

Infrastructure as a Service (IaaS) is a way of delivering Cloud Computing infrastructure – servers, storage, network and operating systems – as an on-demand service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service on demand.

II. RELATED WORK

Nam Yem Li highlights PDP scheme use for verification to avoid public verification. This paper proposed initial PDP solution to RSA based Hash function to authenticate the remote server storage data. However, due to RSA based cryptography, the entire computing speed is slow. Similarly Qian Wang et al, Proposed a protocol for Integrity verification in Multi cloud that is provided by improving the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication.

### A. Comparison between DES and RSA algorithm

<table>
<thead>
<tr>
<th>Features</th>
<th>DES</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key used</td>
<td>The same key is used for encryption and decryption purpose</td>
<td>Difference keys are used for encryption and decryption purpose</td>
</tr>
<tr>
<td>Scalability</td>
<td>It is a scalable algorithm due to varying the key size and block size</td>
<td>No scalability occurs</td>
</tr>
<tr>
<td>Avalanche effect</td>
<td>No more effected</td>
<td>More effected</td>
</tr>
<tr>
<td>Power consumption</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Throughput</td>
<td>Very high</td>
<td>Low</td>
</tr>
</tbody>
</table>

### B. We can define easily that DES is better than RSA

- DES uses a single key instead of two keys.
- The key size of des algorithm is 56 bits.
- The DES key use for both encryption and decryption.

![Figure 1: key diagram for DES algorithm](image-url)
III. INFORMATION SECURITY REQUIREMENTS

A. Identification & authentication

In Cloud computing, identified the user who access cloud computing services respect of cloud computing models and it should be allows the authorized user.

B. Authorization

Authorization is an important for security and it play a main role in maintaining integrity in cloud computing. Authorization is maintained by the system administrator in a Private cloud.

C. Confidentiality

The concept has been introduced confidentiality is made secure information and any unauthorized user cannot access your information without your permission because the cloud computing uses the multiple distributed database.

D. Integrity

The concept of integrity is to play a good role in security analysis and it makes your data secure and cannot manipulate user your data any unauthorized user. And now these days we use the RSA algorithm in PDP schemas ACID (atomicity, consistency, isolation and durability) properties of the cloud’s data should without a doubt be robustly imposed across all Cloud computing deliver models.

E. Non-repudiation

Non-repudiation in Cloud computing can be obtained by applying the traditional e-commerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services (digital receipting of messages confirming data sent/received).

F. Availability

Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document which highlights the trepidation of availability.

IV. THE SECURITY CHALLENGES

A. Privileged User Access

The means of privileged user access are that it processed Sensitive data outside the enterprise brings with it an inherent level of risk, because the services of outsourced is passing through the physical, logical and personnel controls IT departments exert over in-house programs. Put simply, outsiders users are now insiders.

B. Regulatory Compliance

The regulatory compliance is the main challenges for cloud computing. The whole Organizations are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. The ability to demonstrate to auditors that their data is secure despite a lack of physical control over systems, hinges in part on educating them, and in part on providing them with the necessary visibility into all activity.

C. Data Location

When we use cloud we don’t know where your data is hosted data location is an important challenge of cloud computing.

D. Data Segregation

Data segregation in cloud computing is typically in a shared environment on the data server from other customers. So we segregate data for maintaining cloud security.

E. Recovery

Recovery is also the main challenge for cloud computing because you don't know where your data is, and cloud service provider should maintain your data and service in case of disaster.

F. Investigative Support

The cloud service provider provides investigative support for data and service of cloud computing. With the help of it make more effective and efficient. “Investigating inappropriate or illegal activity may be impossible in cloud computing, because logging and data may be co-located and spread across ever-changing sets of hosts and data centers”.

G. Long-term Viability

The concept of long-term viability is the data is secure for a long time that helpful for decision making, recovery and future prediction. And it also support for maintaining good relationships for business purpose.

V. ADVANTAGES OF CLOUD COMPUTING

A. Less Maintenance

The advantage of cloud computing is less maintenance because the hardware application and bandwidth are managed by the cloud service provider.

B. Continuous Availability

The continuous availability means you can access cloud services to anywhere to any time because the public and cloud services are available wherever you are located.
C. Scalability
The means of scalable is you can pay only for application and data storage that you need.

D. Elasticity
The means of elasticity is you can scale your system on your demands. That is a very good advantage of cloud computing. Private clouds can be scaled to meet your changing IT system demands.

E. Expert service
The expert service is the services are monitored by experts who related to cloud computing and has lots of experience. And they maintain and monitored your data canter staff and technicians.

VI. CLOUD COMPUTING DISADVANTAGES

A. More elasticity means less control
The disadvantage of cloud computing of more elastic means less control. In the case of cloud computing there are several factors, including that make less control of cloud computing, e.g. openness, scalability, elasticity, distributed data store on server ends of cloud computing. These are disadvantages of cloud computing.

B. Not everything fit into cloud computing
Not the everything fits into the cloud in the case cloud computing is ever think is not fit in cloud computing is that the main reason is the openness and infrastructure of cloud computing depend on cloud computing application, operating system and it’s so we easily called has not ever thought fit into the cloud.

VII. FUTURE EXPECTATION
In future work, the security of cloud computing is main issues in terms of data storage security on server ends of cloud computing. Through the cryptography, which use public and private keys the public key encrypts the data and private keys decrypt data. With the help of cryptography we solve exiting problem. And we can use cooperative provable data possession scheme which reduces data block access and also reduce the amount of computation on the server ends. The cloud computing model is one of the promising computing models for both cloud providers and cloud consumers.

Data privacy: the important term of data privacy in cloud computing any unauthorized person cannot access your data that is more important for you

Key management: it also plays a good role in cloud computing the key management in which it’s clear who is controlling encryption /decryption key.

Data Integrity: Data integrity in the case of data integrity any unauthorized user cannot manipulate your data and your data is safe from danger

VIII. CONCLUSION
In this paper, we investigated the problem of data integrity of cloud computing for security analysis. And provide the data security for cloud data storage and it also ensures the correctness of user data storage. With the help of several algorithm use want to solve exiting problem we want to establish the good relationship between client and server. We use the comparative provable data possession with the help of we make the cloud computing more effective and more efficient and we use the DES algorithm in PDP schemas for it take low consumption. We want to secure our data with the help of cryptography and we use public and private key for encryption and decryption of data. In future work we want to implement in DES algorithm for PDP schemas in cloud computing. The concept of data security for cloud computing there are several reasons for making secure cloud computing server ends. The openness, scalability, elasticity, distributed and several factors. In this paper, we investigated the security challenges and the implementation of exiting problem with respect to security of cloud computing. The question arise why we want the secure data storage on server ends? The answer is very simple suppose we store the file on the server and one local copy is also stored on my PC in future suppose the file is corrupt and we access file from the server end is that the file is correct? In the sense there is no manipulate in the file. So we want to make our system secure.

REFERENCES
