A REVIEW OF CLOUD COMPUTING SECURITY ISSUES

SANIL UPADHYAY [1],ABHISHEK CHANDEL [2],ANKIT KUMAR TIWARI [3], TUSHAR VYAS [4] , MANISH MATHURIA[5]

[1,2]B.Tech Scholar, Department of Computer Science & Engineering, VIT, Jaipur, Rajasthan
[3,4]Assistant Professor, Department of Computer Science, Vivekananda Institute of Technology, Jaipur, Rajasthan
[5]Assistant Professor, Department of Computer Science, MACERC, Jaipur, Rajasthan

[1]Sanil.upadhyay12@gmail.com,[2]sainialvin99@gmail.com, [3]ankittiwari148@gmail.com, [4]vyas.tushar@vitj.ac.in, [5]manish.4598@gmail.com

ABSTRACT: *Cloud Computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. In today's era, it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Cloud Computing offers several features like easy deployment, connectivity, configuration, automation and scalability. This paradigm shift raises a broad range of security and privacy issues that must be taken into consideration. There are number of users used cloud to store their personal data, so that data storage security is required on the storage media. The major concern of cloud environment is security during upload the data on cloud server. Multi-tenancy, loss of control, and trust are key challenges in cloud computing environments Data storage at cloud server attracted incredible amount of consideration or spotlight from different communities. For outsourcing the data there is a need of third party. The importance of third party is to prevent and control unauthorized access to data store to the cloud.*

KEYWORDS : Cloud computing, cloud data storage, cloud data security, Deployment models, Privacy, Trust, and Virtualization.

1. INTRODUCTION

Cloud computing is revolutionizing many of our ecosystems. Compared with earlier methods of processing data, cloud computing environments provide significant benefits, such as the availability of automated tools to assemble, connect, configure and reconfigure virtualized resources on demand. However, the shift in paradigm that accompanies the adoption of cloud computing is increasingly giving rise to security and privacy considerations relating to facets of cloud computing such as multi-tenancy, trust, loss of control and accountability. According to the definition , cloud computing is "it is a significant distributed computing model that is directed by financial prudence of balance, in which stake of isolate, fundamental, loading, podium in which a facilities are supplied as per the request of exterior foreign clients through the internet". There are some examples of cloud services like webmail, online file and business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud storage specifies the storage on cloud with almost inexpensive storage and backup option for small enterprise. The actual storage location may be on single storage environment or replicated to multiple server storage based on importance of data [1].

Sensitive information in the context of cloud computing encompasses data from a wide range of different areas and disciplines. Data concerning health is a typical example of the type of sensitive information handled in cloud computing environments, and it is obvious that most individuals will want information related to their health to be secure. This paper presents an overview of the research on security and privacy of sensitive data in cloud computing environments [2].

The mechanism model of cloud storage consists of four layers: storage layer which stores the data, basic management layer which ensures security and stability of cloud storage itself, application interface layer which provides application service platform, and access layer which provides the access platform.

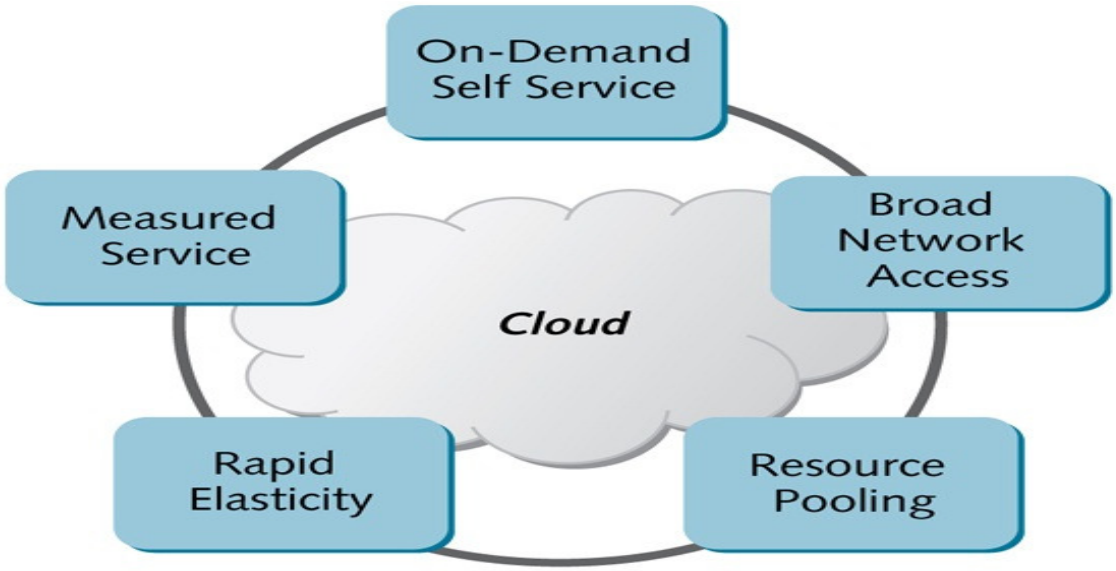

Figure1: Cloud Computing Characteristics

2. KEY CONCEPTS AND TECHNOLOGIES

Over the past few years, major IT vendors (such as Amazon, Microsoft and Google) have provided virtual machines (VMs), via their clouds, that customers could rent. By renting VMs via a cloud, the entire datacenter footprint of a modern enterprise can be reduced from thousands of physical servers to a few hundred (or even just dozens) of hosts.

While it is practical and cost effective to use cloud computing in this way, there can be issues with security when using systems that are not provided in-house. To look into these and find appropriate solutions, there are several key concepts and technologies that are widely used in cloud computing that need to be understood, such as virtualization mechanisms, varieties of cloud services, and "container" technologies [3, 4].

Table 1, Categorization of Cloud Service Models and Features

Service Model	Function	Example
SaaS	Allows consumers to run applications by virtualizing hardware on the resources of the cloud providers	Salesforce Customer Relationship Management (CRM)[3]
PaaS	Provides capability of deploying custom applications with their dependencies within an environment called a container.	Google App Engine[4], Heroku[5]
IaaS	Provides a hardware platform as a service such as virtual machines, processing, storage, networks and database services.	Amazon Elastic Compute Cloud (EC2)[6]

2.1. Virtualization Mechanisms

A hypervisor or virtual machine monitor (VMM) is a key component that resides between VMs and hardware to control the virtualized resource .It provides the means to run several isolated virtual machines on the same physical host. Hypervisors can be categorized into two groups:

• **Type I**: Here the hypervisor runs directly on the real system hardware, and there is no operating system (OS) under it. This approach is efficient as it eliminates any intermediary layers. Another benefit with this type of hypervisor is that security levels can be improved by isolating the guest VMs. That way, if a VM is compromised, it can only affect itself and will not interfere with the hypervisor or other guest VMs.

• **Type II**: The second type of hypervisor runs on a hosted OS that provides virtualization services, such as input/output (IO) device support and memory management. All VM
Interactions, such as IO requests, network operations and interrupts, are handled by the hypervisor.

2.2. Cloud Computing Characteristics

Cloud computing delivers computing software, platforms and infrastructures as services based on pay-as-you go models. Cloud service models can be deployed for on-demand storage and computing power in various ways: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Cloud computing service models have been evolved during the past few years within a variety of domains using the "as-a-Service" concept of cloud computing such as Business Integration-as-a-Service, Cloud-Based Analytics-as-a-Service (CLAaaS), Data-as-a-Service (DaaS) .

3. CLOUD SECURITY AND PRIVACY CHALLENGES

Cloud computing has raised several security threats such as data breaches, data loss, denial of service, and malicious attacks. These threats mainly originate from issues such as multi-tenancy, loss of control over data and trust.
Consequently the majority of cloud providers – including Amazon's Simple Storage Service (S3), the Google Compute Engine and the Citrix Cloud Platform - do not guarantee specific levels of security and privacy in their service level agreements (SLAs) as part of the contractual terms and conditions between cloud providers and consumers. This means that there are important concerns related to security and privacy that must be taken into consideration in using cloud computing by all parties involved in the cloud computing arena [5].

3.1. Security Issues in Cloud Computing

• **Multi-tenancy**: Multi-tenancy refers to sharing physical devices and virtualized resources between multiple independent users. Using this kind of arrangement means that an attacker could be on the same physical machine as the target. Cloud providers use multi-tenancy features to build infrastructures that can efficiently scale to meet customers' needs, however the sharing of resources means that it can be easier for an attacker to gain access to the target's data.
• **Loss of Control**: Loss of control is another potential breach of security that can occur where consumers' data, applications, and resources are hosted at the cloud provider's owned premises. As the users do not have explicit control over their data, this makes it possible for cloud providers to perform data mining over the users' data, which can lead to security issues. In addition, when the cloud providers backup data at different data centers, the consumers cannot be sure that their data is completely erased everywhere when they delete their data. This has the potential to lead to misuse of the un-erased data. In these types of situations where the consumers lose control over their data, they see the cloud provider as a black-box where they cannot directly monitor the resources transparently.
• **Trust Chain in Clouds**: Trust plays an important role in attracting more consumers by assuring on cloud providers. Due to loss of control (as discussed earlier), cloud users rely on the cloud providers using trust mechanisms as an alternative to giving users transparent control over their data and cloud resources. Therefore cloud providers build confidence amongst their customers by assuring them that the provider's operations are certified in compliance with organizational safeguards and standards.

3.2. Privacy Considerations of Processing Sensitive Data

The security issues in cloud computing lead to a number of privacy concerns. Privacy is a complex topic that has different interpretations depending on contexts, cultures and communities. It worth nothing that privacy and security are two distinct topics although security is generally necessary for providing privacy.
"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

4. SECURITY SOLUTIONS

This section reviews the research on security solution such as authentication, authorization, and identity management that as being necessary so that the activities of cloud providers are sufficiently secure[.

4.1 Authentication and Authorization

This study identifies a set of categories relevant for authentication and authorization for the cloud focusing on infrastructural organization which include classifications for credentials, and adapt those categories to the cloud context. The study also summarizes important factors that need to be taken into consideration when adopting or developing a solution for authentication and authorization – for example, identifying the appropriate requirements, categories, services, deployment models, lifecycle, and entities. Another authentication solution is seen with MiLAMob, which provides a SaaS authentication middleware for mobile consumers of IaaS cloud applications. MiLAMob is a middleware-layer that handles the real-time authentication events on behalf of

consumer devices with minimal HTTP traffic. The middleware currently supports mobile consumption of data on IaaS clouds such as Amazon's S3 [5, 6].

FermiCloud uses another approach for authentication and authorization - it utilizes public key infrastructure (PKI) X.509 certificates for user identification and authentication.

Another feature of the authorization system in this solution is that it develops a new concept using role inheritance for evaluating the trustworthiness of the system. In another study, Sendo et al. propose a user-centric approach for platform-level authorization of cloud services using the OAuth2 protocol to allow services to act on behalf of users when interacting with other services in order to avoid sharing usernames and passwords across service.

4.2 Identity and Access Management

The authors also present an authorization system for cloud federation using Shibboleth - an open source implementation of the security assertion markup language (SAML) for single sign-on with different cloud providers. This solution demonstrates how organizations can outsource authentication and authorization to third party clouds using an identity management system. Stiller et al. also propose an integral federated identity management for cloud computing. A trust relationship between a given user and SaaS domains is required so that SaaS users can access the application and resources that are provided. In a PaaS domain, there is an interceptor that acts as a proxy to accept the user's requests and execute them. The interceptor interacts with the secure token service (STS), and requests the security token using the WS-Trust specification.

E-ID authentication and uniform access to cloud storage service providers is an effort to build identity management systems for authenticating Portuguese citizens using national identification cards for cloud storage systems. In this approach, the Oath protocol is integrated for authorizing the cloud users. The e-ID cards contain PKI certificates that are signed by several levels of governmental departments. A certification authority is responsible for issuing the e-ID cards and verifying them. The e-ID cards enable users for identity-based encryption of data in cloud storage.

4.3 Confidentiality, Integrity, and Availability

Santos et al. extend the Terra design that enables users to verify the integrity of VMs in the cloud. The proposed solution is called the trusted cloud computing platform (TCCP), and the whole IaaS is considered to be a single system instead of granular hosts in Terra. In this approach, all nodes run a trusted virtual machine monitor to isolate and protect virtual machines. Users are given access to cloud services through the cloud manager component. The external trusted entity (ETE) is another component that provides a trust coordinator service in order to keep track of the trusted VMs in a cluster. The ETE can be used to attest the security of the VMs. A TCCP guarantees confidentiality and integrity in data and computation and it also enables users to attest to the cloud service provider to ensure whether the services are secure prior to setting up their VMs. These features are based on the trusted platform module (TPM) chip. The TPM contains a private endorsement key that uniquely identifies the TPM and some cryptographic functions that cannot be altered.

4.4 Security Monitoring and Incident Response

Anand presents a centralized monitoring solution for cloud applications consisting of monitoring the server, monitors, agents, configuration files and notification components. Redundancy, automatic healing, and multi-level notifications are other benefits of the proposed solution which are designed to avoid the typical drawbacks of a centralized monitoring system, such as limited scalability, low performance and single point of failure [8, 9].

Brinkmann et al. present a scalable distributed monitoring system for clouds using a distributed management tree that covers all the protocol-specific parameters for data collection. Data acquisition is done through specific handler implementations for each infrastructure-level data supplier. Data suppliers provide interoperability with cloud software, virtualization libraries and OS-level monitoring tools.

4.5 Security Policy Management

In the authors propose a generic security management framework allowing providers of cloud data management systems to define and enforce complex security policies through a policy management module. The user activities are stored and monitored for each storage system, and are made available to the policy management module. Users' actions are evaluated by a trust management module based on their past activities and are grouped as "fair" or "malicious". An appropriate architecture for security management which satisfies the requirements of policy definitions (such as flexibility, expressiveness, extendibility and correctness) has been implemented. The authors evaluated the proposed system on a data management system that is built on data storage.

Takabi et al. Introduce policy management as a service (PMaaS) to provide users with a unified control point for managing access policies in order to control access to cloud resources independently of the physical location of cloud providers. PMaaS is designed specifically to solve the issue of having multiple access control authorization mechanisms employed by cloud service providers that restrict the flexibility of applying custom access control to a particular service [10, 11].

There are three main requirements for building a general policy enforcement framework. First it must support various data types such as image, structured and textual data. Secondly, in a distributed environment there need to be several compute engines such as Map/Reduce, relational database management systems or clusters. Finally, access policy requirements in terms of access control policies, data sharing policies, and privacy policies need to be integrated with the general policy management framework. .

5. PRIVACY-PRESERVATION FOR SENSITIVE DATA IN CLOUD COMPUTING

Over the time, organizations have collected valuable information about the individuals in our societies that contain sensitive information, e.g. medical data. Researchers need to access and analyze such data using big data technologies in cloud computing, while organizations are required to enforce data protection compliance.

There has been considerable progress on privacy preservation for sensitive data in both industry and academia, e.g., solutions that develop protocols and tools for anonymization or encryption of data for confidentiality purposes. This section categorizes work related to this area according to different privacy protection requirements. However, these solutions have not yet been widely adopted by cloud service providers or organizations.

6. CONCLUSIONS

This paper described several cloud computing key concepts and technologies, such as virtualization, and containers. We also discussed several security challenges that are raised by existing or forthcoming privacy legislation.

The results that are presented in the area of cloud security and privacy are based on cloud provider activities, such as providing orchestration, resource abstraction, physical resource and cloud service management layers. Security and privacy factors that affect the activities of cloud providers in relation to the legal processioning of consumer data were identified.

6 REFERENCES:

1. M.Sharma, H.Bansal, AK. Sharma, Cloud Computing: Different Approaches & Security Challenges,International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2011

2.P. Kaur, S. Kaushal, "Security concerns in cloud computing", High Perform. Archit. Grid Comput., pp. 103-112, 2011.

3. Pearson Siani, "Privacy security and trust in cloud computing" in Privacy and Security for Cloud Computing, London:Springer, 2013

4."A survey on security issues and solutions at different layers of Cloud computing", J. Supercomput., vol. 63, no. 2, pp. 561-592, 2013.

5. AlashoorTawfiq, "Cloud computing: a review of security issues and solutions", International Journal of Cloud Computing, 2014.

6.IBM Blue Cloud project, http://www03.ibm.com/press/us/en/pressrelease/ 22613.wss.

7. Y. Zhang et al., "Cross-VM Side Channels and Their Use to Extract Private Keys", Proc. 19th ACM Conf. Computer and Comm. Security, pp. 305-316, 2012.

8. Dinesha H A and Agrawal V K 2012 Multi-level authentication technique for accessing cloud services International Journal on Cloud Computing: Services and Architecture (IJCCSA) 2 31-39

9. Doelitzscher F, Sulistio A, Reich C, Kuijs H and Wolf D 2011 Private cloud for collaboration and e-Learning services: from IaaS to SaaS J. Computing-Cloud Computing 91 23-42

10. Hamlen K, Kantarcioglu M, Khan L and Thuraisingham B 2012 Security issues for cloud computing Optimizing Information Security and Advancing Privacy Assurance: New Technologies 8 150-162

11. Jain S, Kumar R, Kumawat S and Jangir S K 2014 An analysis of security and privacy issues, Challenges with possible solution in cloud computing Proc. of the National Conf. on Computational and Mathematical Sciences (COMPUTATIA-IV) 1-7