IJITKM 0973-4414 Volume-10, Number-2 Jan-June 2017 pp. 141-149 available online at www.csjournals.com

Data Security Issues in Cloud Environment: A Survey

Er. Seema Rani
Assistant Professor, Computer Science and Engineering, CDLSIET, Sirsa.

Abstract
Customers can now choose software and information technology services based on their needs and rent these services from supplier of network services, and it's capable of modifying its requirements to grow or shrink. This service is provided by the infrastructure provider, a third party; it's called cloud computing. Numerous benefits are offered to the user by cloud computing, including flexibility, superior scalability economics, resilience to issues, and the possibility to outsource non-core tasks. Recent years have seen cloud computing gain popularity in the industry due to its appealing features, which has motivated both industry and academic research. The popularity of cloud computing as a technology has increased recently. It's a way to store, retrieve, and move files and applications via the Internet rather than your local computer. It offers a wide range of services. Furthermore, data saved on the cloud is typically not readily lost. It allows for customization and lessens network complexity. Furthermore, it is simple for hackers to release data that is stored on the cloud. Organizations can adopt cloud computing as a more cost-effective solution since it requires no upfront costs, and its frequent and extensive use is growing daily. Even with all the advantages that a cloud computing platform can provide, there are some concerns and uncertainties about the security risks involved. The primary cause of security problems is external control on organizational structure and management, which may jeopardize the organization's private and confidential data. There is a very real risk of availability, confidentiality, and integrity breaches involving private and sensitive information in this computer environment. The fundamental reason behind the growth of cloud computing is these security issues and obstacles. Appropriate security measures must be implemented. Additionally, it is easy for hackers to leak data stored on the cloud.
Keywords: Cloud Service, Cloud Security, Threats.

I INTRODUCTION

Cloud-based computing is quickly becoming most advantageous tool to businesses looking for a scalable, affordable, adaptable, and flexible computing solution for routine operations. A network of centralized computer infrastructure that can be swiftly set up, scaled to meet user needs, and requires no maintenance effort is provided by cloud computing [1].Network users can access configurable computing resources (servers, networks, storage, apps, and services) anywhere, anytime, and without the management or involvement of a service provider by utilizing a cloud computing paradigm. The primary areas of worry have been privacy and general security, in contrast to the benefits of cloud computing [2]. It is exceedingly challenging for users to administer or control a cloud. A cloud's resources originate externally. Despite having more robust and dependable management skills and a stable cloud computing system

infrastructure, cloud computing still has issues with risks to security that come from both inside and outside sources. The fundamental idea behind cloud computing is its architecture and the way it responds to user requests. The user rents computer resources for the duration of their use, and the resources are always kept somewhere else under someone else's ownership. [3].

This cloud architecture consists of four deployment types, three service models, and five basic features. The five essential elements are extensive network access, self-service on-demand, measurable service, rapid flexibility, and resource pooling. Three service delivery methods are available in the cloud: PaaS (Platform as a Service), SaaS (Software as a Service), and IaaS (Infrastructure as a Service). There are four different deployment methods available: Public, Private, Community, and Hybrid. The rest of the paper is organized in this manner. Section I highlights the introduction. Section II outlines the essential characterstics of cloud computing. Section III presents cloud deployment models. Section IV presents the security challenges and Section V explains security issues based on cloud delivery and deployment models. The paper is concluded in Section VI.

II ESSENTIAL CHARACTERISTICS[14][15]:

1. Self-service on-demand

Users have the ability to independently get computational resources, like server time and network storage, without the need for direct human interaction with each service provider.

2. Broad network access

The functionalities are obtainable via network, employing common protocols that enable utilization on a range of thick- and thin-client devices, including computers, tablets, workstations, mobile phones etc.

3. Pooling of resources

In a multi arrangement, providers pool their computing resources to service numerous customers. Depending on user demand, various virtual and physical resources are dynamically allocated and redistributed. Customers can define location preferences at a higher level, such nation, state, or datacenter, even though they typically have little control over the exact location of these resources. Resources include memory, computing power, storage, and network throughput.

4. Rapid elasticity

Elastic provisioning and release of capabilities allows them to quickly scale up or decreased in reaction to the need. From the user's perspective, the abilities that are accessible for provisioning frequently appear infinite, permitting appropriation in any amount at any moment.

5. Service measurement

Including particular kind of service, cloud systems automatically manage and optimize resource usage, including processing, storage, bandwidth, and active user accounts. This makes it feasible to monitor, control, and report on resource usage continually, providing transparency to the client and service provider.

III MODELS FOR CLOUD DEPLOYMENT

There are four main deployment models for cloud computing. The four primary cloud computing deployment models are shown in Figure 1.

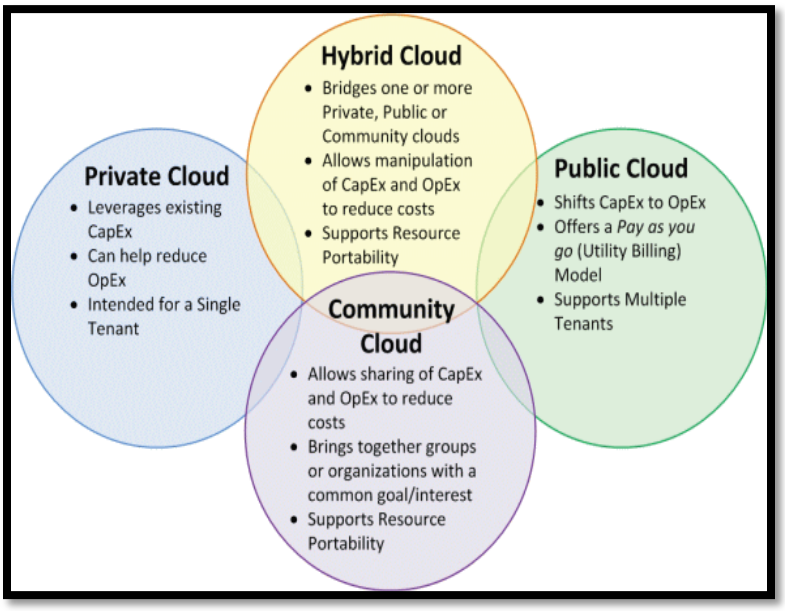

Figure.1 Models for Cloud Deployment

1. Public Cloud:

This publicly accessible cloud infrastructure may be owned, operated, and managed by a commercial company, governmental organization, or a mix of these. The cloud provider's premises are the only location for the public cloud. Here, third-party service providers or any other external entity can access and administer cloud infrastructure. Since shared apps, although there isn't always a risk of attack on data stored on public clouds, these are less secure than alternative models. This methodology is adaptable enough to handle sporadic requests for cloud environment optimization[6,7,8].

2. Private Cloud

An infrastructure on the cloud that is only available to one company and its many users, including business units. The company itself, a third party or both of them together may own manage in addition run this infrastructure, which may be located on or off site. This approach

guarantees the management of continuous privacy and security issues of cloud computing. Both apps and infrastructure are combined in this architecture for user sharing. In this case, the company using the cloud is in charge of managing its own apps and resources. Due to internal use, where only designated users and the company itself may use the cloud's services, this is more secure. Because only the internal organization and designated users may use the cloud infrastructure's services, which is more secure [4].

3. Community Cloud

A certain customer community is the only one to have access to this cloud infrastructure collectively that is composed of businesses with similar goals, security needs and policies. A third party, a number of community organizations, or a mix of them may take on ownership, management, and operation. The communal cloud could be located on or off campus. In this case, regardless of the required solution, members of a specific community or organizations who share concerns about security, projects, applications, research, and jurisdiction share cloud computing infrastructure because it is vital to have a shared and common central cloud computing facility. A collection of private clouds can be thought of as a community cloud[6,7].

4. Hybrid Cloud:

A mix of two or more distinct cloud infrastructures, whether private, public, or communal, connected by standardized or proprietary technologies but remaining autonomous. Applications and data can be moved around thanks to this connectivity, as demonstrated by features like load balancing between clouds through cloud bursting. In this instance, the fundamental qualities of each cloud computing model are retained when two or more are combined to form a composite cloud. In this scenario, two or more clouds are linked to external cloud services that are all contained within a secure network and are administered centrally as a single entity. Hybrid clouds are able to provide virtual cloud services and more secure control by making use of every resource inside their cluster of public and private clouds [6].

IV SECURITY CHALLENGES IN CLOUD COMPUTING

Numerous security issues that arise with cloud computing can be divided into two primary categories: issues that cloud providers deal with and issues that their clients confront. It is the provider's responsibility to guarantee the security of their apps, infrastructure, and customer data. Customers also need to confirm that the supplier has put in place sufficient security measures to safeguard their data.

As outlined by Gartner [9], the subsequent security concerns warrant consideration:

• **Privileged Access**: The hiring and administration of administrators with such credentials poses concerns when identifying who has privileged or specialized access to data.

• **Data Location**: Clients might be worried about how much control they actually have over where their data is located in the cloud.

• **Data Segregation**: Ensuring that encryption is accessible at all times leads to expert designers and testers of encryption methods conducting research.

• **Data Availabilit**y: Clients wonder if the cloud provider can transfer their whole dataset to an alternative environment in the case of an environment breach or unavailability.

• **Regulatory Compliance**: In order to ensure compliance with applicable rules, customers want reassurance from cloud vendors that they are prepared to go through certifications for security and external audits.

• **Recovery**: When discussing data recovery in disaster situations, it is important to take into account the vendor's capacity to provide full restoration as well as the turnaround time.

• **Investigative Support**: To guarantee a secure cloud environment, assess the vendor's competence to look into improper or unlawful activity.

• **Long-Term Viability**: Clients need to consider what will happen to their data in the event that the cloud vendor fails, including how their data will be returned and formatted.

V SECURITY ISSUES BASED ON CLOUD DELIVERY & DEPLOYMENT MODELS

When putting a cloud implementation into practice, Its services include its platform, storage, software, and networking infrastructure, all of which can be tailored to the needs of the user, as shown in Figure 2.

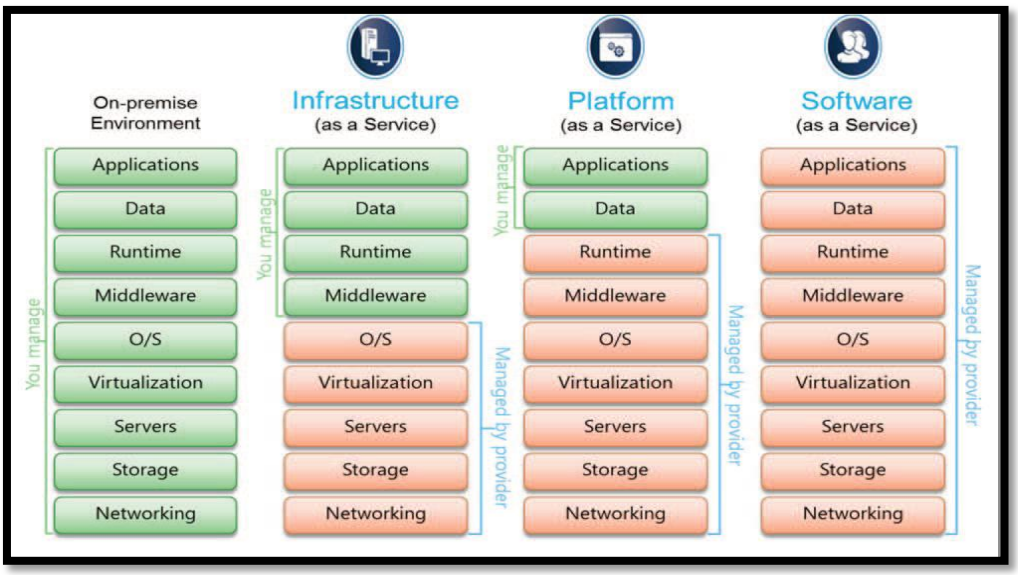

Figure.2 Deployment Model for delivery of a Cloud

1. Software as a Service (SaaS): Because providers are largely responsible for security, clients are dependent on the security measures that providers deploy. Because private clouds are more secure than public clouds, the former require more stringent security measures. SaaS makes it difficult for consumers to maintain security, and private clouds could need more extensibility for customisation. Data security, data locality, data integrity, data segregation, data access, data confidentiality, network security, authentication and authorization, availability, and identity management are important security components for SaaS application development that are emphasized by Gartner [10].

2. Platform as a Service (PaaS): transfers accountability for security to clients developing apps on supplied platforms. The service provider's system provides software and development tools for this platform. It facilitates the development of apps without requiring understanding of the cloud computing system's core workings. PaaS provides a comprehensive environment for software development, including client-side planning, designing, testing, and implementation. Here, every virtual computer needs to be protected from harmful intrusions. This platform includes Windows Azure and WOLF cloud middleware. The primary aim of providers is to isolate client workspaces and applications, which means that clients must uphold authentication checks and preserve application integrity [5].

3. Infrastructure as a Service (IaaS) highlights the power of the consumer to manage data kept on the hardware of the provider. Users are responsible for protecting their operating systems, apps, and content, and cloud providers are required to provide basic data protection. Customers can use a network to access these applications, which are hosted by any vendor. Because SaaS supports web services and service-oriented architecture (SOA), it is a more widely used delivery model. Usually, it operates on a pay-as-you-go or subscription basis. SaaS provides a multi-tenancy design that supports numerous concurrent users. Here, web browser security is crucial because software is typically accessed through it. The technologies that are available for protecting data on the cloud include Secure Socket Layer (SSL), Web Services (WS) security, and encryption of XML. Examples of SaaS are Facebook and Sales Force [5].

Public clouds require extra security measures to be trusted because of their wide area network accessibility, which makes them intrinsically less safe when taking deployment methods into account. Private clouds give more security customized for individual companies, and hybrid clouds—which combine public and private clouds—offer centralized security administration.

- **Authorization**: Authorization is a crucial information security need for maintaining referential integrity in cloud computing. It entails claiming authority and privileges over the flow of processes in the cloud computing environment. Appropriate authorization is necessary regardless of the delivery style employed, particularly in public clouds, where a single service provider's computer resources are shared by a large number of clients. Authorization in private clouds is usually managed by the system manager.

- **Authentication & Identification**: In public and private clouds, identity and authentication are essential for managing privacy, compliance, data collecting, and threats from the inside and outside. It is essential that the cloud service provider be able to set up secure architecture to safeguard client data and stop illegal access. Before accessing any data via the cloud, each cloud user is verified and validated based on their credentials thanks to the deployment of identity and authentication processes. This means that in both public and private clouds, identity and authentication are essential security requirements.
- **Integrity**: Using due diligence is part of the integrity required in cloud computing, especially when gaining access to data. Every model of cloud computing delivery should firmly enforce the cloud data ACID (Atomicity, Consistency, Isolation, and Durability) attributes[11].
- **Confidentiality:** Confidentiality plays a big element, when it comes to keeping control over data that is spread over several databases for enterprises. Maintaining the privacy of users and their data that is accessed electronically makes it possible to apply information security policies throughout different cloud application levels. The protection of data, which is difficult to ensure in public cloud systems, can be enhanced by utilizing several private clouds managed by reputable businesses[12].
- **Availability:** Most important need for cloud computing is availability, which affects choices between private, public, or hybrid cloud providers and delivery methods. Concerns about resource and service availability amongst the client and the cloud provider are brought to light by the service level agreement. Availability is a prerequisite for Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) in both public and private cloud environments. In private clouds, where all services are internal to the business, availability for Software as a Service (SaaS) is equally essential[12].
- **Non-Repudiation**: Token provisioning and standard e-commerce security protocols can be used to accomplish non-repudiation in cloud computing when it comes to data transmission within cloud apps. To ensure the non-repudiation of messages confirming data transferred or received, this also includes the use of timestamps, digital signatures, and confirmation receipt services.

VI CONCLUSION

Security risks, such as the increased vulnerability of cloud systems to assaults by unauthorized users or undesired activity constantly threaten widespread adoption of cloud computing systems. Verify whether or not appropriate security precautions have been implemented before implementing a cloud infrastructure. The ability of cloud computing platforms to scale up or down in accordance with user requirements and to share hardware and software resources at a reasonable cost has been demonstrated and validated. If the user is not utilizing the amenities, there are essentially no fees. In addition to issues like DoS, network security, data security and locality in SaaS models, network and host intrusion in PaaS and IaaS, and issues related to

confidentiality, integrity, availability, and authenticity (CIAA), this study looks at the security issues related to cloud computing environments. Methods for reducing the risks have also been discussed. Despite the fact that cloud computing is still latest, experts are working to improve its security and usability to lower the overall cost of starting a business. Instead of concentrating on the storage of data, the choice of application, or the data usage by employees, an organization should concentrate on its core business. A single window of access must be provided for all of these functions in cloud environment. Cloud computing is capable to emerge as the leading virtual, cost-effective, scalable, flexible, user-friendly, and secure platform for IT-enabled services in very near future.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," US Nat'l Inst. of Science and Technology, 2011.

[2] Zhou M., Zhang R., Xie W., Qian W., Zhou A., "Security and privacy in cloud computing: a survey", In Proceedings of IEEE 6th International Conference on Semantics, Knowledge and Grids, Pp 105–111, 2010.

[3] Bisong, A. and Rahman, S.S.M.,"An Overview of the Security Concerns in Enterprise Cloud Computing", International Journal of Network Security & Its Applications, 3(1), Pp 30-45, 2011, doi:10.5121/ijnsa.2011.3103.

[4] S. Arnold, "Cloud computing and the issue of privacy", KM World, Pp 14-22, Jul 2009.

[5] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Bandic, I.: Cloud Computing and emerging IT platforms: vision, hype, and relatity for deliverling computing as the 5th utility. Future Generation Computer System 25(6), 599–616 (2009)

[6] Takabi, H., Joshi, J.B.D.: Security and privacy challenges in cloud computing environment. IEEE Journal on Security and Privacy 8(6) (November 2010)

[7] Yang, J., Chen, Z.: Cloud computing research and security issues. In: The Proceeding of IEEE International Conference on Computational Intelligence and Software Engineering, pp. 1–3 (2010)

[8] Kaur, P., Kaushal, S.: Security concerns in cloud computing. In: Accepted For International Conference on High Performance Architecture And Grid Computing-2011. Chitkara University, Rajpura (2011) 454 A. Verma and S. Kaushal

[9] Brodkin, J.: Gartner: Seven cloud-computing security risks. In: Infoworld 2008 (2008),

[10] Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Application, 1–11 (2010)

[11] S. Subashini, v. Kavitha , 2011. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications volume 34, issue 1, pages 1–11.Elsevier

[12] Randy Garcia, c. Edward chow. identity considerations for public sector hybrid cloud computing solutions .2015. 2015 international conference on computer communication and informatics (iccci -2015), Jan. 08 – 10, 2015, Coimbatore, india. IEEE

[13] Debasish jana, debasis bandyopadhyay, controlled privacy in mobile cloud.2015.in IEEE 2nd international conference on recent trends in information systems (retis).IEEE.

[14] Zhifeng xiao and yang xiao. 2013. Security and privacy in cloud computing .in IEEE communications surveys & tutorials, vol. 15, no. 2.IEEE.

[15] Ashish Kumar Singh, Ashutosh Rawat, Jithin James and N. Jeyanthi., 2015. CAESAR CLOUD: A Comprehensive Approach for Enhancing Cloud Security and Service Availability based on Reputation. In International Journal of Cloud-Computing and Super-Computing Vol.2, No.2 (2015), pp.21-28.IJCS.