Data Security in Cloud Computing

Vidhi Sharma, Vaibhav Tyagi, Vaibhav Srivastava

*Department of Computer Science & Engineering, IPEC*

*Sahibabad, Ghaziabad, Uttar Pradesh 201010, India*

*(Approved by AICTE & Affiliated to AKTU, Lucknow, Uttar Pradesh)*

*1900300100242@ipec.org.in*

*1900300100240@ipec.org.in*

*1900300100239@ipec.org.in*

**Abstract** — This paper is an overview of the issues in data security in cloud computing. This paper will go into details of methods of data protection and approaches used to ensure maximum data protection by reducing risks and threats. It is beneficial to store data in cloud but it also poses risks by exposing data to applications which might have security loopholes in them. The security problem of cloud computing is huge and can prevent the rapid development of cloud computing. This study is based on all the cloud service models i.e. SaaS (Software as a Service), PaaS (Platforms a Service) and IaaS (Infrastructure as a Service) and cloud deployment models i.e. public, private, hybrid and community cloud models.

**Keywords**— Data Security, Cloud Computing, Data Protection, Privacy, Risks, threats, cloud service models and cloud deployment models.

1. INTRODUCTION

[1] Cloud computing is the on-demand availability of computer system resources. It is the development of parallel computing, distributed computing, grid computing, and consists of Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). It is an emerging technology and has drawn enough attention of industries. In the simple words, cloud computing or cloud means storing and accessing data and programs over the internet instead of storing it in your hard drives. [2] The word “cloud” is used as metaphor which define web as a space where computing has been preinstalled and exists as a service which includes data, operating systems, applications, storage and processing power exist on the web ready to be shared and delivered. Cloud computing can much improve the availability of IT resources and has many advantages over other computing techniques. Users can use the IT infrastructure with Pay-per-Use-On-Demand mode; this would benefit them and they will save a huge amount of money spend in buying the physical resources that may be vacant.

**Organization.** The rest of the paper is organized as follows: In Section II, we define Cloud Service Models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Then, we define Cloud Deployment Model in Section III. In Section IV, we explain about Data Security and need of data security in cloud computing. Further we discuss about methods to ensure security in Section V.

II. CLOUD SERVICE MODELS

There are different service models available for the cloud. The three most common models are SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Different model provides different level of manageability and customization for client’s solution. [4] Fig. 1 shows a cloud reference architecture.

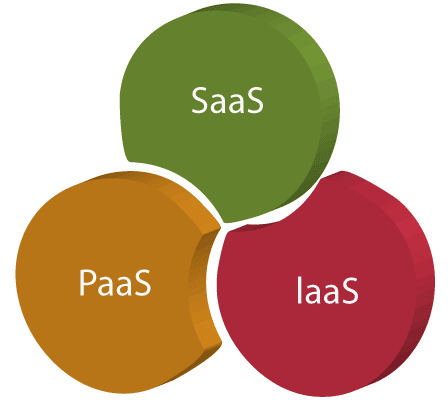


Fig. 1. The cloud reference architecture

1. *Software as a Service (SaaS)*

SaaS is also known as "on-demand software". Software as a Service (SaaS) cloud consumers release their applications in a hosting environment, which is accessed through networks from various clients (e.g. Web browser etc.) by application users. An example of this would be Google’s Gmail. This email application is completely managed and accessed over the internet. Users are not required to install any software on their local device to be able to use it. Other Examples of SaaS include Dropbox, Google Docs, Microsoft Office Suite and so forth. SaaS applications are usually simple in design to ensure ease of use for a wide range of users. From a perspective of user, this offers the least amount of customization for the application itself.

1. *Platform as a Service (PaaS)*

Platform as a Service (PaaS) is a development platform which supports the full “Software Lifecycle” that allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. Thus, the difference between SaaS and PaaS is that SaaS only hosts completed cloud applications whereas PaaS offers a development platform that hosts Cloud Computing along with Research Issues, Challenges, Architecture, Platforms and Applications. PaaS offers built-in security, web service interfaces, and scalability. An example of PaaS is Google AppEngine.

1. *Infrastructure as a Service (IaaS)*

Infrastructure as a Service (IaaS) cloud consumers utilize IT infrastructures (storage, networks and other fundamental computing resources) provided in the IaaS cloud straightway. It is also called Hardware as a Service (HaaS). The main preference of using Infrastructure as a Service is that it helps users to avoid the cost and complexity of buying and managing the physical servers. Virtualization is broadly used in IaaS cloud. The primary strategy of virtualization is to set up independent virtual machines (VM) that are isolated from underlying hardware and other VMs.[3] IaaS resources such as storage devices, bandwidth, virtual machines, IP addresses, monitoring services, firewalls, etc. are accessible to the customers on rent. The fee is based upon the amount of time the customer owns a resource. An example of IaaS is Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE) etc.

III. CLOUD DEPLOYMENT MODELS

Cloud deployment model depicts the accurate type of cloud environment based on ownership, size, and access. It also defines the nature and purpose of the cloud. Most organizations implement cloud infrastructure to put down capital expenditure and operating costs. [4]Fig 2 shows types of cloud deployment models.

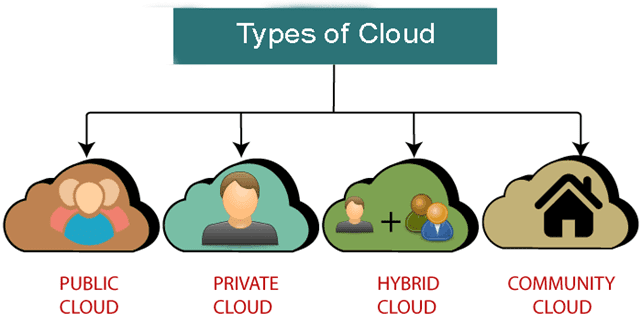


Fig. 2. Types of cloud deployment models.

1. *Public Cloud Model*

[5]Public Cloud allows systems and services to be easily accessible to the general public. The IT giants such as Google, Amazon and Microsoft offer cloud services via the Internet.

Public cloud operates on the pay-as-per-use model and administered by the third party, i.e., Cloud service provider. Public cloud is owned, managed, and operated by businesses, universities, government organizations, or a combination of them. Few examples of companies providing public cloud model facilities are Amazon, Microsoft, IBM, Google, etc. This cloud model is open for use. This type of cloud computing is a true instance of cloud hosting where the service providers supply services to various clients. The major drawback about the public clouds is that they are not completely secured.

1. *Private Cloud model*

Public and Private cloud model architectures are very similar. There is slight difference between a public and a private model from the technical point of view. As public cloud is available to the general public private cloud model is owned by only one specific company. Hence, it is also called an internal or corporate cloud. Private clouds are highly private and secured i.e. Private cloud resource sharing is highly secured.

1. *Community Cloud*

A community deployment model largely bear a resemblance to a private one; the only difference is the set of users. While a private type model suggests that only one company owns the server, in the case of a community one, various companies with similar backgrounds share the infrastructure and related resources. Community Cloud model allows systems and services to be obtainable by a set of organizations. It shares the infrastructure among various organizations from a specific community. It can be supervised internally by organizations or by the third-party. Some example of such community is where organizations/firms are there along with the financial institutions/banks. In comparison to public cloud, public cloud is more secure but less secure than the private cloud.

1. *Hybrid Cloud*

 Hybrid cloud model is totally integrated, i.e. it can be a combination of two or more cloud servers, i.e. private, public or community combined as one architecture, but remain individual units. Hybrid cloud deployment model safeguards and controls strategically important assets. It does so in the most cost- and resource-effective way possible for each specific case.

IV*.* DATA SECURITY AND NEED OF DATA SECURITY IN CLOUD COMPUTING

*A. Data Security*

Data security refers to the protection of all forms of digital data from malicious intruders, and from the unwanted actions of unauthorized users, such as a cyber-attack or a data theft. It’s a concept that covers every aspect of information security, be it the physical security of hardware and storage devices to administrative and access controls or the logical security of software applications. It also includes organizational policies and procedures.

*B. Need for Data Security*

The spectrum covered by the internet and the global networks are expanding day by day, hence more and more people are engaging in online computing. Their day to day online activities involve website browsing, sharing of personal data and utilisation of various online services. When so much private information is being shared over the internet with each passing second, it becomes essential to pay attention to the security aspect of all this information. Data security is required to keep the user data safe, away from any kinds of threats or malicious hackers. Confidentiality and integrity of this information should be maintained at every point of time. Basically, data security is a must for maintaining the CIA (confidentiality, integrity, availability) triad of computer system security.

1. Data loss: since the third party is handling the data so there is no guarantee of data security.
2. Hacked interfaces and APIs: when a user accesses data from a service provider, API is needed and that can be hacked by hacker.
3. Data breach: data can be leaked while browsing.
4. Vendor lock in: vendor acts like a middle party between service provider and user, and between multiple service providers and that also needs to be secured.
5. Account hijacking: attacker can access the important credentials like password, id, through which can easily access the service from service provider.
6. Data privacy and confidentiality: many times the services provider stores the important and confidential data and that data need to be secured.

1. *Data Security and the Cloud*

Securing cloud-based infrastructures requires a different approach than the traditional model of situating defences at the network’s perimeter. [6] It demands comprehensive cloud data discovery and classification tools, plus ongoing activity. monitoring and risk management. Cloud monitoring tools can sit between a cloud provider’s database-as-a-service (DBaaS) solution and monitor data in transit or redirect traffic to your existing security platform. This allows for policies to be applied uniformly no matter where the data resides.

In terms of cloud computing, security has two major aspects, first, what constitutes the cloud security, and the second, the potential threats that can hamper the data security stored on the cloud. The components of cloud security:

1) Set of policies: All service providers over the cloud must come up with efficient and strict security policies to ensure that the data of people using their services remains safe and confidential.

2) Control (access control): It is to be ensured that the policies need to be executed strictly by the user to ensure security.

3) Procedure and technologies: Cloud security involves the procedures and technology that secure cloud computing environments against both external and insider cybersecurity threats. [7] Cloud computing, which is the delivery of information technology services over the internet, has become a must for businesses and governments seeking to accelerate innovation and collaboration.

1. *Threats*

1. DOS (Denial of Service): tries to bring the server down.
2. MIM (Man in the middle): listens to communication between cloud and client.
3. NS (network sniffing): monitoring all the traffic in the network.
4. PS (Port Scanning): hacker tries to steal about ports used.
5. SIA (SQL injection attack): tries to steal user credentials from the database.
6. XSS (Cross Site Scripting Attack): embedding harmful links.

1. *Cloud Security Governance*

[6]Cloud security governance refers to the management model that facilitates effective and efficient security management in a closed environment to achieve business targets. Requirements of security governance in cloud computing:

* 1. For ensuring the different security aspects within the organization.
  2. For defining the best practices of security within the organization.

It's important to sign out of the accounts or online sessions to stop anyone else from gaining access to our files—especially in the case of shared computers. Unmonitored accounts with ongoing sessions leave the data vulnerable and exposed and are

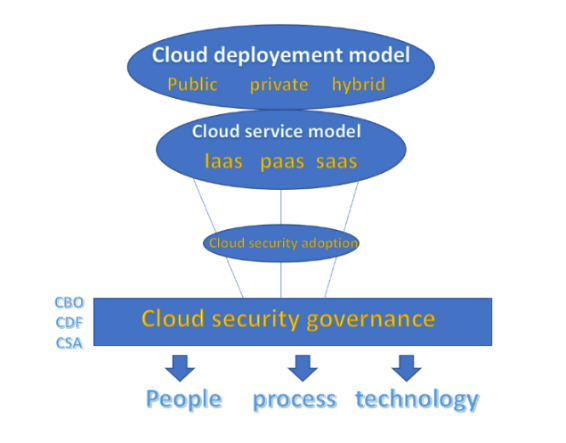


Fig. 3. Cloud Security Governance

CBO: Cloud Business Office, monitor different activities, fulfil requirements.

CSA: Cloud Security Alliance (CSA) is a not-for-profit organization, responsible for updates that improves security.

V.   METHODS TO ENSURE SECURITY

Ensuring the security of the data is an equal responsibility of both the users and the cloud service providers. There are certain strategies that can be followed by both of these groups in order to achieve maximum data security over the cloud.

*A. Methods to secure data security from service provider’s end*

* + 1. 1) Understand the lifecycle of data: Large businesses that run over the cloud and have successful security policies know their data. More importantly, they know where it is stored and how it is being used. Mapping data flow enables companies to better assess the vulnerable or exposed points. Additionally, large companies employ discovery tools that help them to make sure that the accessibility of data is possible for the authorized personnel only.

2) Encryption: To protect their data, the service providers on the cloud often make use of encryption for computers, data at rest, data in transit, and data in the cloud. Encryption serves as a security precaution for remote-transfer of data, as it makes sure that only the sender and receiver can understand the encrypted message, no third party can decrypt the data even if they succeed at stealing it mid transfer. Encryption helps secure devices and maintain data integrity regardless of what network a device is working on.

3) Use cloud security tools: Large companies today use the cloud extensively, from data storage to using it as a software platform. They use certain cloud security tools for encrypting data before it is uploaded to the cloud, monitoring end-points, categorising data according to risk levels and tracking data movement within the cloud. For example, AWS (amazon web services) utilizes a variety of such tools like GuardDuty, AWS shield, and Cloud Watch.

4) Educate employees: Employees and human error cause the majority of data breaches according to a Red Team security report.to avoid such events, large companies are now putting more emphasis on training both low-level and high-level employees in data protection. Using access management tools substantially helps large companies in restricting access to sensitive and confidential data, making sure only those who are authorized can access it.

5) Develop BYOD policies: Developing a BYOD (bring their own devices) policy is becoming more and more critical for large companies. The personal devices on which the employees work are not uniformly secure. [8] Moreover, since employees usually take these devices home, they are outside the company’s safe network. To resolve this issue, many large companies restrict what sensitive information can be transferred to personal devices or devices that go off company property. Another method is to employees the option to upgrade their device security to the level of the company’s devices. For example, some companies have an automatic delete program designed to wipe confidential information from a device if it goes outside a certain geolocation perimeter.

*B. Methods to secure data security from user’s end*

1) Use Strong Passwords and Two-Factor Authentication: Strong passwords are essential for keeping your online accounts and personal information safe and away from cyber criminals, and enabling Two-Factor Authentication provides an additional layer of security.

2) Auditing of Files: It is beneficial to run a regular audit of all the shares that are currently active on account. For those shares that do need to stay active, users can change the status of these shares to read only unless the other parties absolutely need to be able to edit files. For example, Dropbox web interface and Google Drive offer these features.

3) Check on Connected Apps and Account: Hackers and intruders might try to steal user data through another account that's connected to the users cloud storage. Having connections between various accounts and apps makes computing easy, but it also makes the user account more vulnerable. Users must make sure to regularly check which third-party applications have access to their cloud storage, and remove any that they are not actively using.

4) Enable Account Recovery Options i.e. Backup: The idea behind maintaining a backup is to generate a copy of data that can be recovered in the event of a data failure. [9] Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data.

5)  Sign out when not using the accounts: It's important to sign out of the accounts or online sessions to stop anyone else from gaining access to our files—especially in the case of shared computers. Unmonitored accounts with ongoing sessions leave the data vulnerable and exposed and are the easiest way for the hackers to gain privileged access to confidential information.

VI.      CONCLUSIONS

The trend of improving the ways of storing data in the cloud is increased certainly due to increase in use of cloud computing for storing data. If not protected in a correct manner, data available in the cloud can be at risk. This paper discussed about data security, threats to data in the cloud and methods to ensure data security. A rich amount of techniques have been proposed by analysts for data protection and to attain highest possible level of data security in the cloud. We have also observed that the common solutions used to secure data in Cloud infrastructure such as encryption and access control are the classical solutions used to secure data in a traditional environment. These solutions are often combined and/or adapted to the cloud. We have also observed that the common solutions used to secure data in Cloud infrastructure such as encryption and access control are the classical solutions used to secure data in a traditional environment. These solutions are often combined and/or adapted to the cloud. A future plan is to investigate the other security issues in the cloud computing environment and we have to design other security model with best security features using some encryption techniques for data concealment in cloud computing.

ACKNOWLDGEMENT

First and foremost we are extremely grateful to Ms. Kumud Alok and Ms. Neha Verma for their invaluable advice, continuous support, and patience during our research. Their immense knowledge and plentiful experience have encouraged me during this research. I would also like to thank Dr. Diksha Dani for their technical support on my study. Finally, we would like to express our gratitude to our parents and friends, without their immense understanding and encouragement, it would be impossible for us to complete our research.

REFERENCES

1. *“Cloud Computing: A beginners guide”*, Available: www.cuelogic.com
2. *“What is Cloud Computing”*, Available: www.pcmag.com
3. *“Cloud Computing Tutorial”*, Available: www.tutorialspoint.com
4. *“Cloud Computing”,* Available: www.javatpoint.com
5. “*IT consulting: Cloud Computing”,* Available: www.gcoe.com
6. “*What is data security”,* Available: www.ibm.com
7. *“What is cloud security”,* Available: www.mcafee.com
8. *”Data security methods for large business”,* Available: https://blog.rsisecurity.com/5-data-security-methods-for-large-businesses/
9. *“*Backup and recovery solutions”, Available: https://technoveraco.com/