IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

Data Security with Cloud Computing – A Research Paper

Siddhesh Mote, Shravani Kharade, Samruddhi Takawale, Mrs. Trupti Kulkarni
Department of Design Analytics and Cyber Security
MIT Arts, Commerce and Science College Alandi, Pune, India

Abstract: *This paper discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to it concerning security. The paper will go in to details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. Security is a concern here as the data is stored on remote server with multi user capabilities. The data is at the risk of unauthorized access thereby reducing reliability and privacy. Therefore, there is need to secure the data which may in the form of text, audio, video, etc. There are numerous algorithms designed by the researchers for securing the data on the cloud. The paper will go in to details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. The paper will also provide an insights on data security aspects for data-in-transit and data-at-rest. The study is based on all the levels of SaaS , PaaS and IaaS.*

Keywords: Data Security, Cloud Computing, Data Protection, Privacy, Risks and threats

I. INTRODUCTION

The term word Cloud Computing has emerged recently and is not is widespread use. Of the several definitions which are available, one of the simplest is, "a network solution for providing inexpensive, reliable, easy and simple access to IT resources" [1].The most important service offered by cloud is storage wherein the users store the required data. Security is a concern here as the data is stored on remote server with multi user capabilities. The data is at the risk of unauthorized access thereby reducing reliability and privacy.

Data integrity can be defined as protecting data from unauthorized modification or deletion. An example of this is easily understood if you think about online banking.

There are many reasons why **data security** is important to organizations in all industries all over the world. Organizations are legally obliged to protect customer and user data from being lost or stolen and ending up in the wrong hands. For example, industry and state regulations like the California Consumer Privacy Act (CCPA), the European Union's General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) outline organizations' legal obligations to protect data.

Data cybersecurity is also crucial to preventing the reputational risk that accompanies a data breach. A high-profile hack or loss of data can result in customers losing trust in an organization and taking their business to a competitor. This also runs the risk of serious financial losses, along with fines, legal payments, and damage repair in case sensitive data is lost.

The full scope of cloud security is designed to protect the following, regardless of your responsibilities:

- **Physical networks** — routers, electrical power, cabling, climate controls, etc.
- **Data storage** — hard drives, etc.
- **Data servers** — core network computing hardware and software
- **Computer virtualization frameworks** — virtual machine software, host machines, and guest machines
- **Operating systems (OS)** — software that houses
- **Middleware** — application programming interface (API) management,
- **Runtime environments** — execution and upkeep of a running program
- **Data** — all the information stored, modified, and accessed

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

- **Applications** — traditional software services (email, tax software, productivity suites, etc.)
- **End-user hardware** — computers, mobile devices, Internet of Things (IoT) devices, etc.

A major concern in adaptation of cloud for data is security and privacy [4]. It is very important for the cloud service to ensure the data integrity, privacy and protection. For this purpose, several service providers are using different policies and mechanism that depend upon the nature, type and size of data.

This type of data can be extremely sensitive and the consequences of exposing this data on a public cloud can be serious. In such cases, it is highly recommended to store datausing internal organizational cloud. This approach can help in securing data by enforcing on-premises data usage policy.

However, it still does not ensure full data security and privacy, since many organizations are not qualified enough to add all layers of protection to the sensitive data.[2]

This paper is the study of data security techniques used for protecting and securing data in cloud throughout the world. It discusses the potential threats to data in the cloud and their solutions adopted by various service providers to safeguard data.

Fig.1 data security in cloud computing[3]

II. WHAT ARE THE BENEFITS OF CLOUD DATA SECURITY?

Greater visibility

Strong cloud data security measures allow you to maintain visibility into the inner workings of your cloud, namely what data assets you have and where they live, who is using your cloud services, and the kind of data they are accessing.

Easy backups and recovery

Cloud data security can offer a number of solutions and features to help automate and standardize backups, freeing your teams from monitoring manual backups and troubleshooting problems. Cloud-based disaster recovery also lets you restore and recover data and applications in minutes.

Cloud data compliance

Robust cloud data security programs are designed to meet compliance obligations, including knowing where data is stored, who can access it, how it's processed, and how it's protected. Cloud data loss prevention (DLP) can help you easily discover, classify, and de-identify sensitive data to reduce the risk of violations.

Data encryption

Organizations need to be able to protect sensitive data whenever and wherever it goes. Cloud service providers help you tackle secure cloud data transfer, storage, and sharing by implementing several layers of advanced encryption for securing cloud data, both in transit and at rest.

Lower costs

Cloud data security reduces total cost of ownership (TCO) and the administrative and management burden of cloud data security. In addition, cloud providers offer the latest security features and tools, making it easier for security professionals to do their jobs with automation, streamlined integration, and continuous alerting.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

Advanced incident detection and response

An advantage of cloud data security is that providers invest in cutting-edge AI technologies and built-in security analytics that help you automatically scan for suspicious activity to identify and respond to security incidents quickly[4].

Fig.1 Data security in cloud computing[5]

III. SECURITY MODELS IN CLOUD COMPUTING

1. Cloud security deployment model: -

The cloud deployment model identifies the specific type of cloud environment based on ownership, scale, and access, as well as the cloud's nature and purpose. The location of the servers you're utilizing and who controls them are defined by a cloud deployment model. It specifies how your cloud infrastructure will look, what you can change, and whether you will be given services or will have to create everything yourself. Relationships between the infrastructure and your users are also defined by cloud deployment types[6].

Public Cloud:

The name says it all. It is accessible to the public. Public deployment models in the cloud are perfect for organizations with growing and fluctuating demands. It also makes a great choice for companies with low-security concerns. Thus, you pay a cloud service provider for networking services, compute virtualization & storage available on the public internet.

Private Cloud

Now that you understand what the public cloud could offer you, of course, you are keen to know what a private cloud can do. Companies that look for cost efficiency and greater control over data & resources will find the private cloud a more suitable choice.

It means that it will be integrated with your data center and managed by your IT team. Alternatively, you can also choose to host it externally. The private cloud offers bigger opportunities that help meet specific organizations' requirements when it comes to customization. It's also a wise choice for mission-critical processes that may have frequently changing requirements.

Hybrid Cloud

As the name suggests, a hybrid cloud is a combination of two or more cloud architectures. While each model in the hybrid cloud functions differently, it is all part of the same architecture. Further, as part of this deployment of the cloud computing model, the internal or external providers can offer resources.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

Let's understand the hybrid model better. A company with critical data will prefer storing on a private cloud, while less sensitive data can be stored on a public cloud. The hybrid cloud is also frequently used for 'cloud bursting'. It means, supposes an organization runs an application on-premises, but due to heavy load, it can burst into the public cloud.

2. Cloud Service Models

Infrastructure as a Service (IaaS):

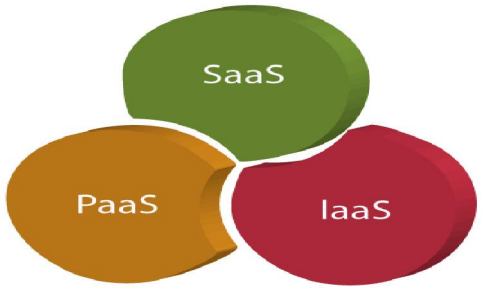
IaaS is also known as Hardware as a Service (IaaS). It is a computing infrastructure managed over the internet. The main advantage of using IaaS is that it helps users to avoid the cost and complexity of purchasing and managing the physical servers.

Platform as a Service (PaaS):

PaaS cloud computing platform is created for the programmer to develop, test, run, and manage the applications.

Software as a Service (SaaS):

SaaS is also known as "**on-demand software**". It is a software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser.



IV. PROTECTING DATA USING ENCRYPTION

Encryption techniques for data at rest and data in transit can be different. For examples, encryption keys for data in transit 57 can be short-lived, whereas for data at rest, keys can be retained for longer periods of time.

Different cryptographic techniques are used for encrypting the data these days. Cryptography has increased the level of data protection for assuring content integrity, authentication, and availability. In the basic form of cryptography, plaintext is encrypted into cipher text using an encryption key, and the resulting cipher text is then decrypted using a decryption key as illustrated in Fig 4.

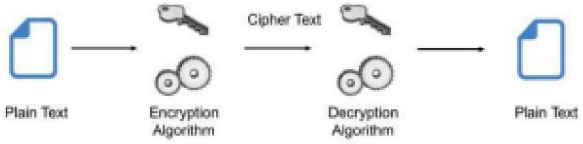


Fig 4. Basic Cryptography process

V. WHAT ARE THE THREE STATES OF DATA.

What is data at rest?

Data at rest refers to data in cloud, or any data that can be accessed using Internet. This includes backup data as well as live data. As mentioned earlier, sometimes it is very difficult for organizations to protect data at rest if they are not maintaining a private cloud since they do not have physical control over the data. However, this issue can be resolved by maintaining a private cloud with carefully controlled access.

What is data in motion ?

Data in motion or data in transit refers to **information traveling from one point to another** which includes email, instant messaging, collaborative tools, or any other communication channel.

Due to its nature of being transmitted, **this type of data is susceptible to interception attacks,** which is the most common way your data can be stolen.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

What is data in motion?

Data in motion or data in transit refers to **information traveling from one point to another** which includes email, instant messaging, collaborative tools, or any other communication channel.

Due to its nature of being transmitted, **this type of data is susceptible to interception attacks**, which is the most common way your data can be stolen[9].

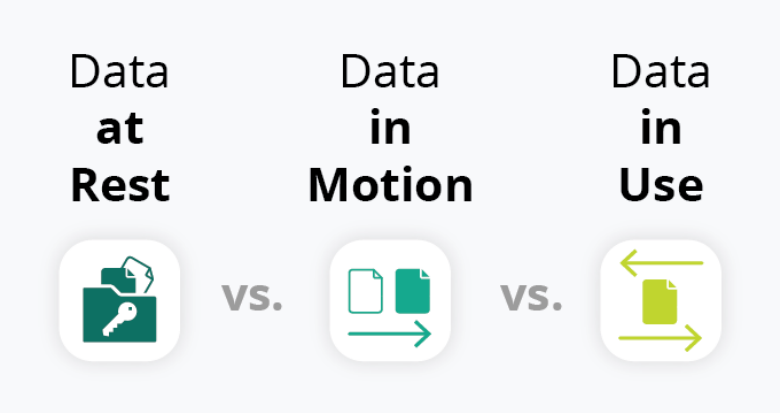


Fig.5

VI. CONCLUSION

Improved use of cloud computing for storing data is increasing the style of improving the ways of storing data in the cloud. Data presented in the cloud can be at risk if not protected in a lawful manner. This paper "an efficient approach on data security with cloud computing environment: comprehensive research" discussed the risks and security threats to data in the cloud and given an overview of three kinds of security concerns.Data in different states has been discussed along with the techniques which are efficient for encrypting the data in the cloud. The study provided an overview of block cipher, stream cipher and hash function which are used for encrypting the data in the cloud whether it is at rest or in transit.

REFERENCES

[1]. J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secur., vol. 1, no. September 2011, pp. 3–22, 2014.
[2]. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," 2015.
[3]. https://www.mieuxtechnologies.com/tag/data-security-for-cloud-computing/ image
[4]. https://cloud.google.com/learn/what-is-cloud-data-security?hl=en
[5]. https://benh.vn/data-security-in-cloud-computing-a-comprehensive-guide-for-data-analysts-88322/ image.
[6]. https://www.geeksforgeeks.org/cloud-deployment-models/
[7]. https://www.javatpoint.com/cloud-deployment-model
[8]. https://www.javatpoint.com/cloud-service-models
[9]. https://jatheon.com/blog/data-at-rest-data-in-motion-data-in-use/
[10]. F. Yahya, V. Chang, J. Walters, and B. Wills, "Security Challenges in Cloud Storage," pp. 1–6, 2014.