IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 10, October 2021

DOI: 10.17148/IARJSET.2021.81037

Comprehensive Overview of Data Security Challenges and Its Solutions in Cloud Computing

Sheikh Md Zubair Md Zahoor

Former Research Scholar, Computer Science, OPJS University, Churu, Rajasthan, India

Abstract: Cloud Computing is becoming more popular, and it shares technologies with Grid Computing, Utility Computing, and Distributed Computing. Users can construct applications in the cloud and access them from anywhere using cloud service providers such as Amazon IBM, Google's Application, Microsoft Azure, and others. Cloud data is stored and accessible on a remote server through the use of cloud service providers' services. Because the data is sent through a channel to a remote server, security is a big problem (internet). Security concerns must be solved before Cloud Computing may be implemented in a business. In this paper, we discuss data security concerns in a cloud-based environment, as well as ways for overcoming them.

Keywords: Cloud Computing; Data Security; Data Access

I. INTRODUCTION

Cloud computing is a next-generation internet-based computing system that allows users to access and work with a variety of cloud applications with ease and customization. By connecting the cloud application to the internet, cloud computing allows users to store and access cloud data from anywhere. Users can save their local data in a remote data server by using cloud services. Data stored in a remote data center can be accessed and controlled using cloud services offered by cloud service providers. As a result, data kept in a remote data center for processing should be handled with extreme caution.

Cloud computing security is currently the most pressing issue to be solved. Data is at danger if suitable security measures are not implemented for data operations and transmissions. Because cloud computing allows a group of people to access the same data, there is the prospect of a large data security risk. By identifying security challenges and ways to address these challenges, the strongest security measures can be adopted. It is apparent from Fig. 1 that Data Security and Privacy are the most crucial and critical factors to address.

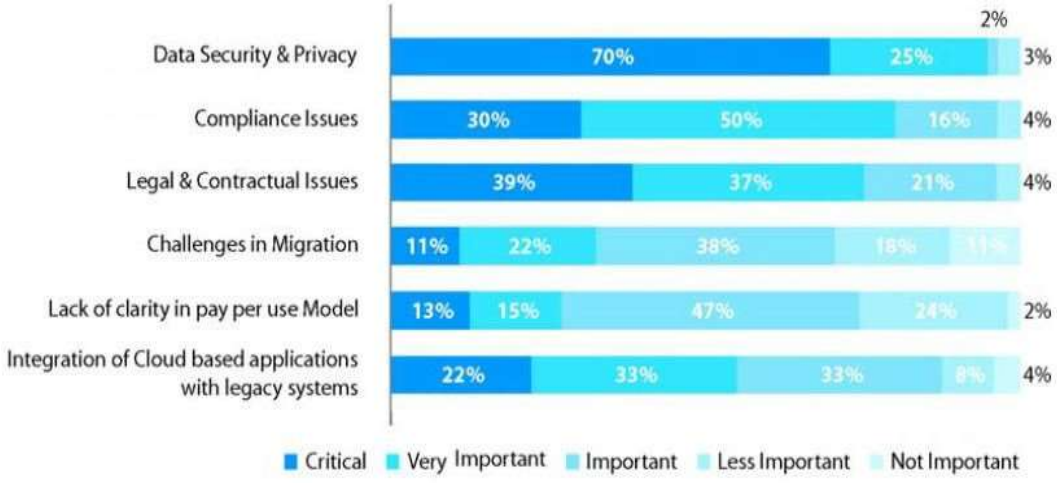

Figure 1: Data Security and Privacy - Major Inhibitor to Cloud Adoption.

II. LITERATURE SURVEY

In the literature review, several of the recommended solutions for dealing with security challenges in cloud computing were reviewed.

During cloud engineering, Popovi and Hocenski reviewed the security risks, requirements, and challenges that cloud service providers confront. Behl delves into the security concerns that come with working in a cloud setting. He also

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 10, October 2021

DOI: 10.17148/IARJSET.2021.81037

talked about the current security methodologies for securing cloud infrastructure and apps, as well as their shortcomings. Cloud computing security, reliability, and availability were examined by Sabahi. He also suggested a workable solution to a number of security concerns. Based on a research of cloud architecture, Mohamed E.M et al provided a data security model for cloud computing. They also used software to improve their job in the cloud computing Data Security Model. Wentao Liu describes some cloud computing systems and examines cloud computing security issues and strategies in light of cloud computing concepts. E. Mathisen outlined some of the most important security challenges that cloud computing is guaranteed to face, as well as current approaches that address these weaknesses.

III. CLOUD COMPUTING MODELS

Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are some of the cloud computing service models available (IaaS). Customers use SaaS services to execute applications on a cloud architecture since the services are offered by the service providers. Web browsers can be used to access these applications. PaaS (Platform as a Service) is a method of renting hardware, operating systems, storage, and network bandwidth over the internet. The customer can rent virtualized servers and associated services to run existing applications or develop and test new ones using the service delivery paradigm. In IaaS, the customer is given the ability to manage processes, storage, networks, and other basic computing resources that are useful for managing arbitrary software.

IV. DATA SECURITY CHALLENGES

As we transition to an internet-based cloud paradigm, we must place a high priority on data security and privacy. Data loss or leakage can have a significant impact on an organization's business, brand, and trust. Figure 2 illustrates this. With 88 percent of Critical and Very Significant issues, data leak protection is the most important factor. Data segregation and protection, on the other hand, has a 92 percent influence on security challenges.

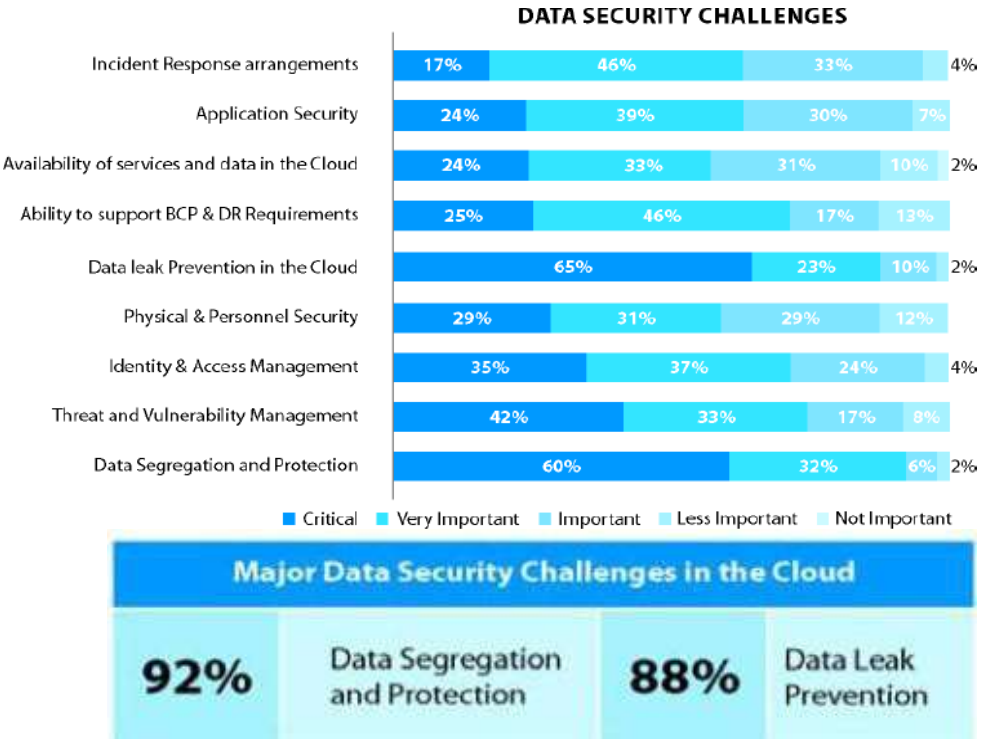

Figure 2: Data Security Challenges.

Security

There is a risk of data misuse when numerous organizations share resources. To avoid risk, data repositories, as well as data that is stored, transported, or processed, must be secured. Data security is one of the most pressing concerns in cloud computing. It is critical to offer authentication, authorisation, and access control for data stored in the cloud to improve cloud computing security. The three most important aspects of data security are:

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 10, October 2021

DOI: 10.17148/IARJSET.2021.81037

Confidentiality

The top vulnerabilities should be examined to guarantee that data is safe from assaults. As a result, security tests such as Cross-site Scripting, Access Control Mechanisms, and others must be performed to protect data from malicious users.

Integrity

Thin clients are used to give protection to client data when only a few resources are available. To ensure data integrity, users should not keep personal information such as passwords.

Availability

Availability is the most crucial issue in some firms that are experiencing significant downtime. It is contingent on the vendor's and client's agreement.

Locality

Data in cloud computing is scattered over a number of areas, making it difficult to locate data. When data is relocated to other geographical regions, the rules that govern that data may change as well. As a result, with cloud computing, there is a problem with compliance and data privacy rules. Customers should be aware of where their data is stored, and the service provider should inform them.

Integrity

The system should be secure enough that data can only be edited by those who are allowed to do so. To avoid data loss in a cloud-based system, data integrity must be properly managed. To maintain data integrity, all cloud computing transactions should adhere to ACID properties. Because HTTP services are used, most online services have a lot of challenges with transaction management. Transactions are not supported by the HTTP service, and delivery is not guaranteed. It can be dealt with by incorporating transaction management within the API.

Access

Data access is primarily concerned with data security policies. Employees in an organization will be granted access to a piece of data according on the company's security policies. Other employees in the same organization are unable to access the same data. To ensure that data is exchanged only with authorized users, a variety of encryption algorithms and key management procedures are employed. Using various key distribution systems, the key is only distributed to authorized parties. Data security regulations must be strictly maintained to protect data from unauthorized users. Due to the fact that all cloud users have access via the internet, privileged user access is required. To avoid security risks, users might employ data encryption and protection techniques.

Confidentiality

Cloud users store data on remote servers, and information such as data, films, and other media can be saved with a single or multiple cloud providers. Data confidentiality is one of the most critical requirements when data is kept on a remote server. Users should be informed of which data is stored in the cloud and how accessible it is to protect data confidentiality and categorization.

Breaches

Another key security concern to be focused on in the cloud is data breaches. Because the cloud stores enormous amounts of data from multiple users, a malevolent user may infiltrate the cloud, making the entire cloud environment vulnerable to a high-value attack.

Segregation

Multi-tenancy is one of the most important aspects of cloud computing. There is a risk of data infiltration since multi-tenancy permits multiple users to store data on cloud servers. Data can be accessed by injecting client code or utilizing any application. As a result, data must be stored separately from the rest of the customer's data. Data segregation

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 10, October 2021

DOI: 10.17148/IARJSET.2021.81037

vulnerabilities can be detected or discovered utilizing tests such as SQL injection aws, Data validation, and insecure storage.

Storage

There are numerous difficulties with data kept in virtual computers. One such issue is data storage reliability. Virtual computers must be stored in a physical infrastructure, posing a security concern.

Operation of Data Centers

Organizations that deploy cloud computing applications must protect user data in the event of data transfer delays and disasters. There is a problem with data storage and access if data is not adequately managed. The cloud providers are liable for data loss in the event of a disaster.

V. SOLUTIONS TO DATA SECURITY CHALLENGES

Encryption is recommended as a better way to secure data. It is preferable to encrypt data before storing it on a cloud server. The Data Owner can provide authorization to a specific group member so that they can quickly access data. To control data access, heterogeneous data centric security will be deployed. To strengthen data security in the cloud, a data security model that includes authentication, data encryption and integrity, data recovery, and user protection must be created. Data protection can be used as a service to secure privacy and data security.

To prevent data from being accessed by other users, data must be encrypted, which renders the data completely unreadable, and standard encryption can complicate availability. Before uploading data to the cloud, users should double-check that the data is saved on backup disks and that the keywords in the files have not changed. Before transferring to cloud servers, calculate the hash of the file to make sure that the data is not tampered with. This hash calculation can be used to ensure data integrity, however maintaining it is quite complex. Combining identity-based cryptography and RSA Signature can give an RSA-based data integrity check. To separate data from different users, SaaS requires precise boundaries both at the physical level and at the application level. In cloud computing, a distributed access control architecture can be used to govern access. Credential or attributed-based policies are superior for identifying unauthorized users. Permission as a service can be used to tell a user which parts of their data they can access. The owner can assign the majority of computation-intensive tasks to cloud servers without revealing the data's contents thanks to a fine-grained access control method. For secure data processing and sharing amongst cloud users, a data-driven architecture might be built. Threats are detected in real time using a network-based intrusion prevention system. To process huge files of various sizes and to provide remote data security It is possible to employ an RSA-based storage security mechanism.

VI. CONCLUSIONS AND FUTURE WORK

Although cloud computing is a new growing technology that offers a variety of benefits to users, it also poses a number of security concerns. In this paper, data security concerns are discussed, as well as solutions to these challenges, in order to mitigate the risk associated with cloud computing. Concrete cloud computing security standards could be defined in the future. Advanced encryption techniques for storing and retrieving data from the cloud can be employed to enable safe data access. Proper key management techniques can also be used to distribute the key to cloud users, ensuring that only authorized individuals have access to the information.

REFERENCES

[1]. L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud definition, in: ACM SIGCOMM Computer Communication Review, 2008.p.50-55.
[2]. M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6.
[3]. Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.
[4]. Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges, in: MIPRO, 2010 Proceedings of the 33rd International Convention, 2010.p.344-349.
[5]. Akhil Bhel, Emerging Security Challenges in Cloud Computing. Information and Communication Technologies, in: 2011 World Congress on, Mumbai, 2011.p.217-222.
[6]. Farzad Sabahi. Cloud Computing Security Threats and Responses, in: IEEE 3rd International Conference on Communication software and Networks(ICCSN), May 2011.p.245-249.
[7]. Eman M.Mohamed, Hatem S Abdelkader, Sherif EI Etriby. Enhanced Data Security Model for Cloud Computing, in:8th International Conference on Informatics and Systems(INFOS), Cairo, May 2012.p.12-17.
[8]. Wentao Liu. Research on Cloud Computing Security Problem and Strategy, in: 2nd International Conference on Consumer Electronics. Communications and Networks (CECNet), April 2012.p.1216-1219.
[9]. Eystein Mathisen. Security Challenges and Solutions in Cloud Computing, in: International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 2011.p.208-212.

