IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁑ Impact Factor 7.39 ⁑ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115149

Using Encryption Algorithms in Cloud Computing for Data Security and Privacy

Mr.Parin.J.Patel[1], Mr.L.N.Yadav[2], Mr.V.M.Rakhade[3]

Student, Department of Computer Science and Engineering,Shri Sai College of Engineering and Technology, Bhadravati, India[1]

Asst. Professor, Department of Computer Science and Engineering, Shri Sai College of Engineering and Technology, Bhadravati, India[2]

Asst. Professor, Department of Computer Science and Engineering, Shri Sai College of Engineering and Technology, Bhadravati, India[3]

Abstract: Cloud computing is the next big thing in information technology after the internet; some say it's a metaphor for the internet. It is an Internet-based computing technology in which software, shared resources, and information is delivered to consumers and devices on-demand and on a pay-per-use basis. Even though the cloud is becoming increasingly popular, usability and respectability issues, data protection and privacy issues, and other security issues continue to be major roadblocks in the field of cloud computing. The primary concern for cloud storage is privacy and security. Encryption is a well-known technology for safeguarding sensitive information. The use of a combination of public and private key encryption to conceal sensitive user data, as well as cipher text retrieval. The paper investigates the viability of using an encryption algorithm for data security and privacy in cloud storage.

Keywords: Online storage, cypher text retrieval, Privacy and encryption techniques.

I. INTRODUCTION

Cloud computing is a versatile, cost-effective, and time-tested platform for delivering business and consumer IT services over the Internet. Cloud computing is more vulnerable to security threats and vulnerabilities because it supports distributed service-oriented architecture, multi-users, and multi-domain administrative infrastructure. At the moment, security and privacy are major concerns in cloud adoption. The opportunities for intrusion within a cloud environment are numerous and lucrative. Cloud service providers who host the services are more concerned with security and privacy issues. In most cases, the provider must ensure the security of their infrastructure as well as the security of their client's data and applications by implementing security policies and mechanisms. While the cloud customer must ensure that the provider has implemented adequate security measures to protect their data. The problems are classified into several broad categories, including trust, architecture, identity management, software isolation, data protection, and availability. Reliability, ownership, data backup, data portability and conversion, multiplatform support, and intellectual property are all important considerations.

II. CLOUD COMPUTING FRAMEWORK

Service Models: These are the three most common cloud computing service models.

2.1 SaaS (software as a service).

SaaS (Software-as-a-Service): It is also known as software on demand and is built on a multi-tenant architecture. Software such as word processors, CRM (Customer Relationship Management), and so on, as well as application services such as schedules and calendars, are executed in the "cloud" to manipulate data. Custom services are combined with third-party commercial services to create new applications using service-oriented architecture. It is a pay-as-you-go software delivery model for business applications such as accounting, content delivery, human resource management (HRM), enterprise resource planning (ERP), and so on.

DOI: 10.17148/IJARCCE.2022.115149

2.2 Platform as a Service (PaaS).

Platform-as-a-Service (PaaS): This cloud layer offers computing platforms and solution stacks as a service. Platform-as-a-Service allows the user to focus on application design, development, testing, deployment, and hosting, as well as application services such as team collaboration, web service integration, and database integration, security, scalability, storage, persistence, state management, and application versioning, without having to worry about the underlying hardware and software layers.

2.3 IaaS (Infrastructure as a Service).
IaaS (Infrastructure-as-a-Service): Infrastructure as a service provides a virtualization platform as a service. Clients can purchase these resources as an outsourced service rather than purchasing servers, software, data center space, or network equipment. To put it another way, the client relies on third-party infrastructure services to support its operations, which include hardware, storage, servers, and networking components.

III. CLOUD DEPLOYMENT MODELS

3.1 Public.
This model represents an openly accessible cloud environment the general public can access. It is referred to as an external cloud or multi-tenant cloud. Customers can gain access to resources and pay for them. The public cloud can host both individual services and collections of services.

3.2 Private.
A private cloud, also known as an internal cloud or on-premise cloud, provides limited access to its resources and services to consumers who are part of the same organization that owns the cloud. In other words, infrastructure that is managed and operated exclusively for one organization to maintain a consistent level of control over security, privacy, and governance can be preserved.

3.3 Hybrid.
A hybrid cloud is a mix of public and private cloud services. It offers the advantages of multiple deployment models. It enables the enterprise to manage a steady-state workload in the private cloud, and if the workload increases, it can request intensive computing resources from the public cloud, then return if no longer required.

3.4 Community.
This deployment model pooled resources with many organizations in a community with similar concerns (like security, governance, compliance, etc). It usually refers to special-purpose cloud computing environments that are shared and managed by a group of related organizations in a common domain or vertical market .

IV. ISSUES IN CLOUD DATA STORAGE.

Cloud computing relocates application software and databases to large data centers, where data and service management may not be completely trustworthy. This one-of-a-kind feature, however, introduces a slew of new security challenges that aren't well understood. In this article, we will concentrate on cloud data storage security, which has always been an important aspect of service quality. To ensure the accuracy of user data in the cloud.

A. Trust: Trust is defined as relying on a person or thing's integrity, strength, ability, and surety. It is a problem to entrust your data to a third party that provides cloud services. Recent occurrences such as Amazon's Elastic Compute Cloud service crashed during a system upgrade in April 2013, knocking customers' websites offline for several hours to several days. The Sony PlayStation Network was hacked the same month, exposing the personal information of 78 million people worldwide. In June, a software bug at cloud storage provider Dropbox allowed visitors to log in to any of its 24 million customers' accounts with any password or none at all.

B. Privacy: Unlike the traditional computing model, cloud computing makes use of virtual computing technology, which allows users' data to be scattered across multiple virtual data centers rather than remaining in the same physical location, even across national borders. At this time, data privacy protection will face legal system controversy. Users, on the other hand, may leak sensitive information when using cloud computing services. Attackers can perform critical task analysis based on the computing task submitted by users .

DOI: 10.17148/IJARCCE.2022.115149

C. Security: Cloud service providers use encryption for data storage and transmission, as well as user authentication and authorization. Many clients are concerned about the security of remote data in the hands of criminals and hackers. Cloud providers are acutely aware of the problem and are deploying significant resources to address it.

D. Ownership: When data is moved to the cloud, some people are concerned about losing their rights or being unable to protect the rights of their customers. Many cloud providers address this issue with user-friendly agreements. According to the agreement, users should seek legal counsel from their preferred legal representative].

E. Performance and Availability: Businesses are concerned about the acceptable levels of performance and availability of cloud-hosted applications.

F. Legal: A cloud service provider and a client receiving the service may have concerns about the cloud provider's location, infrastructure, the physical location of the data, and outsourcing of the cloud provider's services, among other things.

G. Multi-Platform Compatibility: The integration of cloud-based services across different platforms and operating systems, such as OS X, Windows, Linux, and thin-clients, is a bigger issue for IT departments using managed services. Typically, a customized adaptation of the service resolves any issues. As more user interfaces become web-based, the need for multiplatform support will diminish.

H. Intellectual Property: A company invents something new and incorporates cloud services into its design. Is it still possible to patent the invention? Alternatively, a cloud service provider may claim that invention or leak the information to a competitor.

I. Data Backup: Cloud providers use redundant servers and routine data backup processes, but some people are concerned about having control over their backups. Many service providers now offer data dumps onto media or allow users to back up data via regular downloads.

These are some of the areas where cloud computing must excel and solve problems. Security, privacy, and intellectual property are the major threats to the growth of cloud computing that must be addressed.

V. OVERVIEW OF OUR APPROACH

Our goal is to create a repository to facilitate data integration and sharing across clouds while maintaining data confidentiality. We will use an encryption technique to ensure data security on data storage .

The goal of our system.
1. To create a system that will provide cloud storage with security and privacy.
2. To create an encryption-based system for protecting sensitive data in the cloud and to structure how the owner and storage service provider will work with encrypted data.
3. To create a system in which the user stores its data on the cloud, the data is sent and stored on the cloud in encrypted form. As in normal cases in cloud computing, when a user logins to the cloud and stores data on a cloud storage device, the data stored on the server cloud is not very secure because it can be readable by anyone with access to the server cloud, leaving data vulnerable.
4. Create a retrieval system in which the user retrieves data in encrypted form and decrypts it at its own site using a public and private key encryption, with both keys working at the user level.

V. CONCLUSION

Our research indicates that security and privacy are the major issues that must be addressed; therefore, efforts are being made to develop many efficient systems that can provide security and privacy at the user level while also maintaining the user's trust and intellectual property rights. Our strategy, State Encryption, is one such method that can provide users with peace of mind, and having control over data encryption and decryption will boost consumer confidence and attract more people to the cloud platform.

DOI: 10.17148/IJARCCE.2022.115149

REFERENCES

[1]. Asst.Professor, Mr L.N.Yadav , "Predictive Acknowledgement using TRE system reducing costs and bandwidth" IJRECE VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) ISSN: 2348-2281

[2]. Asst.Professor, Mr V.M. Rakhade,"Reducing Routing Distraction in IP Networks using Cross-Layer Methodology" (ICRTEST 2017) Volume: 5 Issue: 1(Special Issue 21-22 January 2017) ISSN:2321-8169

[3]. Rich Maggiani, solari communication. "Cloud computing is changing how we communicate".

[4]. Randolph Barr, Qualys Inc, "How to gain comfort in losing control to the cloud".

[5]. Greg Boss, Padma Malladi, Dennis Quan, Linda Legregni, Harold Hall, HiPODS,www.ibm.com/developerworks/websphere/zones/hipods

[6]. Tharam Dillon, Chen Wu, Elizabeth Chang, 2010 24th IEEE International Conference on Advanced Information Networking and Applications ,"Cloud computing: issues and challenges". [7]June13,2009,http://server.zol.com.cn/183/1830464.html.

[7]. Elinor Mills, January 27,2009. "Cloud computing security forecast: clear skies".

[8]. Jianchun Jiang, Weiping Wen, "Information security issues in cloud computing environment",Netinfo Security,doi:10.3969/j.issn.1671-1122.2010.02.026.

[9]. http://en.wikipedia.org/wiki/Cloud_computing.