WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Overview of Controlling Dual Access for Cloud-Based Data Storage and Exchange

R. Vijetha[1], B. Mamatha[2], M. Manikanta[3], G. Uday Kiran[4]

[1]Professor, Department of Computer Science Engineering, Siddhartha Institute of Technology & Sciences, Hyderabad, India
[2]Department of Computer Science Engineering, Siddhartha Institute of Technology & Sciences, Hyderabad, India
[3]Department of Computer Science Engineering, Siddhartha Institute of Technology & Science, Hyderabad, India
[4]Department of Computer Science Engineering, Siddhartha Institute of Technology & Sciences, Hyderabad, India

ABSTRACT-

Both corporations and academic institutions have shown a significant amount of interest in cloud-based data storage systems in recent years due to the fact that these systems are simple to operate and save money. In order to safeguard user privacy and maintain data privacy, service providers are required to establish secure methods of storing and sharing data. This is because the system operates on an open network. When it comes to protecting sensitive data from being hacked, encryption is the most effective method. A simple encryption of data, on the other hand, is not sufficient to meet the requirements of data management in the actual world. In addition to this, it is essential to implement stringent access control for software download requests.in order to prevent attacks that could make it difficult for people to access services, it is important to take into consideration the possibility of economic denial of sustainability.

This system manages dual access to cloud storage by putting in place a mechanism that manages requests to view data as well as requests to download data. As a result, the system remains both secure and effective. This study shows two different dual access control systems, each of which was designed to address a particular situation.

I.INTRODUCTION

When dealing with download requests, using dummy ciphertexts is a quick approach to handle the situation. Over the course of the past few decades, cloud storage services have gained a significant amount of popularity among both businesspeople and academics. Because it offers a number of advantages, including simple access and the elimination of the requirement to manage data on a local level, it is frequently utilized in a variety of Internet-based business systems, such as Apple iCloud. In order to save money, an increasing number of individuals and enterprises are opting to store their data in remote cloud services rather than modernizing their local data management systems through the process of modernization. On the other hand, consumers who utilize the Internet may not fully embrace cloud-based storage services because they are concerned about the possibility of security breaches occurring with data that is outsourced. It is possible that data that has been outsourced will need to be shared with a greater number of individuals in certain real-world scenarios. For example, Alice, who is a Dropbox user, might send her friends images that she has uploaded. Due to the fact that Alice is not utilizing data encryption, she must first create a sharing link before she can send the photographs to her friends. Although it provides some access restriction against unauthorized users (for instance, those who are not friends with Alice), the sharing link may still be available at the administrative level of Dropbox. This is the case even if it provides some access limitation. It is a good idea to encrypt data before uploading it to the cloud in order to keep it safe and private. This is because the cloud operates on an open network, which is not very trustworthy. Using an encryption technology (such as AES) directly on the data that is being outsourced is one solution that can be considered.

One form of attack that is frequently used against cloud storage systems is known as a resource-exhaustion attack. A malicious user could perform denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks in order to exhaust all of the resources that are available on the cloud storage service server. This is because a service user in a public cloud has the ability to make an endless number of download requests with the cloud. Because of this, the cloud service would be unable to fulfill the requirements that are stipulated by actual users. The "pay-as-you-go" model suggests that increasing the amount of resources used could be detrimental to the economy. Those who make use of cloud services will see a significant increase in their expenses if the attacks get more severe. The target of this assault is the economic resources of those who use the cloud, and it is an example of an attack known as an Economic Denial of Sustainability (E DoS). It is possible for network attackers to view encrypted download data, which could result in information breaches (such as file size). This is in addition to the fact that uncontrolled downloads could result in financial loss. Therefore, it is of the utmost importance to have clear guidelines of how to handle requests to download encrypted data that has been outsourced. On the other hand, developing a comprehensive system that guarantees control over both access to data and requests to download it cannot be accomplished just through the utilization of the CP-ABE approach. Confirm that the individual who is going to receive the data is authorized to decode it or not. It is necessary for Alice, the owner

of the data, to upload a large number of "testing" ciphertexts to the cloud in addition to the "real" encryption of the data. "Testing" ciphertexts are encryptions of phony communications that adhere to the same access constraints as the "real" data. Their purpose is to test the integrity of the data. When a user by the name of Bob contacts the cloud system with a request to download something, the system instructs him to randomly decrypt one of the "testing" ciphertexts. When they get a clear result or decryption.

II. SYSTEM ANALYSIS

EXISTING SYSTEM Although CP ABE can provide you with access to specific data, it is not sufficient or effective on its own to prevent network denial of service attacks, particularly distributed denial of service attacks in the cloud. This literature has a number of different suggestions for how to put a halt to the attack. According to Xue et al. [38], previous study did not do a good job of examining at E DoS attacks at both the algorithmic and protocol levels. This criticism was made by the researchers. They then devised a method to safeguard cloud data sharing against the attacks that were being carried out. However, [38] has two issues to deal with. It is necessary for the owner of the data to generate a number of challenge ciphertexts in order to thwart the attack. This will increase the amount of work that the computer needs to perform. Second, as a test, a data user is required to decrypt one of the challenge ciphertexts on their own. Because of this, a number of expensive operations, such as pairing, are required. In addition to the fact that delivering ciphertexts over the network demands a significant amount of bandwidth at the same time, both parties are required to do more complex calculations. As far as computing power is concerned, people do not have a complete understanding of how powerful the cloud is. The findings of this study reveal a novel approach to effectively combating the attack, which significantly reduces the expenses associated with computing and communication. Recently, Antonis Michala proposed a method for individuals to share data that makes use of both symmetric searchable encryption and attribute-based encryption (ABE). Because of this, individuals are able to search directly on encrypted content. In order to allow for the revocation of keys in ABE, the SGX protocol will be equipped with a revocation authority. The protocol was improved by Bakas and Michala with the addition of a hybrid encryption method. This technique makes it simpler to transfer data between several users by making the process as simple as sharing data with a single user. Protecting the symmetric key that is used to encrypt data, which is stored in an SGX enclave, is the responsibility of an ABE method.

III. PROPOSED SYSTEM

This study presents a novel approach to resolving the issues that have already been recognized as being problematic areas. This method is known as dual access control. Attribute-based encryption, often known as ABE, is an effective method for safeguarding data stored in cloud storage systems. In addition to providing you with precise control over the data that is outsourced, it conceals the data. The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) method is an effective method for encrypting data because it enables the establishment of access policies that specify who is permitted to access encrypted information and what the rights of those individuals are. In this work, we investigate how CP-ABE can be utilized within our system. On the other hand, utilizing the CP-ABE technique alone is not sufficient to create a comprehensive system that maintains control over both data access and download requests. You can control download requests in a number of different ways. One of these ways is by using fake ciphertexts to check the decryption rights of data recipients. It is necessary for Alice, the owner of the data, to upload a large number of "testing" ciphertexts to the cloud in addition to the "real" encryption of the data. It is the encryptions of phony communications that adhere to the same access requirements as the "real" material that are referred to as the "testing" ciphertexts. Any time a user by the name of Bob requests to download something, the cloud will request that he decrypt one of the "testing" ciphertexts in a random fashion. If Bob is able to successfully offer an accurate result or decryption, which demonstrates that he possesses the appropriate decryption credentials, then Alice grants Bob permission to view the actual data. By doing so, the cloud is able to assist Bob in precisely recovering her text.

IV. H/W REQUIREMENTS

Processor: Pentium –III/IV Speed: 1.1 G h z

RAM: 256MB (min)

Hard Disk: 120 GB

V. SOFTWARE REQUIREMENTS

Operating System: Windows XP/7. Coding Language: Java/J2EE

Web Server: Tomcat7.x Database: MySQL 5:5

VI. IMPLEMENTATION

TECHNOLOGY USED Java technology is both a programming language and a platform. The Java Programming Language The Java programming language is a high- level language that can be characterized by all of the following buzzwords: • Simple • Architecture neutral • Object oriented •Portable • Distributed • High performance •Interpreted • Multithreaded • Robust • Dynamic • Secure With most programming languages, you either compile or

interpret a program so that you can run it on your computer. The Java programming language is a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called Java byte codes —the platform independent codes interpreted by the interpreter on the Java platform. The interpreter parses and runs each Java byte code instruct ion on the computer. Compilation happens just once; interpretation occurs each time the program is executed. The following figure illustrates how this works

The Java Platform A platform is the hardware or software environment in which a program runs. We've already mentioned some of the most popular platforms like Windows 2000, Linux, Solaris, and MacOS. Most platforms can be described as a combination of the operating system and hardware. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms. The Java platform has two components: • Java Virtual Machine (Java VM). • The Java Application Programming Interface (Java API) Every Java interpreter, whether it's a development tool or a Web browser that can run applets, is an implementation of the Java VM. Java byte codes help make "write once, run anywhere" possible. You can compile your program into bytecodes on any platform that has a Java compiler. The byte codes can then be run on any implementation of the Java VM. That means that as long as a computer has a Java VM, the same program written in the Java programming language can run on Windows 2000, a Solaris workstation, or on an iMac.

VII. CONCLUSION

We discussed a significant and ongoing issue that arises with sharing data on the cloud, and we demonstrated two different approaches to managing access to the data. DDoS and EDoS assaults are not a problem for the systems that have been mentioned. When it comes to CP-ABE frameworks, we assert that the strategy that is utilized to manage download requests is universally applicable. When compared to the fundamental CP-ABE design, our experiments demonstrate that the suggested systems do not add a significant amount of additional effort or any more communication expenses. Our cutting-edge approach is predicated on the assumption that the sensitive data contained within the enclave cannot be removed. In recent research, it has been demonstrated that enclaves have the potential to unwittingly grant a malicious host access to certain secrets by means of memory access patterns or other side-channel attacks. Therefore, the concept of transparent enclave execution has arrived at this point. An extremely challenging endeavor is the creation of a dual access control system for the purpose of transferring cloud data from a transparent enclave. In the future, we will focus on finding the appropriate solution to the problem on our own.