SECURE DATA TRANSFER BASED ON CLOUD COMPUTING

P. SHANMUGAPRIYA[1], K.S.V.SRINIVAS[2], RAMPAM PAVAN KUMAR[3]

[1]Associate Professor, Computer Science and Engineering, SCSVMV, Kanchipuram
[2]B.E Graduate (IV year), Computer Science and Engineering, SCSVMV, Kanchipuram
[3]B.E Graduate (IV year), Computer Science and Engineering, SCSVMV, Kanchipuram

---

Abstract - *Data security and access control is one of the most difficult ongoing research projects in cloud computing because consumers outsource their sensitive data to cloud providers. Cloud storage sends a user's data to massive data centres located far away from the user and over which the user has no control. When someone examines a specific piece of data, they will have no idea that there is any hidden information. This method allows users to submit data as a secret message and then lock the data with a key or password. This key encrypts the data so that it cannot be read even if it is hacked. To decrypt, the receiver will require the key. the information that has been hidden The user then sends the key to the receiver, inputs the key or password for data decryption, and pushes the decrypt key to obtain confidential data from the sender. This distinct aspect of the cloud introduces a slew of new security issues that must be fully comprehended and addressed.*

***Key Words*: Decryption, Encryption, Private Key, Security, Public Key.**

1. INTRODUCTION

Cloud computing is a term that refers to a number of various types of computing concepts that involve a large number of computers connected via a real-time communication network (typically the internet). Cloud computing is a jargon word that lacks a well-defined scientific or technological definition. Cloud computing is a synonym for distributed computing via a network in science, and it refers to the ability to run a programme on multiple linked machines at once. More generally, the term refers to network-based services that appear to be delivered by real server hardware but are actually delivered by virtual hardware emulated by software operating on one or more real machines. Because virtual servers do not exist physically, they can be moved around and scaled up (or down) on the go without affecting the end user - akin to cloud computing.

Cloud computing is the use of on-demand computer resources that may be accessed across a network. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) are the three types of services available (SaaS). Because of its ability to reduce processing costs while enhancing scalability and flexibility for computer services, cloud computing is one of today's trendiest study areas.

Cloud computing has evolved as a modern technology that has expanded in recent years and is expected to become the next big thing in the coming years. Because it is new, it is confronted with new security concerns and obstacles. It has progressed from a notion to a significant portion of the IT business in recent years.

Cloud computing is commonly recognized as the adoption of SOA, virtualization, and utility computing, and it is based on three architectures: SaaS, PaaS, and IaaS. Each cloud computing technology has its own set of issues and obstacles. In contrast to traditional computing methods, data and applications are managed by the service provider in a cloud computing environment.

This naturally raises concerns about the data's security and protection from both internal and external threats. Encryption is a common method of concealing private or sensitive data within something that appears to be nothing. Encryption essentially takes advantage of human perception; human senses are not trained to hunt for files containing information. Decryption decodes encrypted data such that it can only be decrypted by an authorized user since it contains a key or password. Despite its benefits, storing user data in the cloud raises a number of security risks that must be thoroughly examined before it can be considered a reliable solution to the problem of avoiding local data storage.

1.1 Scope of the project

We can safely store data on the cloud in our proposed system by encrypting and decrypting it. On the cloud, we can also safely share data. The transmitter encrypts data with a public key, which is then decrypted by the receiver with a private key. As a result, even if a hacker obtains the data, he will be unable to decode it until he obtains the private key, ensuring that data on the cloud is secure.

1.2 Literature Survey

The internet was introduced to the world in 1990, and for the first time, we saw distributed computing power realized on a large scale. Cloud computing is a process that allows us to use a scaled distributed computing environment within the constraints of the internet. As we all know, cloud computing is surrounded by a lot of hype. Because cloud computing is still in its early stages and rapidly expanding, we are constantly discovering new security flaws that will pose a challenge to cloud computing.

Brad [Microsoft General Counsel] During a keynote address to the Brookings Institution policy conference, cloud computing for Business and Society, Smith also highlighted data from a poll commissioned by Microsoft measuring cloud computing for business and society. The perspectives of business leaders and the general public on cloud computing. According to the survey, while 58 percent of the general public and 86 percent of senior business leaders are excited about the possibilities of cloud computing, more than 90 percent of these same people are concerned about their own data's access, security, and privacy in the cloud.

2. PROJECT DESCRIPTION

One of the key concerns in the cloud computing arena is cloud security. Storing personal and sensitive data on a third-party storage media exposes you to the danger of data theft and exploitation by malevolent individuals. The danger is so great that it has deterred governments and many other large organisations from moving their operations to the cloud. In the cloud, traditional techniques of safeguarding files and information are no longer necessary. In order to make cloud more secure and dependable, extensive research and study is being conducted in this subject. AES encryption and Diffie Hellman Key Exchange are two technologies that stand out among these massive research projects. The latter method is so powerful that even today's most powerful computers may take millions of years to crack the code and read the file. Our method opposes encrypting the file with any conventional encryption technology and then utilising Diffie Hellman for user authentication. As a result, the files can be safely saved in the public domain without the risk of being accessed by unauthorised individuals.

Problem Statement:

Cloud security is quickly establishing itself as a major difference and competitive advantage among cloud providers. Cloud security may soon be more secure than the level attained by IT departments using their own hardware and software, thanks to the application of more robust security approaches and policies. The lack of trust in the cloud provider is a major roadblock to shifting IT systems to the cloud. The cloud provider, in turn, must enforce stringent security measures, which necessitates increased client trust. A robust trust foundation must be in place to improve mutual trust between the user and the cloud provider. To various people, cloud computing might mean different things. A consumer utilizing a public cloud application and a medium-sized organization using a customized suite of business apps on a cloud platform will undoubtedly have distinct privacy and security concerns, and this will result in a different set of benefits and hazards. The real value that the user tries to protect, however, remains constant.

The value that is at danger for an individual can range from civil liberties to the contents of bank accounts. The worth of a business can range from crucial trade secrets to business continuity and public reputation. Much of this is difficult to assess and convert into common value metrics.

The goal of this transition is to weigh the benefits of cloud adoption against the hazards of doing so. Why isn't everyone using cloud computing if it's so beneficial? Because the cloud functions as a large black box, nothing inside it is visible to the client, who leads to two major issues: Integrity It's a measure of how confident you are that your data in the cloud is safe from unintentional or malicious alteration.

As a result, data should be stored on cloud servers honestly, and any violations can be identified. Privacy All sensitive data, such as credit card numbers, is hidden in this approach, and only authorized users has access to it. Google Docs had a major problem on the SAAS cloud in 2009. Google Docs allows users to edit documents online while also sharing them with others. However, once these documents were shared with anyone, they became available to everyone. As a result, in this era of personal privacy, personal data should be protected at all costs.

Proposed Method:

Data protection as a service (DPaaS) is a set of security primitives offered by a cloud platform, such as secure data using encryption, logging, and key management that enforce data security and privacy and provide evidence of privacy to data owners, even in the presence of potentially compromised or malicious applications.

By combining the existing encryption technology and cloud computing system, the suggested system proposes a new approach for storing files in the cloud. Most consumers are uneasy about the fact that cloud Server providers can access their extremely private or confidential files for a variety of reasons. This could be for reasons like maintenance, security thread claims, or even normal file backups. Normally, these justifications are sufficient to safeguard the cloud Server's status and performance. Users, on the other hand, are hesitant to upload sensitive data to cloud servers.

Stand-alone-application:

The text was encrypted and decrypted using multiple symmetric encryption algorithms in a stand-alone application. It's a graphical user interface (GUI) application that encrypts and decrypts text using the sender's and receiver's keys. Later, this text is submitted to an internet directory.

Diffie-Hellman:

There were four methods to execute in this module. The tasks were as follows: For a new user, generate a private key of the specified length. Using a user's private key, generate a public key for him. Generate a secret key from a public and private key pair.

It was one of the original public-key protocols, named after Whitfield Diffie and Martin Hellman. It is a technique of securely transferring cryptographic keys over a public channel. In the world of cryptography, DH is one of the earliest practical examples of public key exchange. . Encryption and decryption are controlled by separate keys, E and D, in a public key cryptosystem, making computing D from E computationally impossible. The encrypting key E can thus be made public without jeopardizing the decrypting key D.

The Diffie-Hellman Key Exchange Protocol was founded on this philosophy. As a result, each network user can save his encrypting key in a public directory. This allows any system user to send a message to any other user that is encrypted so that only the intended receiver can decrypt it. A public key cryptosystem is a multiple access cypher as a result. Any two people can therefore hold a private chat, regardless of whether they have ever interacted before. Each sends messages to the other encrypting them with the receiver's public enciphering key and deciphering them with his own secret deciphering key. The Diffie–Hellman key exchange creates a shared secret between two parties that can be used for secure data transmission over a public network.

Prime Number:

A prime number (or prime) is a natural number that cannot be produced by multiplying two smaller natural numbers. The selection of prime number is the only user-defined pre-existing parameter in the Diffie-Hellman protocol. The prime number p should be large enough to withstand the attacks that have been made against it. NFS (attack on the network file system) is the most efficient assault; it has been employed against numbers on the order of 2768. It would seem prudent to choose a p that is significantly larger than that; at the very least, 1024 bits, and more practically, at least 1536 bits. Another characteristic of p is that p1 must have a large prime factor q. And one should be aware of p1's factorization. We'll probably be safe if we choose a random prime p and a random generator g, but we won't be certain (If the order of your random g has some minor factors, we might leak a few bits of the secret exponent.).

Technique:

Follow the Diffie Hellman key exchange protocol's mathematical implementation.

The number p is a prime number.

The primitive root modulo of p is g.

1. Alice and Bob agree to use a p = 23 modulus and a g = 5 base.

2. Alice generates her private key (a key she should not disclose with anyone) as 4.

3. As a result, Alice's public key will be 54 percent 23 = 625 percent 23 = 4.

4. Bob generates his private key (a key he should not share with anyone) as 3.

5. As a result, Bob's public key will be 53 percent 23 = 125 percent 23 = 10.

6. Now Alice obtains Bob's public key and creates a secret key. i.e. (Bob's public key, Alice's private key) mod p=> (104) % 23 => 10000 % 23 => 18.

7. On the other hand, Bob generates a secret key using a similar procedure, i.e. (public key of Alice Private Key of Bob) mod p => (43) percent 23 => 64 percent 23 => 18.

As a result, it is mathematically shown that they create the identical key without knowing each other's private key. This is how the Diffie-Hellman Key Exchange Protocol is implemented.

Encryption:

On the internet, encryption is frequently used to safeguard user information exchanged between a browser and a server, such as passwords, payment information, and other sensitive information that should be kept private. Encryption is also extensively used by organizations and people to safeguard sensitive data held on computers, servers, and mobile devices such as phones and tablets. There are a variety of encryption schemes available, including:

- Blowfish
- RSA
- Twofish
- AES
- Triple DES

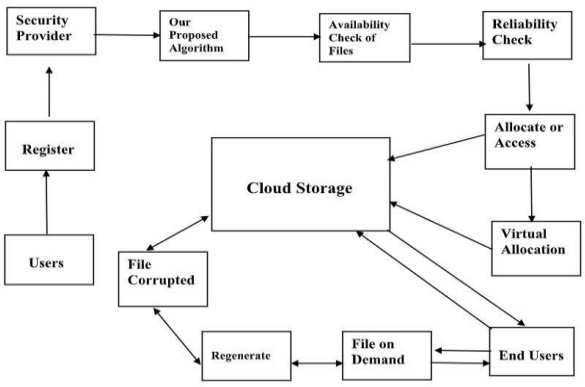
AES is the technique we employed in our project, and it's discussed here.

Advanced Encryption Standard:

The Advanced Encryption Standard (AES) is the most popular and commonly used symmetric encryption method today (AES). It has been discovered that it is at least six times faster than triple DES. A replacement was required because the key size of DES was too small. Triple DES was created to address this flaw; however it was discovered to be sluggish. With cryptographic key sizes of 128, 192, and 256 bits, the AES offers three fixed 128-bit block ciphers. The key size is limitless, but the block size is limited to 256 bits. The Data Encryption Standard (DES) Feistel network is not used in the

AES architecture, which is based on a substitution-permutation network (SPN).

Architecture:



Modules Description:

Login: A login is a collection of credentials used to verify a user's identity.

Authentication: It is a process of verifying the identity of a person or device using a username and password. Different users first register in the cloud.

Security Provider: It checks the authentication of the user to upload a file of the owner by generating a private key. The cloud server stores the encrypted file.

Availability of Files: Any file requested from the authorized user is checked by the availability of the resource in the cloud storage.

Reliability Check: The resources availability is stored in a separate file called Reliability Check.

Allocation: The virtual machine allocates the resources or resources are not allocated.

Regeneration: If the file is present, the end user easily receives the file or else if the file is corrupt then the file is regenerate and delivered to the end user based on demand.

Algorithm:

Step1: Create an account.

Step2: Generates Public and Private Key by using Diffie Hellman Key Algorithm.

Step3: Select the file which has to be sent.

Step4: Enter your private and public key of receiver's and upload the file.

Step5: The uploaded file will be encrypted.

Step6: Now receiver will decrypt the file with his private key and sender's public key.

3. CONCLUSIONS

For the future generation of IT applications, cloud computing is a promising and growing technology. Data security and privacy concerns are the biggest roadblocks to cloud computing's rapid rise. Reduced data storage and processing costs are a must for any firm, and data and information analysis is always one of the most critical jobs for decision-making in any organization. As a result, no organizations will move their data or information to the cloud unless the cloud service providers and users have established confidence. Researchers have offered a number of strategies for data protection and achieving the maximum level of data security in the cloud. However, there are still a lot of holes that can be filled by improving these procedures. To make cloud computing acceptable to cloud service users, further effort is needed in this field. This article examined several data security and privacy strategies, with a focus on data storage and use in the cloud, for data protection in cloud computing settings, with the purpose of fostering user trust in cloud service providers.

The goal of the proposed project is to solve the problem of safe cloud file storage. This approach is a basic implementation of the proposed methodology that can be improved and tailored to meet specific requirements. It suggests using encryption and Diffie Hellman to create a double layer of security for cloud-based files.

REFERENCES

[1] Jianbing Ni, Kuan Zhang, Yong Yu, Tingting Yang, Identity-based Provable Data Possession from RSA Assumption for Secure Cloud Storage**,** Published in: IEEE Transactions on Dependable and Secure Computing,2020.

[2] R. Patil Rashmi ,Yatin Gandhi,Vinaya Sarmalkar, Prajakta Pund,Vinit Khetani, RDPC: Secure Cloud Storage with Deduplication Technique, Published in: 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),2020.

[3] Nouman Kabir, Shaharyar Kamal, Secure Mobile Sensor Data Transfer using Asymmetric Cryptography Algorithms**,** Published in: 2020 International Conference on Cyber Warfare and Security (ICCWS), 2020.

[4] Bindhu Raj L.R.Vandana, Santhosh Kumar B.J.Integrity based Authentication and Secure Information Transfer over Cloud for Hospital Management System, Published in: 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020.

[5] Shafiq Riaz, Ali Haider Khan, Muhammad Haroon, Sadia Latif, Sana Bhatti, Big Data Security and Privacy: Current

Challenges and Future Research perspective in Cloud Environment, Published in: 2020 International Conference on Information Management and Technology (ICIMTech), 2020.

BIOGRAPHIES

- Mrs.P.Shanmugapriya is an Associate Professor in Computer Science and Engineering Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya deemed to be university, Enathur, Kanchipuram, India.

- Mr. K. S. V. Srinivas, Student, B.E. Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya deemed to be university, Enathur, Kanchipuram, India.

- Mr. Rampam Pavan Kumar, Student, B.E. Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya deemed to be university, Enathur, Kanchipuram, India.