LEVERAGING CRYPTOGRAPHIC APPROACHES TO SECURE CLOUD STORAGE

Naman Kudesia, Prateek Saxena, Vineet Agarwal

BBDITM, Lucknow

ABSTRACT: Cloud computing is the process of remotely operating, organizing, and accessing equipment and programming assets. It provides data storage, infrastructure, and applications online. Cloud computing provides consumers with a virtual computing environment in which to store data and run applications. However, because cloud administrators store and manage client information outside of the purview of customers, cloud computing has brought security issues.

Virtualization is becoming a key component of cloud computing, but we can only utilize it if it provides solid protection and security.

Cryptography is the art of attaining security via the use of various encryption techniques to safeguard or secure cloud data. Various cryptographic encryption algorithms are employed in the cloud to safeguard data that will be utilized or stored there.

It enables consumers to securely use shared cloud administrations since any information provided by cloud providers is encrypted.

Cloud cryptography protects sensitive data without slowing information sharing.

Cloud cryptography helps us to secure vital data outside of our corporate IT environment when it is no longer under our control.

Because there is no such mechanism in the cloud that provides actual and physical control over the storage of information, the only way we can ensure that the information spreading through the cloud is protected, encrypted, and stored cryptographically is by employing various cryptographic techniques and algorithms. As a result, many cryptographic issues that pose a danger to cloud computing are examined in this work. This paper is a survey of specific security issues raised by the use of cryptography in a cloud computing system, as well as how to implement data security solutions that provide reliable security and sensitive data protection, such as cloud data protection through encryption and cryptographic key management.

KEYWORDS: Cloud Computing, Cloud Technology, Cryptographic Algorithm, Infrastructure, Internet, Security Issue, Ciphertext, Cloud Provider, Cryptography, Encryption, Decryption, MitM

Introduction

Cloud computing is a framework for giving on-demand network access to a pooled pool of configurable computing resources (e.g., networks, servers, storage, software, and services) that may be instantly provided and released with no maintenance effort or involvement from service providers.

In cloud computing, resources are abstracted and virtualized from the cloud provider's IT infrastructure and made available to the user. Cloud infrastructure provides several advantages to cloud customers and other important stakeholders.

Some of these advantages include access to data stored in the cloud regardless of location, pay-on-demand, flexibility and elasticity, and cost savings by avoiding the purchase of hardware and other IT infrastructure. Despite these advantages, cloud computing is not without its drawbacks. Security is the primary worry in the cloud computing sector. The first and most obvious issue is privacy concerns. That is, if another entity is storing all of your data, how can you be sure it is safe and secure? Because cloud computing is powered by the internet, data moved to the cloud might be examined by anyone from anywhere when security is hacked. Hackers are willing to go to any length to steal data. From selling your personal information to competitors and individuals on the dark web to locking your storage and data until you pay them off, they may simply remove anything to hurt your firm and justify their acts on ideological grounds. This will have a significant impact on the firm's reputation, as well as diminishing consumer interest in the brand, leading to customer loss. In any event, hackers are a big threat to your cloud-based data. Because your data is stored on someone else's computer, you may be vulnerable to any security measures they provide. Organizations have little control over what happens to their data in the cloud since the cloud provider manages everything, including security.

DATA SECURITY IN CLOUD

Many enterprises and government agencies have been lured to migrate sensitive data to the cloud due to the multiple benefits that cloud computing provides. This provides a chance for attackers to exploit cloud computing vulnerabilities and compromise cloud security. They can cause harm to enterprises by stealing data, performing man-in-the-middle attacks, and jeopardizing data integrity. Many cloud giants, such as Google, Amazon, and Microsoft, have implemented different safeguards to secure customer data housed on their cloud systems. However, data in all three data states should be safeguarded against unwanted access (data at rest, data in transition, and data being processed). Some businesses are aware of these security concerns and encrypt important data before shifting it to the cloud. This adds a layer of protection for the client's data while it is in transit.

CRYPTOGRAPHY

The most popular approach for maintaining secure communication between two parties in the presence of a third party is cryptography. If A (Riya) and B (Rohan) transmit messages to one other and do not want outsiders to view or modify the content of their communications, they are requesting secure communication. A transmission medium T is employed in this connection, therefore A transmits his message to B via TAn invader I is a third party who wishes to disrupt this communication by gaining access to/changing the message. Whenever a message is on its route to its destination, it is vulnerable to being accessed by I, who can execute the following actions:

1. He can block the communication, preventing it from reaching its intended recipient and thereby violating availability.

2. He can intercept the transmission, making it no longer secret, and therefore destroying the secrecy.

3. He can alter the message's substance, therefore jeopardizing its integrity.

4. He can forge a message, impersonate sender A, and deliver it to B. This also compromises the message's integrity. The security of messages can be jeopardized in two-way communications due to the four listed threats. Encryption methods are employed in cryptography to address all of these security concerns. Encryption is the most significant approach for ensuring communication security.

Encryption is one of the most secure methods of avoiding MitM attacks since even if the data is intercepted, the attacker will be unable to understand it. There are two basic types of encryption algorithms in cloud cryptography. There are two types of encryption algorithms: symmetric and asymmetric.

A.Algorithm for Symmetric Encryption (Secret Key Cryptography) The Symmetric Encryption Algorithm employs a single key for encryption and decoding. Examples of this encryption scheme are mentioned briefly below.

- **The standard for Data Encryption (DES)**
  DES is a data encryption technology that employs a secret key for both encryption and decryption. It employs a 64-bit secret key, of which 56 bits are produced at random and the remaining 8 bits are utilized for error detection. It makes use of a data encryption algorithm (DEA), a secret block cipher with a 56-bit key that operates on 64-bit blocks. It is the prototypical block cipher—an algorithm that converts a fixed-length string of plaintext bits into a ciphertext bit string of the same length. The DES architecture allows users to implement it in hardware and utilize it for single-user encryption, such as encrypted information saved on a hard drive.
- **Blowfish**
  Blowfish is a symmetric method that was supposed to replace the DES or IDEA algorithms. It encrypts and decrypts data using the same secret key. The technique divides the data into 64-bit blocks and generates keys ranging from 32 to 448 bits in length. Blowfish is utilized in password protection systems for e-commerce websites

to secure payments because of its rapid speed and overall efficiency. It is a Feistel cipher with 16 rounds that operates on 64-bit blocks. Unlike DES, however, its key size spans from 32 bits to 448 bits.

- **AES (Advanced Encryption Standard):**
  (AES) It is a standard developed by the National Institute of Standards and Technology (NIST) for encrypting electronic data. It also aids in the encryption of digital data such as telecommunications, banking, and government data. It is used by US federal entities to protect sensitive unclassified information. AES is a symmetric-key technique, which means that both encryption and decryption use the same key. It is an iterated block cipher that operates by repeatedly repeating the stated stages. It features a 128-bit block size with key sizes of 128, 192, and 256 bits for AES-128, 192, and 256 bits, respectively. AES's architecture makes it efficient in both software and hardware, and it also operates across various network levels.

B.Asymmetric Encryption Algorithm (Public-Key Cryptography) This encryption technique was developed to address key management issues. It employs both a public and a private key. The public key is made public, whilst the sender maintains the private key private. Asymmetric encryption employs a key pair consisting of a public key available to everyone and a private key held only by the key owner to guarantee secrecy, integrity, authentication, and nonrepudiation in data management.

- **Rivest Shamir Adleman (RSA) Algorithm**
  The RSA cryptosystem is a public-key cryptosystem used for Internet encryption and authentication. To conduct computations with two huge prime numbers, RSA employs modular arithmetic and elementary number theory. RSA is widely utilized in a wide range of products, platforms, and sectors. It is regarded as one of the de facto encryption standards. RSA algorithms are built into the operating systems of companies such as Microsoft, Apple, and Novell. The most widely used asymmetric algorithm is RSA. The RSA algorithm's security is based on the computational difficulties of factoring huge integers that are the product of two large prime numbers. It is simple to multiply two prime integers, but RSA is predicated on the difficulty of computing the original numbers from the product.
- **Elliptic Curve Cryptography (ECC)**
  ECC is contemporary public-key cryptography that was designed to reduce the use of bigger cryptographic keys [6]. To obtain a short, rapid, and strong cryptographic key, the asymmetric cryptosystem relies on number theory and mathematical elliptic curves (algebraic structure). Because of the ECC's tiny key size, Elliptic Curve Cryptography has been proposed to replace the RSA technique.

Conclusion

Various cryptographic algorithms utilised in cloud computing were examined and analyzed in this paper, as were some of the cryptography methods employed by certain prominent cloud computing organizations. A novel method for encrypting data as it moves from the cloud user's platform to the cloud provider's platform was presented and explored. Moving ahead, I will emphasis further on reconciling the suggested algorithm's security with usability and efficiency, as well as evaluating its compatibility with other cloud platforms.

BIOGRAPHIES

Naman Kudesia

B.Tech (CSE) 3rd Year

BBDITM, Lucknow

Prateek Saxena

B.Tech (CSE) 3rd Year

BBDITM, Lucknow

Vineet Agarwal

Assistant Professor

BBDITM, Lucknow