Cloud Cryptography Data Security Aspect and Features

Sumit Kumar
Dept of master of computer application

Rakshita Kiran P
Asst professor

Dayananda Sagar College of Engineering
Kumaraswamy layout, Bangalore, India

Abstract

In the realm of data security, the ultimate line of defense lies within the tier of data security itself. If this layer is compromised, the principles of confidentiality, integrity, and availability, as defined by the CIA's triad, are undermined. However, enhancing security often comes at the cost of system performance and usability. This paper addresses the foundational aspects of cloud computing and highlights the prominent challenge it faces: security. The study investigates various cryptographic methods employed by leading cloud providers and proposes an alternative algorithm for encrypting data during transit from users to the cloud. The proposed approach aims to ensure data security and protect against Man-in-the-Middle (MitM) attacks like sniffing. In conclusion, the paper emphasizes the importance of further research into the suggested cryptographic algorithm to guarantee comprehensive data protection and privacy across all three data states.

Introduction

Cloud Computing, ensuring the security and confidentiality of data is of dominant importance. Cryptography, a cornerstone of data protection, emerges as a vital component in safeguarding sensitive information within cloud environments. By employing cryptographic techniques, cloud computing leverages the power of encryption and key management to fortify data security and maintain the privacy of critical assets.

Cloud computing cryptography revolves around the application of cryptographic algorithms and principles to counter the risks associated with data storage, transmission, and processing. Encryption, the process of converting plain, readable data into an unreadable form using encryption algorithms and keys, stands as a fundamental pillar in this realm. Through encryption, data is transformed into ciphertext, rendering it indecipherable to unauthorized entities. Whether it is encrypting data prior to uploading it to the cloud or safeguarding data during its transmission, encryption acts as a robust shield against unauthorized access and interection.

Not only do cloud users have the ability to employ client- side encryption to protect their data before entrusting it to
the cloud, but cloud providers themselves also play a significant role in implementing encryption mechanisms. By encrypting data at rest, cloud providers ensure the stored information remains secure and impervious to unauthorized access. Effective encryption key management is crucial, as it guarantees the controlled and secure generation, storage, and exchange of encryption keys. Proper key management practices safeguard the integrity and

confidentiality of data, allowing only authorized individuals to access and decrypt the encrypted information.

By integrating cryptography into cloud computing, organizations can instill trust, mitigate risks, and maintain control over their sensitive data. The synergy between cloud computing and cryptography empowers businesses to harness the benefits of cloud services while upholding the highest standards of data security. As cloud computing continues to evolve, the role of cryptography becomes even more vital in fortifying the foundations of confidentiality, integrity, and availability in this dynamic and interconnected digital landscape.

Data Security in Cloud

In cloud computing, data security stands as a dominant concern that demands distinctive attention. As organizations and government agencies entrust their sensitive information to cloud environments, the vulnerabilities inherent in this paradigm become potential avenues for attackers to breach the sanctity of data. Exploiting these weaknesses, these assailants can perpetrate acts of data theft, engage in man-in-the-middle attacks, and risk the integrity of crucial information.

While cloud providers like Google, Amazon, and Microsoft have taken commendable strides in fortifying the security of their platforms, organizations must be proactive in safeguarding their data across its entire lifecycle: at rest, in transit, and during processing. Recognizing the significance of encryption, some forward-thinking entities elect to encrypt their sensitive data prior to its migration to the cloud. By employing this proactive measure, organizations preserve control over data security, mitigating risks associated with entrusting
information to third-party cloud providers.employing this proactive measure, organizations preserve control over data security, mitigating risks associated with entrusting information to third-party cloud providers.

Encryption, an indispensable pillar of data protection, transforms information into an unintelligible format that can only be deciphered with the possession of the corresponding decryption key. Through this process, the confidentiality and integrity of data remain intact during its transmission, impeding unauthorized access and assuring that only approved parties can access and explain the encrypted information.

Embracing data security in the cloud necessitates a comprehensive approach. While cloud providers bear a significant responsibility in implementing robust security measures, organizations must also assume a proactive role in protecting their sensitive data. Encryption emerges as a potent weapon in this endeavor, empowering organizations to retain authority over their data security by encrypting it prior to its sojourn into the cloud. By adopting this strategy, organizations bolster their defense mechanisms, assuring the confidentiality and integrity of their data in an ever-evolving threat landscape..

ABOUT CRYPTOGRAPHY

Cryptography is a method of cover information in order to hide it from unwanted users. Data transmission in ciphertext format is a common security practice used to protect sensitive information from unauthorized access. The ciphertext is created by encrypting the plaintext using a cryptographic algorithm and a key. The key is a secret value that is used to scramble the plaintext in a way that only the intended recipient can decrypt it.This key is kept confidential and only approve entities have access to it Encryption is one of the safest ways to avoid MitM attacks because even if the transmitted data gets intercepted, the attacker would be unable to decipher it.

A. *Symmetric Encryption Algorithm*

Symmetric encryption algorithms are a fundamental component of modern cryptography, playing a pivotal role in securing sensitive data. Unlike asymmetric encryption algorithms that rely on pairs of public and private keys, symmetric encryption employs a single key for both the encryption and decryption processes. Then this shared secret key must be kept secret and known only to the communication parties.

Symmetric encryption algorithms utilize a symmetric key to transform plaintext data into ciphertext, making it unintelligible to unapproved entities. The same key is then used to change the process, converting the ciphertext back into its original plaintext form. This inherent simplicity and efficiency of symmetric encryption make it ideal for encrypting large volumes of data and achieving fast encryption and decryption speeds.

There are numerous well-established symmetric encryption algorithms that have been widely adopted and trusted in various applications. Some notable examples include:

1) Data Encryption Standard

The Data Encryption Standard stands as an seminal standard in the realm of data encryption. It encompasses a symmetric encryption algorithm that employs a single secret key for both the encryption and decryption processes. Notably, DES employs a 64-bit secret key, generated with 56 bits of randomness, while the remaining 8 bits serve error detection purposes.

At its core, DES leverages a secret block cipher known as the Data Encryption Algorithm. This block cipher operates on fixed-length blocks of 64 bits, utilizing the 56-bit key to transform plain text data into an equivalent-length cipher text. This distinctive characteristic defines DES as a block cipher, specifically designed to facilitate the secure transformation of fixed-size blocks.

An intriguing feature of DES is its hardware feasible, enabling its application in scenarios requiring single-user encryption, such as the encryption of files stored in encrypted form on a hard disk.

It is worth noting, however, that the security strength of DES has diminished over time due to advancements in computational power and the emergence of more secure encryption algorithms. Consequently, DES is no longer considered suitable for applications demanding robust security. Nonetheless, DES retains historical significance within the field of cryptography and serves as a precursor to subsequent, more advanced encryption algorithms.

Please note that the above response provides a unique portrayal of the Data Encryption Standard (DES), emphasizing its key characteristics and historical significance while aiming to present the information in a distinctive manner.

2) Advanced Encryption Standard (AES)

The Advanced Encryption Standard represents an pivotal advancement in the realm of data encryption. It stands as a cutting-edge symmetric encryption algorithm that has gained widespread recognition and adoption for its robust security and efficient performance. AES supersedes its predecessor, the Data Encryption Standard (DES), providing enhanced strength and versatility.

AES operates on a block cipher principle, employing a secret key shared between the encryption and decryption processes. Unlike

DES, AES supports key sizes of 128, 192, or 256 bits, enabling a higher level of security and adaptability to varying encryption requirements.

At its core, AES utilizes a substitution-permutation network structure, combining substitution and permutation operations to achieve its cryptographic transformations. This intricate structure ensures a high degree of confusion and diffusion, making AES resilient against various cryptographic attacks.

One notable advantage of AES is its ability to efficiently leverage modern computing hardware, including specialized instruction sets and parallel processing capabilities. This allows for fast and efficient encryption and decryption operations, making AES suitable for a wide area of applications, from securing sensitive data in storage and transit to enabling secure communication channels.

AES has been extensively scrutinized by the cryptographic community and has undergone rigorous evaluation processes to validate its security. As a result, it has been adopted as a standard encryption algorithm by government agencies, organizations, and industries worldwide.

In summary, the Advanced Encryption Standard (AES) stands as a state-of-the-art symmetric encryption algorithm, surpassing its predecessor DES in terms of security and versatility. Its robustness, efficiency, and widespread adoption have positioned AES as the go to choice for securing sensitive data in numerous applications, providing peace of mind and confidentiality in an increasingly interconnected and data-driven world.

3) Blowfish

Blowfish is a symmetric encryption algorithm developed as an alternative to DES and IDEA. It operates using a single secret key for both encryption and decryption processes. The algorithm divides data into 64-bit blocks and supports key lengths ranging from 32 bits to 448 bits.

With its high speed and efficiency, Blowfish finds applications in various domains, including password protection tools and securing e-commerce websites for payment transactions. It employs a 16-round Feistel cipher structure, operating on 64-bit blocks.

One notable advantage of Blowfish over DES is its expanded key size, ranging from 32 bits to 448 bits, allowing for greater security. This larger key space enhances its resistance against brute-force attacks and strengthens data protection.

Overall, Blowfish's combination of speed, efficiency, and adaptable key sizes has made it a popular choice in scenarios where strong encryption is required, making it an authentic option for securing sensitive data in diverse applications.

B. *Asymmetric Encryption Algorithm*

An asymmetric encryption algorithm, is a cryptographic technique that utilizes a pair of mathematically related keys to secure data communication and protects sensitive information.

In this algorithm, there are two distinct keys: a public key and a private key. The public key is freely distributed and can be accessed by anyone, while the private key is kept confidential and only known to the key owner.

1) Rivest Shamir Adleman (RSA)

River shamir adleman, a widely used in public key crypto system, plays a significant role internet encryption and authentication in internet. It leverages modular arithmetic and elementary number theories , Modular arithmetic and elementary number theory are two mathematical concepts that are used in cryptography to carry out computations involving two large prime numbers.

RSA system has gained extensive adoption across various industries, platforms, and products, making it one of the standard encryption methods. Major companies such as Microsoft, Apple, include RSA algorithms into their operating systems.

As an asymmetric algorithm, RSA relies on the computational complexity of factoring large integers, which are the product of two large prime numbers, to ensure its security. While multiplying prime numbers is straightforward, the strength of RSA lies in the difficulty of calculating the original numbers from their product.

The security of RSA algorithm rests upon the challenge of factoring these large integers efficiently. The complexity involved in factoring forms the foundation of RSA's security. This complexity introduces a barrier that makes it computationally infeasible to retrieve the original prime numbers from their product without knowing the private key.

With its widespread usage and robust security properties, RSA remains one of the most popular asymmetric encryption algorithms. Its presence in operating systems and its extensive implementation in various domains highlight its importance in ensuring secure communication and protecting sensitive data.

2) Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography is an innovative cryptographic system that leverages the properties of ovoid curves to provide secure and efficient encryption, digital signatures, and key exchange protocols.

Unlike traditional cryptographic systems based on prime number factorization, ECC exploits the algebraic structure of ovoid curves over finite fields. By utilizing the discrete logarithm problem on elliptic curves, ECC achieves a high level of security with shorter key lengths compared to other encryption algorithms which are asymmetric.

The elegance of ECC lies in its ability to offer strong security while conserving computational resources. It provides excellent resistance against attacks, including brute force and quantum computing-based attacks, making it suitable for resource-constrained devices and emerging technologies.

ECC's versatility and efficiency have led to its widespread adoption in various applications, such as secure communication protocols, digital signatures, and secure mobile devices. Its efficient implementation and smaller key sizes contribute to faster computations, reduced bandwidth requirements, and improved system performance.

The ingenuity of Elliptic Curve Cryptography has propelled it to the forefront of modern cryptography, enabling secure and scalable solutions in an increasingly connected and digital world. As a result, ECC continues to shape the landscape of cryptographic systems, offering enhanced security and efficiency for a wide range of applications.

CRYPTOGRAPHY TECHNIQUES USED BY SOME CLOUD GIANTS

Cloud giants, including Google, Amazon, and Microsoft, employ various cryptography techniques to safeguard the security and privacy of data within their cloud platforms. These techniques encompass:
Encryption at Rest: Cloud providers utilize robust encryption algorithms to encrypt data before storing it on their servers. This ensures

that even if unauthorized access occurs, the data remains unintelligible without the corresponding decryption key. Advanced encryption algorithms like AES with 256-bit keys are commonly employed.

Transport Layer Security (TLS): TLS, is extensively used to establish secure communication channels between clients and cloud platforms. It encrypts data during transit, thwarting eavesdropping attempts and upholding the integrity and confidentiality of the information. TLS employs cryptographic protocols to verify the server's authenticity, negotiate encryption algorithms, and establish a secure connection.

Public Key Infrastructure (PKI): PKI forms a foundational aspect of cloud security, facilitating secure authentication, data exchange, and encryption. Cloud providers employ digital certificates, public-private key pairs, and certificate authorities to verify user identities, preserve data integrity, and establish secure connections. PKI ensures that data remains encrypted and confidential during transmission.

Multi-Factor Authentication (MFA): Cloud giants implement MFA techniques to enhance user authentication and access control. MFA combines multiple authentication factors, such as passwords, biometrics, tokens, or smart cards, to fortify user verification. This mitigates the risk of unauthorized access by adding an additional layer of security beyond traditional username and password authentication.

Homomorphic Encryption: Cloud providers explore homomorphic encryption techniques that autorize computer computition to be performed directly on encrypted data without requiring decryption. The approach allows sensitive information to be processed securely while maintaining data privacy. Homomorphic encryption is particularly valuable for scenarios where data owners wish to preserve the confidentiality of their data while allowing computations to be carried out on it.

Key Management: Effective key management practices are essential in cloud computing. Cloud giants employ secure mechanisms for key generation, distribution, and storage. Key rotation strategies, involving regular key changes, are implemented to minimize the impact of potential key compromises. Key escrow and access controls ensure that only authorized entities possess the necessary encryption keys, safeguarding the confidentiality and integrity of the data.

ALGORITHMS

These algorithm you described is a client-side encryption approach, where data is encrypted by the client before being transmitted and stored in the cloud. This process involves converting plain text into cipher text using encryption techniques. By encrypting the data before transmission, the algorithm aims to protect against data theft and man-in-the-middle attacks.

In man-in-the-middle attack, an attacker obstruct communication between two parties and can potentially access or manipulate the transmitted data. However, by encrypting the data at the client-side, even if the attacker manages to obstruct the encrypted data, they would not be able to understand or derive any meaningful information from it without the decryption key.

Client-side encryption provides an additional layer of security by ensuring that data remains confidential and unreadable to unauthorized individuals, including potential attackers. This approach helps mitigate the risk of data theft and unauthorized access during the transmission and storage of sensitive information in the cloud.

A. Encryption Algorithm

Convert the character to its ASCII code. This can be done by looking up the character in an ASCII table. This can be done by dividing the ASCII code by 2 and rounding down. The

remainder will be the significant bit of the binary number. The quotient can then be divided by 2 and rounded down again, and so on, until the entire ASCII code has been converted to a binary number. If the ASCII code is not equal to 8 bits, add preceding 0s to the binary number until it is 8 bits long. For example, the binary equivalent of the ASCII code for 'A' is 01000001.
Find out the one's complement of the last 4 bits. This can be done by flipping each bit in the last 4 bits to the opposite value. For example, the 1's complement of the last 4 bits of 01000001 is 10111110.
Convert the generated binary code to an ASCII character. This can be done by looking up the binary code in an ASCII table. For example, the ASCII code for 10111110 is -7.
Transmit the ASCII code to the cloud. This can be done using a variety of methods, such as HTTP, FTP, or SSH.

B. Decryption Algorithm

Find the ASCII code of the ciphertext character. This can be done by looking up the character in an ASCII table. For example, the ASCII code for the ciphertext character 'N' is 78. Convert the ASCII code to binary. This can be done by dividing the ASCII code by 2 and rounding down. The remainder will be the least significant bit of the binary number. The quotient can then be divided by 2 and rounded down again, and so on, until the entire ASCII code has been converted to a binary number. If the ASCII code is not equal to 8 bits, add preceding 0s to the binary number until it is 8 bits long. For example, the binary equivalent of the ASCII code for 'N' is 01001110. Reverse the last 4 bits of the generated 8-bit binary value. This can be done by simply reversing the order of the last 4 bits. For example, the reversed binary value of 0100111 is 10111001.
Convert the generated binary value to ASCII code. This can be done by looking up the binary code in an ASCII table. For example, the ASCII code for 10111001 is 'Q'.

CONCLUSION

This paper, focuses on discussing and reviewing different cryptographic algorithms in cloud computing. Additionally, a new algorithm was proposed specifically for encrypting data during its transition from the cloud user to the cloud platform provider’s. The proposed algorithm aimed to strike a balance between security, usability, and efficiency.

Moving forward, the future plans to further refine and enhance the proposed algorithm. This involves conducting tests to ensure its compatibility with various cloud platforms, as compatibility is crucial for the algorithm's practical implementation and widespread adoption.

The author also intends to address usability and efficiency aspects, recognizing the importance of making the algorithm user-friendly and efficient in terms of computational resources. By considering these factors, the proposed algorithm can better meet the needs and requirements of cloud computing environments, providing robust data protection while maintaining practicality and performance.

Overall, the paper highlights the ongoing research and development efforts in the field of cloud computing cryptography, with the aim of advancing the security measures in cloud environments and addressing the specific challenges and requirements of data encryption in transit.