International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Volume 30, Issue: Special), April 2018
An Indexed and Referred Journal with Impact Factor: 2.75
ISSN (Online): 2347-601X
www.ijemhs.com

Cloud Cryptography - A Security Aspect

Richismita Rout, Assistant Professor, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar
Prabir Kumar Singh, UG Student, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar
Rupashree Panda, UG Student, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar
Asi Bhima Raju, UG Student, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar

Abstract- **If all of the top levels of security fail, the final and most critical tier, data security, must not fail [1]. By breaching this layer of defence, the CIA's triad principles of confidentiality, integrity, and availability are undermined. However, increasing security reduces the performance of the system and usability. This paper addresses the fundamentals of cloud computing as well as its key challenge: security. This paper examines a variety of cryptographic methods used by major cloud providers. It proposes an alternative algorithm for encrypting data in transit from the user to the cloud in order to ensure data security and defend against Man-in-the-Middle (MitM) attacks like sniffing. The paper concludes by urging further study into the proposed cryptography algorithm in order to ensure data protection and privacy in all three data states.**

Keywords:* *Ciphertext, Cloud Provider, Cryptography, Encryption, Decryption, MitM

I. INTRODUCTION

Cloud computing is a framework for offering on-demand network access to a pooled pool of configurable computing resources (e.g., networks, servers, storage, software, and services) that can be quickly provisioned and released with limited maintenance activity or service provider involvement [7]. In cloud computing, resources are abstracted and virtualized from the cloud provider's IT infrastructure and made accessible to the customer.Cloud infrastructure provides various advantages to cloud consumers and other core stakeholders. Some of these benefits are access to data stored on the cloud regardless of the location, pay-on-demand basis, flexibility and elasticity, and economic benefits by saving the company from buying hardware and other IT infrastructure [11].Despite all these benefits, cloud computing has its fair share of concerns. The main concern in the cloud computing industry is security [10]. The first and most obvious concern is privacy considerations[1]. That is if another party is housing all your data, how do you know that it's safe and secure? Since the internet powers cloud computing, data migrated to the cloud could be assessed by anyone from anywhere when security is breached. Hackers can go to any extent in order to compromise data [3].From selling your confidential information to rivals and those on the dark web to encrypting your storage and data unless you pay them off, or they can simply delete anything to harm your company and defend their actions based on ideological views [1].This will have a massive effect on the company's reputation, as well as depleting the interest consumers have in the company, resulting in customer loss [11].Whatever the case, hackers are a serious concern for your data managed on a cloud. Because your data is held on someone else's computers, you may be at the mercy of whatever security measures they support [1]. Organizations do not have much control over what happens to their data as everything on the cloud including security is managed by the cloud provider.

II. DATA SECURITY IN CLOUD

The numerous benefits that come with cloud computing have enticed many organizations and governments agencies to move their sensitive data to the cloud [11]. This avails an opportunity for attackers to also exploit the vulnerabilities in cloud computing and breach the security of the cloud. Fuelled by different agendas, they can hurt organizations through data theft, perform man- in-middle attacks, and compromise the integrity of data [6]. Many cloud giants like Google, Amazon, and Microsoft have adopted various measures to protect data stored on their cloud platforms by their clients [11]. But data should be protected against unauthorized access in all three data states (data at rest, data in transition, and data being processed). Some organizations are aware of these security issues and encrypt their sensitive data before migrating it to the cloud. This provides another level of security from the client's side for their data in transit.

III. CRYPTOGRAPHY

Cryptography is a method of concealing information in order to hide it from unauthorised users [10]. Transmitted data is obscured and rendered in a ciphertext format that is unreadable and incomprehensible to an unauthorised user. A key is utilized to transform cipher text to plain text. This key is kept confidential and only authorised entities have access to it [6]. 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. In cloud cryptography, there are two major types of encryption algorithms. These are: symmetric and asymmetric encryption algorithms [8].

A. Symmetric Encryption Algorithm (Secret Key Cryptography)

Symmetric Encryption Algorithm uses one key for both encryption and decryption [8]. Examples of this encryption algorithm a briefly discussed below.

- *Data Encryption Standard (DES)*

DES is a standard for data encryption that uses a secret key for both encryption and decryption. It adopts a 64-bit secret key, of which 56 bits are randomly generated and the other 8 bits are used for error detection. It employs a data encryption algorithm (DEA), a secret block cipher employing a 56-bit key operating on 64-bit blocks [10]. It is the archetypal block cipher- an algorithm that takes a fixed-length string of plaintext bits and transforms it into a ciphertext bit string of the same length. DES design allows users to implement it in hardware and use it for single-user encryption, such as files stored on a hard disk in encrypted form [9].

- *Advanced Encryption Standard (AES)*

It is a National Institute of Standards and Technology (NIST) specification for encrypting electronic data. It also helps to encrypt digital information such as telecommunications, financial, and government data. It is being used by US government agencies to sensitive unclassified materials [10].AES consists of symmetric key algorithm: both encryption and decryption are performed using the same key. It is an iterated block cipher that works by repeating the defined steps multiple times. It has 128-bit block size, with key sizes of 128, 192, and 256 bits for AES-128, AES-192, and AES-256, respectively [8]. The design of AES makes its use efficient in both software and hardware and also works at multiple network layers.

- *Blowfish*

Blowfish is a type of symmetric algorithm designed to replace DES or IDEA algorithms. It uses the same secret key to encrypt and decrypt data [10]. The algorithm splits the data into a block length of 64 bits and produces a key ranging from 32 bits to 448 bits. Due to its high speed and overall efficiency, blowfish is used in password protection tools to e-commerce websites for securing payments. It is a 16-round Feistel cipher working on 64-bit blocks. However, unlike DES, its key size ranges from 32 bits to 448 bits [9].

B. Asymmetric Encryption Algorithm (Public-Key Cryptography)

This encryption algorithm was introduced to solve key-management problems [10]. It involves both a public key and a private key. The public key is publicly available, whereas the sender keeps the private key secret. Asymmetric encryption uses a key pair comprising of public key available to anyone and a private key held only by the key owner, which helps to provide confidentiality, integrity, authentication, and nonrepudiation in data management [9].

- *Rivest Shamir Adleman (RSA) Algorithm*

RSA is a public-key cryptosystem for Internet encryption and authentication. RSA uses modular arithmetic and elementary number theories to perform computations using two large prime numbers [8]. The RSA system is widely used in a variety of products, platforms and industries. It is one of the de-facto encryption standards. Companies such as Microsoft, Apple and Novell build RSA algorithms into their operating systems [4]. RSA is the most popular asymmetric algorithm. The computational complexity offactoring large integers that are the product of two large prime numbers underlies the security of the RSA algorithm [10]. Multiplying two prime numbers is easy, but RSA is based on the complexity of calculating the original numbers from the product [9].

- *Elliptic Curve Cryptography (ECC)*

ECC is modern public-key cryptography developed to avoid larger cryptographic key usage [6]. The asymmetric cryptosystem depends on number theory and mathematical elliptic curves (algebraic structure) to generate a short, quick, and robust cryptographic key [8]. Elliptic Curve Cryptography has been proposed to replace the RSA algorithm because of the small key size of the ECC [2].

IV. CRYPTOGRAPHY TECHNIQUES USED BY SOME CLOUD GIANTS

Google has adopted multiple layers of encryption to protect the data on its Google Cloud platform. Google uses Advanced Encryption Standard (AES 128 and AES 256) encryption algorithms to encrypt data at rest on their cloud platform. Google divides customers data into multiple chunks and encrypts each chunk with different encryption keys [3]. The data and the generated encryption key are wrapped together by another encryption key providing another layer of protection and these encryption keys are exclusively used in Google’s central Key Management Service [3]. When a piece of data is revamped, it is encrypted with a new key rather than the old key. Since each chunk of data is encrypted with a special key, if one chunk of data is breached, it has no effect on the other chunks. Google uses Access Control Lists (ACL) to ensure that each chunk can only be decrypted by Google services acting in authority with access at the time [3]. This ensures data protection and safety by preventing unwarranted access. The global distribution of the chunksof data means that for an attacker to get access to data they have to (1) find all locations of the various chunks corresponding to the data they want and (2) know the encryption keys of each of the individual chunks of this data [1]. Amazon S3 stores object redundantly across multiple facilities in an Amazon S3 region [5]. This redundancy helps in repairing data if there are data corruption issues. In addition, Amazon S3 also uses versioning to reserve every version of every object stored in the Amazon S3 bucket [11]. Versioning allows us to easily recover from unintended user actions and application failures [5]. The server-side encryption used by Amazon while the data is at rest i.e., stored in disks at Amazon S3 data centres is similar to that of Google and it uses 256-bit AES to encrypt the data [3]. Microsoft adopts a shared responsibility when it comes to ensuring data security and privacy on their Azure cloud platform [4].

V. PROPOSED ALGORITHM

The proposed algorithm is for encrypting data at the client-side before transmitting it for storage in the cloud. This will convert plaintext into ciphertext and prevent data theft through man-in-the-middle attacks. That is, even if an attacker can intercept the data, he would not be able to read the actual data or get any reasonable meaning from it.

***A.** Encryption Algorithm*

1. Convert the character to its ASCII code
2. Convert the ASCII code to its equivalent 8-bit binary number. If it is not equal to 8 bits, add preceding 0s.
3. Find the 1’s complement of the last 4 bits.

4. Convert the generated binary code to an ASCII character and transmit it to the cloud.

Example: Let say we want to send ‘A’ over the cloud. First, we convert plaintext ‘A’ to its ASCII code i.e., 65. We then convert the 65 to its 8-bit binary number. 65 in binary is 1000001 but since it’s not equal to 8 bits, we add 1 preceding 0 to get 01000001. We then find 1’s complement of the last 4 bits. This will give us 01001110. Finally, we convert this 8-binary number to its ASCII code character, ‘N.

B. *Decryption Algorithm*

1. Find the ASCII code of the character.
2. Convert the ASCII code to binary. Add preceding 0s if not equal to 8 bits.
3. Reverse the last 4 bits of the generated 8-bit binary value.
4. Convert the generated binary value to ASCII code.

The original character (plaintext) is the character that matches the ASCII code.

Using the above example to convert the cipher-text to plaintext:

First, convert the cipher-text ‘N’ to ASCII code i.e. 78. 78 is then converted to binary to get 1001110 but since it’s not equal to 8 bits, we add a preceding 0 to get 01001110. We then reverse the last 4 bits to get 01000001 and convert this binary value to its ASCII equivalent. The original character or plaintext is the character that matches the ASCII code generated.

V1. CONCLUSION

In this paper, various cryptographic algorithms used in cloud computing were discussed and reviewed some of the cryptography algorithms used by some major players in cloud computing. A new algorithm to encrypt data in transition from the cloud user to the cloud provider’s platform was proposed and discussed. Paving forward, I will be working more on balancing the security of the proposed algorithm with usability and efficiency and testing its compatibility with the various cloud platforms.

REFERENCES

[1] Cyber Chief Magazine, Cybersecurity 2020 Top Trends Shaping Management Priorities, Ed 8.

[2] Douglas R. Stinson, Cryptography: Theory & Practice, Chapman and Hall Publications.

[3] Google Platform Encryption Whitepaper. Encryption at Rest in Google Cloud Platform. Retrieved from https://cloud.google.com/security/encryptionat-rest/default-encryption

[4] Information Security Management System for Microsoft Cloud Infrastructure. Retrieved from http://aka.ms/mgmtcloud

[5] Janakiram MSV. Amazon Brings Artificial Intelligence to Cloud Storage to Protect Customer Data. (August 20, 2017). Retrieved from https://amp/s/www.forbes.com/sites/janakirammsv/2017/08/20/amazon-brings-artificialto-cloud-storage-to-protect-customerdata/amp

[6] J.N., Aws and Z.F. Mohamad. Use of Cryptography in Cloud Computing. Conference Paper published in IEEE November 2013.

[7] Mell, P., Grance, T. (September 2011). The NIST Definition of Cloud Computing. Retrieved from http://csrc.nist.gov/publications/detail/sp/800- 145/final#pubs-abstract-header

[8] Narang, Ashima and Deepali Gupta. Different Encryption Algorithms in Cloud. April, 2018. ResearchGate.

[9] Prasad,P, A. Parul. Cryptography Based Security for Cloud Computing System.

[10] Stallings, William. Cryptography and Network Security (6th Edition). Pearson, 2014

[11] Velte, T. A, Velte, T. J., Elsenpeter, R. Cloud Computing: A Practical Approach.