Cloud Computing – Cryptography

[1]Miss Ruchira Gajanan Mankar,
[2]Prof. Prashant P. Patil

[1]PG Student, [2]Asst.Prof. Bharti Vidyapeeth(Deemed) University, Pune

Yashwantaro Mohite Institute of Management Karad, Maharashtra

[1]PG & MCA Department,
[1]PG Student , Karad, India.

1) Abstract -

Cloud Cryptography is encryption that safeguards data stored within the cloud. Several measures are being placed within cloud cryptography which adds a strong layer of protection to secure data to avoid being breached, hacked or affected by malware. Any data hosted by cloud providers are secured with encryption, permitting users to access shared cloud services securely and conveniently. Cloud Cryptography secures sensitive data without delaying the delivery of information.

Cryptography within the cloud employs coding techniques to secure information which will be used or hold on within the cloud. It permits users to handily and firmly access shared cloud services, as any information that's hosted by cloud suppliers is protected with coding. Cryptography within the cloud protects sensitive information while not delaying info exchange.

Cryptography within the cloud permits for securing essential information on the far side your company IT atmosphere, wherever that information is not any longer beneath your management. Cryptography knowledgeable Ralph sociologist Poore explains that "information in motion and knowledge at rest square measure best protected by cryptanalytic security measures. within the cloud, we have a tendency to don't have the posh of getting actual, physical management over the storage of knowledge, that the solely manner we will make sure that the data is protected is for it to be hold on cryptographically, with USA maintaining management of the cryptanalytic key."

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

2) Introduction-

Cloud computing may be a framework for giving on-demand network access to a pooled pool of configurable computing resources (e.g., networks, servers, storage, software, and services) which will be quickly provisioned and free with limited maintenance activity or service supplier involvement [7]. In cloud computing, resources area unit abstracted and virtualized from the cloud provider's IT infrastructure and created accessible to the client. Cloud infrastructure provides varied benefits to cloud consumers and different core stakeholders. a number of these benefits area unit access to knowledge hold on on the cloud despite the location, pay-on-demand basis, flexibility and elasticity, and economic edges by saving the corporate from shopping for hardware and different IT infrastructure [11].Despite of these edges, cloud computing has its honest share of issues. the most concern within the cloud computing business is security [10]. the primary and most obvious concern is privacy considerations[1]. That is if another party is housing all of your knowledge, however does one recognize that it's safe and secure? Since the net powers cloud computing, knowledge migrated to the cloud can be assessed by anyone from anyplace once security is broken. Hackers can visit any extent so as to compromise knowledge [3].From selling your counselling to rivals and people on the dark net to encrypting your storage and knowledge unless you pay them off, or they'll merely delete something to harm your company and defend their actions supported ideological views [1].This will have an enormous result on the company's name, in addition as depleting the interest consumers have within the company, leading to client loss [11].Whatever the case, hackers area unit a heavy concern for your knowledge managed on a cloud. as a result of your knowledge is command on somebody else's computers, you will be at the mercy of

whatever security measures they support [1]. Organizations do not have abundant management over what happens to their knowledge as everything on the cloud as well as security is managed by the cloud supplier.

1. Data Security in the Cloud

The numerous edges that go along with cloud computing Have enticed several organizations and governments agencies to move their sensitive information to the cloud [11]. This avails associate degree opportunity for attackers to conjointly exploit the vulnerabilities in cloud computing and breach the protection of the cloud. Fuelled by totally different agendas, they'll hurt organizations through information larceny, perform man- in-middle attacks, and compromise the integrity of knowledge [6] Several cloud giants like Google, Amazon, and Microsoft have adopted numerous measures to safeguard information hold on their cloud platforms by their purchasers [11]. however information ought to be protected against unauthorized access all told 3 information states (data at rest, data in transition, and information being processed). Some organizations area unit alerts to these security problems and encipher their sensitive information before migrating it to the cloud. This provides another level of security from the client's facet for their information in transit.

2. 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 no repudiation 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 of factoring 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].

3. 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.

4. 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/defaultencryption

[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-toprotect-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#pubsabstract-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.