IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

A Review on Cloud Security Services and Key Management

Prathmesh Arun More
Student, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *Cloud Computing is one of the demanding computer system resources, exclusively for data storage and computing power. The architecture of cloud models scares the security of existing technologies when open in a cloud environment. Thus, the user of the cloud must know the danger before uploading the data in the new environment. Cloud Cryptography is an approach towards security in the cloud as cloud computing uses an internet-based computing model that furnishes resources through (CSP) Cloud Service Provides and also the (CU)cloud user without buying any basic framework and pursue a pay per use basis..*

Keywords: Cloud Cryptography, Cloud Computing, Symmetric, Asymmetric, Algorithms, Key

I. INTRODUCTION

Cloud Computing is storing and accessing data and programs over the internet which could be stored in a remote area or place instead of your computer. A cloud is just a place where you can store the data and can access it via the internet anytime. Cloud Providers are the companies that offer computing service and charge according to the usage.

Cloud Computing has caused a major improvement in the IT sector, it not only allowed to store data in a remote area but also allowed to access the data from anywhere in the world. To secure all the data cloud cryptography is used, so what does cloud cryptography do? It encrypts that is it converts the data in an unreadable format and decrypt whenever the user needs it using some algorithm. This type of service is now provided by a large number of companies like ScienceSoft, Sophos, HyTrust, CipherCloud and many more. There are not only advantages but also disadvantages to a cloud. The major disadvantage is it requires the internet without that it cannot do any good. Second, comes is about its security, how good maybe a cloud is secure there is always an attacker or hacker finds a way in, the only way to terminate this is to upgrade the security from time to time.

II. LITERATURE REVIEW

Cloud Cryptography plays a major role in cloud computing from encrypting the data to decrypting it. Most of the researcher cover the topics or the key research topic are its services, modules, benefits, attacks, algorithms, etc. May researcher hasn't touched or researched about is, how we can prevent different types of attacks on cloud and how combining more than two algorithms can help us to achieve a major step in cloud cryptography security. More than two companies collaborating and coming forward to create or give security towards cloud computing. Cloud cryptography has also become business as providing security to the crucial data is important. Talking about the business company provides different types of services to the user but the user has to pay for it.

Another major problem that occurs in cloud cryptography is, how strong the algorithms can provide security? Are there any vulnerabilities in it that can lead to the loss of data?

III. CLOUDS IN CLOUD COMPUTING

1. **Public:** In a public cloud, everyone can access the data, that is the whole computing infrastructure is situated on the establishment of a cloud company that willingly offers the cloud service. The major problem here is with the security and tampering of data.
2. **Private:** A Private cloud is basically cloud for the computing infrastructure itself and not a sharing one. This type of cloud is for a company, in other words, the private cloud acts as an intranet. Here, the security is of top quality and an unauthorized user cannot access the cloud.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

3. **Community:** A cloud shared between two or more than two organizations to achieve a common goal or to get in a professional community or geographic community.
4. **Hybrid:** A Hybrid is a combination of two or more cloud can be (private and public or private and community or public and community) depends on the ambition. We can anchor the most important applications on our server to give them top-level security or keep them more secure and keep the secondary applications somewhere else.
5. **Virtual Private Cloud[3]:** A Virtual Private Cloud is a mini or a small cloud within the public cloud environment which is an on-demand configurable pool of computing resource which provide a certain level of isolation between the organization, which can be denoted as users.

IV. CLOUD SERVICES

1. **Infrastructure as a service(Iaas):** Iaas is categorized as one of the main cloud computing resources on the internet. Iaas cloud computing provides us with virtual computing resources. It also provides computer resources like hardware, software and different storage devices but on user demand. Examples Linode, AWS (Amazon Web Service).
2. **Platform as a service(Paas):** Paas allows the user to buy or subscribe access to the platform to release their application and software. Examples AWS Elastic Beanstalk, Windows Azure.
3. **Software as a service(Saas):** Saas allows us to run the application directly without installing it, the user just needs to open or access it or can open it through a web browser. Saas is basically managed by the mediator. Examples are Microsoft Azure, Google Compute Engine (GCE).
4. **Communication as a service(Caas)[1]:** Caas is not categorized as the main computing model. In Caas can be called an outsourced enterprise communication for a single vendor, allows to communicate over voice IP(VoIP), videoconference and collaboration. Caas as emerge as Saas. Examp1les Docker Swarm, Google Kubernetes.
5. **Function as a service (Faas)[6]:** Faas allows user to build, run and manage application without any complexity and compromising the infrastructure which can be released with development and dispatch of an application. Examples Internet of things, Batch Processing, etc.
6. **Monitoring as a service(Maas)[5]:** Maas is a framework that eases the deployment of different monitoring functions for other service and application which already exist in the cloud.

V. CLOUD COMPUTING BENEFITS

1. Cost savings.
2. Strategic edge.
3. High speed.
4. Reliability.
5. Backup and restore data.
6. Collaboration.
7. Allows pay per user.

VI. ATTACKS THAT CAN OCCUR ON CLOUD

	Attacks	Description
1.	**Man-in-the-Middle Attack**	A man-in-the-middle attack is caused when there are vulnerabilities in the cloud. The hacker reconfigures and enters the communication between the two users. Man-in-middle has two types of Passive attack and Active attack. In a passive attack, the attacker's main motive is to get the data but does not modify it and in Active attack, it can modify or delete the data and can send wrong data towards the receiving end.
2.	**Denial of service**	Also called a DoS attack, is an attack in which the hacker sends n number of packets or spam by which it overloads the system called flooding and makes the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

		service unavailable for the user. The attack can be more dangerous if the attacker sends a request from different machines called DDoS.
3.	**Cloud malware injection attack**	This attack is done so the attacker can gain control over the user information. The hacker adds a corrupted service module, so what it does is redirect all the requests towards the hacker end. Examples of malware injection are SQL injection attacks and cross-site scripting.
4.	**Advanced persistent threats (APTs)**	ATPs allows the hacker to steal sensitive data stored and that too without getting detected by any legitimate user. The worst part is it allows a hacker to adept security measures. Then the hacker can move around the networks and use network traffic to perform its malignant activity.
5.	**Cryptographic Attack**	In this attack, the attacker finds the weakness of the cryptographic system by which it bypasses through the security of the cryptographic system the process is also called cryptanalysis.
6.	**Side Channel attack (SCA)**	In this attack, the attacker places a malicious virtual machine on the same home machine or the targeted machine. This attack can be stopped by simply designing a more secure system.
7.	**Insider attack**	By its name the insider attack, the attacker is located within the organization or their employee that purposely violates the policy. This attack can be stopped by cloud developers just by increasing the level of security/access to the cloud environment.

VII. CONCEPT

7.1 Cloud Cryptography

Cloud Cryptography is originated from the Greek word κρυπτο, that is to hidden/Secret. In Cryptography a readable word or sentence or any file is converted into a non-readable format and the receiver gets the message in a readable or in the original form/format. This is done by using different encryption techniques to secure the data that can be later stored in a cloud. So, the data shared will be in an encrypted format so it becomes convenient for the user to access that data. In cloud cryptography, two-phase takes place one is cloud encryption and cloud decryption.

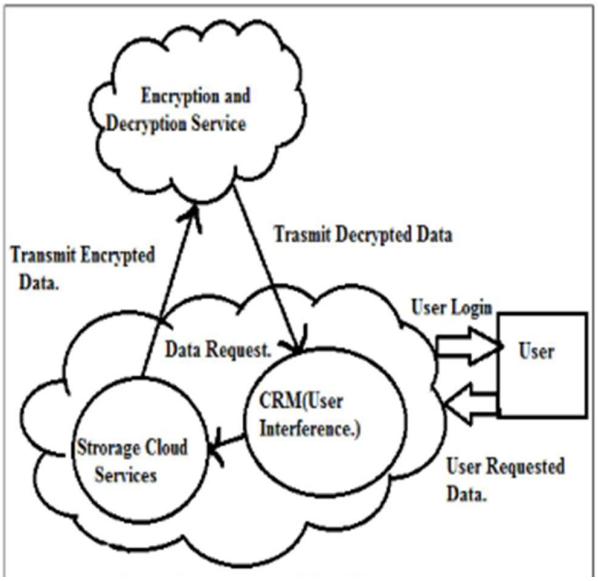

Fig 1. Data retrieval of cloud computing[7]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

7.2 Cloud Encryption

Cloud Encryption takes place before the data reaches the cloud. Cloud data that is going to get store inside the cloud gets encrypted before it reaches the cloud through a cloud encryption service. These services provide us with a range that which data gets encrypted from sensitive data like credentials to any data that is uploaded.

Encryption is one of the best ways for effective data security because the files, data present in the cloud get scrambled in a way that it becomes impossible to decrypt it without any key. Once the data is encrypted it can only be decrypted by a key so the companies make sure that only authorized user gets access to their sensitive data and even if the data is lost it will in a decrypted format which is although meaningless.

7.3 Cloud Decryption

Cloud Decryption happens when the key matches its security code because without its impossible to decrypt a file or data of the cloud. Decryption takes place when a certain data is requested by the user, the request reaches the cloud then cloud forward that data towards and decryption cloud service which decrypt the data using the key.

VIII. CRYPTOGRAPHY AND ITS TYPE

There are various types of an algorithm for cryptography but the most basic types of cryptography are Symmetric and Asymmetric key cryptography. Some can also be classified as the sub-categories of symmetric and asymmetric. Other algorithms used in cryptography are Rivest Shamir and Adelman (RSA), Diffie-Hellman Exchange, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple-DES, Blowfish Algorithm, Homomorphic Algorithm, Serpent Algorithm, etc.

8.1 Life-Cycle and Management of Key

A key plays a crucial role in cryptography. Without a key, the algorithm depends on itself for the cryptography process, while using the key the attacker can know about which type of algorithm is used in it, but if we use the key that can be symmetric keys or asymmetric keys which are private keys so even the attacker gets the data it's useless without the key. Key should be generated randomly because the randomly generated keys give more effective power to encryption. To generate, protect, rotate, distribute and retirement of the key, is known as “key Life-Cycle”.

Key Management is done by a key management system which designs different types of key and also keeps them active. Keys are generated and protected by hardware devices called hardware security modules (HSMs).

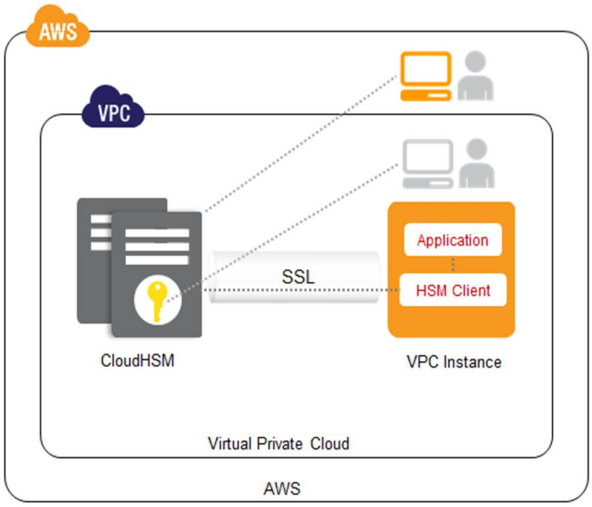

Fig 2. AWS Cloud Hardware Security Modules [8]

8.2 Symmetric Key Cryptography

In Symmetric key cryptography, the data or any file is encrypted using a key by the sender and at the receiver, end wants to decrypt the data or that file, the same key is used. The sender and receiver will have the same key to encrypt

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

and decrypt, which is agreed by both of them. The only way to read the encrypted data is to apply the key given by the sender. If an attacker wants to decrypt the data without the key brute force action will come in handy. The longer the encryption key, the harder it takes to crack it. Two commonly used symmetric encryptions are block and stream, which are the two types of a cipher. As by the name block cipher will take a block of data and will encrypt it using the key. For example, we are having 64-bit of data, the block cipher will take the whole 64-bit or divide into two part of 32-bit. In-stream cipher the data is divided 1-bit of data is encrypted at a time. For example, we are 8-bit so the stream cipher will divide it into 8 different parts of 1-bit each.

8.3 Asymmetric Key Cryptography

In Asymmetric key cryptography, the data or any file is encrypted using one key that is public key given by the sender and the decryption is done by using another key called private key that is also given by the sender to the receiver. If the receiver does not have the private key given by the sender it cannot decrypt the data or file in it. On the other side if the private key gets in the hand of an attacker the data can be easily stolen. Asymmetric key cryptography is complex and heavy so it's more time for the process to complete.

IX. ALGORITHMS AVAILABLE IN CRYPTOGRAPHY

9.1 Symmetric Algorithms.

1. AES (Advanced Encryption Standard),
2. DES (Data Encryption Standard).
3. IDEA (International Data Encryption Algorithm).
4. Blowfish (Is a Drop-in replacement for DES or IDEA).
5. RC4(Rivest Cipher 4).
6. RC4(Rivest Cipher 5).
7. RC4(Rivest Cipher 6).

9.2 Asymmetric Algorithms

1. EIGamal.
2. RSA(Rivest-Shamir-Adelman).
3. DSA (Digital Signature algorithm).
4. Elliptic curve technique.
5. PKCS (Public-Key Cryptography Standards).

.

X. EXPLANATION OF SYMMETRIC ALGORITHMS

10.1 DES (Data Encryption Standard)

Data Encryption Standard can be called an asymmetric key algorithm. It converts 64-bit plain text into blocks of 64-bit ciphertext using keys. As it is a symmetric key it will use only one key for encryption and decryption. It follows the implementation of Feistel cipher. A Feistel cipher is dividing the inner or internal state of the cipher which is in multi-round and only operates a single part in each round of encryption and decryption. On the side of encryption site, DES takes about 64-bit "Plain Text" and also creates a 64-bit ciphertext, at the decryption site, then it takes that 64-bit ciphertext and again convert it in a 64-bit "Plain Text", and same 56-bit cipher key is used for both encryption and decryption [4]. It starts with initial permutation and ends with final permutation in between containing (P-boxes) called as straight Permutation boxes.

10.2 AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is one of the most popular algorithms used worldwide as it faster than DES. In AES the round may increase or decrease depending on the length of the key. It uses 10 rounds for 128-bit, 12 rounds for 192-bit and 14 rounds for 256 bits. AES encryption process has four sub-process.

1. Sub Bytes: Here the box is called as S-box gives the design by taking 16 bytes of input which gives us a matrix.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

2. Shift Rows: In shift rows, we follow certain steps to shift it to the left or any fall-off entry are re-inserted on the right of the row.
3. Mix Columns: We use a special mathematical function to transform. Take four bytes of one column is done by the function and change them into new four bytes to modify or replace the original column. We get a new matrix of 16 bytes.
4. Addround key: The new 16 bytes can be considered as 128 bits and XORed to 128 bits of the round key. To get the ciphertext it should be the last round or the resultig128 bits get interpreted and a similar round begins again.

10.3 IDEA (International Data Encryption Algorithm)

International Data Encryption Algorithm is a symmetric key block, it uses 16 bits of fixed-length plaintext, which are then encrypted in 4 chunks of 4 bits and each of the chunks produces 16 bits of ciphertext.The key of IDEA is divided into 8 blocks, 4 bits each. It has 4 complete rounds and one-half round. Each of the rounds is of 14 steps that have operations like

1. Bitwise XOR.
2. Addition modulo (2^4)
3. Multiplication modulo (2^4) + 1

When the four rounds are completed, the final half-round only takes 4 steps out of 14 steps. Each of the rounds contains binary notation which must be converted to equivalent decimal notation. After this, we perform the operation and to get the result, once we get the result is then converted again back to the binary representation to get results called the final result. IDEA contains a key schedule which has steps to perform the algorithm.

XI. EXPLANATION OF SYMMETRIC ALGORITHMS

11.1 Rivest Shamir and Adelmann (RSA)

In the RSA algorithm, we have two one is a public key and the other is a private key. By the name public key, it is easily obtained and the private key is only given to the receiver by the sender. So, to decrypt the message private key necessary. But RSA is not fully secured, the public key is the multiplication of two large prime numbers and the private key that is sent to the receiver by the sender is also derived from the same prime numbers. So, if an attacker applies a proper factorization on that large number the private key can be easily cracked. So, the strength of the encryption depends on the size of the key greater the number or we can say double or triple the key size more secure it is, but it also means slow processing of data which takes more time.

11.2 Procedure

We start with two prime number, can be p and q.

$N=p^*q$

Derived Number (i) should be greater than 1 and less than (p-1) and (q-1). Public keys are a pair of two numbers n and i. Private key d can be calculated from p, q and e we get, id= 1 mod (p-1) (q-1) this is a basic formula of extended Euclid.

11.3 Encryption Formula

$C=Pi \bmod n.$

11.4 Decryption Formula

Pt (PlainText) = $Cd \bmod n.$

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

11.5 DSA (Digital Signature Algorithm)

Digital Signature Algorithm is a (FIPS) federal information processing standard that is established on the mathematical concepts of exponentiation and discrete logarithm. We can say it is an alternative to the algorithm like EIGamal and Schnorr. A digital signature is a value calculated from the data and that value is cryptographic.

A. Process of DSA (Digital Signature Algorithm)

In DSA the private key is considered as signature key and the public key as the verification key, the signer who has the private key gives its data to the hash function, the work of the hash function is to generate a hash of that data. Now we have the hash value as well as the signature key to be inserted in the signature algorithm which gives us the digital signature. These go to the verifier which verifies it by sending them to the verification algorithm which gives us some value as output.

The hash function which we run earlier is run again by the verifier to generate a hash of data. To check whether the digital signature is valid or not, the hash value and the output we got from the verification algorithm are matched together. We create a digital signature using the private key and only the signer can have this. The importance of digital signature is message authentication, data integrity, and non-repudiation. To encrypt there are two possibilities in DSA, sign then encrypt and encrypt-then-sign, the data first goes to the receiver and using the public key it moves forward to the hash function, when the encrypted data and digital signature with senders private key are combined together we get the original data.

XII. CONCLUSION

This review paper contains, what is cloud computing? how cloud computing provides us with different types of cloud-like public, private, community, hybrid, and virtual private clouds. It also provides us with different service which protects our data and allows us to access it anytime, services like Iaas, Paas, Saas, Faas and Caas.

Talking about the benefits of it, it is cost-saving, it is reliable, provides us high speed that is the server is maintained so we can upload data as well as download it. The challenges or we can say the security problem faced by cloud computing are the attack performed on it by attacker and hacker. Some of the attacks are Denial of services, man-in-the-middle, cryptographic attack and many more.

To understand cloud cryptography, we need to understand the algorithm used in it or we can say the encryption and decryption process performed in it. The most basic algorithms used are symmetric and asymmetric. These two furthermore categorized, they contain many algorithms that are used in cryptography. Talking about another concept of cryptography we use keys in the algorithm to maintain, manage and keep them running for a long time we use hardware security modules that look after the keys. The various algorithm uses different types of cryptography and has a various formula which defines their strength

REFERENCES

[1]. Aws Naser Jaber, Mohamad Fadli Bin Zolkipli, Use of Cryptography in Cloud Computing, Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang.
[2]. Gunavathy.S, Dr.MEENA.C, A survey: data security in cloud using cryptography and steganography.
[3]. G. Kishore Kumar, Dr. M. Gobi, Role of Cryptography & its Related Techniques in Cloud Computing Security.
[4]. Sathyalakshmi.L, A.Mohanarathinam, V.S.Jayanthi, Critical review of cryptographic techniques.
[5]. Chakrawati Jain, Avinash Sharma, Retrival Process in Cloud Computing: An Assessment.
[6]. Faas [Online], Available: https://www.esds.co.in/blog/cloud-computing-types-cloud/#sthash.9AkRYn4x.dpbs
[7]. Types of cloud services [Online], Available: https://www.esds.co.in/blog/cloud-computing-types-cloud/#sthash.9AkRYn4x.dpbs
[8]. Data retrieval of cloud computing [Online], Available: https://www.ijser.org/paper/A-CRM-Based-Cryptography-Service-for-Ensuring-Security-in-Cloud-Computing.html
[9]. Life Cycle and management of key [Online], Available: https://www.ijser.org/paper/Secure-Cloud-Computing-Using-Encryption-and-Decryption-Method.html

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

[10]. AWS Hardware Security Module [Online], Available: https://aws.amazon.com/blogs/aws/aws-cloud-hsm-secure-key-storage-and-cryptographic-operations/

[11]. Data Encryption Standard [Online], Available: https://www.geeksforgeeks.org/simplified-international-data-encryption-algorithm-idea/

[12]. Advanced Encryption Standard [Online], Available: https://www.geeksforgeeks.org/simplified-international-data-encryption-algorithm-idea/

[13]. International Data Encryption Algorithm [Online], Available: https://www.geeksforgeeks.org/simplified-international-data-encryption-algorithm-idea/

[14]. Blowfish Algorithm [Online], Available: https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/

[15]. Rivest, Shamir and Adelmann Algorithm [Online], Available: https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_understanding_rsa_algorithm.htm

[16]. Digital Signature Algorithm [Online], Available: https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm