IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Cryptography and Secure Cloud Computing

Dr Indu Sahu
Assistant Professor
Vivekananda Institute of Professional Studies, Delhi, India

Abstract

Cloud computing is a platform that expands the computing capabilities of software systems and the individuals and organisations that use them without incurring the expenditure of setting up new and advanced infrastructure. Cloud computing brings with it the concept of sharing resources and a third party who sets up the infrastructure required for it, and enables this resource sharing. However, shared computing resources bring with the fear of user’s data being compromised as it is stored on a common environment, which is accessible by multiple users. Despite the huge advantages that cloud computing provides like, economic expenditure, pooled resources, scalability and elasticity, consumers is still very reluctant to deploy their commercial enterprise onto the cloud. Their major concern is the security of the data that they store on the cloud, and due to this fear of data being compromised, they mostly refrain from using cloud computing. Different deployment models of the cloud have different security issues. Therefore, everyone who uses cloud services should be aware of the potential threats that are posed by the different cloud deployment models while uploading data into this new environment. This paper explores the threats in the different cloud models and the different cryptography techniques that are used to overcome the same. This paper is a survey of specific security issues brought by the use of cryptography in a cloud computing system.

Index Terms— Cloud encryption, cryptographic algorithms, cloud security infrastructure.

Introduction

The rapidly growing cloud technology offers scalable and flexible solutions for businesses and individuals and has completely transformed the way business organisations and individual developers work these days. The user need not have a very high end device, his device can be a basic device capable of connecting itself to an internet, limited by memory, storage or computing ability. Using the cloud technology, he can use all computing resources available remotely at some location, known as the remote cloud server. The idea is that there is a cloud service provider, who provides all computing resources on the internet for which the user of those resources has to pay the service provider. So, it is a pay as you use service.

Cloud computing has some great advantages like, you pay only for the services that you use and the time for which you use those services, because these are metered services. Another major advantage is that these services are available anywhere and anytime because they come to you through the internet, so where ever you can connect your device to an internet connection, you can avail these services. And off course, one huge advantage being that you need not spend on setting up a high-end infrastructure or buying computing machines with high configuration. As part of the resources, storage is also provided to the user as a service, so most of the user’s data is also stored on a remote server somewhere that is managed by the cloud service provider.

This is where the vulnerability begins, because as the data is stored on the cloud, new security challenges are introduced. The privacy, security and trust issues with the service provider arise in a big way and are a major concern for the user, as he shifts to the cloud service. So, there is a need to protect that data against unauthorized access, modification or denial of services etc.

However, a key issue that will impact on the success of Cloud computing and may obstruct the expansion of 5G and CPSC is data protection, privacy and trust. Particularly, the risk of data leakage and unauthorised access increases when your data is stored in the cloud environment. Then secondly, attacks and intrusions that are challenging the security of Cloud Data Centres will continue to target these data centres. Thirdly, the data owner probably does not completely trust data management procedures such as storage, backup, migration, deletion, updates, searches, queries and access to cloud services. The reliability of data management should be checked by the data owners as a priority(Yan et al., 2017).

Fourthly, there is a possibility that the privacy of data could be exposed to unauthorised parties in cloud services.
It is important that any sources of intrusions, threat or attacks should be trackable. The points discussed above introduce a huge security challenge, particularly for big data storage and management. Cloud data security, privacy and trust are indeed becoming key issues that impact the success of cloud computing.

Encipherment is one of the most popular security mechanisms used for providing the Confidentiality service to the data stored on the cloud and protecting that data against sniffing or unauthorized access and traffic analysis. The data can be kept confidential by using a variety of cryptosystems available. These cryptosystems are classified as symmetric and asymmetric. The strength of a cryptosystem can be determined by the strength of algorithm design and the strength and the size of the key being used.(Masthan & Venkatesh Sharma, 2019)

Cryptography is extensively used to ensure privacy of data and trust in cloud computing. But most existing solutions are impractical. Storing encrypted data in the cloud reduces immensely the risk of data leakage, it makes it hard to perform auditing on data management. Encryption/ decryption keys need to be managed for access control and revocation, and this introduces additional computational and transmission costs. Additionally, operations such as fusion, aggregation, and mining on encrypted data are computationally exhaustive, so they are hard to be implemented due to its inefficiency. Cryptography in cloud computing promises many novel solutions and at the same time, many challenges are yet to be overcome.

There are three data security objectives: availability, confidentiality and integrity. Cryptography is used to ensure the confidentiality of data stored in the cloud. Cryptography is considered to be a combination of three algorithms in today's world. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. hashing algorithms ensure the integrity of the data.

Both asymmetric and symmetrically key algorithms are available to encrypt data stored in the cloud. Cloud computing stores a lot of databases, and when compared to the symmetric key algorithm, it is slower for such a big set of database asymmetric keys.

This research paper explores the role of cryptography in addressing these challenges and ensuring the confidentiality, integrity, and availability of data in cloud environments. This paper reviews numerous cryptographic techniques, and other practices used to secure data in transit, at rest, and during processing within the cloud. Through a complete analysis, this paper aims to provide insights into the current state of cryptographic solutions in cloud security and to guide future research in enhancing the resilience of cloud-based systems. This paper is organised as follows: Section 2 describes the security issues in the three deployment models of the cloud, section 3 discusses the major symmetric key cryptosystems and the asymmetric key cryptosystems, section 4 summarises the role of these cryptosystems in the security of data on the cloud. Finally, section 5 concludes the discussion.

2. Security issues in Cloud Computing

When it comes to privacy and security, cloud is greatly affected by the threat of that. The people such as the vendors must make sure that the people using cloud does not face any problem such as data loss or theft of data. There is a chance where a malicious user or hacker can get into the cloud by impersonating a legitimate user, there by affecting the entire cloud thus affecting many people who are using the infected or affected cloud. Some of the problems which are faced by the Cloud computing are:

1. Data theft
2. Integrity of data
3. Privacy problems
4. Loss of data
5. Infected Applications
6. Exact location of data
7. Vendor level Security
8. User level Security

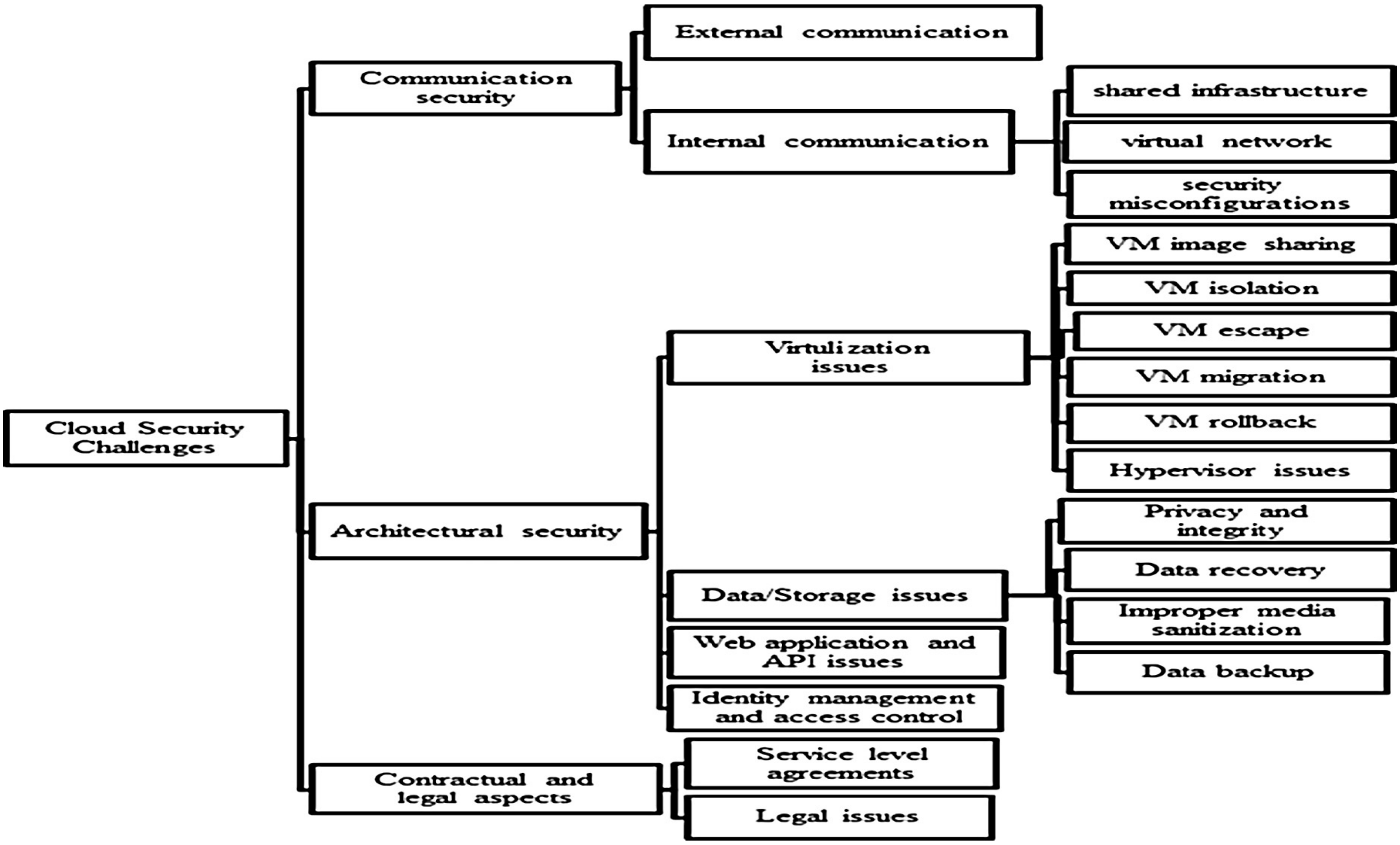

Figure 1 : Security Challenges in Cloud(Ali et al., 2015)

2.1 Security Issues of Deployment Models in Cloud

Figure 1 briefly describes the cloud deployment models. The different cloud deployment models namely public cloud, private cloud, and hybrid cloud have some security issues described below briefly:

	Infrastructure is manages and owned by	**Infrastructure is located at**	**Accessed by users**	**Example**
Private Cloud	Organization	On-Premises	Trusted	Federal Agency
Hybrid Cloud	Organization and Third Party Provider	Both On and Off-Premises	Both Trusted and Non Trusted	Amazon Web Services
Public Cloud	Third Party Provider	Off-Premises	Non-Trusted	Salesforce.com

Table 1: Brief description of Cloud Deployment Models

2.1.1 Security Concerns in Public Cloud

A public cloud is accessible by multiple customers publicly and therefore all customers are using shared computing resources. The Service provider has given access to the services to everyone who access the cloud. Though, providing basic security is his responsibility and he does that under his service agreement with the customer, there are some issues faced in a public cloud are as follows:

a) Security mechanisms in a public cloud are completely under the control of the service provider and therefore it is difficult to keep the data secure. Therefore, meeting the basic security requirements, namely integrity, availability, and confidentiality, becomes difficult during various stages of operation.
b) As the resources are openly shared on the public cloud, chances of a data breach are very high. Therefore, it is important to select the service provider very carefully so as to avoid these kind of risks.
c) If the cloud service provider has engaged a third-party vendor, it is important that the customer verifies the service level agreements (SLAs) as well as the contingency plans in case of any failures .
d) To prevent insider attacks, SLAs should be verified along with the levels to which data will be encrypted and authenticated to protect it from malicious intruders.

2.1.2 Security Concerns in Private Cloud

A private cloud is a cloud model which is completely controlled by one organization thereby providing total control over the cloud resources and flexibility to implement any security mechanism to that one organisation. However, some security concerns are still there:

(a) During the use of virtualization techniques, it is possible that the virtual machines (VMs) communicate with the wrong Virtual Machines, which leads to a lot of security risks. To prevent such security breaches, it is important to use appropriate encryption and authentication mechanisms.
(b) In order to avoid any security risk, the host operating system must be protected from any malware threat. It is also important that the communication between the host operating system and the guest VMs should not be direct but instead it should be via some physical interfaces.
(c) The consumers of private clouds are capable of controlling the cloud and use its infrastructure through a web interface. Therefore, it is important to protect various HTTP requests by using standard web-based application security mechanisms.
(d) There is a possibility of threats and attacks arising from within the organisation so a security policy needs to be developed, that would prevent insider attacks.

2.1.3 Security Concerns in Hybrid Cloud

A hybrid cloud is a combination of both public and private cloud. Usually, organisations that setup and maintain a private cloud, which is housed on premises of the organisation, sometimes also uses some computing resources that are available on the public cloud. In this kind of a setup also, certain security issues have been recognised in a hybrid cloud. Some of these are as follows:(Kumar et al., n.d.)

(a) To maintain a uniform security policy across the entire network, a proper infrastructure policy, such as IPS signatures, firewall rules, and user authentication, should be applied.
(b) To ensure the compliance of public and private cloud provider and maintaining coordination between them is difficult to ensure in a hybrid cloud.
(c) When public and private clouds are integrated in a hybrid environment, security management is essential. Hence, existing policies, such as authentication, authorization, and identity management, need to be modified to address these complex integration issues.
(d) Hybrid clouds need to manage tasks across multiple domains and not many administrators have this kind of experience and knowledge exposing it to various risks.

The discussion on the security concerns of deployment models introduces cloud specific security risks and the vulnerabilities of the system due to the network and the data communication through the internet. We saw that in case of public cloud the risks are due to the sharing of resources. Resource pooling being an important characteristic of the cloud. it allows the use of the same set of resources by multiple users through the concept of multi-tenancy and virtualization technologies. Multi-tenancy offers elasticity and optimizes the use of resources but also posses the risk of data leakage as the data stored on the public cloud is visible multiple users.

The services on the cloud are available on-demand through the internet, that's another important characteristic of the cloud through the web interface but this causes a high probability of unauthorized access to the data. For which authentication services need to be put in place. Likewise, in order to use PAAS or IAAS through a virtual environment introduces its own set of risks like erroneously communicating virtual machines.

The private cloud deployment model is setup and used by a single organisation, the set of risks involved are the same as a conventional system. The public, community, and hybrid clouds models are more risky because multiple users have access to these cloud models and there is a third party involvement for administrative purposes and also for maintaining the cloud setup. This third party is whom we are calling the cloud service provider and the problem is that we need to trust this third party and the consumer is really not sure how much to trust. Therefore, there are trust issues also, in addition to the multiple other security issues. Now, due to these trust issues, it is very important for the consumer to verify the SLA very carefully

3. Symmetric and Asymmetric Key Crypto Systems

Cryptosystem, a term that refers to a set of algorithms that encrypt and decrypt messages and data, that can be interpreted only by those, for whom, they are meant. It is a short form for cryptographic systems. Cryptography means, 'secret writing'. As stated by Behrouz A. Forouzan, in his book on Network Security & Cryptography, cryptography is "the term we use to refer to the science and art of transforming messages to make them secure and immune to attacks". These cryptosystems comprise of algorithms for generating a key, encipher and decipher. The Key, is the heart of an encryption/ decryption algorithm. The strength of the key decides how secure is our message after being encrypted. Basically, there are two types of cryptosystems, viz, Secret Key Cryptosystems, where the same secret key is used for encryption and decryption. This makes the algorithm completely reversible, i.e., when the plaintext is the input and the key is applied to it, output is the ciphertext and when the ciphertext is the input, using the same key, the output is the plaintext. The other type of cryptosystem is the Asymmetric Key cryptosystem. Here, two keys are in use, one key, usually known as the public key of the receiver, is used to encipher the message and the ciphertext when received at the destination can be decrypted using the receiver's private key. This section discusses briefly some of the most commonly used symmetric as well as asymmetric cryptosystems. (Forouzan, 2012)

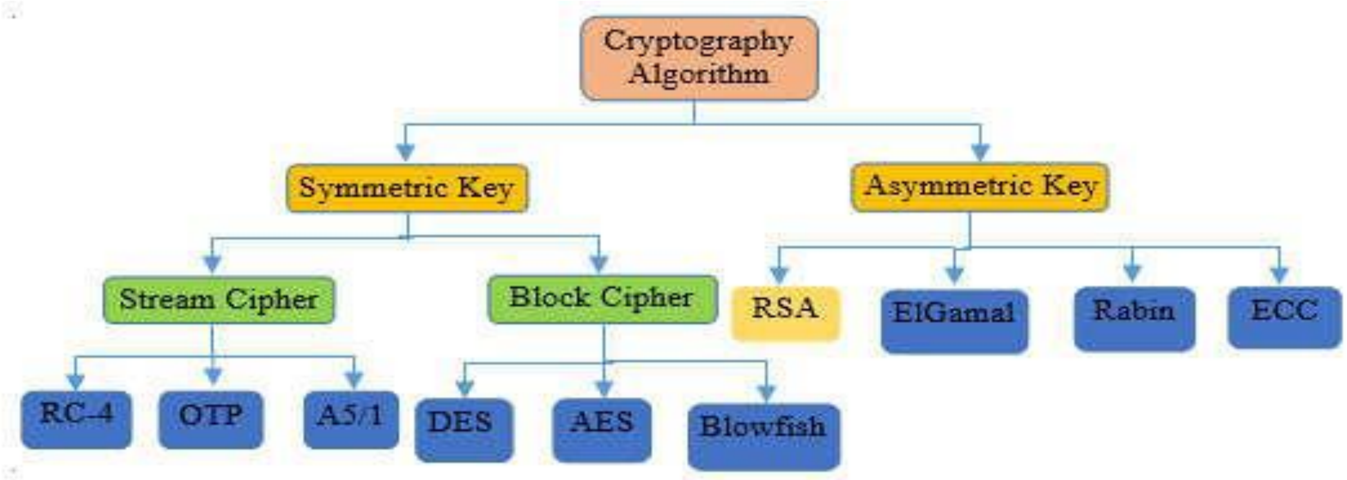

Figure 2: Classification of Cryptographic systems

3.1 Symmetric Key Cryptosystems

3.1.1 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). The algorithm accepts a 64-bit blocks of data with 56 bits key as plaintext input. Plaintext message is divided into 64-bit blocks; the last block is padded if the size of the block is less than 64 bits. DES algorithm consists of two permutations (P-boxes) and sixteen Feistel rounds. The complete encryption/decryption process is divided into three phases. First phase is the Initial permutation and the last phase is the final permutations. Initial permutation rearranges the bits of the 64-bit plaintext block. This is followed by the 16 Feistel rounds in the second phase. Each round applies a unique 48-bit round key to the plaintext bits to produce a 64-bit output. There is random key generator that generates sixteen 48-bit keys (one unique key for each round) out of the 56-bit secret key. Finally, the last phase performs a final permutation, a reverse operation of initial permutation and the final output is a 64-bit cipher text block. It is this cyphertext block which is transmitted to the destination.

DES derives its strength from the avalanche effect that it displays, that means, a small change in the plaintext or the key displays a massive change in the ciphertext. This makes cryptanalysis very difficult.

3.1.2 TRIPLE DATA ENCRYPTION ALGORITHM (3DES)

An enhanced version of DES is 3DES. It performs 3 rounds of encryption using DES on each plaintext block. The size of the plaintext block is 64 bits and it consists of 48 rounds in all. The algorithm uses a 168-bit key, which is later permuted to 16 individual subkeys, one each for the 16 Feistel rounds of DES. Each of the 16 subkeys are of size, 48 bits. 8 S-boxes are present. For the decryption process the whole encryption process is reversed. In the first stage, DES algorithm is used to encrypt the plaintext block using key K1, followed by the decryption of the output obtained from stage 1, using DES with key K2, in stage 2. The output of stage 2 is encrypted once again using DES and key K3, this is the third stage of 3DES. The output thus obtained from stage 3 using the key K3, is the ciphertext, which is transmitted to the destination. Decryption of the cipher text is exactly the reverse of the encryption process. During decryption, key K3 is used for decryption and then the key K2 is used for encryption and finally in the last stage it is decrypted using the key K1. Triple DES based cryptosystem is considered to be much more secure as compared to the DES based cryptosystem, but 3DES based systems are usually slow since it performs the DES process three times but provides high security using similar encryption process but in opposite order.

3.1.3 ADVANCED ENCRYPTION STANDARD (AES)

Another block cipher, AES is also based on Feistel network, which uses 128 bits block size and varying key length of 128, 192 and 256 bits. Depending on the key length, the number of rounds performed for encryption vary between 10, 12, or 14 rounds. Each round in AES algorithm performs Key expansion, Sub-byte generation, Column-mix and Add-round key. Since it uses variable length key bits, AES provides high level of security. Security of encryption depends on how long it takes for an attacker to find a key. The combined boomerang and rectangle attack with related key differentials uses the weakness of few non-linear transformations in key-schedule algorithms and can break some reduced round versions of AES. It can break 192-bit, 9 rounds AES by using 256 different related keys.

It is the most adopted symmetric encryption. It performs computation on bytes rather than on bits, AES treats 128 bits of plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. The algorithm operates on an entire data block by using substitutions and permutations. The key size used for an AES cipher specifies the number of transformation rounds used in the encryption process.

3.1.4 CAST-128

CAST-128 is yet another block cipher algorithm, which is based on the Feistel function and has 12 to 16 rounds of processing. The algorithm uses a 64-bit block and a key of length, 40-128 bits. If the key size is greater than 80 bits, there are 16 rounds of processing done. The basis of high security of CAST 128 is the fact that it uses variable key sizes of 128 and 256 bits. Due to this variable key length, the resistance against both linear and differential attacks is also increased. CAST-128 can be broken by 2^17 chosen plaintexts. The 64-bit key version is susceptible to differential related-key attack.

3.1.5 BLOWFISH

Blowfish is a block cipher algorithm also based on the Feistel function which uses a 64-bit block and key size ranges from 32 - 448 bits. The algorithm has a block size of 64 bits and it consists of two basic steps. In step 1, key expansion is done. The P-array consists of 18 sub keys of 32-bit each. There are four 32-bit S-boxes which contains 256 entries each. Then the data encryption is done using XOR operations. It has a wide range of applications where the key is not changed frequently. Blowfish performs 16 processing rounds. Key expansion and Data Encryption are the two main functions performed by this algorithm.

3.2 Asymmetric Key Cryptosystems

Asymmetric key or public key cryptography, uses a pair of keys, one for encryption and the other for the decryption process. When a sender wishes to send an encrypted message to the desired destination, the source uses the publicly shared key of the recipient to encrypt the message and at the destination, the recipient uses his private key for decrypting the message. This means that, everyone in the network has a pair of keys to himself, one is his public key, also called encryption key, that he publishes for everyone to view and use on the network; and the second key is his private key, also called as decryption key, that he keeps to himself as a secret. Encipherment, Digital Signatures and Key Exchange are the uses of asymmetric key cryptographic functions. Encipherment, where the sender encrypts the plaintext message using the recipient's public key to produce the ciphertext block and the recipient decrypts the ciphertext using his own private key. The second application is the use of Digital Signature, where, the sender encrypts the message or a small block of data with his private key and this is verified by decryption of the same using the sender's public key. This works for authentication of the sender and provides non-repudiation service. Thirdly, public key cryptography is also used in exchange of a session key between the sender and the recipient. There are two asymmetric key algorithms that we go on to discuss here, RSA and Deffie Hellman.

3.2.1 The RSA algorithm

RSA (Rivest-Shamir-Adleman) is an asymmetric key cryptographic algorithm. (Source:(Stallings, 2005)) A block cipher that encrypts and decrypts data blocks, where plaintext and ciphertext are integers between 0 and n for some n. In RSA, Encryption and Decryption can be done as follows:

CT = PTe (mod n)
PT = CTd (mod n) = (PTe)d (mod n) = PTed (mod n)

n is known to the sender as well as the receiver. e is known to the sender and d only to the recipient. Thus, RSA has,
PuKey={e,n} and PrKey={d,n}

The algorithm may be summarized as follows:

The generation of key in the RSA algorithm is based on two very large prime numbers and their prime factors, and factorization is a hard problem to crack.

1. Let x and y, be the two large prime numbers
2. Let n be x × y
3. Let there be f(n) = (x − 1) × (y − 1)
4. Choose an integer e such that e ∈ (1,f(n)), and: gcd(e, f(n)) = 1, e and f(n) must be coprime
5. Calculate an integer d, so that d ≡ e −1 (mod f(n))

At the end of this algorithm, we have been able to generate two asymmetric keys to be used for encryption /decryption later: the first- a public key consisting of n and e, and the secondly, d and n comprise the private key. The keys may be written as:

PuKey = {e, n} and PrKey = {d, n}

Here, in this key generation process, x and y, the very large prime numbers used are usually atleast 512 bits, that makes n, 1024 bits (recall that, n = x × y). This amounts to adding complexity to the whole process and making the cryptanalysis process significantly tougher in terms of brute force attacks.

Now, that the (public, private) key pair is generated, encryption and decryption is done using the following formula:

Encryption: CT = PTe (mod n), where PT is the message in plaintext.
Decryption: PT = CTd (mod n), where CT is the ciphertext.

For encrypting a message, the sender is supposed to use the public key of the recipient, so that it is decrypted using the specific private key of the recipient. This makes a dictionary attack tougher to succeed by increasing the level of complexity of the encryption. RSA algorithm is used for the purpose of creating a digital signature, for the key exchange between the sender and the receiver for a session or for encrypting and decrypting the messages to be transmitted. The RSA algorithm gets its strength in security and reliability from its key generation process, as it is highly complex compared to the other cryptographic algorithms. (Stallings, 2005)

3.2.2 Diffie-Hellman

Diffie-Hellman is a public key cryptographic algorithm, that is used to securely exchange a secret key between two users. The secret key thus exchanged can later be used for encryption/ decryption of all messages exchanged between these two users. The Diffie-Hellman algorithm derives its strength from the difficulty of computing discrete logarithms.(Stallings, 2005)

The algorithm may be summarized as follows: (Source of this algorithm: (Forouzan, 2012))

Firstly, there are two publicly known numbers p and q, where, p is a large prime number of order 1024 bits. Whereas, q is a generator of order p-1

1. A randomly selects a large number x so that x ∈ [0, p-1] and calculates R1 = qx (mod p)

2. B randomly selects a large number y , so that, y ∈ [0, p-1] and calculates R2=qy (mod p).

3. A transmits R1 to B.

4. B transmits R2 to A.

5. A computes Key = (R2)x (mod p)

6. B computes Key = (R1)y (mod p)

Key = (qx (mod p))y (mod p) = (qy (mod p))x (mod p) = qxy (mod p)

Key is the secret key for the session. Both, A and B, have been able to compute the same value without y known to A and without x known to B.

The symmetric key shared between A and B using the Diffie-Hellman key exchange algorithm is qxy (mod p)

Now that we have seen and understood the working of the popular symmetric and asymmetric algorithms, let us see how these algorithms perform when used for encrypting data that is to be stored on the mobile cloud.(Sahu et al., 2022)

4. Role of Cryptosystems in Cloud Security

Data leakage or the data being compromised or being accessed by an unauthorised user, are the major security concerns of the users of cloud computing. To combat these fears, cryptography is used extensively as a solution. The commonly used symmetric key encryption/ decryption algorithms are AES, Blowfish and at times triple DES. Asymmetric-key algorithms in the security architecture of cloud computing are used to generate keys for encryption and decryption. The most commonly used asymmetric-key algorithms for key generation in cloud security are: RSA, IKE, Diffie-Helman Key Exchange.

The solution that comes to the rescue of the users of cloud computing, when they decide to store their data on the cloud is encryption. Everyone who wishes to store his/her data on the cloud, first encrypts that data using some symmetric key algorithm and then stores the data in encrypted form. So, the fear of the data being compromised is handled. In this solution the one problem that is faced is that, if the encrypted data needs to be processed while its stored on the cloud, then what can be done. For this, there are two solutions, first, we decrypt the data that is to be processed, then process it in its original form, and finally encrypt it again. In this case the consumer must give the private key to the server to decrypt the data prior to performing the desired calculations, which may compromise the confidentiality of the data stored in the Cloud. Here, the issue is that as soon as we decrypt the data for the purpose of processing it, the data immediately becomes vulnerable to attacks. Secondly, we have to bear the overheads of decrypting the data and then encrypting it again after processing, which is computationally exhaustive as well as expensive. This problem however, can be solved by using homomorphic encryption, which allows certain computations to be performed on encrypted data, so data need not be decrypted before processing it while it is in encrypted form and on the cloud.

4.1 **Homomorphic Encryption:** Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on ciphertext and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is a much required characteristic of modern communication system architectures. Homomorphic encryption allows the chaining together of different services without exposing the data to each of those services. Homomorphic Encryption systems are required to perform operations on encrypted data without decrypting it ,therefore no private key is needed; only the consumer will possess the secret key he used for the purpose of encryption. While decrypting the result of any operation that is performed on the encrypted data, we observe that the result is the same as if the operation was performed on the original unencrypted data.

The Homomorphic encryption is distinguishing, according to the operations that are performed on raw data.(Shakeeba Khan & Sakshi Deshmukh, 2014)

a) Additive Homomorphic encryption: additions of the raw data.
b) Multiplicative Homomorphic encryption: products for raw data.

5. Conclusion

While doing some operation on the stored data in classical cryptography, the time taken to compute is more as compared to the HE cryptosystem. Since in the case of classical cryptography, the ciphertext has to be decrypted first and then only the operation is possible, therefore the time of computation is high. Unlike classical cryptography, the HE cryptosystem allows the user to operate on the ciphertext itself which helps to reduce the computational time. In this work, the author has implemented classical RSA along with HE RSA and HE Pail Lier for doing multiplication or addition after encryption.

The result shows that the time for classical RSA is higher as compared to the other two. In this work, we have also discussed the importance of cryptography in cloud computing along with the disadvantage faced in classical cryptography which is being removed by applying the homomorphic cryptography. The computation time of RSA and Pallier HE cryptosystem depends upon the key size. If the key size is more, the computation time and cost will also increase severely.

Bibliography

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*, 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Forouzan, B. a. (2012). Cryptography and Network Security. In *Network and Application Security*. https://doi.org/10.1201/b11517-7

Kumar, R., Jitendra, S. ·, Sanjeev, A. ·, Narendra, S. ·, Chaudhari, S., & Shukla Editors, · K K. (n.d.). *Lecture Notes in Networks and Systems 100*. http://www.springer.com/series/15179

Masthan, K., & Venkatesh Sharma, K. (2019). Secured information sharing in mobile cloud computing using access controls. *International Journal of Innovative Technology and Exploring Engineering*, *8*(12), 1559–1564. https://doi.org/10.35940/ijitee.L3120.1081219

Sahu, M. I., Pandey, U. S., & Scholar, R. (2022). A SECURE SOLUTION FOR MOBILE CLOUD COMPUTING. *International Journal of Research and Analytical Reviews*. www.ijrar.org

Shakeeba Khan, M. S., & Sakshi Deshmukh, M. S. (2014). International Journal of Computer Science and Mobile Computing Security in Cloud Computing Using Cryptographic Algorithms. In *International Journal of Computer Science and Mobile Computing* (Vol. 3, Issue 9). www.ijcsmc.com

Stallings, W. (2005). Cryptography and Network Security: Principles and Practices. *Cryptography and Network Security*, 592. http://www.amazon.com/Cryptography-Network-Security-William-Stallings/dp/0131873164

Yan, Z., Deng, R. H., & Varadharajan, V. (2017). Cryptography and Data Security in Cloud Computing. In *Information Sciences* (Vol. 387, pp. 53–55). Elsevier Inc. https://doi.org/10.1016/j.ins.2016.12.034