Comparison of Cryptography Enhanced Encryption of Cloud Security

[1]Karthik. M, Assistant Professor, Dept. of Computer Science, DhanrajBaid Jain College, Chennai,India.karthikmohan2006@gmail.com

[2]Kanimozhi. S, M.Phil. Scholar, Dept. of Computer Science, DhanrajBaid Jain College,

Chennai,India.nevathasivakumar10@gmail.com

ABSTRACT:

Cryptography is critical and always for the integrity in addition to the safety of records which is to be stored within the cloud. Many cryptographic algorithms are to be had to resolve information security issue in cloud. Algorithms cover data from unauthorized users. Encryption algorithms have vital position in the information security of cloud computing. Examples algorithms are AES, DES, RSA, Homomorphic, and so on. Two operations carried out by using the examples of algorithms are encryption and decryption. Encryption is the method of converting records into scrambled form and decryption is the process of changing facts from scrambled shape to readable shape symmetric algorithms use one key for encryption and decryption at the same time as asymmetric algorithms use two keys for encryption and decryption at the same time as asymmetric algorithms use two keys for encryption and decryption. Security is an crucial aspect in cloud computing for making sure customers information is positioned on the relaxed mode within the cloud. The protection issues inclusive of confidentiality and integrity of cloud statistics in records safety are vital within the cloud. In this paper has discusses the various benefits of primary protection challenges of cloud computing, it additionally highlights the various cryptography encryption algorithms as the essential solution of security demanding situations. Moreover this paper has in comparison the performance of each algorithm in cloud cryptography.

Keywords:

Computing Technologies, Encryption Algorithms, Data Security, Cloud Computing, Cloud Cryptography.

1. INTRODUCTION:

Cloud computing is the quickest developing technology, offers diverse over to the internet. It can serve many centres to the enterprise including sources, infrastructure, platform and so forth, by means of paying amount on call for foundation over network with the functionality of growth or decrease the requirements. This technology can meet any IT necessities at any time. It can serve maximum of the hardware and software facilities required for groups for storing, developing, dealing with, strolling consumer software on cloud in lease or rent basis, it provides assets as a carrier to more than one clients by using virtualization. This technology facilitates many IT company inside the enterprise. It can serve facilities irrespective of the scale of the groups. These services gave new face to the computing technology. According to NIST, Cloud computing is a model for permitting handy, on-call for network get right of entry to a shared pool of configurable computing

assets that may be hastily provisioning and launched with minimum control effort or provider company interaction. Various cloud service companies are Amazon, Google, IBM, Microsoft, and Salesforce.Com, offer their cloud infrastructure for services. The security issues are numerous in cloud computing and at the web in fashionable, and numerous cryptography algorithms had been designed to protect the records not simplest at cloud stage but additionally on the packages stage on computers. Cryptography specifically refers to a specific technology wherein ciphers are designed especially circulate ciphers and block ciphers in addition to the hash capabilities. Encryption is a way in which the regular text is transformed to some secret textual content for the safety and integrity of the text.

2. BENEFITS OF CLOUD COMPUTING:

There are most important advantages offered by means of cloud computing there are explained below:

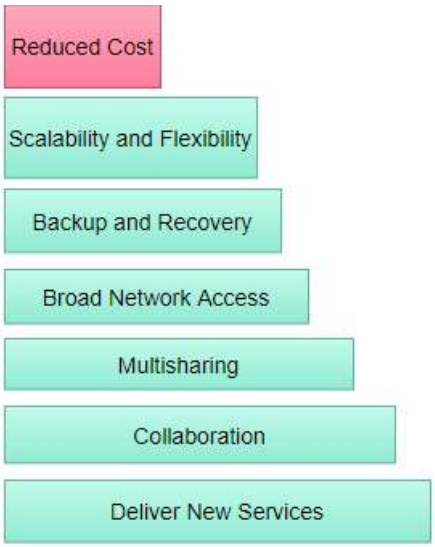

Fig: 1 Benefits of Cloud Computing

1. Reduced Cost:

Cloud computing provide facility to start an IT agency with much less attempt and preliminary price. Cloud computing offerings are shared through more than one purchasers within the global. It reduces the value of service because of big quantity consumers. Its charges amount relying upon using infrastructure, platform and different services, this allows consumers to lessen the cost by using specifying the extract requirements. Companies can without problems growth or decrease their enterprise market.

2. Scalability and Flexibility:

Cloud computing can assists agencies to start with small installation and grow to a big circumstance pretty swiftly, and then scale back if necessary. Also, the ability of cloud computing lets in corporations to apply greater sources at top times, permitting them to fulfil consumer demands. Moreover cloud computing is ready to satisfy any peak time requirement by putting in place with excessive potential servers, storages and so forth., this facility enables consumers to fulfil any sort of requirements irrespective of the size of the venture.

3. Backup and Recovery:

Since all the information is stored in the cloud, backing it up and restoring the identical is noticeably plenty simpler than storing the same on a physical device. Also has many strategies to recover it from any kind of disaster; best and new strategies are adopting by most cloud provider vendors to fulfil any form of disaster. Cloud carriers can get any type of technical and other guide very speedy than any in my view set up corporations regardless of their geographical limitations.

4. Broad Network Access:

Cloud offerings are delivered through open community, it is able to be accessible at any time everywhere inside the world. These facilities can be accessed by way of diverse devices including cell phones, laptops, PDAs, and so on., with distinctive systems. Consumers can access their files and other packages whenever from everywhere via the use of their mobiles. This has accelerated the price of adopting cloud computing era.

5. Multisharing:

Cloud computing offers offerings with the aid of sharing of architectures and other packages over internet for unmarried and more than one customer by means of virtualization and multi-tendency. With the cloud running in a dispensing and shared mode, a couple of users and packages can work extra efficiently with price of discounts by way of sharing commonplace infrastructure.

6. Collaboration:

Major tasks or programs are turning in via the effort of a couple of organization of humans operating together. Cloud computing offer a convenient way to work institution of human beings collectively on a not unusual mission or programs in an powerful way.

7. Deliver New Services:

Cloud offerings are supplied by using multi-national corporations like Amazon, Google, IBM, Microsoft, Salesforce.Com, etc., those companies can easily supply any new software/product at the release time itself.

3. CRYPTOGRAPHY

It is a technology used to comfy touchy statistics. Confidentially is the essential security service supplied by means of cryptography. Keeping statistics invisible to unauthorized users. Components of cryptosystem are follows:

Plain text: original form of information, information to be included during transmission and garage.

Cipher textual content: it's miles the unreadable form of the plaintext after encryption operation.

Encryption algorithm: used to transform plaintext to cipher textual content, it is mathematical manner.

Decryption set of rules: it performs opposite operation of encryption algorithm, convert cipher text to standard textual content.

Encryption key: it's far a fee used by sender with set of rules to convert plaintext to cipher text.

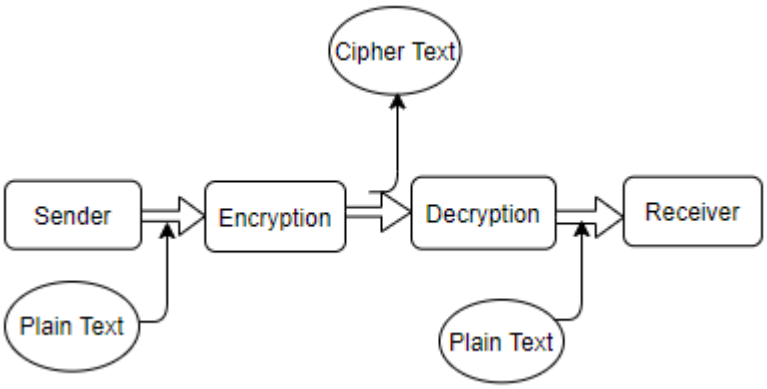

Fig:2 Cryptography Key Techniques

4. ENCRYPTION ALGORITHMS FOR CLOUD SECURITY

Encryption algorithms have vital role within the subject of cloud protection. Many algorithms are available for cloud security. Most beneficial algorithms for cloud safety are mentioned below:

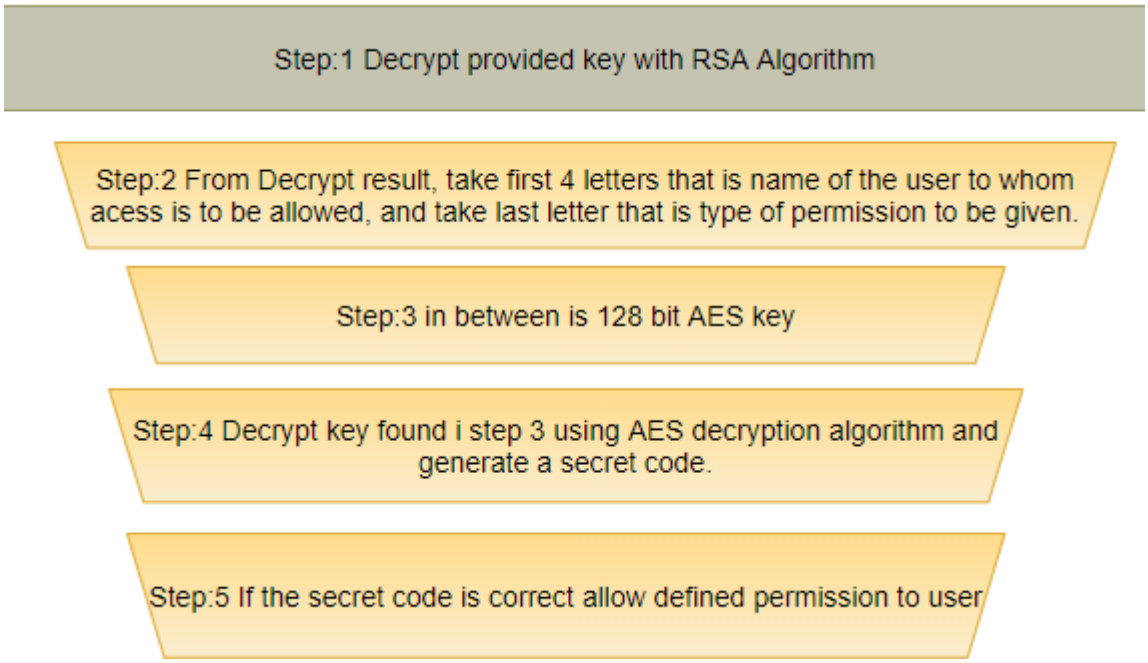

Fig:3 Encryption algorithms for cloud security

1. Data Encryption Standard (DES):

The records encryption popular (DES) is a symmetric key block cipher published through the national institute of requirements and generation (NIST). It users unmarried key

(secret key) for each encryption and decryption. It operates on sixty four-bit blocks of information with 56 bits key. The round key length is forty eight bits. Entire simple textual content is divide into blocks of 64bits length; last block is padded if essential. Multiple variations and substitutions are used for the duration of in order to boom the problem of acting a cryptoanalysis at the cipher. DES set of rules includes two permutations (P-boxes) and 16 Feistel rounds.

Entire operation can divided into 3 segments. First phase is preliminary permutation and last segment is the final variations.

1. Initial permutation rearranges the bits of sixty four-bits plain text. It isn't always using any keys, working in a predefined form.

2. There are sixteen feistel rounds in 2d segment. Each rounds makes use of a exclusive forty eight-bit spherical key applies to the apparent textual content bits to produce a 64-bit output, generated consistent with a pre-defined set of rules. The round key generator generates 16 48-bit keys out of a fifty six-bits cipher key.

3. Finally last segment preform final permutation, opposite operation of initial permutation and the outputs is 64-bit cipher text.

2. Advanced Encryption Standard (AES):

AES is a symmetric key block cipher posted by using the countrywide institute od standards and era (NIST). Most adopted symmetric encryption is AES. Its operates computations on bytes as an alternative bits, treats 128 bits of undeniable textual content block as sixteen bytes. These sixteen bytes are arranged in 4 columns and four rows for processing as a matrix. Its operates on whole statistics block by using using substitutions and permutations. The key used for an AES cipher specifies the number of transformation rounds used within the encryption manner.

Possible keys and variety of rounds are as following:

*10 rounds for 128-bit keys.

* 12 rounds for 192-bits keys.

* 14 rounds for 256-bits keys.

3. Rivest-Shamir-Adleman(RSA):

RSA is a public key cipher advanced through Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is most famous uneven key cryptography algorithm. This set of rules uses diverse information block length and diverse size keys. It has asymmetric keys for each encryption and decryption. It makes use of top numbers to generate the public and private keys. These two exceptional keys are used for encryption and decryption purpose. This set of rules may be widely labelled into three ranges; key generation by means of the usage of high numbers, encryption and decryption. RSA nowadays is used in masses of software products and can be key exchange, digital signatures, or encryption of small blocks of facts. This set of rules is mainly used for at ease conversation and authentication upon an open conversation channel.

While evaluating the overall performance of RSA set of rules with DES and RSA, when we use small values of P & Q (top numbers) are selected for the designing of key, then the encryption process turns into too vulnerable and one can be capable of decrypt the data via using random opportunity concept and facet channel attacks. On the alternative hand if big p & q lengths are selected then it consumes more time and the overall performance receives degraded in comparison with DES. Operation pace of RSA encryption algorithms is sluggish evaluate to symmetric algorithms, moreover it isn't always relaxed than DES.

4. Homomorphic Algorithm:

It is an encryption set of rules that offer high-quality computation facility over encrypted facts (cipher text) and return encrypted result. This algorithm can clear up many problems associated with security and confidentiality issues. In this algorithm encryption and decryption taking location in consumer site and company site operates upon encrypted statistics. This can solve chance even as transferring facts between purchaser and carrier provider, it cover plaintext from provider issuer, operates upon cipher textual content best. Homomorphic encryption allows complicated mathematical operations to be accomplished on encrypted statistics without the usage of the unique statistics. For plaintexts X1 and X2 and corresponding cipher textual content Y1 and Y2, a homomorphic encryption scheme permits the computation of X1 teta X2 form Y1 and Y2 without the use of P1 teta P2. The cryptosystem is multiplicative or additive homomorphic depending upon the operation teta which may be multiplication or addition.

5. ENCRYPTION TECHNIQUES APPLIED WITHIN CLOUD COMPUTING

Numerous encryption methods have been carried out within the cloud computing, and some of them are discussed here. Cryptography is the maximum not unusual approach by using which the users can get authenticated as well as the communique machine may additionally get authenticated.

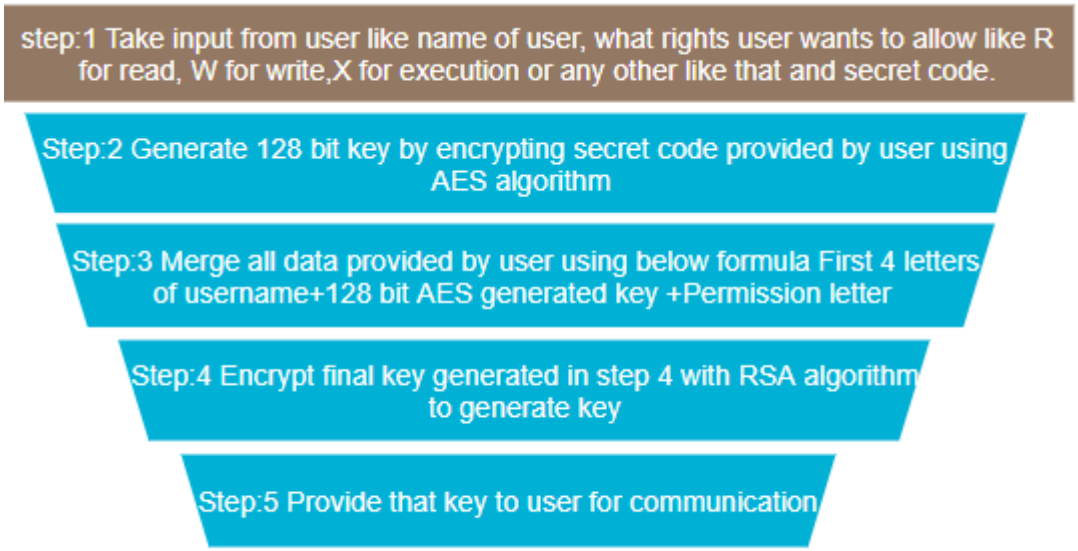

Fig:4 Encryption Technique with Cloud Computing

5.1 Identity Based Encryption:

This strategy particularly enables in certificate control and control of public key for the public key infrastructure. Outsourcing computation right here is put to the identity based totally encryption at the same time as the identical scheme for the server has also been proposed. The operation of the important thing generation is assigned to the key update cloud carrier company after which the omitted operations are quite simple. This scheme makes use of the general public key cryptography where the server of some third birthday celebration specifically makes use of the simple identifier like the e mail addresses for the technology of the public key that can then be beneficial in the decryption of the electronics messages. Such sort of encryption approach by massive reduce the complexity of even as encryption technique and case is furnished for in reality the administrator's and the users.

5.2 Attribute-Based Encryption (ABE):

In this sort of encryption, the maximum commonplace them is cipher textual content attribute based totally encryption. Some of the researches have additionally counselled a new characteristic primarily based encryption approach with the hierarchical name characteristic primarily based encryption. The brand new one is as compared via the researcher with the two previous forms of attribute-based totally encryption strategies which have been handiest cipher textual content and key policy.

User's personal key particularly guarantees get admission to policy for the algorithm. The primary distinction among the today's and antique attributed based totally encryptions techniques is that the vintage ones are particularly dependent on the access policy. In the key coverage attribute set after which gives the proprietor of the information the policy and key pair. The complete message then gets decrypted best if the attribute within cipher text particularly complies with the coverage of key access. The cipher text gets attached to the get entry to policy except getting decrypted with the attributes delight.

5.3 Fully Homomorphic Encryption:

This method ensures the security of the information used within the conversation or the garage or additionally which are used with the equipment similar with the traditional cryptography. This also adds some extra attributes of the computing at the encrypted statistics and the looking of the encrypted facts and extra. Big drawback connected with the conventional encrypted techniques is if the information is to be manipulated, so it requires getting coded first. The completely homomorphic encryption performs the computation with the encrypted information that's then despatched. For this, a few particular scheme became prepared where the calculations had been completed.

6. SECURITY ISSUES IN CLOUD COMPUTING:

Cloud computing can offer limitless computing sources on call for which reduces capital costs, improves accessibility, improve flexibility. Despite of its deserves, one of the maximum large barrier stopping companies from getting into the cloud is security. Security is a non-stop consideration in IT-related initiatives. There are numerous safety troubles for cloud computing as it encompasses many technology including networks, databases, operating systems, virtualization, assets scheduling, transaction management, load balancing, concurrency manage and reminiscence management.

For example: the interconnection the system by means of community in a cloud has to be relaxed. In addition, virtualization paradigm in cloud computing outcomes in several protection worries. Data security entails encryption the statistics and ensuring that suitable guidelines are enforced for records sharing.

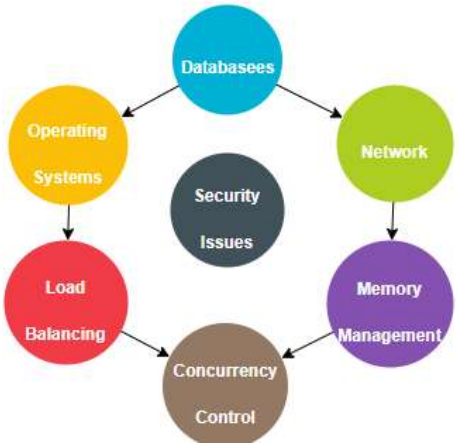

Fig:5 Security Issues in Cloud Computing

To preserve protection facts integrity, confidentiality, and availability audit manipulate are very critical so that any 1/3 person or intruder can't sniff into the message sent by means of parties. There are greater issues on those problems are as follows:

A. Data confidentiality:

Data confidentiality approach most effective approved person can get admission to the proprietor's data. A key thing of shielding statistics confidentiality would be that best the encryption. Encryption make sure right humans can examine the information.

B. Data integrity:

The cloud gadget integrity means to shield records from being modified with the aid of unauthorized events. Data integrity can be acquired by means of strategies inclusive of RAID like strategies and virtual signature.

C. Availability:

The goal availability for cloud computing systems is to ensure its uses will them at any time everywhere. As its net-native nature. Cloud structures lets in its users to permit it customers to access the system (e.g., applications, and offerings) from wherever.

D. Control:

Within the cloud gadget control means adjust using the system collectively with the programs, its infrastructure and the statistics.

E. Audit:

It intends to watch what occurred in the cloud framework. Audit potential might be covered as an extra layer within the virtualized operation framework facilitated on the virtualized gadget to offer centres looking what took place in the framework. It is notably extra at ease

than this is integrated with the programs or into the software themselves. Sine it's far able watch the whole get entry to period.

7. CONCLUSION AND FUTURE WORK:

Cloud information safety on the cloud would be the fundamental problem for all of the service carriers and data safety has many troubles like confidentiality, integrity, surveillance, reliability, availability, safety. The paper mentioned diverse cryptography strategies that may be used in cloud computing environment in order that the data may be securely shared with the authorized users by using adopting the cryptographic strategies.

The capacity of homomorphic algorithm to perform operations on encryption records permits high safety than different algorithms including RSA, DES, and AES. Future paintings is to enforce hardware or software program approach with homomorphic algorithm to offer safety on cloud from any sort of security attack.

REFERENCE:

[1] Analysis of diverse Encryption Algorithms in cloud Computing, Nasarul Islam K.V, Mohamed Riyas.K.V, IJCSMC, Vol.6, Issue. 7, July 2017, ISSN 2320-088X.

[2] Encryption strategies inside the cloud, Khalid Alshafee, Volume 7, Issue 7, July-2016, ISSN 2229-5518.

[3] Modern Encryption Techniques for cloud computing.

[4] Implementation of DNA Cryptography in cloud computing and using Huffman set of rules, Socket Programming and New Approach to at ease cloud statistics.

[5] Cryptography in cloud computing: A Basic Approach to ensure protection in cloud RishavChatterjee, Sharmistha Roy, Volume 7 Issue No.5, ISSN 2321 3361.