ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.3

A Survey on Data Security in CSP using Cryptographic Key

M. Anitha[1], K. Nandhini[2]
M. Phill Research Scholar[1], Assistant Professor[2]
PG and Research Department of Computer Science
Chikkanna Government Arts College Tirupur, Tamilnadu, India

Abstract:
Cloud Computing turned into the most predominant innovation in recent years. Cloud facilitates its users by providing virtual resources via internet. The amount of users using this technology has exploded. Therefore, cloud users expect more safe and security for their data. One can secure the data from being accessed illegally by encrypting it with a key with various methods of Advanced and data encryption standard. Cryptography is basic for the security and honesty of the information that is put away in the cloud. A few cryptographic techniques are utilized to ensure the respectability of information for different applications. A specific security strategy makes utilization of various cryptographic strategies to encode information and make it into an un-meaningful structure, which would then be able to be decoded just with the assistance of a key. Cryptographic systems are fundamental for the classification of the information spared. For this reason this paper give a survey on different cryptographic system utilized for the encryption technique for giving security by putting away the encoded information in the cloud.

Keywords: Cloud Computing, Security, Cryptographic, Symmetric, Asymmetric

I. INTRODUCTION

Cloud computing gives a common pool of assets, including information storage room, systems, PC preparing power. The cloud is a virtualization of assets that keep up and oversees itself [1]. Cloud computing is Pay per-Use-On-Demand display that can helpfully get to shared IT assets through the Internet Where the IT assets incorporate long range informal communication destinations, webmail, online business applications and system Services. Cloud Service Provider (CSP) can improve the accessibility of IT assets and along these lines give in this manner give the possibility to cost decrease through advanced and productive figuring. Cloud additionally incorporates the significant hazard, for example, security, information respectability, organize reliance and centralization. As the security isn't given in cloud numerous organizations receive their one of a kind security structure [2]. Security is the central point of any advancement amid which unapproved gatecrasher can't get to your record or information in the cloud. The Cloud Security Alliance is a non-benefit association shaped to advance the utilization of best practices for giving security confirmation inside distributed computing. In fig.1 its shows the architectural principles which constitute cloud computing data storage devices. It describes a cloud data storage environment where user can store the data on cloud.

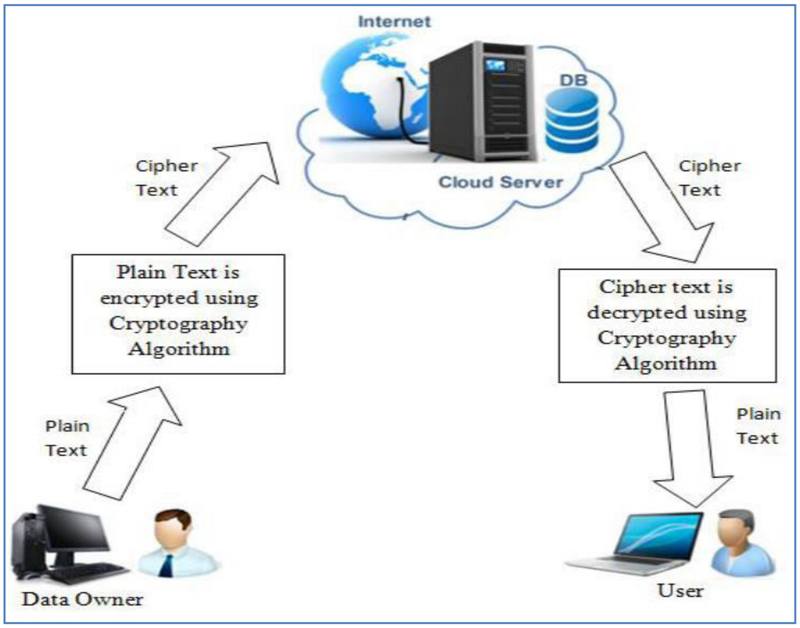
Internet
DB
Cloud Server
Cipher Text
Cipher Text
Plain Text is encrypted using Cryptography Algorithm
Cipher text is decrypted using Cryptography Algorithm
Plain Text
Plain Text
Data Owner
User

Figure.1.Cloud architecture for data storage

As increasingly more data on people and organizations is put in the cloud, concerns are starting to develop about exactly how safe a domain it is. With such a lot of our outstanding task at hand moving to the cloud, security in Cloud computing is under extended examination [3]. With the extending reputation of distributed storage, the threats for security, information joining, and protection of information is positively growing. In like manner, the cloud supplier must consider the security and protection as the testing factors for information sharing viability [4]. Cloud Service provider is managing the customer information. For the security of information protection, delicate information must be scrambled before re-appropriating, which makes viable information usage a testing errand. Utilizing the encryption strategies for the security in the Cloud computing is vital. In this examination, the investigation of various encryption methods which are being used in Cloud computing security will be performed. Numerous security strategies for cloud utilize different cryptographic systems. Cryptographic systems have turned out to be fundamental for security in cloud. A key is utilized for information encryption and unscrambling [5]. This aide in ensuring privacy and respectability of information. It guarantees security of information being partaken in cloud and furthermore enables information to be put away safely. Cryptography alludes to the investigation of planning figures. Encryption alludes to the technique for changing over plain content to mystery content (figure content) which must be persued by proprietor of mystery key. At present different cryptographic algorithms were utilized for giving security to the cloud. Cryptography for the most part alludes to an alternate science in which figures are planned especially stream figures and block figures just as the hash capacities. Encryption is a procedure in which the customary content is changed over to some mystery content for the assurance and uprightness of the content. Predominantly two classes of the encryption algorithms are there symmetric algorithms and asymmetric algorithms.

II. LITERATURE REVIEW

Khalid Alshafee ("Encryption Techniques in the Cloud", IJSER Volume 7, Issue 7, July 2016. [7] Cryptography is basic and fundamentally for the uprightness just as the security of information which is to be put away in the cloud. Here are various cryptographic techniques connected for this reason on some cloud which predominantly secures the information just as the applications on the cloud air. Explicit security method doesn't essentially utilize single encryption plot rather it makes utilization of various encryption plans for the encryption of the information and convert the information to garbled configuration and later on decoded utilizing some extraordinary key. Various encryption systems at this point are accessible for the security of the information in the different applications. The cryptographic plans are viewed as fundamental for the information privacy that is spared over the cloud. Cloud computing share the assets, for example, programming, administrations, stage, and foundation. So utilizing the cryptographic procedures inside the cloud will guarantee the information security and uprightness which is generally required in cloud climate. In this examination, distinctive encryption systems utilized in the cloud condition are dissected to discover which is most appropriate in what limit. Debasis Das "Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi-Party Computation", 2018 IEEE. [8] Cloud figuring is a creating innovation that is yet hazy to numerous security issues. Information in the untrusted mists can be scrambled utilizing encryption calculation. Randomizing this information gives greater security which can be accomplished by cushioning idea in the cloud. In this paper, the client's information is encoded utilizing cushioning plan, called Optimal Asymmetric Encryption Padding (OAEP) together with Hybrid Encryption algorithms that depends on RSA (i.e., HE-RSA), so as to enable various gatherings to figure a capacity on their sources of info while protecting Integrity and Confidentiality.The Homomorphic Encryption(HE) is performed on encoded information without decoding it in computationally ground-breaking mists and the Secure Multi-Party Computation (SMPC) can be utilized in the cloud to guarantee security and protection of the clients. In this paper, we have proposed a plan that incorporates the multi-party algorithms with homomorphic encryption to permit figurings of encoded information without decoding. The cryptographic procedures utilized in our cloud show are portrayed and the overheads are contrasted and Homomorphic Encryption and Multi-Party Computation. Abdelkader Moumen and HocineSissaoui("Images encryption method using steganographic LSB method, AES and RSA algorithm." *Nonlinear Engineering* 6, vol no. 1 (2017) [9] Vulnerability of correspondence of computerized pictures is a critical issue these days, especially when the pictures are imparted through uncertain channels.to improve correspondence security, numerous cryptosystems have been exhibited in the picture encryption writing. This paper proposes a novel picture encryption procedure dependent on aalgorithms that is quicker than current strategies. The proposed algorithms dispenses with the progression in which the discharge key is shared amid the encryption procedure. It is figured dependent on the symmetric encryption, lopsided encryption and steganography speculations. The picture is scrambled utilizing a symmetric calculation, at that point, the mystery key is encoded by methods for a topsy-turvy algorithms and it is covered up in the figured picture utilizing a least critical bits steganographic plot. The investigation results demonstrate that while getting a charge out of the quicker calculation, our technique performs near ideal as far as precision. Rui Zhang, RuiXue "Searchable Encryption for Healthcare Clouds: A Survey", DOI 10.1109/ TSC. 2017. 276 2296, IEEE. [10] Healthcare cloud applications need accessible encryption with the accompanying two abilities for securing information protection and access security: (1) the human services suppliers need to impart the scrambled information to approved clients and empower questioning over encoded information, and (2) they likewise need to keep the inquiry catchphrases and related pursuit activities private to such an extent that social insurance information facilitating specialist co-ops can't access unapproved substance or follow and deduce touchy information put away in the medicinal services cloud. This review paper depicts the idea of accessible encryption (SE) with regards to social insurance applications and portrays the SE use cases into four situations in medicinal services. At that point we give an extensive outline of the four agent SE methods: Thus, we are agreeable to mechanical review of the condition of craftsmanship accessible encryption models and the hidden key procedures, rather than itemized verifications and developments of the individual SE algorithms . We portray how the current SE plans identify with and vary from each other, and call attention to the associations between the SE systems and the security and protection prerequisites of social insurance applications and the open research issues.

III CRYPTOGRAPHIC KEY TECHNIQUES:

Cryptography mainly refers to a different science in which ciphers are designed particularly stream ciphers and block ciphers as well as the hash functions. Cryptography method i) Plaintext is the first message before being changed, ii) Cipher content is the yield of an encryption procedure for example encoded content or message in its coded comprehensible structure. iii) Encryption calculation: An encryption algorithms changes the plaintext into figure content. The sender utilizes an encryption calculation. iv) Decryption calculation: A decoding algorithms changes the figure message once more into plaintext. The recipient utilizes decoding algorithmsv) Key: A key is a number (or set of numbers) that the figure, as a calculation, works on it [11].Cryptography is an art which hides the information from unauthorized users over the network. It works with the following components:

***Plain text:** Its original file that needs to be sent over the network.

***Cipher text:** It is the unreadable form of original file that is converted into unreadable form.

***Encryption:** It converts the original file (plain text) into unreadable file (Cipher text) as shown in fig3.1.

***Decryption:** It converts the unreadable file(Cipher Text)into readable file(plain text) as shown in fig 3.2

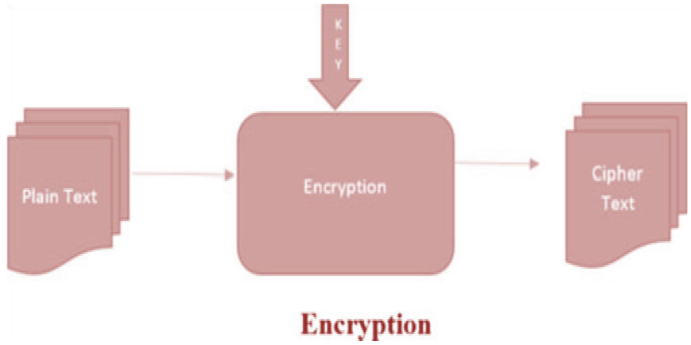

Figure.3.1 Encryption

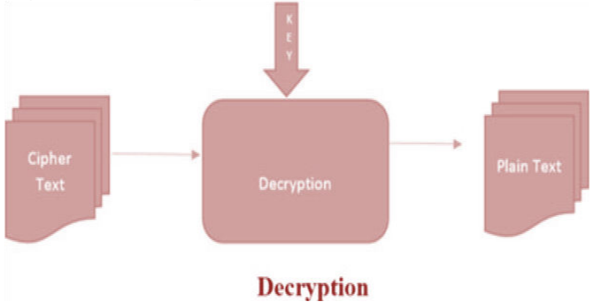

Figure.3.2 Decryption

In Cryptography,there are two types of key-based encryption
a). Symmetric(or secret key) as shown in fig 3.3.
b).Asymmetric(or public key) as shown in fig 3.4.

a)Symmetric KeyAlgorithms:
Symmetric utilizations uses a single key, which works for both encryption and decryption. The symmetric frameworks give a two channel framework to their clients. It guarantees confirmation and approval. Symmetric-key algorithms are those algorithms which utilizes a single key for both encryption and decryption[11]. The key is kept as confidential. Symmetric algorithms have the benefit of not taking in a lot of algorithms power and it works with fast in encryption. Symmetric-key algorithms are partitioned into two kinds: Block figure and Stream figure. In bock figure input is taken as a block of plaintext of fixed size contingent upon the kind of symmetric encryption calculation, key of fixed size is connected on to block of plain content and after that the yield block of indistinguishable size from the block of plaintext is gotten. In Case of stream figure one piece is scrambled at a specific time.

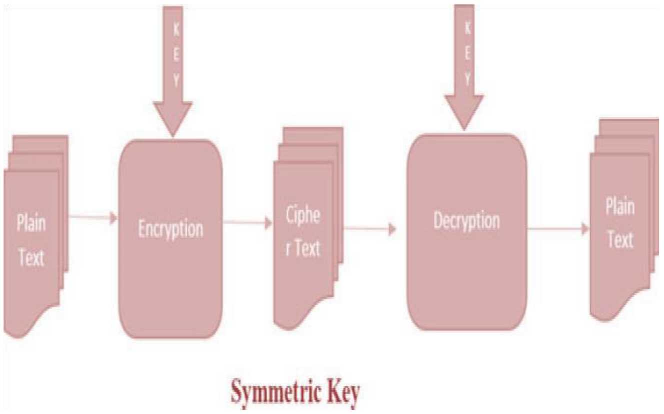

Figure.3.3 Symmetric Key

b)Asymmetric KeyAlgorithms:
It is relatively a new concept unlike symmetric cryptosystem. Different keys are used for encryption and decryption. This is a property which set this plan not the same as symmetric encryption plot. Every recipient has its very own unscrambling key, by and large alluded to as his private key [12]. Beneficiary needs to create an encryption key, alluded to as his open key. By and large, this kind of cryptosystem includes confided in outsider which formally pronounces that a specific open key has a place with a particular individual or substance as it were.

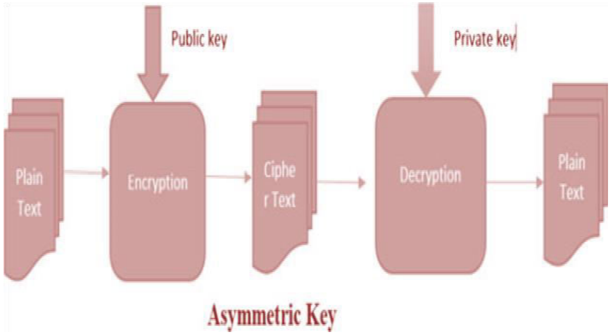

Figure.3.4 Asymmetric Key.

IV. RESULT DISCUSSION:

In the Cryptosystem, algorithms are considered secure if an attacker cannot determine any properties of the plaintext or key, given the ciphertext. An attacker should not be able to determine anything about a key given a large number of plaintext/cipher text combinations which used the key.

a. Advanced Encryption Standard (AES)
In cryptography, the Advanced Encryption Standard is type of symmetric-key encryption algorithm. AES is a block figure with

a block length of 128 bits. It grants three unmistakable key lengths: 128, 192, or 256 bits. Here propose AES with 128 pieces key length. AES algorithms guarantee that the hash code is encoded in a safe way. The encryption strategy involves 10 rounds of dealing with for 128-piece keys. Except for the last round for every circumstance, each and every other round is indistinct. Its algorithms is as per the following: Key Expansion, Initial Round - Round Keys are included. Rounds, Sub Bytes—a non-uniform substitution step where every bite is substituted with another as per a table [13, 14]. Lines are moved—a transposition step where each line of the state is moved consistently a specific number of steps. Sections are blended—a blending task which works on the segments of the state, joining the four bytes in every segment 8. Include Round Key every byte of that specific state is joined with the round key; each round key is gotten from the given figure key utilizing a key timetable. Last Round, Sub Bytes, Shift Rows, Add Round Key.

b. Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a block figure and goes under symmetric key cryptography. found in January 1977 by the National Institute of Standards and Technology, named as NIST. At the encryption site, DES just takes a 64-bit plaintext and makes a 64-bit figure content, at the decoding procedure, it takes a 64-bit figure message and makes a 64-bit plaintext, and same 56 bit figure key is utilized for both encryption and unscrambling. The encryption procedure is made utilizing two changes (P-boxes), which we call introductory and last stage, and sixteen Fiestel rounds. Each round utilizations an alternate kind of 48-bit round key which is created from the figure key as per a predefined algorithms [15].

c. Triple DES

Triple DES ended up being unreasonably moderate for proficiency as the DES algorithms was created for mid-1970's equipment and did not deliver proficient and compelling programming code. Triple DES has three fold the number of rounds as DES and is correspondingly slower. The execution evaluation shows that Triple DES cryptography can be used for data security. Moreover, concede algorithms of data encryption exhibits that greater size of data fabricates the data defer time for encoding data. Triple DES estimation, it is dynamically secure to take a gander at other symmetric key computations, and produce best result for less planning time and modifies. Triple Data Encryption Standard, or 3DES, is a present standard, and it is a block figure. It resembles the more settled system for encryption, Data Encryption Standard, which uses 56-bit keys. In any case, 3DES is a symmetric-key encryption that uses three individual 56-bit keys. It scrambles data on various occasions, which implies your 56-bit key transforms into a 168-piece key. Amazingly, since it encodes data on numerous occasions, this system is much slower than others [16]. In like manner, in light of the fact that 3DES uses shorter block lengths, it is less requesting to unscramble and spill data. Regardless, various money related associations and associations in different diverse undertakings use this encryption technique to keep information checks

d. Rivest Shamir Adleman (RSA)

RSA algorithm includes two keys named as open and private. The public key is utilized for encryption process and the private key is utilized for decryption. Both the keys utilize the same figured 'N' esteem. The RSA algorithm is lavishly used to encode the information to furnish security all together that solitary the fitting customer can get to it. The most broadly used Public Key technique is known as the RSA. The RSA addresses in a general sense an unequal encryption/decoding system. The Public key passed on to all of the clients through which they are talented to encode the message and private key which is used with the true objective of decoding is kept characterized and isn't uncovered to all. To upgrade the security level the proposed system uses another encryption algorithms after the RSA encryption [17]. The found out k esteems included prime numbers as opposed to Random Numbers as in High Speed and Secure RSA calculation.

e. Digital Signature Algorithm

The DSA by and large alludes to the Digital Signature Algorithm. The DSA wind up planned as an encryption calculation. The DSA was progressed by the NSA to be used by the United States government as a standard for virtual marks. RSA, then again, appears at the issue of calculating numbers as the essential issue of its improvement. The name DSA illuminates its overwhelming trademark. This is programming that is particularly developed for marking, and thusly it is entirely renowned with virtual marks. This is because of the reality DSA produces the keys immediately. At the point when quicker encryption is required, RSA is favored on the grounds that it scrambles each message and mark for marking in. At the point when needing decoding, DSA is quicker especially in light of reality that it's miles particular for a solitary capacity most straightforward. There is a couple of "bother" in utilizing additional than-1024-piece DSA. Every client has a private and open key pair [18, 19]. Open keys are thought to be known to people in general when all is said in done. Private keys are never shared. Anybody can confirm the mark of a client by utilizing that client open key. Just the owner of the client private key can perform signature age. A hash work is utilized in the mark age procedure to acquire a consolidated rendition of information, called a message digest. The message digest is then contribution to the advanced mark algorithms to produce the computerized mark. The advanced mark is sent to the proposed verifier alongside the message. The verifier of the message and mark confirms the mark by utilizing the sender's open key.

VII CONCLUSION:

Privacy and integrity of data in information security are fundamental in the cloud. Security of information is of outrageous need in this present time and cryptography assumes a noteworthy job in cloud condition. Cloud computing is utilized to share asset as administration, programming as administration, foundation as administration, stage as administration to the customers. The utilization of cryptography is vital for the upkeep of security in the cloud. This paper gives a relative investigation of the few cryptographic procedures used in the security to process the cloud security. There are numerous cryptographic procedures that have been being used for security in the cloud. This article audits a portion of the methods that have been utilized in the cloud condition which in AES, DES, Triple DES, RSA and DSA. From the best of our insight AES assumes a noteworthy job for giving security to the cloud information and furthermore DSA give a quicker component to cryptographic technique.

VIII. REFERENCE

[1]. Qian Wang, Cong Wang, KuiRen, Wenjing Lou, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services‖, IEEE Network, 2010.

[2]. Siani Pearson and AzzedineBenameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in 2nd IEEE International Conference on Cloud Computing Technology and Science, USA, 2010.

[3]. Cong Wang, Qian Wang, and KuiRen, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", Department of ECE, Cong Wang, Illinois Institute of Technology.

[4]. RohitBhore and Dr. Rahila Sheikh"Secure Data Storage Scheme Using Cryptographic Techniques in Cloud Computing", IJCSN, Volume 5, Issue 1, February 2016

[5]. Krunal Suthar, P. K. H. G. a. H. P., 2012. "Analytical Comparison of Symmetric Encryption and Encoding Techniques for Cloud Environment". International Journal of Computer Applications, pp. 16-19.

[6]. Kaur, S., 2012. "Cryptography and Encryption In Cloud Computing". s.l., s.n., pp. 242-249.

[7]. Khalid Alshafee,"Encryption Techniques in the Cloud", IJSE.R Volume 7, Issue 7, July 2016.

[8]. Debasis Das, "Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi-Party Computation", 2018 IEEE.

[9]. Moumen, Abdelkader, HocineSissaoui. "Images encryption method using steganographic LSB method, AES and RSA algorithm." *Nonlinear Engineering* 6, no. 1 (2017): 53-59.

[10]. Rui Zhang, RuiXue, et al, "Searchable Encryption for Healthcare Clouds: A Survey", DOI 10.1109/ TSC. 2017.27 62296, IEEE.

[11]. Yogesh Kumar, Rajiv Munjal, Harsh Sharma, Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", International Journal of Computer Science and Management Studies, ISSN: 2231-5268.

[12]. https://techdifferences.com/difference-between-symmetric-and-asymmetric-encryption.html

[13]. Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography by M.Sudha , M.Monica Advances in Computer Science and its Applications 32 Vol. 1, No.1, March 2012 Copyright ©World Science Publisher, United States.

[14]. Dr. Prerna Mahajan &AbhishekSachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013

[15]. Aman Kumar, Dr. SudeshJakhar, Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[16]. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, ISSN 2151-9617.

[17]. SatishN .chalurkari ,Nileshkhochare ,B.B. mashram, "Survey on Modular Attack on RSA Algorithm", International Journal of Computational Engineering & Management, ISSN: 2230- 7893.

[18]. MohitMarwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, EISSN 0976-3945.

[19]. Swati Chaudhaary, "Secure Data Communication in Cloud Computing using Proposed DSA", IJARCCE, Vol. 4, Issue 8, August 2015.