International Journal of Research in Advent Technology, Special Issue, NCRCEST 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Information Security in Cloud Computing: A Survey

A. Arulprakash[1], Dr. R. Viswanathan[2], Dr.R.Anandan[3]
Research Scholar[1], Professor[2],Professor[3].
[1,2]Galgotias University, Greater Noida, [3]Vels University, Chennai.
prakash875@gmail.com,rvnathan06@gmail.com, anandan.se@velsuniv.ac.in

Abstract: Cloud computing is gathering of services for system storage, hardware and networking, these kinds of services are given to client. Cloud storage is effectively getting to anyplace whenever of the information since cloud is work in remote area. It utilizes the capacity benefit given by the cloud supplier. Information isn't anchor in the cloud on the grounds that the unapproved client can attempt to utilization of the private information. So, giving the information security it utilizes the distinctive encryption strategy to ensure the information. So that in the proposed system it uses the staggered encryption algorithm. In the staggered encryption it consolidates two distinct algorithms for giving the better security.

Keywords: Cloud computing, Encryption Algorithms, Information security.

1. INTRODUCTION

The cloud definition given by National Institute of standard and Technology (NIST) says that: "Cloud computing could be a model for empowering advantageous on interest arrange access to a typical pool of configurable computing resources" (e.g. networks, servers, storage application and services) that is immediately provisioned and released with least administration exertion or service provider interaction. [1]. within the cloud computing there's no have to store information within the desktop or mounted location pc. you'll be able to store the information in an exceedingly server and you'll be able to access the information in any remote location using of the web topology. Cloud computing provides an oversized quantity of information is simply stored within the cloud. the benefits of victimisation cloud computing are: i) reduce hardware and maintenance cost ii) accessibility round the globe iii) flexibility and extremely automated process. Characteristics of Cloud Computing.

Ultra large scale: In the cloud computing there are numerous organizations utilizes cloud server. Google has possessed more than one million servers. Indeed, even in Amazon, IBM, Microsoft, Yahoo, they have more than several thousand servers. So, the size of cloud is huge [2].

Virtualization: Cloud figuring gives client to go anyplace, through any sort of terminal. Clients can accomplish or share it securely through a simple way, whenever, anyplace. [3].

High dependability: Cloud utilizes information multitranscript blame tolerant, the algorithm hub isomorphism replaceable, etc to guarantee the high unwavering quality of the administration. Utilizing cloud computing is more solid than nearby PC.

Versatility: Cloud computing will manufacture numerous applications supported by cloud, and one cloud will support completely different applications running it at an equivalent time.

High extendibility: The size of cloud will extend dynamically to fulfil the progressively demand.

On demand service: Cloud might be a monstrous asset pool that you essentially can buy per your need; cloud is just similar to running water, electric, and gas that might be charged by the number that you basically utilized.

Cloud computing provides the various services. All these services place into the 3 models:
Software as service (Saas),
Platform as service (Paas)
Infrastructure as service (Iaas).

Software as a Service (SaaS): In SaaS model, it performs application package. User will access databases and application software's on demand or want of users.

Platform as a Service (PaaS): In PaaS models, computing platform like internet server, package, information and therefore the background for artificial language execution is provided by the service suppliers.

Infrastructure as a Service (IaaS): in step with IETF (Internet Engineering Task Force), computers or virtual machines, computing power and alternative physical resources like space for storing square measure provided on demand by the IaaS suppliers

Cryptography is procedure connected for encryption and decoding. Encryption implies the plain text is converted into the cipher text or some coded structure utilizing of the diverse encryption algorithm. With the end goal of information security and decoding is inverse of encryption. In the decryption the ciphertext is converted into the plain text r unique text utilizing the decoding algorithm. Ordinary cryptography is additionally alluded as symmetric encryption or single key encryption. Same key is utilized for encryption and decryption. Public key cryptography is indicated as unbalanced encryption or public key encryption. Separate keys are used for encryption and decoding. The encryption procedure comprises of aalgorithm and a key. The key is an esteem free on the particular of the plain text. The algorithm will deliver an alternate yield contingent upon the particular key being applied around then. Changing the key changes, the yield of the algorithm. When the ciphertext is created, it might be transmitted to distributed storage. Upon gathering, the ciphertext can be changed back to the first plaintext by utilizing a decryption algorithm with a similar key that was utilized in encryption [4].

In spite of that cloud computing specialist organizations depict the security and unwavering quality of their administrations, yet real there are various security issues are made in distributed computing administrations. The administration isn't as protected and solid as they guarantee. In 2009, the real distributed computing sellers progressively seemed a few mishaps. Amazon's Simple Storage Service was intruded on twice in February and July 2009. This incident realized some framework regions relying upon a single kind of limit organization were constrained to a stop. In March 2009, security vulnerabilities in Google Docs even provoked authentic spillage of customer private information. Google Gmail also showed up an overall dissatisfaction up to 4 hours.It was revealed that there was dead serious security weakness in VMware virtualization programming for Mac structure in May 2009. People with ulterior points of view can abuse the defencelessness in the Windows virtual machine on the host Mac to execute poisonous code. Microsoft's Azure disseminated processing stage moreover happened an authentic power outage disaster for around 22 hours. Genuine security episodes even lead to fall of distributed computing merchants. As executives' abuse prompting loss of 45% client information.

Presently information in the cloud isn't sheltered and secure in light of the fact that some outside substances are consistently visited to the cloud for hacking the information. To give a security on specific information we use encryption/cryptography strategy. There is diverse algorithm as of now exits however in this paper one more idea two distinctive algorithm that are consolidate or joining each other for giving the better security. At the point when just a single algorithm is utilized for giving information security it gives less security. However, more than one algorithm that are connecting with one another then it works effective way and furthermore give the better security as contrast with the single algorithm. In this paper it uses to unexpected algorithm in comparison to are joining to one another one is symmetric block cipher and another is uneven block cipher. Symmetric block cipher is utilizing just a single key for encryption and asymmetric block cipher utilizes the private key just as public key for encryption and decoding. Two algorithms that are consolidating each other are called as Hybrid encryption.

2. LITERATURE SURVEY

To verify the cloud security objectives of the information, incorporate three points in particular. Confidentiality, Integrity and availability (CIA). Encryption is used two sorts of calculation symmetric and asymmetric algorithm. In the symmetric algorithm it uses private key for encryption and a comparable key is used for decryption. Additionally, deviated it uses overall population key for encryption and private key is appropriated to all using of the private key decode the data. [6].

Data Encryption standard: DES is a block cipher. It utilizes the 56-bit key and 64-bitblocks. DES has a perplexing arrangement of tenets and information. It has quick equipment executions and moderate programming implementations.DES takes 64-bit plain text and makes 64-bitciphertext at decryption side. It utilizes two permutation starting permutation and last permutation and 16 Feistel rounds. Each round utilization distinctive 48-bit round key [4].

Advanced Encryption Standard: Advanced Encryption Standard (AES) is symmetric key block cipher.AES is non Feistel cipher.AES encoding information with block size 128 piece. It utilizes 10, 12, or 14 rounds. The key size might be utilized in the AES 128,192 or 256 bits. AES works 4*4 segments matrix is called as state.

Triple-DES (3DES): It utilizes three 56-bit keys and performs three encryption/decryption disregards the block.

DESX: In DESX it joining 64 extra key bits to the plaintext before encryption, adequately builds the key length to 120 bits.

Rivets Ciphers: Named for Ron Rivets, it utilizes the diverse algorithms.

RC2: A 64-bit block cipher utilizing variable-sized keys intended to supplant DES. The key size was restricted to 40 bits.

RC4: A stream cipher utilizing variable-sized keys.

RC5: A block cipher supporting an assortment of block sizes (32, 64, or 128 bits), key sizes, and number of encryptions ignores the information.

Blowfish: A symmetric 64-bit block cipher imagined by Bruce Schneider; improved for 32-bit processors with expansive information stores, it is essentially quicker than DES on a Pentium/PowerPC-class machine. Key lengths can shift from 32 to 448 bits long. Blowfish, accessible uninhibitedly and proposed as a substitute for DES or IDEA, is being used in countless.

RSA: RSA is Asymmetric encryption algorithm it implies that public key is conveyed to just for encryption and private key is utilized to decoding. The key size is 1024 bits. In the RSA secluded exponential is utilized for encryption and decoding. It utilizes two examples a and b where a is public key and b is private key.

Elliptic curve cryptography: The ECC is the general population key cryptography it depends on logarithmic structure over limited fields. Key length of the ECC is 135 piece and square size is variations not fixed size of square is utilized. The primary preferred standpoint of ECC is littler key size diminishing stockpiling and transmission necessities [5].

3. PROPOSED STUDY

In cloud computing information security is most essential factor to shield the information from some outside substances is the testing errand because of this assignment. It utilizes the diverse encryption algorithm there is symmetric and asymmetric strategy is utilized for scramble and decode information. In symmetric private key is utilized for encryption and same key is utilized for decoding however primary problem is keeping up the key is troublesome assignment savage power assault can be happening.

In asymmetric encryption it utilizes two distinctive key public key and private key. utilizing of the private key it scrambles the information and public key is conveyed to all the collector then the utilizing of people in general key it unscrambles the information. In this instrument may likewise brute force attack or the issue of keeping up the key.

when it utilizes single for the encryption it not gives the better security but rather when two algorithms are consolidating to one another at that point joining algorithm give better security contrasting with single algorithm. In proposed examine the two unique algorithms that are utilizes DES and RSA. The DES is a symmetric encryption algorithm that utilizes just a single key for both and RSA is an uneven encryption it utilizes two asymmetric keys, for example, private key and public key utilizing of private key it scrambles the information and public key it decodes the information. However, when just a single DES algorithm is utilized for information encryption it give less security or it likewise RSA is utilized it give less security. In any case, when we utilize the two algorithms that are consolidate or join each other then it gives a superior security. We utilize a staggered encryption in the staggered encryption the first run through the plain text is encoded utilizing the DES algorithm then the DES produce the yield as a first-dimension encryption. In the wake of applying the RSA then it produces the yield as a second dimension.

TABLE I. Comparison between various algorithms

Algorithm	Block Size(Bits)	Key size (Bits)	Speed	Security
DES	64	56	Low	Less
3DES	128	112,168	Low	Less
RC2	64	8-128	Fast	High
RC6	128	128,192	Fast	Secure
AES	128	128,192, 256	Fast	More Secure
BLOW FISH	64	32-448	Fast	More Secure
RSA	86	214	Fast	More Secure

There are various existing systems used to actualize security in cloud storage. A portion of the current encryption algorithms which were actualized as pursues;

A. Data Encryption Standard (DES) Algorithm: DES [6] is a symmetric-key block cipher disseminated as FIPS-46 in the Federal Register in the year 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES taken a 64-bit plaintext and makes a 64-bit ciphertext, at the decoding site, it takes a 64-bit cipher message and creates a 64-bit plaintext, and same 56-bitcipher key is utilized for both encryption and decryption. The encryption procedure is made of two changes (P-boxes), which we call introductory and last stage and sixteen Feistel rounds [7]. Each round takes another 48-bit round key made from the cipher key. DES plays out a fundamental change all in all 64-bit block of data. It is then part into two, 32-bit sub-blocks, L0 and R0 which are then passed into what is known as Feistel rounds. Every one of the rounds are unclear and the effects of extending their number is twofold - the algorithms security is extended and its common profitability lessened. Around the completion of the sixteenth round, the 32-bit L15 and R15 yield sums are swapped to make what is known as the pre-yield. This [R15, L15] link is permuted utilizing a capacity which is the precise converse of the underlying stage. The yield of this last stage is the 64-bitciphertext.

The capacity f is comprised of four segments:

- Expansion P-box
- A whitener (that includes key)
- A gathering of S-boxes
- A straight P-box.

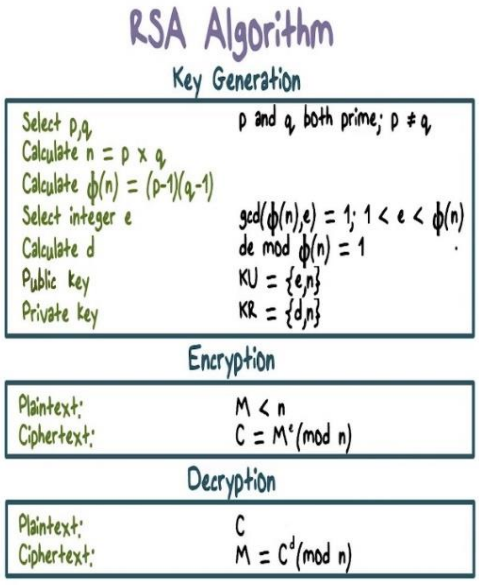
***B. RSA Algorithm*:** The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adelman. It depends on a property of positive whole numbers. RSA utilizes particular exponential for encryption and decryption. RSA is aalgorithm for public key cryptography, includes an public key and a private key. The public key can be known to everybody and is utilized for scrambling messages. Messages encoded with the public key must be decrypted utilizing the private key. RSA utilizes two examples, e and d, where e is public and d is private. Let the plaintext is M and C is cypher text, at that point at

Encryption $C = M^e \bmod n$

And at decryption side

$M = C^d \bmod n$.

Where n is an exceptionally vast number, made amid key age process.



DES algorithm and RSA algorithm gives security in cloud storage. In existing frameworks just single dimension encryption and decryption is connected to Cloud information stockpiling. Digital offenders can without much of a stretch split single dimension encryption. These days Cyber Criminals can without much of a stretch access information stockpiling. In Personal Cloud Storage

critical information, documents and records are depended to an outsider, which empowers Data Security to wind up the principle security issue in Cloud Computing. In Cloud Storage any association's or person's information is put away in and open from numerous disseminated and associated assets that involve a cloud. To give secure correspondence over circulated and associated assets verification of put away information turns into an obligatory errand. We have proposed a blend of two diverse security algorithms to dispense with the security difficulties of Personal Cloud Storage. We have taken a blend of algorithms like: DES and RSA. DES (Data Encryption Standard) is a symmetric key algorithm, in which a solitary key is utilized for both encryption/decryption of information. Though RSA is aasymmetric key algorithm, the algorithm that utilizes distinctive keys for encryption and decryption purposes. A client can transfer information in Personal Cloud Storage. Transferring document DES and RSA Encoding plans are utilized to scramble information.

The means of Multi-level encryption will be as per the following:

- Upload information.
- Now usage of DES Algorithm happens.

The Data Encryption Standard (DES) is a block cipher. It encodes information in blocks of size 64 bits each. That is 64 bits of plain text goes as contribution to DES, which produces 64 bits of ciphertext. The real key utilized by DES algorithm for encryption is 56 bits long. The encryption procedure is made of two stages (P-boxes), which we call beginning and last change, and sixteen Feistel rounds

- DES has 16 rounds, implies the primary algorithm is rehashed multiple times to deliver ciphertext. As number of rounds builds, the security of framework increments exponentially.
- The main dimension encryption is created utilizing DES algorithm
- Now apply RSA algorithm on scrambled yield of DES algorithm to produce second dimension encryption.
- In RSA algorithm open key is utilized for encryption.
- Once the information is scrambled utilizing RSA algorithm, it will be put away in Database of Cloud Storage.

The means of Multi-level decoding will be as per the following:

- DES and RSA algorithms are utilized to decode information.
- First apply the RSA algorithm (decoding plan) utilizing private key. This algorithm will create first dimension decode information.
- Now apply the DES decoding algorithm on first dimension decrypted information.
- DES decoding algorithm utilizes the equivalent 56 bit length key for decryption.
- DES algorithm of decryption will create Plain text.

In Our proposed algorithm, usage of the DES algorithm happens to produce first dimension encryption. And after that we apply the RSA algorithm on the encoded yield of DES algorithm to create second dimension encryption. Furthermore, same Process happens for unscrambling utilizing DES and RSA algorithms. Means we connected staggered Encryption and Decryption to give security to distributed storage information.

4. CONCLUSION

Cloud computing can turn out to be progressively secure utilizing cryptographic algorithms. Cryptography is the system for information secure by changing over the information into coded or non-coherent structures. However, the current cryptographic Algorithms are single dimension encryption algorithms. Unapproved individual can without much of a stretch split single dimension encryption. Consequently, framework which utilizes staggered encryption and decoding it gives greater security to Cloud Storage.

As our proposed algorithm is a Multilevel Encryption and Decryption algorithm. In this way, in our proposed work, just the approved client can get to the information. Regardless of whether some interloper (unapproved client) gets the information inadvertently or deliberately, he should need to decrypt the information at each dimension which is a troublesome undertaking without a substantial key. It is normal that utilizing staggered encryption will give more security to Cloud Storage than utilizing single dimension encryption.

REFERENCES

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing, version 15, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov).

[2] Parneet Kaur and Sachin Majithia, "Various Aspects for Data Migration in Cloud Computing and Related Reviews", International Journal of Computer Sciences and Engineering, Volume-02, Issue-07, Page No (83-85), Jul -2014, E-ISSN: 2347-2693.

[3] Sandha, M.Ganaga Durga," Study on Data Security Mechanism in Cloud Computing",IEEE conference no-33344.

[4] William Stallings, Cryptography and Network Security: Principles and Practices, Fifth edition, Prentice Hall, ISBN-13: 978- 0136097044, 2010.

[5] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr.AtanuRakshit, "C loud security issues" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.

[6] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

[7] Amazon Web Services: Overview of Security Processes, may 2011.

[8] L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security & Privacy Magazine, vol. 7, pp. 6164, July2009.

[9] P.ShanthiBala," Intensification of Educational Cloud Computing and Crisis of Data Security in Public Clouds",IJCSE Vol. 02, No. 03, 2010, 741-745.

[10] K Hashizume et al., An analysis of security issues for cloud computing, Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013.

[11] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka,and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control. pages 85–90, 2009.

[12] Wang, J.K.; Xinpei Jia, Data Security and Authentication in hybrid cloud computing model, Global High Tech Congress on Electronics (GHTCE), 2012 IEEE, On page(s): 117-120.

[13] ShivlalMewada, Umesh Kumar Singh and Pradeep Sharma, "Security Enhancement in Cloud Computing (CC)", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Vol.-01, Issue-01, pp (3137), Jan -Feb 2013.

[14] K. Dubey, M. Namdev, S. Shrivastava, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", IEEE sixth international conference, 2012.

[15] Prakash G. L ,Dr. Manish Prateek, Dr Inder Singh, ,"Efficient Data Security Method to Control Data in Cloud Storage System using Cryptographic Techniques ",IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India