International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 10 | Oct 2019 www.irjet.net p-ISSN: 2395-0072

DATA SECURITY IN CLOUD COMPUTING USING CRYPTOGRAPHIC ALGORITHMS

Siddharth Singh[1], Varun Kumar[2], UtkarshVerma[3], Azhagiri M[4]

[1,2,3,4]SRM Institute of Science and Technology, Ramapuram, Chennai-600089, Department of Computer Science and Engineering

---

Abstract: Cloud Computing is a collection of various internet services like servers, storage, databases, networking, software, analytics and intelligence and by employing Cryptographic algorithms in cloud computing the user can store and access data in a secure and protective way so that no third part can access and make changes to the user's data. Cryptography handles protection of critical data where the data is no longer under the control of user. In this paper we use AES algorithm to assure that the data is ciphered and is kept safeguarded. This would counteract undesirable interruption into individual information and absence of institutionalization, for example one specialist co-op may have start to finish encryption while others don't.This paper deals with the use of AES algorithm in PaaS cloud computing service.By using AES algorithm the strength of the security is high(90%) when compared to other security services (RSA, DES and hash functions).

Index terms- AES, DES, 3DES, PaaS

I. INTRODUCTION

Cryptography is the method and study of mathematically manipulating data so that it can be stored and transmitted securely. The act of manipulating the above mentioned data is called encryption, and the manipulated data is called encrypted. Encrypted data goes through a process called as decryption, before its original form is revealed. In case the encryption method is logical, then the following encrypted data will not be decrypted in a given amount of time by anyone who does not have a secret token, called an encryption key. Cryptography is the method of converting or encoding of a simple text or data into some unreadable form so that, that data can be read only by an authorized user. This method prevents the mishandling of the data by any foreign or unauthorized user. It provides privacy and security of the data. There are three types of cryptographic techniques that are used to encode data. Cryptography is additionally utilized in distributed computing to verify the online information.

Distributed computing is a procedure of conveying on the web transmission and capacity of information benefits in which assets are recovered from the Internet through electronic devices and applications, instead of an immediate association with a server. Instead of keeping records on an exclusive hard drive or nearby stockpiling gadget, cloud-based storageenables a client to spare information to a remote database. Distributed computing is anything but a solitary bit of technologyrather, it's a framework, principally included three administrations: foundation as an administration (IaaS), programming as an administration (SaaS) and stage as an administration (PaaS). SaaS has the quickest development rate, trailed by IaaS.Involving cryptographic techniques in cloud computing helps in secure transfer of data online. It also helps in secure storage of online data so that it can only be accessed by an authorized user holding an authorization key with the help of which the data can be encoded. Introduction of cryptography to encode data online in the cloud servers has completely changed the way of online sharing of data between the users. The users can now freely transfer, store or access data online without any fear of their data being hacked by any other user. The introduction of keys such as public and private keys further increases the security of text or data. The public key is available to all using which the data is encoded from one end and then the data is send to the other end. The private key is available only to the intended user who is authorized to access the data. When the data reaches the other end the private key held by the user is used decode and read the data.

In the cloud the data is not under anyone's control and so that data is vulnerable to hacking and being accessed by an unauthorized user. In such a case, Cryptography in cloud computing ensures reliability and integrity of online storage and transmission of data.

This paper deals with some efficient functions and methodologies to ensure the data is ciphered and is kept protected.

II. RELATED WORK

In the recent years, a lot of research has been performed on how the cryptographic techniques have been used in the area of cloud computing.

In one of the paper [1], the creator explains the significance of security in distributed computing and how encryption can shield correspondences and put away data from unapproved get to. The idea utilized is the procedure of content information that are scrambled in type of figure content to shield information from unapproved get to. The central theme of this examination paper is to grow how secure is the one's data set on cloud and what are the different security issues one should be stressed over when making usage of the cloud. They have utilized the calculation in portraying the way toward coordinating AES into cloud's information security. Until further notice, AES is most progressive and received calculation for performing cryptography in both the spots equipment and programming. No productive cryptanalytic ambushes against AES has been found to date. The segment of versatile key length allows a dimension of future fixing against exhaustive key attacks.

In one of the other paper [2] the creator talks about the investigation of information in the cloud and perspectives identified with it concerning security. Accessibility of information in the cloud is gainful for some applications however it presents hazards by presenting information to applications which may as of now have security escape clauses in them.So likewise, use of virtualization for circulated processing may danger data when a guest OS is continued running over a hypervisor without knowing the faithful nature of the guest OS which may have a security stipulation in it. Their paper additionally gives an understanding on information security perspectives for Data-in-Transit and Data-at-Rest. We have utilized the short clarification about the calculation and it's restrictions on usage in current online information security in our paper.

One of alternate[3]papers in whichthe creator analyzes the utilization of ECC in compelled situations where security is the fundamental issue and talks about the premise of its security, investigates its execution and ultimately, overviews the utilization of ECC applications available today is described. The idea depicted is the utilization of FIFO to actualize RR booking and utilizing scientific change to irreversibly scramble data.We have used the explanation about time sharing systems in cloud computing which is an alternative version of encryption of data.

In another paper[[4] the creator proposes and executes a calculation which would encode the records transferred on such online distributed storage benefits and would decode the document once it has been downloaded utilizing the keys that were produced amid encryption. This would forestall undesirable interruption into individual information and absence of institutionalization, for example one specialist co-op may have start to finish encryption while others don't.The description about the various subparts present in the algorithm which is used for encrypting and decrypting data is what we used from the paper.

In paper[5] published discusses about the symmetric block cipher that can be used as a substitute for DES. The blowfish algorithm has been used and the benefits of blowfish algorithm in domestic and exportable use has been discussed.

In the paper[6] the makers deal with the issue of security of data in the midst of data transmission. The essential worry to fear about this paper is the encryption of data so mystery and security can be successfully cultivated. The estimation used here is Rijndael Encryption Algorithm close by EAP-CHAP.

This paper[7] presents a tradition or set of bearings that uses the organizations of an outcast analyst or checker not only to affirm and approve the reliability of data set away at remote servers yet what's more in recuperating and recouping the data as fast as time allows in immaculate structure. The basic great position of this arrangement is the use of cutting edge imprint to ensure the uprightness of neighborhood data. Regardless, the general technique is dangerous and capricious as the keys and data are in like manner encoded and decoded separately.

In another paper[8]the focus is upon the looking over and perception of cloud security issues by proposing crypto counts and amazing measures so as to ensure the data security in cloud. Close by this, we will outline increasingly about some security parts of cryptography by showing some insurance issues of current conveyed figuring condition.

III. SYSTEM DESIGN:

A. System Introduction

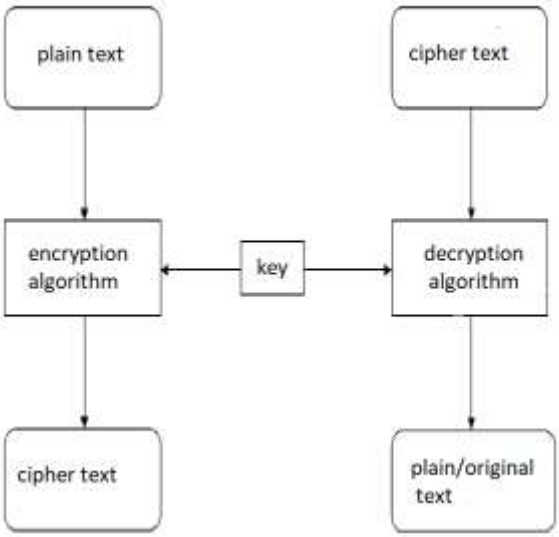

Fig 1 Schematic representation of Encryption and decryption of data

Cryptography is characterized as making composed or created codes that enable information to be stayed quiet. Cryptography changes over information into a non-lucid arrangement for an unapproved user(who dosen't have unscrambling key), enabling it to be transmitted without read or gotten to by unapproved elements and interpreting it once more into a clear organization, thusly giving secure correspondence within the sight of noxious outsiders. Data security in distributed computing can utilize cryptography on a few dimensions. The data can't be perused without giving an unscrambling key. The data keeps up its uprightness amid portage and keeping in mind that being put away. Cryptography additionally helps in approval. This implies the entire procedure of sending and the conveyance of a message can be confirmed.

B. Various Cryptographic Algorithms

1) Symmetric-Key Algorithm*:* Symmetric utilizations single key, which works for encryption just as unscrambling. It guarantees confirmation and approval. The key is kept as mystery. It works with rapid in encryption. Symmetric-key calculations are partitioned into two kinds: Block figure type and Stream figure type. In bock figure input is taken as a square of plaintext of fixed size contingent upon the sort of symmetric encryption calculation, key of fixed size is connected on to square of plain content and after that the yield figure square of a similar size as the square of plaintext is acquired. In Case of stream figure a little bit at a time information is encoded at a specific time. A portion of the instances of Symmetric-key calculations utilized in distributed computing are as per the following : Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES). It is otherwise called Secret-Key calculation.

2) Asymmetric-Key Algorithm: This calculation is known as open key cryptography and utilizations open and private keys to scramble or unscramble information. The keys referenced is essentially a gathering of extensive numbers that have been combined together however are unidentical (unbalanced). Open key in the pair can be imparted to everybody while the other key in the pair is known as the private key is stayed discreet. Both of the keys can be utilized to encode a message while the contrary key from the one used to scramble the message is regularly utilized for decoding.

3) RSA Algorithm: The calculation was developed by three researchers named Ron Rivest, Adi Shamir, and Len Adleman and hence, it is named as RSA cryptographic calculation. It is Asymmetric encryption Type calculation it implies that open key is disseminated to for encryption and private key is utilized to unscrambling .The key size is 1024 bits. In the RSA measured exponential is utilized for encryption and unscrambling. It utilizes two examples x and y where x is open key and y is private key. Messages hidden with the utilization of open key can be decoded just by utilizing the private key. This private key

fundamentally go about as a computerized mark. After encryption it is then given to the customer for check of client utilizing the server's known open key.

4) AES Algorithm: AES represents Advanced Encryption Standard. It goes under symmetric-key calculation. It is the most utilized and proficient Symmetric-key calculation among others. It was distributed by the National Institute of Standards and Technology (NIST). It is worked on bytes as opposed to bits, it treats 128bits of plaintext hinder as 16bytes. These 16bytes is prepared as a 4-4 framework. The greater part of the Computers currently incorporate equipment AES bolster making it quick. Besides, it is the More secure than DES and Most embraced symmetric encryption calculation.

IV. DATA ENCRYPTION AND TRANSMISSION THROUGH AES

AES encryption is the FIPS endorsed cryptographic calculation is utilized to ensure enduring electronic information.

• It is symmetric square figure for encoding and decoding data.

• Encryption part changes over a snippet of data or information into figure content while decoding includes transformation of the figure message back to basic lucid information.

The highlights of AES are –

- Symmetric Key, symmetric square figure
- 128-bit information, 128/192/256-piece keys.
- Stronger and quicker than DES and Triple-DES
- Provides full particular and configuration subtleties

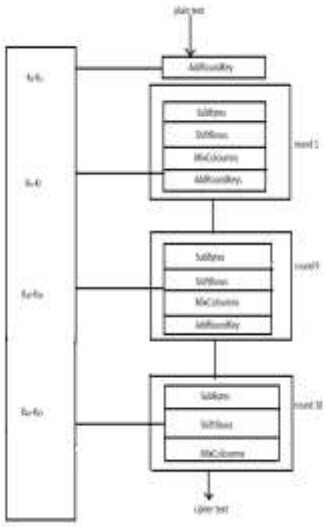

Fig2Architecture diagram of AES Encryption algorithm

AES encryption plays out the majority of its calculations on bytes as opposed to bits. Along these lines, AES treats the 128 bits of a plaintext hinder as 16 bytes. These 16 bytes are orchestrated preparing as a 4x4 network for example in four sections and four lines Unlike in DES, the quantity of rounds in AES is a variable amount and relies upon the length of key. AES encryption utilizes 10 rounds for 128-piece keys, 12 rounds for 192-piece keys and 14 rounds are utilized for 256-piece keys. Every one of these rounds utilizes an alternate and extraordinary 128-piece round key, determined from the first AES key.

V. PSEUDO CODE

AddRoundKey(s, &m[0])

For n=1 step 1 to 9

SubBytes(s)

ShiftRows(s)

MixColoumns(s)

AddRoundKey(s, &m[n*4])

End for

SubBytes(s)

ShiftRows(s)

AddRoundKey(s, &m[40])

State depicts the original key size of the data, which is divided into SubBytes of 16 bytes each. Then this state is made to undergo through shift transformation into a re-ordered state matrix, MixCloumnswhere it is multiplied with a matrix containing 4 bytes and then the AddRoundKey procedure where it is made to undergo the logoical XOR process where it deals with the 16 byte matrix.

VI. ENCRYPTION PROCESS

Here, the process is restricted to mainly the description of a typical round of AES encryption. Each round of encryption comprises of four sub-processes. The first round process is given below as following –

To calculate the number of rounds (NR) in Encryption process, we use the key size(represented by KS) and Block size(represented by BS). Key size is divided by block size and the whole equation is added by 6.

The formula is given as: NR= (KS/BS) + 6

For example let KS=128

BS=32

NR= (128/32) + 6= 10 rounds

A) Byte Substitution (sub bytes): The 16 input bytes are substituted by looking up a fixed table called the S-box given in the specified design. The resultant product is a matrix of four rows and four columns. Here we have taken 128 as the key size which will have 10 rounds

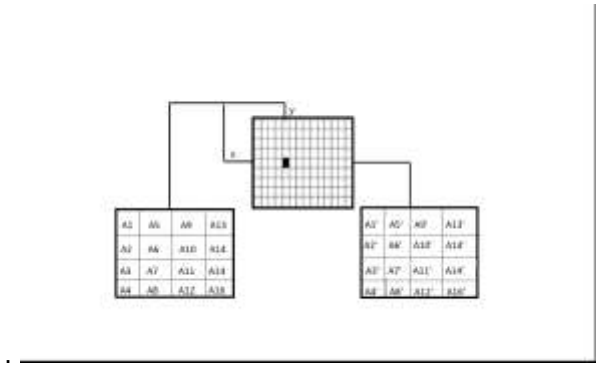

Fig 4: Byte Substitution

B) Shift Rows: Each of the four rows of the 4x4 matrix is shifted one byte row to the left. Any entries that fall off from allocation are re-inserted on the right side. Shift is carried out as follows –

- 1st row isn't shifted to the left but is kept as it is.
- The 2nd row gets shifted 1 (byte) position to the left.
- The 3rd row gets shifted 2 positions (ie 2 bytes) to the left.
- The 4th row gets shifted 3 positions (3 bytes) to the left.
- The result achieved is a new 4x4 matrix consisting of the same 16 bytes but shifted to the left with respect to each other. Let the original 4x4 Matrix be N with elements A_1 to A_n.

Applying Left shift in accordance to the rule of rows,

1st row= No shift. Elements maintain their positions.

2nd row= [A_{n-1}] for every element

3rd row=[A_{n-2}]for every element

4th row= [A_{n-2}] for every element.

Thus, post the shifting process the elements formed in order are allocated to the 4x4 matrix N'.

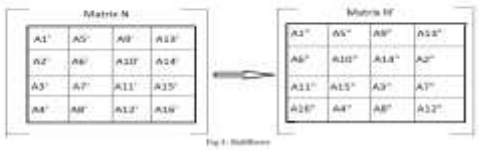

Fig 5: Shift Rows

C) MixCLoumns: Every section of four bytes each gets changed and utilized to an extraordinary numerical capacity. This math work takes as information the four bytes of one segment and yields four totally new bytes, which at that point are utilized to supplant the first section. Another new framework comprising of 16 new bytes is gotten from this task. This progression is overlooked in the last round. For example estimation of first byte A1'' is duplicated with 02, 03, 01 and 01 and XORed to create new A1''' of coming about network. The duplication proceeds against one grid push at once against each estimation of a state segment.

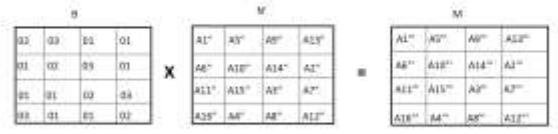

Fig 6: MixColumns

A matrix representing 4 bytes is considered. It is made to be of the 4x4 order. The indexed elements are written from 01 to 03. Let this matrix by B

This matrix B is then multiplied with N'. The resultant matrix is a 4x4 matrix M.

Formula: [B] x [N]'= [M]

D) AddRoundKey: The 16 bytes of the 4x4 framework are currently considered as 128 bits and are made to experience XOR intelligent procedure to the 128 bits of the round key. The ciphertext yield is gotten just in the last round. Generally the 128 bits are considered as 16 bytes and the procedure restarts.

B) Decryption Process: The procedure of decoding of an AES ciphertext is backward request to that of the encryption procedure with comparative procedure. Each round comprising of the four procedures are directed this time in a turned around request –

- Add round key
- Mix segments
- Shift columns
- Byte substitution

The encryption and decoding calculations should be independently actualized since the sub forms in each round backward way.

VII. APPLICATION

The framework portrayed above utilizations the AES with the end goal of encryption and unscrambling of the information with the principle motivation behind utilizing this calculation being to give greater security to the information which will be transferred on to the cloud.. For the open cloud cases have been taken from Microsoft purplish blue and is made utilizing the Linux with i5 processor with the Ram being of 8 GB limit. The utilization of most recent processor diminishes the reaction time for transferring and conveying of information at the proprietor and client's end individually. The measure of the decoding key is another basic factor in the framework build of distributed storage. The unscrambling key is required to be kept versatile as clients may utilize the capacity administration from various shifting customers. The information that is encoded through AES encryption calculation is put through to the PaaS cloud server where it is designated a mystery key while in Transit through the cloud stage. PaaS takes care of delivering, and overseeing programming applications. The key is mystery and is available just to detached clients at the less than desirable end or when the information is taken from the distributed storage. The scrambled information's key code is utilized to open the protected information and decode it with a similar system however in invert request.

The main purpose of using PaaS in this setup of transferring data is that it provides a platform and has its own set of deployable functions which minimizes hardware use from the end of the user. For example to share data between the company this setup has its own platform with its assigned features rather than consuming the whole digital infrastructure for the process thus helping faster sharing of data and keeping the multi tasking ability of the servers active

VIII. RESULTS

Factors	DES	3DES	AES
Key Length	Key length is56 bits	Length is168 bits (k1, k2 and k3) Length is 112 bits (k1 and k2)	Length is 128, 192, 256 bits. It varies w.r.t rounds
Round(s)	It has 16 rounds	It has 48 rounds	For 10 rounds - 128bit Key For 12 rounds -192 bit key For 14 rounds - 256 bit key
Block Size	64 bits	64 bits	128 bits
Speed	The speed is Slow	The speed is Very Slow	The speed is Fast
Security	Not Secure Enough	Sufficient Security	Relatively better Security practically

The concerns regarding security problems in cloud computing has often kept organizations distant from

uploading data in a secure manner, thus the introduction of encryption of data before being uploaded to the cloud the data is much more secure and private, being less prone to external intrusions or hacking. The data passes through the gateway in a safer way. Implementation of AES encryption further enhances the security of data because of its advantages over other encryption algorithms such as DES or RSA. Some of these advantages are:

- It is one of the most spread commercial and open sources existing currently.
- It uses higher length key sizes like 128, 192 and 256 bits for encryption making it more robust and resistant against hacking.
- Uses minimal storage space and is the fastest to implement in both encryption and decryption.

With the data being on a virtual source it is companies have rescinded from taking responsibility of it is implemented in both hardware and software thereby making it the most robust security protocol.

After analyzing the symmetric algorithms mentioned in the paper AES was found the most secure, faster and better among all the existing algorithms with no evident serious weaknesses, there are some flaws in symmetric algorithms such as weak keys, insecure transmission of the secret key, speed, flexibility, authentication and reliability. This means that Original plain text is able to be recovered provided the encryption is applied twice with one of these weak keys. DES is very slow when implemented in software algorithm and is best suited to be implemented in hardware.DES has the encryption speed higher than on.3DES does not always provide extra security making use of double and triple encryption as well as is very slow when implemented practically in software. As it is derived from DES and it being already slow on software, Triple-DES is considered safe but slowest and not practical enough.

IX. CONCLUSION

Distributed computing is a fairly encouraging and convincingly rising innovation for the up and coming age of IT applications. The principle obstacles toward the fast development of distributed computing are information security and protection issues. AES encryption is the quickest technique that has the adaptability and versatility and can be effectively actualized and executed. This is on the grounds that the required memory for AES calculation is not exactly the Blowfish and DES calculation. AES calculation has a high security level since the bits utilized are the 128, 192 or 256-piece key. It indicates obstruction

against a large group of assortment of assaults to be specific square assault, key assault, key recuperation assault and differential assault. In this manner, AES calculation is a profoundly secure encryption technique existing in the encryption showcase. When the information is encoded with AES, it can likewise ensure against future assaults, for example, crush assaults. AES encryption calculation utilizes insignificant extra room and yields superior exhibitions with no shortcomings.

X. REFERENCES

[1] ShaffiBansal, GagandeepJagdev "Analyzing working of AES and DES algorithm in cloud security", International journal of research studies in computer science and engineering(IJRSCSE), Volume 4, Issue 3, 2017.

[2] Sajjan R.S, Vijay Ghorpade and VishwajitDamblikar "Survey paper on data security in cloud computing", International journal of Computer Sciences and engineering, volume 4, special issue 4, june 2016.

[3] Wendy Chou, "Elliptic Curve Cryptography and its Applications to Mobile Devices", University of Maryland, College Park.

[4] Prerna, ParulAgarwal, "Cryptography Based Security for Cloud Computing System", Volume 8, No. 5, May-June 2017 International Journal of Advanced Research in Computer Science.

[5] Rishav Chatterjee, Sharmistha Roy, "Cryptography in cloud computing: A basic approach to ensure security in cloud", International journal of Engineering Science and Computing, May 2017.

[6] Sanjoli Singla, Jasmeet Singh, "Cloud computing security using encryption technique", IJARCET, vol.2, ISSUE 7.

[7] Anjali Arora, "A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers", International Journal of Computer Science and Information Technology & Security, 2012.

[8] Bhaskar SM, Ahson SI, "Information Security A Practical Approach", Narosa Publishing House, India, 2008.

[9] Gupta B, Agrawal DP, Yamaguchi S, "Handbook of research on modern cryptographic solutions for computer and cyber security", IGI Global, 2016.

[10] Yogesh M, Rohit K V, Mahipal S S, Rajeev K, "Secure Cyber Network to Sharing Information through Cryptography & Stenography". EngTechnol Open Acc. 2019; 2(5): 555598.