January – February 2020
ISSN: 0193-4120 Page No. 13335 - 13340

Secure Cloud Data Computing using Different Algorithms

R Yogesh Rajkumar[1], K P Kaliyamurthie[2]

[1]Research Scholar, BIHER- Bharath Institute of Higher Education and Research, Chennai, India.
[2]Professor, Department of Computer Science and Engineering, BIHER- Bharath Institute of Higher Education and Research, Chennai, India.
[1]yogesh.rajkumar@gmail.com

Article Info
Volume 82
Page Number: 13335 - 13340
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 24 February 2020*

Abstract

Cloud Computing suggests toward the conveyance of IT resources – hardware, services, applications or infrastructure upon the online network. Cloud Computing is causing a major move in the IT business. New innovations have been created, and now there are various ways to virtualize IT framework and to access the required applications on the Internet, through online applications. Examples of cloud service suppliers are Gmail, Amazon, Yahoo, IBM, Cisco Systems and so on. Benefits of cloud storage is straightforward way in signify way in as far as anyone is concerned everyplace, in any case, every time, adaptability, versatility, expenditure effectiveness, as well as peak accuracy of the information. As there are many advantages of cloud computing we have to secure or ensure data against unauthorized clients. Within these study articles, the planned job ideas are eliminating the worries about information confidentiality utilizing cryptographic algorithm for enhancing the protection within cloud as stated toward other views of cloud clients.

Keywords; *Cloud Computing, Cryptographic, RSA, DES and AES Algorithms.*

I. INTRODUCTION

Cloud computing often suggested like basically "The Cloud" has been the delivery of requisition computing asset upon the web which charges based on the utilizing. Cloud service permits persons as well as companies toward utilize software as well as hardware which has been controlled through unknowns on distant location. Instances of cloud service incorporate web document repository, public systems administration locales, email, as well as web commerce application. The cloud computing system permits contact toward data as well as PC assets as of everywhere where system associations are accessible [1-2]. The word Cloud refers toward a net otherwise web. Ultimately, Cloud has been somewhat, and are accessible on distant locations. Cloud could provide service upon PC, i.e., upon public PCs otherwise upon personal PCs, i.e., Wide Area Network, Local Area Network otherwise Virtual Private Network. Application, such as, electronic mail, webinar, customer relationship management (CRM), every single one run within cloud [3].

Figure 1 depicts the categories of cloud computing. These are SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service) as well as IaaS (Infrastructure-as-a-Service). Software-as-a-Service has been known like 'On Demand Software', PaaS is a programming platform for designers and IaaS is a way to convey a cloud computing infrastructure like server, storage, organize and operating framework. Service models have been named like SPI model as Software, Platform as well as Infrastructure Models. Software as a Service (SaaS): Since the word articulates, this allots through the S/W otherwise electronic application. Electronic applications have been constructed utilizing web programming as PHP, JAVA, Dot Net, and so on. It permits

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13335 - 13340

individual toward execute real over the web application. Eg.Google Docs. Platform as a Service (PaaS): Platform as a Service gives way for clients toward take a shot at internet applications otherwise S/W. These allow clients toward build claim cloud application utilizing provider explicit instruments as well as language. Eg Google App Engine. Infrastructure as a Service (IaaS): clients utilize distant framework, lets clients for executing several application which is required upon cloud H/W of its personal choice. Eg. Personal cloud, committed facilitating, half and half facilitating. One more example Amazon gives flexible computing. Individual could request for 1GB Memory, 256 RAM, 1 GB data every month server approximately. Amazon EC2. Security goals of information incorporate three focuses called: accessibility, privacy, as well as reliability. Privacy of information within the cloud has been done through cryptography.

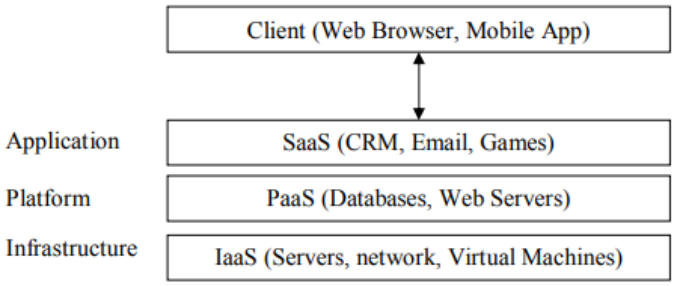

Fig.1 Service Model

Cryptography presently has been viewed as mixture of three sorts of algorithm which are Symmetric-key algorithms, Asymmetric-key algorithms as well as Hashing. Honesty of information has been guaranteed through hashing algorithm [2]. Information Cryptography has been a technique for ensuring information and communication utilizing codes with the goal that those for whom the information is projected be able to study as well as practice this. The prefix "Grave" means "covered up" and the addition "graphy" means "composing". The major aspire of cryptography protects information protected as of intruders. Cryptography in the cloud ensures delicate data without delaying information exchange. Data Encryption in the cloud is the way toward transforming or encoding data before it's moved to cloud storage. To encode information on cloud repository symmetric-key as well as asymmetric-key algorithm is used. Cloud repository has a huge arrangement of database. For these huge databases asymmetric-key algorithm's execution is more slow while comparing with symmetric-key algorithm.

II. LITERATURE REVIEW

In 2012, PriyankaArora, Arun Singh as well as HimanshuTyagi [7] proposed Evaluation along with Comparison of Security concerns over Cloud Computing background. Within this paper they actualized several cryptographic algorithm over a cloud arrange that reasons where the algorithms executed has been further effective compared to utilizing it in a particular framework.

In 2013, SajjadHashemi [8] projected distinctive protection challenge on cloud information repository. "SajjadHashemi as well proposed several ideas for increasing the protection of information repository within the cloud computing frameworks". SajjadHashemi utilized algorithms acc toward issue otherwise challenges experienced within protection. E.g, he utilizes Advanced Encryption Standard, Data Encryption Standard.

During 2013, Vijay. G. R, along with A.Rama Mohan Reddy [5] proposed information protection within Cloud supported upon Trusted Computing background. The pros of this projected plan is expanding the believed computing innovation within the cloud computing condition for achieving the believed computing prerequisites on behalf of the cloud computing which satisfies the believed cloud computing. In 2014 SwarnalataBollavarapu with Bharat Gupta [3] projected information protection framework. This framework utilizes algorithm as Rivest–Shamir–Adleman,Elliptic-curve cryptography as well as RC4 for encrypting as well as decrypting method.

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13335 - 13340

In 2015, Shakeeba S. Khan and Prof.R.R.Tuteja [2] proposed protection during Cloud Computing utilizing Cryptographic Algorithm. This proposed algorithm is a Multilevel Encryption as well as Decryption algorithms. In these manners, just the approved client could contact the information. In 2016, Salim Ali Abbas, Ph.D and Amul Abdul BaqiMaryoosh [6] proposed information protection for Cloud Computing supported upon Elliptic Curve Integrated Encryption Scheme (ECIES) as well as Modified Identity based Cryptography (MIBC). This paper proposes a progressively adaptable and powerful plan for addressing information repository protection issues into cloud computing.

In 2016, Mini Batra and Anil Arora [9] proposed an audit on Cloud Computing Security. This paper gives audit of various security aspects of cloud data storage. In 2017, NidhiDahiya and Mrs. Sunita Rani [4] proposed survey on Cloud Computing Security. This assessment article gives an outlook otherwise plan regarding the issues which could happen within a cloud computing framework by different protection concerns.

III. DIFFERENT ALGORITHMS FOR CLOUD SECURITY

The projected framework has been intended for maintaining protection of content records as it were. These projected frameworks uses Data Encryption Standard as well as Rivest–Shamir–Adleman algorithms for generating encryption while customer uploaded the contented records into Cloud repository as well as backwards Data Encryption Standard along with Rivest–Shamir–Adleman algorithms for generating unscrambling once customer downstream document as of Cloud repository, in support of increasing protection.

Algorithm:

1. Choose two large prime P & Q
2. Calculate N = P * Q
3. Select the public key (i.e. encryption key) E such that it is not a factor of (P - 1) and (Q - 1).
4. Select the private key (i.e. decryption key) D such that following equation is true:
   (D * E) mod (P - 1) * (Q - 1) = 1
5. For encryption calculate cipher text CT from the plain text PT as follows:
   CT = PTE mod N
6. Send CT as the cipher text to the receiver
7. For decryption, calculate the plain text PT from the cipher text CT as follows:
   PT = CTD mod N

Data Encryption Standard (DES) Algorithm:

The Data Encryption Standard (DES) has been a symmetric-key square figure distributed like FIPS-46 within the Federal Register in January 1977 through the National Institute of Standards and Technology (NIST). By the encryption site, DES acquires a 64bit cleartext as well as generates 64-piece figure content, on the unscrambling location, this obtains a 64-piece figure message as well as creates a 64-piece cleartext, as well as similar 56-piece figure input has been utilized in support of mutually encryption as well as decoding. The encryption procedure has been prepared of two permutations (P-box), which calls initial and final permutations, also sixteen Feistel adjusts. Every iteration utilizes an alternate 48-piece iteration key produced as of the figure key.

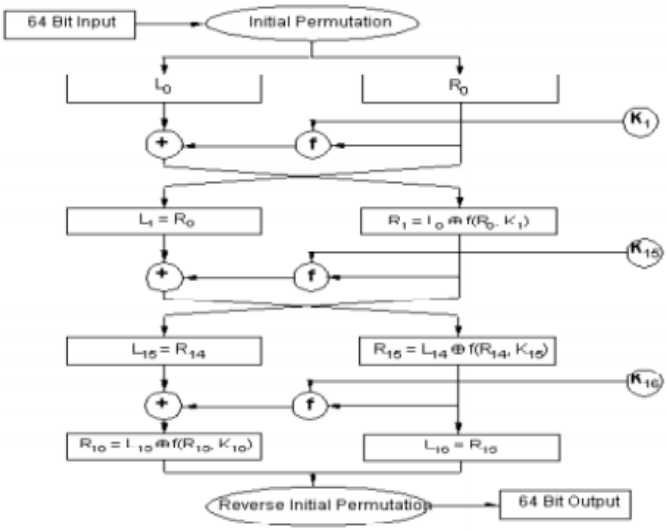

Fig.2 Encryption with DES

Here, Data Encryption Standard plays out an initial permutation upon the whole 64-piece square of information which has been part as two, 32-piece

Published by: The Mattingley Publishing Co., Inc.

TEST Engineering & Management

January – February 2020
ISSN: 0193-4120 Page No. 13335 - 13340

sub-squares, L0 plus R0 that has been accepted within which is known as Feistel adjusts [12]. Every iteration is same as well as the impact of growing its quantity is double - the algorithm protection has improved, as well as their sequential productivity diminished. By the finish of the sixteenth iteration, the 32-piece L15 as well as R15 yield number is exchanged for creating which is termed like the pre-yield. These [R15, L15] concatenations are permuted utilizing a capacity and it has been the precise converse of the initial permutation. The yields of these final permutations are the 64-piece figure content.

RSA Algorithm:

The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adleman. This has been supported upon a assets of affirmative numbers. Rivest, Adi Shamir, and Leonard Adleman utilizes modular exponential for encryption as well as decoding. Rivest, Adi Shamir, and Leonard Adleman algorithm is for open key cryptography, includes an open key as well as a private key. People in general key are identified to everybody that is utilized to encode message. Message scrambled by people in general key be able to decode utilizing the private key. RSA utilizes two examples, e as well as d, in which e is open, also d is private. Let the cleartext is M and C is figure content, by that point at encryption.

$C = Me \bmod n$

Moreover by decryption side

$M = Cd \bmod n$

Where n is a huge number, produced through key generation method. RashmiNigoti, utilizes Data Encryption Standard algorithm and, Ron Rivest, Adi Shamir, and Leonard Adleman algorithms to give protection toward cloud repository. Within real frameworks just, single level encoding as well as decoding should be enforced toward Cloud information repository. Digital culprits could straightforwardly crack single level encryption.

IV. RESEARCH METHODOLOGY

We recommend a framework that utilizes staggered encryption as well as unscrambling for giving greater protection to Cloud repository. As in "Security in Cloud Computing utilizing Cryptographic Algorithms" they utilized RSA and DES, we'll use RSA, DES and AES to give greater security. This has projected a mixture of three diverse protection algorithms for eliminating the protection challenge of private Cloud repository. This has a mixture of algorithms like: Data Encryption Standard, Advanced Encryption Standard and RSA. DES (Data Encryption Standard) has been a symmetric key algorithm, where a solitary key has been utilized to encrypt/unscrambling of information. Ron Rivest, Adi Shamir, and Leonard Adlemanhas been an asymmetric key algorithm, which utilizes various key to encrypt as well as decoding uses. AES (Advanced Encryption Standard) has been a symmetric key algorithm, wherein similar key has been utilized toencryption as well as unscrambling.

The proposed framework is intended to maintain security of content documents as it were. The proposed framework configuration centers on the accompanying destinations that has been useful on the increase the protection of information repository.

For Encryption of text files:

- Upload Text file.
- Implementing the DES algorithm of Encryption to generate first level encryption
- Implementing the AES algorithm of Encryption to generate second level encryption
- Implementing the RSA algorithm of Encryption to generate third level encryption
- Store Cipher Text into Database

For Decryption of text files:

- Read Cipher Text from Database
- Implementing the RSA algorithm of Decryption to generate first level decryption
- Implementing the AES algorithm of Decryption to generate second level decryption
- Implementing the DES algorithm of Decryption to generate Plain text
- Display Plain Text to User

For protected communication upon conveyed as well as linked asset authentication of take away data turn within a mandatory job.

According to Fig 3, Step of Multi-level encryption is:

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13335 - 13340

1. Upstream the content document.

2. Presently executions of Data Encryption Standard Algorithms take place. The Data Encryption Standard (DES) algorithms are a square figure. This scrambles information within squares of range 64 bits every one where 64 bits of clear content go as contribution toward Data Encryption Standard that generates 64 bit of cipher content. The definite key utilized in Data Encryption Standard algorithms to encrypt has been 56 bit long. The encryption procedure has been prepared of two permutations (P-boxes), known as initial as well as final permutation, plus sixteen Feistel adjusts. The principal level encryptions are produced utilizing Data Encryption Standard algorithms.

3. Presently put in AES algorithms upon scrambled yield of Data Encryption Standard algorithms for generating 2nd level encryptions.

4. Presently put in Ron Rivest, Adi Shamir, and Leonard Adleman algorithms upon encoded yield of AES algorithms for generating third level encryptions.

5. During Ron Rivest, Adi Shamir, and Leonard Adleman algorithms open key has been utilized to encrypt. Ron Rivest, Adi Shamir, and Leonard Adleman algorithms are a Block Cipher where all messages are linked toward a figure.

6. When the data has been scrambled utilizing Ron Rivest, Adi Shamir, and Leonard Adleman algorithms, this would be placed within Databases of Cloud repository. furthermore while downstreaming document converse Data Encryption Standard, AES as well as Ron Rivest, Adi Shamir, and Leonard Adleman algorithms have been utilized for decoding information.

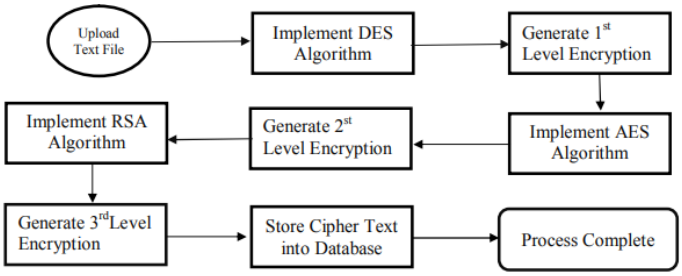

Fig.3 Multilevel Encryption

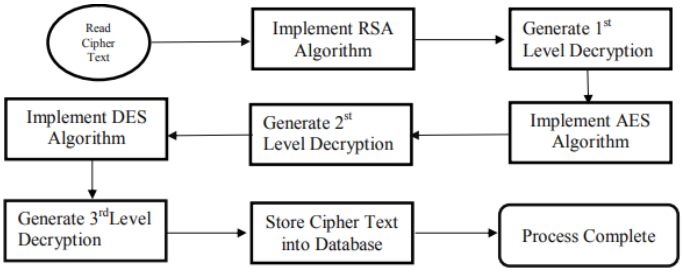

Fig.4 Multilevel Decryption

Within these projected framework, execution of the Data Encryption Standard algorithms take place for generating 1st level encryption. Furthermore RSA algorithms are applied to generate second level encryption and at last AES algorithms for generating third level encryption. As well as same procedure is repeated to decode utilizing converse Data Encryption Standard, AES plus RSA algorithm. Also Encryption and Decryption algorithm has been applied for giving protection to cloud repository information.

V. CONCLUSION

Cloud Computing can turn out to be progressively secure utilizing cryptographic algorithms. Cloud computing furnishes companies with new alternatives for managing infrastructures and new plans of action. Cloud Computing is affected by data security, robbery, loss of data and respectability. To avert it we are utilizing diverse degree of cryptography algorithms. Cryptography is a solitary level encryption and digital culprits are able to simply crack single level encryption. Consequently, propose again a framework that utilizes staggered encryption as well as decoding for giving greater protection to Cloud repository. Staggered encryption is already present, so we are adding extra security

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13335 - 13340

level in it. In this, unauthorized client can't utilize the data easily. We presented three degree of security level that is RSA, DES and AES algorithms. It is all the more dominant at that point single level encryption.

REFERENCES

1. Chandrika1 ,Er. SahilDalwal, "Data Security in Cloud Computing Using Cryptographic Algorithms: A Review", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 7, Issue 1, January 2019, pp.89-94.
2. Shakeeba S. Khan, Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, Vol. 3, Issue 1, January 2015.
3. Prof SwarnalataBollavarapu, Bharat Gupta, "Data Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 4, Issue 3, March 2014.
4. NidhiDahiya, Mrs. Sunita Rani, "Cloud Computing Security: A Review", IJEDR, ISSN: 2321-9939, Volume 5, Issue 3, January 2017.
5. Vijay. G. R, A.Rama Mohan Reddy, "Data Security in Cloud based on Trusted Computing Environment",International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Volume-3, Issue-1, March 2013.
6. Salim Ali Abbas, Ph.D, Amul Abdul BaqiMaryoosh, "Data Security for Cloud Computing based on Elliptic Curve Integrated Encryption Scheme and Modified Identity based Cryptography",International Journal of Applied Information Systems, ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 10 – No.6, March 2016.
7. PriyankaArora, Arun Singh, HimanshuTyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal, ISSN: 2221-0741 Vol. 2, No. 5, 179- 183, 2012.
8. SajjadHashemi, "Data Storage Security Challenges in Cloud Computing", International Journal of Security, Privacy and Trust Management, Vol 2, No 4, August 2013.
9. Mini Batra, Anil Arora, "Cloud Computing Security: A Review", International Journal of Advance Research in Computer Science and Management Studies, ISSN: 2321-7782, Volume 4, Issue 5, May 2016.

Published by: The Mattingley Publishing Co., Inc.