ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Data Security in Cloud Computing Using Cryptographic Algorithms: A Review

Chandrika[1], Er. Sahil Dalwal[2]

M.Tech. Student, Department of Computer Engineering, BIMT Shimla, India[1]

Assistant Professor, Department of Computer Engineering, BIMT Shimla, India[2]

ABSTRACT: Cloud Computing refers to the delivery of IT resources – hardware, services, applications or infrastructure over the Internet. Cloud Computing is causing a major shift in the IT industry. New technologies have been developed, and now there are various ways to virtualize IT system and to access the needed applications on the Internet, through web-based applications. Examples of cloud service providers are Gmail, Amazon, Yahoo, IBM, Cisco Systems etc. Benefits of cloud storage are easy access means access to your knowledge anyplace, anyhow, anytime, scalability, resilience, cost efficiency, and high reliability of the data. As there are many benefits of cloud computing we need to secure or protect data against unauthorized users. In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using cryptographic algorithms to enhance the security in cloud as per different perspective of cloud customers.

KEYWORDS: Cloud Computing, Cryptographic Algorithm, RSA, DES, AES.

I. INTRODUCTION

Cloud Computing often referred to as simply “The Cloud” is the delivery of on-demand computing resources over the Internet on a pay for use basis. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available [1]. The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud.
SERVICE MODEL [2]

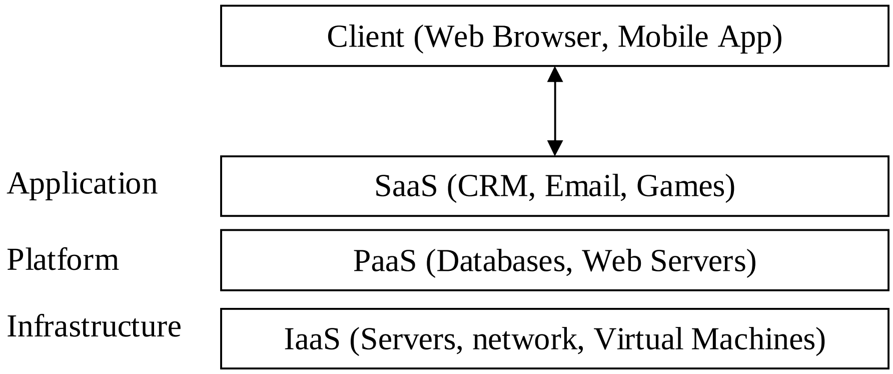
Client (Web Browser, Mobile App)
Application
SaaS (CRM, Email, Games)
Platform
PaaS (Databases, Web Servers)
Infrastructure
IaaS (Servers, network, Virtual Machines)

Figure 1: Service Model

Figure 1 describes the categories of cloud computing. These are SaaS(Software-as-a-Service), PaaS(Platform-as-a-Service) and IaaS (Infrastructure-as-a-Service). SaaS is known as **'On Demand Software'**, PaaS is a programming platform for developers and IaaS is a way to deliver a cloud computing infrastructure like server, storage, network and operating system.

Service model also called as SPI model as Software, Platform and Infrastructure Model. Software as a Service (SaaS): As the name says, it deals with the software or web-based applications. Web based application are those applications that are built using web languages like php, java, .net, etc. this model of cloud allows one to run existing online applications. Ex. Google Docs. Platform as a Service (PaaS): Platform as a Service provides platform to users to work on web application or software. It allows users to create own cloud applications using supplier-specific tools and language. Ex Google App Engine Infrastructure as a Service (IaaS): users use remote infrastructure, allows users to run any applications they want on cloud hardware of their own choice. Ex. Private cloud, dedicated hosting, hybrid hosting. Another Ex. Amazon provides elastic computing. One can ask for 1GB Storage, 256 RAM, 1 GB transfer/month server like this. Amazon EC2.

Security goals of data include three points namely: Availability, Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are Symmetric-key algorithms, Asymmetric-key algorithms and Hashing. Integrity of data is ensured by hashing algorithms [1].

Data Cryptography is a method of protecting information and communication using codes so that only those for whom the information is intended can read and process it. The prefix "Crypt" means "hidden" and the suffix "graphy" means "writing". The main aim of cryptography is to take care of data secure from invaders. Cryptography in the cloud protects sensitive data without delaying information exchange. Data Encryption in the cloud is the process of transforming or encoding data before it's moved to cloud storage. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms.

II. RELATED WORK

In 2012, Priyanka Arora, Arun Singh and Himanshu Tyagi [6] proposed Evaluation and Comparison of Security Issues on Cloud Computing Environment. In this paper they implemented various cryptographic algorithms on a cloud network which concludes that the algorithms implemented are more efficient than using them on single system.

In 2013, Sajjad Hashemi [7] proposed different security challenges for cloud data storage. "He also suggests various concepts to increase the security of data storage in the cloud computing systems". He uses algorithm acc to problem or challenges faced in security. for example, he uses AES, DES.

In 2013, Vijay. G. R, and A.Rama Mohan Reddy [4] proposed Data Security in Cloud based on Trusted Computing Environment. The advantages of this proposed approach are to extend the trusted computing technology into the cloud computing environment to achieve the trusted computing requirements for the cloud computing and then fulfil the trusted cloud computing.

In 2014 SwarnalataBollavarapu and Bharat Gupta [2] proposed data security system. This system uses algorithms like RSA, ECC and RC4 for encryption and decryption techniques.

In 2015, Shakeeba S. Khan and Prof.R.R. Tuteja [1] proposed Security in Cloud Computing using Cryptographic Algorithms. This proposed algorithm is a Multilevel Encryption and Decryption algorithm. Thus, only the authorized user can access the data.

In 2016, Salim Ali Abbas, Ph.D and Amul Abdul BaqiMaryoosh [5] proposed Data Security for Cloud Computing based on Elliptic Curve Integrated Encryption Scheme (ECIES) and Modified Identity based Cryptography (MIBC). This paper proposes a more flexible and effective scheme to address data storage security problems in cloud computing.

In 2016, Mini Batra and Anil Arora [8] proposed a review on Cloud Computing Security. This paper provides review of different security aspects of cloud data storage.

In 2017, Nidhi Dahiya and Mrs. Sunita Rani [3] proposed review on Cloud Computing Security. This Review paper give a view or idea about the problems that can be occur in a cloud computing system at multiple security issues.

III. EXISTING ALGORITHMS FOR CLOUD SECURITY

Method Proposed in Paper [1]:
The proposed system is designed to maintain security of text files only. This proposed system uses DES & RSA algorithm to generate encryption when user uploaded the text files in Cloud Storage and inverse DES & RSA algorithm to generate decryption when user download file from Cloud Storage, for increasing security.

Algorithm [9]:

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 fallows:
   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 [11]:
The Data Encryption Standard (DES) is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56-bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key.

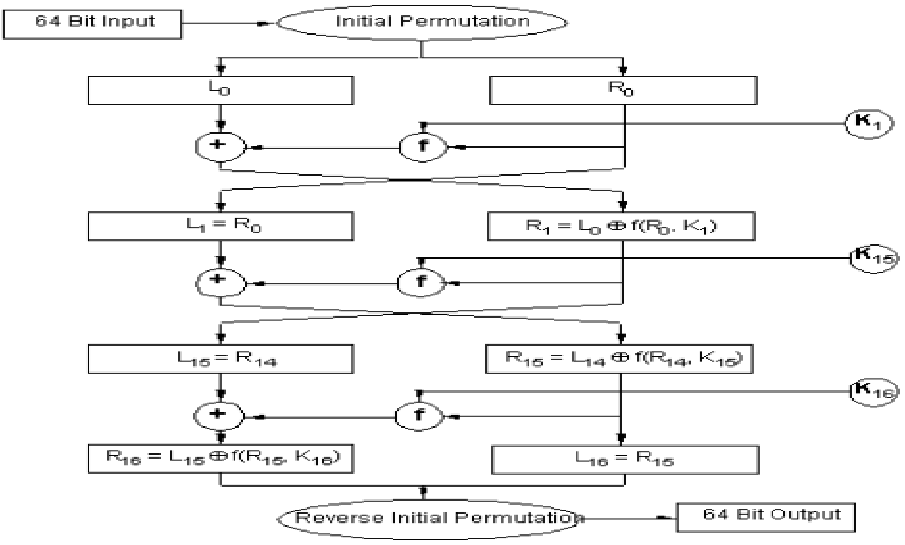
64 Bit Input
Initial Permutation
L_0
R_0
K_1
+
f
$L_1 = R_0$
$R_1 = L_0 \oplus f(R_0, K_1)$
K_{15}
+
f
$L_{15} = R_{14}$
$R_{15} = L_{14} \oplus f(R_{14}, K_{15})$
K_{16}
+
f
$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$
$L_{16} = R_{15}$
Reverse Initial Permutation
64 Bit Output

Figure 2: Encryption with DES

Here, DES performs an initial permutation on the entire 64-bit block of data. It is then split into two, 32-bit sub-blocks, L0 and R0 which are then passed into what is known as Feistel rounds [12]. Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased, and its temporal efficiency decreased. At the end of the 16th round, the 32-bit L15 and R15 output quantities are swapped to create what is known as the pre-output. This [R15, L15] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64-bit cipher text.

RSA Algorithm [13]:

The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

RSA uses two exponents, e and d, where e is public, and d is private. Let the plaintext is M and C is cipher text, then at encryption

$$C = Me \bmod n$$

And at decryption side

$$M = Cd \bmod n$$

Where n is a very large number, created during key generation process. Rashmi Nigoti [13], uses DES algorithm and RSA algorithm for providing security to cloud storage. In existing systems only, single level encryption and decryption is applied to Cloud data storage. Cyber criminals can easily crack single level encryption.

IV. PROPOSED SYSTEM

We propose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage. As in "Security in Cloud Computing using Cryptographic Algorithms" [1] they used RSA and DES, we'll use RSA, DES and AES to provide more security.

We have proposed a combination of three different security algorithms to eliminate the security challenges of Personal Cloud Storage. We have taken a combination of algorithms like: DES, AES and RSA. DES (Data Encryption Standard) is a symmetric key algorithm, in which a single key is used for both encryption/decryption of data. RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. AES (Advanced Encryption Standard) is a symmetric key algorithm, in which same key is used for both encryption and decryption.

The proposed system is designed to maintain security of text files only. The proposed system design focuses on the following objectives which are helpful in increasing the security of data storage.

1) 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.
2) 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.

To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task.

The Block Diagram of proposed work at multilevel Encryption: -

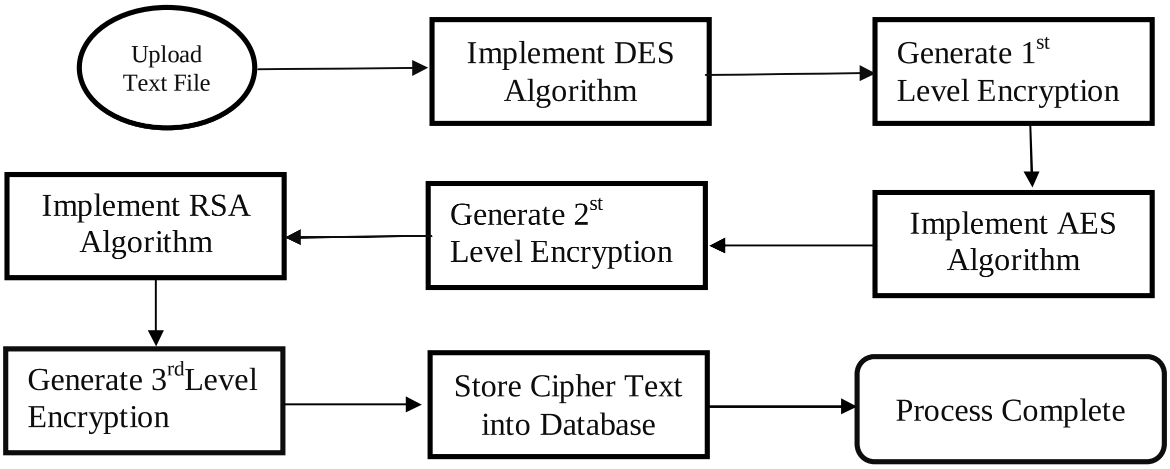
Upload Text File
Implement DES Algorithm
Generate 1st Level Encryption
Implement AES Algorithm
Generate 2st Level Encryption
Implement RSA Algorithm
Generate 3rdLevel Encryption
Store Cipher Text into Database
Process Complete

Figure 3: Block Diagram of Multilevel Encryption

According to Figure 3, Steps of Multi-level encryption will be:

1. Upload the text file.
2. Now implementation of DES Algorithm takes place. The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits ofcipher text. The actual key used by DES algorithm for encryption is 56 bits in length. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds [12]. The first level encryption is generated using DES algorithm.
3. Now apply AES algorithm on encrypted output of DES algorithm to generate second level encryption.
4. Now apply RSA algorithm on encrypted output of AES algorithm to generate third level encryption.
5. In RSA algorithm public key is used for encryption. RSA is a Block Cipher in which every message is mapped to an integer.
6. Once the data is encrypted using RSA algorithm, it will be stored in Database of Cloud Storage. And when downloading file inverse DES, AES and RSA algorithms are used to decrypt data.

The Block Diagram of proposed work at multilevel Decryption: -

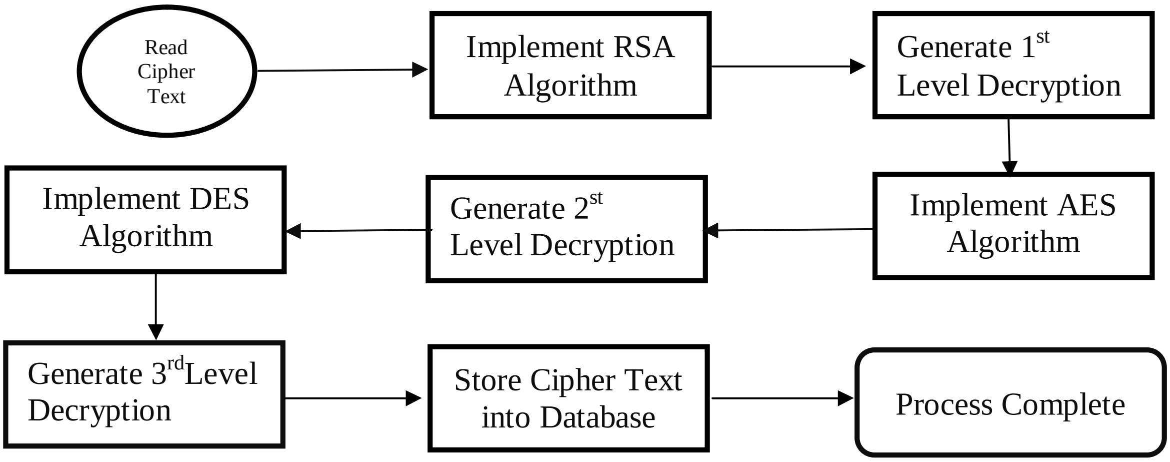
Read Cipher Text
Implement RSA Algorithm
Generate 1st Level Decryption
Implement AES Algorithm
Generate 2st Level Decryption
Implement DES Algorithm
Generate 3rdLevel Decryption
Store Cipher Text into Database
Process Complete

Figure 4: Block Diagram of Multilevel Decryption

In Our proposed System, implementation of the DES algorithm takes place to generate first level encryption. And then we apply the RSA algorithm to generate second level encryption and at last AES algorithm to generate third level encryption. And same process takes place for decryption using inverse DES, AES and RSA algorithms. Means we applied multilevel Encryption and Decryption to provide security for cloud storage data.

V. CONCLUSION

Cloud Computing can become more secure using cryptographic algorithms [1]. Cloud computing provides companies with new options for managing infrastructures and new business models. Cloud Computing is affected by data security, theft, loss of data and integrity. To prevent it we are using different level of cryptography algorithms. Cryptography is a single level encryption and cyber criminals can easily crack single level encryption. Hence, we repropose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage.

Multilevel encryption is already present, so we are adding extra security level in it. In this, unauthorized user can't use the data easily. We introduced three level of security level that is RSA, DES and AES algorithms. It is more powerful then single level encryption.

REFERENCES

1. 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
2. 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
3. Nidhi Dahiya, Mrs. Sunita Rani, "Cloud Computing Security: A Review", IJEDR, ISSN: 2321-9939, Volume 5, Issue 3, January 2017
4. 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
5. 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
6. Priyanka Arora, Arun Singh, Himanshu Tyagi, "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
7. Sajjad Hashemi, "Data Storage Security Challenges in Cloud Computing", International Journal of Security, Privacy and Trust Management, Vol 2, No 4, August 2013.
8. 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
9. Atul Kahate ―Cryptography and Network Security‖ Tata McGraw-Hill.
10. Ujjwal Karna, Gudlanarva Sudhakar, Dr. S Durga Bhavani, "Data Storage Security in Cloud Computing: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 7, Issue 1, January 2017
11. Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, 2012.
12. G. Devi, M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, 2012.
13. Rashmi Nigoti, ManojJhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, March-May 2013. 12