An Integrated Triple Type Security System in Cloud Computing

E. Ravi Kumar, S. Sai Satyanarayana Reddy, M. Babu Reddy

Abstract*: *Cloud computing is most widely used in many companies now a days. Cloud means services available and provided in the web. Security plays a major role in cloud computing to store the various forms of data. Providing quality of security for the cloud storage data is very important. Many cloud providing service companies takes various steps to secure the data. In this paper, the integrated triple type security system is provided for the cloud data. The proposed three way security system provides the encryption to the data uploaded by the data owner and if the user wants to download the available data with encryption key sent by the data owner and decryption key sent by the cloud service provider then the verification of the user can be done by the cloud admin. In this way, the three way data security is implemented.

Index Terms*: *Security, cloud computing, Cloud Service Provider.

I. INTRODUCTION

Cloud is most widely used in many companies for data storage, infrastructure support is provided by the cloud. Reliability is one of the important tasks should be considered by the cloud. Security is one aspect of cloud storage for various formats of files.

To warranty data security, the study of new methods and advancements that can record episodes, grow new guidelines of data security. Specifically, it winds up hard to recognize who is in charge of what, as distributed computing is a foundation fundamentally unique in relation to the conventional model and can be powerfully changed. It ought to be noticed that there is a mental part of this issue. IT outsourcing has not yet gotten such advancement in India as in the West, and numerous administrators are distrustful about exchange of IT foundation administrations to an outside master.

The accompanying conditions must be seen to guarantee dependable security in cloud administrations:

1. Cryptographic strategies for information wellbeing ought to be utilized. Every one of the information that the customer is running inside the administration ought to be safely encoded.

2. The very procedure of exchanging data from the customer and the server should likewise be protected, it is important to utilize a safe information exchange conventions to get to the server..

II. RELATED WORK

From the many references, AES is faster and efficient among the symmetric algorithms [1]. All these algorithms used to transmit data with the encryption and decryption with the various symmetric key methods. High security is provided for the data in cloud storage and key transfer is the issue in symmetric algorithms. From the many experimental results, based on the file format of the storage concluded that DES algorithm takes very less time for data encryption and AES algorithm will take less usage of memory and the time of encryption is very low in case of AES and DES algorithm [2]. RSA will take an outstanding quantity of calculating the resources such as CPU time, memory, and battery power. Among the two existing algorithms, RSA solves the various issues such as key agreement and key exchange produced in secret key cryptography. This will not solve the issue [3]. The Existing algorithms will differ from each other in various features. RSA will not be used for commercial purposes. Using various variables to create the key then the process of encryption becomes weaker and anyone can decrypt the file with random probability theory (RPT) and side channel attacks (SCA) [4]. In DES, if the file size is high the encryption time will take more and performance will be reduced.

Centralized Cloud Data

There is not at all like conventional systems which leave archives and other data information spread calmly between representative work stations, information inside the cloud is unified. Since distributed computing suppliers are ordinarily held to excessively higher principles than in house IT security groups, this regularly implies the information is more secure than individually organize [5]. This information is gotten to just through web programs which can be set to clear their store every single time they are shut. Take this in examination with conveying an email, for instance: The email with connection is dispersed to n number of representatives who are relied upon to use the data appropriately then dispose of or resend it. On account of distributed computing – no information would be sent to the staff individuals. They would have the capacity to sign on to one focal area, see the information, roll out an improvements they required helpfully, at that point log out – all without really downloading the data.

Distributed Cloud Security

Revised Manuscript Received on July 09, 2019

E. Ravi Kumar, Research Scholar, Dept of CSE, JNTUK, Kakinada,India.

S. Sai Satyanarayana Reddy, Dept. of CSE, Vardhaman College of Engineering,Hyderabad, India.

M. Babu Reddy, Dept. of CS, Krishna University, Machilipatnam, India.

Up until now, there has been no real infringement of cloud security. Contrast this and private systems, in which there are various stories each seven day stretch of ruptured information or stolen customer machines [6]. A bunches of individuals are worried about the security in a distributed computing setup. Individuals are accustomed to imagining that something in their control is more secure than if it is out in the open. Despite the fact that that appears like presence of mind, it just isn't valid. Every associated organize are 'out in the open'. Distributed computing basically gives less opportunities to get to that information by its extremely plan.

Security

Security is provided for sensitive data. The purpose of security is to maintain the confidentiality of the data provided by the cryptography and this will hide the original data for unauthorized users. Various components of cryptosystem are followed:

Plaintext: This is in the form of simple text and data is secured during sending and receiving a point of storage.

Cipher text: This can't be in a readable format after encryption.

Encryption Algorithm: This is the mathematical process to convert simple text to ciphertext.

Decryption Algorithm: This is used to convert cipher text to plaintext.

Encryption Key: This will be generated by the selected algorithm to convert simple text to ciphertext.

Decryption Key: This key is used by the receiver with an algorithm to convert the cipher text to simple text.

Encryption Algorithms for Cloud Security Encryption algorithms have vital role in the field of cloud security. Many algorithms are available for cloud security. Most useful algorithms for cloud security are discussed below.

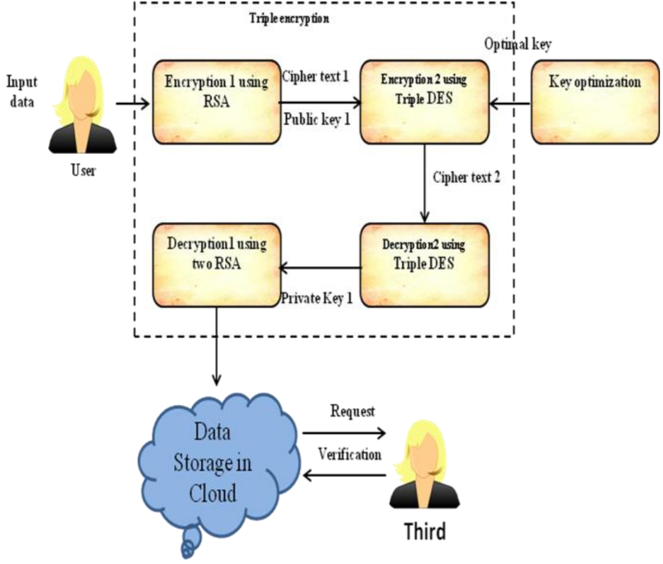

Figure: 1 Flow Diagram

1. Data Encryption Standard (DES)

DES is the encryption algorithm which is utilized to provide encryption for them to the various types of data. This will provide a single key for encryption and decryption. The functionality of DES operates on blocks of 64 of data with 56 bits key. The size of the round key is 48 bits [7].

Any format of data is divided into blocks of 64-bit size and the last block is filled if required. Many probabilities are used to increase the tedious of performing the cryptanalysis on the cipher. This algorithm consists of two permutations (P-boxes) and sixteen Feistel rounds. This functionality is divided into three stages. The initial permutation is the first phase and final permutation is last stage.

2. <u>Triple DES</u>

This is a continuation of the traditional DES algorithm. In the current industry, triple DES is the most recommended system which is widely used the symmetric algorithm.This algorithm uses three personal keys with 56 bits each. The overall key length is 168 bits but it is known that 112-bits are enough. This algorithm manages to make dependable hardware encryption answer for various industries.

1.) The plaintext is rearranged in 64-bit. This will not use any keys.

2.) In the second stage, 16 fiestel rounds and every round use various 48-bit round key applies to the plaintext and produce a 64-bit result. This process will work according to the algorithm [8].

3.) The final permutation performs the reverse operation in early permutation and the output is 64-bit ciphertext.

3. Rivest-Shamir-Adleman (RSA)

The most famous and powerful asymmetric key cryptographic algorithm. This algorithm utilizes a completely different data size and different size keys. It's deviated keys for each cryptography and decipherment. It utilizes 2 prime numbers to provide individuals generally and personal keys. These 2 distinctive keys area unit used for cryptography and unscrambling reason. This calculation is comprehensively organized into 3 phases; key age by utilizing 2 prime numbers, cryptography and decipherment [9].

RSA nowadays is used in several programming things and may be utilized for key trade, computerized marks, or cryptography of very little squares of data. This calculation is preponderantly used for secure correspondence associated verification upon an open correspondence channel whereas contrastive the presentation of RSA algorithm and DES and DES, after we utilize very little estimations of p and letter of the alphabet (prime numbers) area unit chosen for the structuring of key, at that time the cryptography procedure seems to be to a fault feeble and one will presumably decipher the data by utilizing discretional chance hypothesis and facet channel assaults. nonetheless within the event that massive p and letter of the alphabet lengths area unit chosen, at that time it expands over time and therefore the presentation gets debased in examination with DES [10]. Activity speed of RSA cryptography calculations is a moderate distinction with interchangeable algorithms, conjointly it is not verified than DES.

III. HOW TO IMPROVE CLOUD COMPUTING SECURITY

Computing is essentially new if contrasted with the customary in house IT offices, there completes have a tendency to be a deficiency of institutionalization on security issues[11]. A oads of surely understood organizations like Hewlett Packard, IBM, ESDS eNlight Cloud,
and others are starting to

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

contribute in security programs. By its extremely plan and inside the utilization of ordinary safety efforts, for example, encryption, distributed computing security is truly not a hindrance to enter any more. In many trials it turns out to be similarly as secure if not more so than typical in house information systems [12]. As time pushes ahead, the numerous advantages in-worked to distribute computing will guarantee that it remains the focal point of the IT security industry.

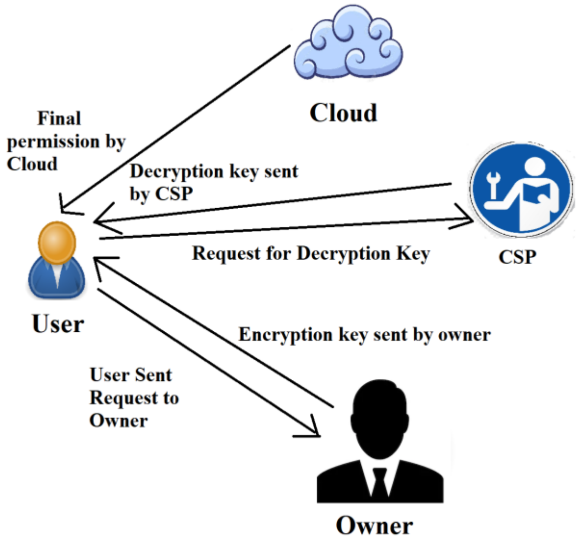
Cloud
Final permission by Cloud
Decryption key sent by CSP
CSP
Request for Decryption Key
User
Encryption key sent by owner
User Sent Request to Owner
Owner

Figure: 2Triple based security System

The following steps to implement the proposed algorithm

Table 1: The performance of proposed model

File size (kb)	Encryption time (ms)			Decryption time (ms)			Execution time (ms)	memory
	RSA	Triple DES	Triple Based Encryption	RSA	Triple DES	Triple Based Encryption		
10	1154	1198	1120	1145	1042	1021	10155	118454
20	1205	1187	1211	1213	1187	1131	11544	124848
30	1278	1214	1241	1254	1205	1178	12359	140087
40	1391	1356	1332	1321	1297	1278	13145	151544

- Data owner (DO) uploads the file f.
- The data is encrypted and key is generated with RSA.
- Again the key is generated with TripleDES and data is encrypted.
- Calculate the encryption time for all the 3 secure algorithms.
- If user wants the key- the user sends the request the DO.
- And also the user has to take permission from Cloud Admin (CA).
- For every request the key is received by the user's mail if DO and CA send the requested key.
- The final encryption is done at the cloud service provider (CSP).
- The CSP encrypts the data and generate the key with TripleDES algorithm.
- For the receiving of the accessing of data mail id of the registered user is used for data accessing.
- Calculate the decryption time for all the 3 secure algorithms.

IV. RESULTS:

In this paper, the implementation is done by using NETBEANS 8.0.2 and JDK 1.8 and MySql 5.7 for the better results. Here some of the functionalities are provided for the accessing of data and giving permission to download the data. Authentication (data owner, user and key authority), Key Generation for the data, Encryption, Decryption and to access the data by the user the secured key should be given by the data owner [13]. This will be done by the internal key generator which gives the permission through the key authority. The key should be send by the cloud admin (key authority) to access the needful data or files.

Authentication

In cloud computing, the storage of the data is done by the authenticated data owners. In this paper, especially data owner and user should authenticate by the cloud admin [14]. This is called as two way security. It is very important that every data owner and also user need to authenticate the system to get access the data available in cloud storage. Every user and data owner should give the exact email and details.

Access Control:

In cloud storage, the access of the data is done by the users. Access control on data mostly very difficult task to get the data access.

Key Generation:

At the data owner point of view the DO needs to upload the files and generate the key for the uploaded file. This is the encryption key for the encrypted data.

Decryption:

The data decryption is done based on the key send by the DO to the user and also the permission should be given by the DO [15].The table appearing below illustrates the file size value of our proposed study; here each file size in kb. Table.1 reveals the time for encryption and decryption for both two fish and OMD5 algorithm. Table.1 is tabulated in the below section,Table 1 demonstrates the performance for proposed model i.e. encryption time, decryption time, execution time and memory. When the file size is taken as 10, the encryption time for RSA is 1154ms, for Triple DES is 1198ms. The decryption time for RSA is 1021ms and for TripleDES is 1042ms. The execution time is 10155ms and for memory are 108454bits. When the file size is taken as 20, encryption time for RSA and Triple DES is 1187ms, 1211ms. And the decryption time for RSA and TripleDES is 1187 & 1213ms. Similarly, for file size at 30 and 40, the encryption, decryption time, execution time and memory are calculated.

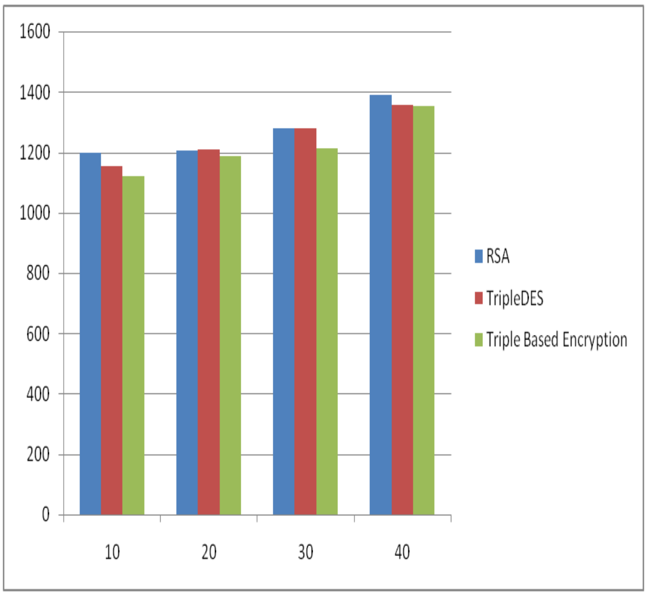

Table: 1 Encryption Time (Sec)

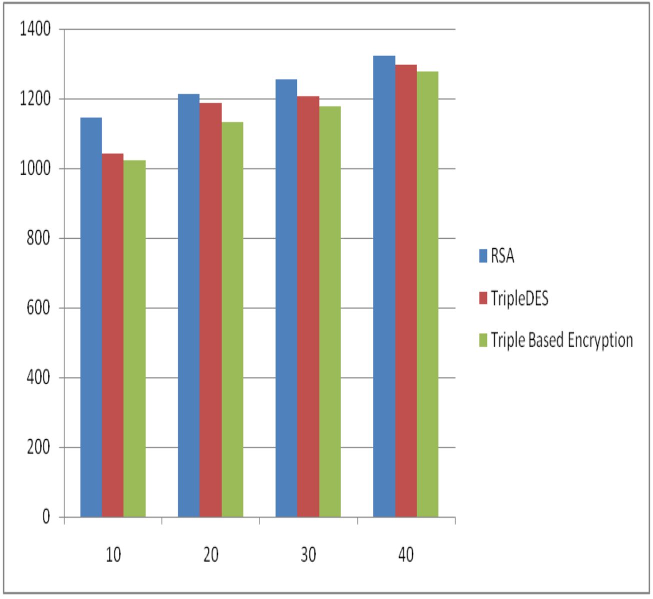

Table: 2 Decryption Time (Sec)

3. Conclusion

In this paper, the integrated triple type security system (ITTSS) is provided for the cloud data. Based on the roles and access permissions to the users the secure data stored and access according to the permissions given to read the data. The proposed system ITTSS secured method to secure sensitive data. After making the experiments on various encryption and decryption algorithms the proposed ITTSS is most performed algorithm for securing the data in the cloud. Using the 3-secret keys with the triple integrated system provides high security and less encryption time.

REFERENCES

1. Shraddha Soni, Himani Agrawal , Dr. (Mrs.) Monisha Sharma, “Analysis and Comparison between AES and DES Cryptographic Algorithm”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012
2. Shashi Mehrotra Seth, Rajan Mishra, “Comparative Analysis Of Encryption Algorithms ForData Communication”, IJCST Vol. 2, Issue 2, June 2011
3. Aman Kumar, Dr. Sudesh Jakhar, 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
4. Gurpreet Singh, Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, International Journal of Computer Applications (0975–8887) Volume 67–No.19, April 2013
5. Rijndael.Advanced Encryption Standard (AES). FIPS. November 23, 2001. http://csrc.nist.gov/publications/fips/fips197/fips197.pdf
6. Hesham Darwish, “ Avanced algorithm design and analysis”.
7. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attributebased encryption for fine-grained access control of encrypted data,” in Proc. Of CCS’06, 2006.
8. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,“Scalable secure file sharing on untrusted storage,” in Proc. of FAST’03, 2003.
9. M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. of EUROCRYPT ’98, 1998.
10. D. Boneh, X. Boyen, and E.-J. Goh, “Hierarchical identity based encryption with constant size ciphertext,” in EUROCRYPT (Lecture Notes in Computer Science), vol. 3494. New York, NY, USA: Springer- Verlag, May 2005, pp. 440–456.
11. C. Gentry and A. Silverberg, “Hierarchical ID-based cryptoraphy,” in ASIACRYPT (Lecture Notes in Computer Science), vol. 2501.New York, NY, USA: Springer-Verlag, 2002, pp. 548–566.

AUTHORS PROFILE

E Ravi Kumar (Eswanadula Ravi Kumar) obtained his Bachelor’s degree in Computer Science and Information Technology from Jawaharlal Technological University, Hyderabad. Then he obtained his Master’s degree in Computer Science and Engineering from Pragati College of Engineering, JNTUK and presently pursuing Ph.D. in Computer Science and Engineering majoring in Cloud Computing from **JNTUK, Kakinada**, Andhra Pradesh, India. Currently, he is working as Assistant Professor of Information Technology, Vardhaman College of Engineering, Hyderabad, and Telangana, India

Dr.S.Sai Satyanarayana Reddy (Seelam Sai Satyanarayana Reddy) received the B.E. degree from the Shivaji University, Kolhapur, Maharashtra, India, the M.E. degree from the Bits Pilani, Rajasthan, India, and the Ph.D. degree from the Bharat University, Chennai, India in 2008. From 2008 to 2014, he worked as Professor in LakiReddy BaliReddy College of engineering, Mylavaram, Andhra Pradesh,India. He is currently working as Principal in Vardhaman College of Engineering, Hyderabad, and Telangana, India. His research interests are in Data mining and data warehousing, cloud computing. He received "VIDYA RATAN" Award from the Economic for Health and Educational Growth:,New Delhi for “ Excellence in Chosen field of activity”.

Dr.M.Babu Reddy (Mukkala.Babu Reddy) received the B.Sc. degree from the Nagarjuna University, Guntur, and Andhra Pradesh, India in 1996, the MCA. degree from Nagarjuna University, Guntur, Andhra Pradesh, India in 1999, and the Ph.D. degree from Nagarjuna University, Guntur, Andhra Pradesh, India in 2010. From 2010 to 2013, he worked as Lecturer-Incharge, SCNR Govt College,Proddutur,YSR dist,Andhra Pradesh ,India. He is currently working as Associate Professor in Krishna University, MachiliPatnam, and Andhra Pradesh, India. His research interests are in Data mining and data warehousing, cloud computing.