IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Secure Storage and Replication using Hybrid Cryptographic Algorithm for Cloud Environment

Arpit Agrawal[1], Sakshi Joshi[2*]

[1]Computer Engineering, Institute of Engineering & Technology, DAVV, Indore, India
[2]Information Technology, Institute of Engineering & Technology, DAVV, Indore, India

Corresponding Author: sakshijoshi888@gmail.com, Tel.: +91-8819022551

Available online at: www.ijcseonline.org

Received: 21/07/2018, Published: 31/July/2018

Abstract—Cloud is the technology which works on distributed and shared environment, with sharing memory, resources, services, virtual infrastructure and platform. This all services can be accessed through internet. However, with several advantages cloud also provides with the disadvantage of security and privacy. Public network and publically access makes cloud insecure from intruders. Sensitive data of cloud is at the big risk because of security threats like attack, man-in-middle, eavesdropping etc. Cloud stores files in a file system with reliable storage of file on the basis of local file system. This storage of file is stored in different computers and thus called as servers which can be accessible to other computers, these are clients. Existing work only deals with achieving confidentiality with not concentrating on integrity and privacy of data at the time of storage. Proposed work achieves user's trust and improves trust on cloud service provider. Architecture for security service is implemented for secure and safe storage of data using web services and technologies.

***Keywords*—** ECC, RC6, Storage, Replication, Cloud environment.

I.INTRODUCTION

Cloud computing provides with the distributed environment, as it is a popular and widely used technology. It serves with key resources and applications related to web based. It works on virtual and parallel computing with providing distributed environment. On demand resources are provided efficiently and effectively through different models like service models and deployment models. Cloud not only provides services but also serves with packages. Only the essential thing with which cloud can be accessed is internet. Cloud based services are formed which is service oriented. Software and hardware are not limited to access in cloud and also not limited to other technologies. Cloud serves with many advantages like it is cost effective and can easily be accessed with high cost device. On the basis of need services are provided to large number of user.

Large amount of investments are done by enterprises to serve users with the cloud services.

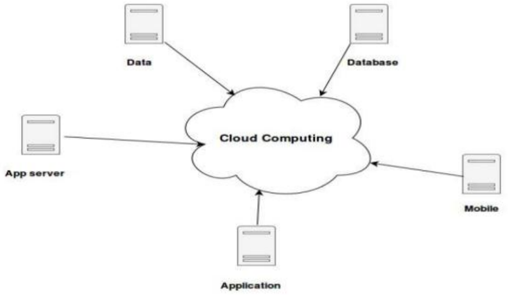


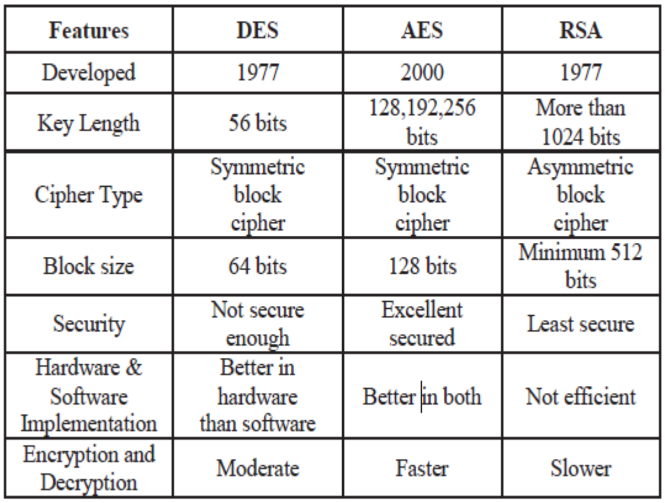
Figure 1. Cloud Computing

II. RELATED WORK

Study of base paper with diagram:

Babitha. M.P and K.R. Ramesh Babu." In[1] address about data security and privacy in cloud environment for the protection of sensitive data. As we know that cloud share distributed resources through network in an open environment, which helps user to access their data from anywhere at any time. Due to open environment issues like privacy and security exists and author proposed this in his paper. Different security services are provided in this paper like confidentiality, authentication, data access etc. with monitoring and managing in delay. Author used AES encryption algorithm for high security of data and confidentiality.

TABLE I. COMPARATIVE ANALYSIS BETWEEN AES, DES AND RSA



Features	DES	AES	RSA
Developed	1977	2000	1977
Key Length	56 bits	128,192,256 bits	More than 1024 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher
Block size	64 bits	128 bits	Minimum 512 bits
Security	Not secure enough	Excellent secured	Least secure
Hardware & Software Implementation	Better in hardware than software	Better in both	Not efficient
Encryption and Decryption	Moderate	Faster	Slower

III. PROBLEM DOMAIN

With the increase in growth of cloud computing some of the problems also arises and this issues needs to be overcome with the changing trends. Large networks are interconnected because of the wide use of services and resources by users. Security is the important term for storage purpose and accessing of data become easy. Security for server and user in cloud is also essential. Security features like authentication, confidentiality and availability. Authentication explores that the user is valid user or not, with no interference of any intruders. Trust between user and service provider is necessary to transfer information.

Data lost can be possible and is at great risk in prospect of security and attackers. For achieving trusted relationship between client and server, security is required.

Limitations of existing work are as:

- Encryption solution becomes less for the purpose of safety storage.
- Replication of data may lead to high availability of data with inconsistency cost.
- If wants to maintain consistency then problem of data traffic can be in advanced way with security also.
- To control replicated file a best solution is provided with reduced traffic and maintain g integrity.
- ECC is more secure than RC6 and AES is more less secure than RC6.
- AES also faces issue of memory overhead.
- Data storage safety is also a big solution.
- In improvement of performance and access time, replication plays an important role.
- For the purpose of safe and easy access of storage, secure replication is required.

IV. PROPOSED SOLUTION

A. System Architecture*:*

System architecture of the complete work can be defined through the below diagram. Below following steps show security during storage.

- On cloud server text file is uploaded as upload service.
- First of all, message digest is calculated of the complete file which measures the integrity of data.
- Complete file is then encrypted using RC6, to serve with first level security.
- After it, the encrypted data which is in ciphered form is divided into chunks which are a block cipher encryption.
- After it ECC algorithm is applied on every ciphered block for second level encryption.
- Distribution and replication are used which replicates ciphered file and store it on multiple location.
- Similarly, decryption steps are performed for the purpose of downloading file.

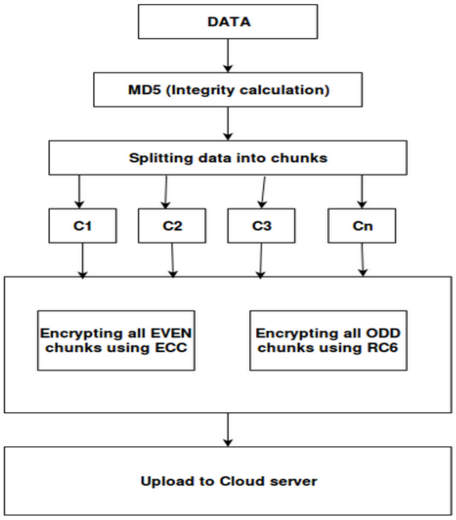

DATA
MD5 (Integrity calculation)
Splitting data into chunks
C1
C2
C3
Cn
Encrypting all EVEN chunks using ECC
Encrypting all ODD chunks using RC6
Upload to Cloud server

Figure2: Proposed Solution

B. Methodology

The methodology used in our work concludes RC6 and ECC algorithm.

1. RC6: RC6 is the Rivest Cipher 6 cryptography derived from RC5, which is a symmetric key block. It is designed to meet the requirements of AES. It supports the block size of 128 bits with wide variety of key size and word length. It is similar in structure to RC5. RC6 performs both the encryption and decryption on data for the purpose of security.

2. ECC : ECC is the Elliptic Curve Cryptography which is researched by Miller and Kibitz. ECC is the public key cryptography. Here, in symmetric key cryptography key is shared between sender and receiver.

It is based on the key cryptography that is the public key cryptography. It is based on sharing of keys, it consists of two keys, one is public key and the other is private key. This algorithm is used in many applications, which is described further in details. With the symmetric key cryptography public key comes in frame. One key is shared in symmetric key cryptography between sender and receiver. Drawback in symmetric key is the compromising of key in between. That is why public key cryptography is in frame, factorization problems arise in integer form.

V. IMPLEMENTAION PLAN

Implementation view of the complete project can be viewed through some of the implementation snapshots which are cited below:

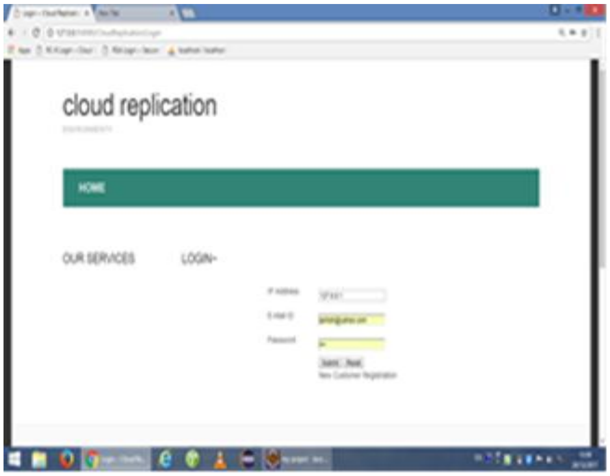


Figure3: Login Page

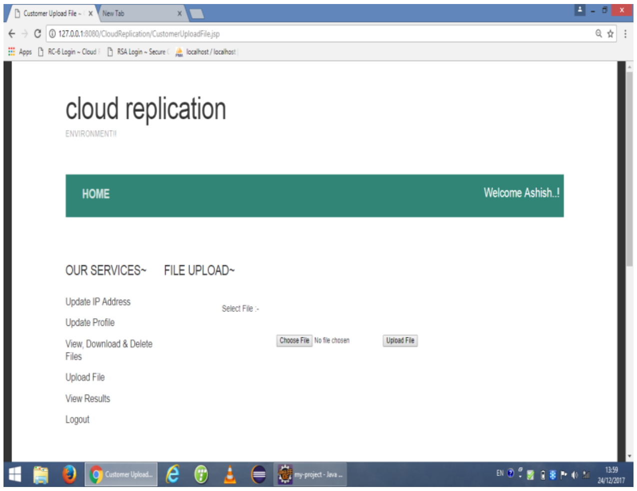


Figure4: Home Page

VI. RESULT

The Proposed system of an online file uploading application. Any can access the application from anywhere at any time over internet.JAVA and JSP are the programming languages used this application. Graphical user interface was created with HTML.Fig.3. shows overall system architecture and activities in proposed model. This application is archived security principal Authentication, confidentiality and integrity. We use MD5 for checked integrity of file. We show the result tables and graph for existing and proposed work.

The proposed result shows the variation in computation time between the existing approach and the proposed approach.

Table 1: AES Computation Time (existing work)

.

File Size (KB)	AES Computation time MS
6	1000
25	850
128	250
108	60
247	76
694	142

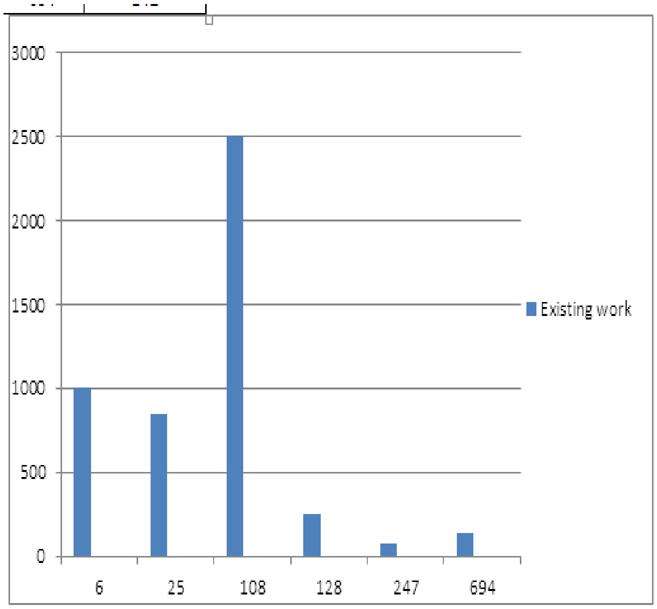


Figure 5: Graph for Existing Work

Table 2: Hybrid Computation Time (Proposed work)

File Size (KB)	**Hybrid Computation time MS**
6	6.27
25	28.81
128	152.91
108	128
247	294
694	829

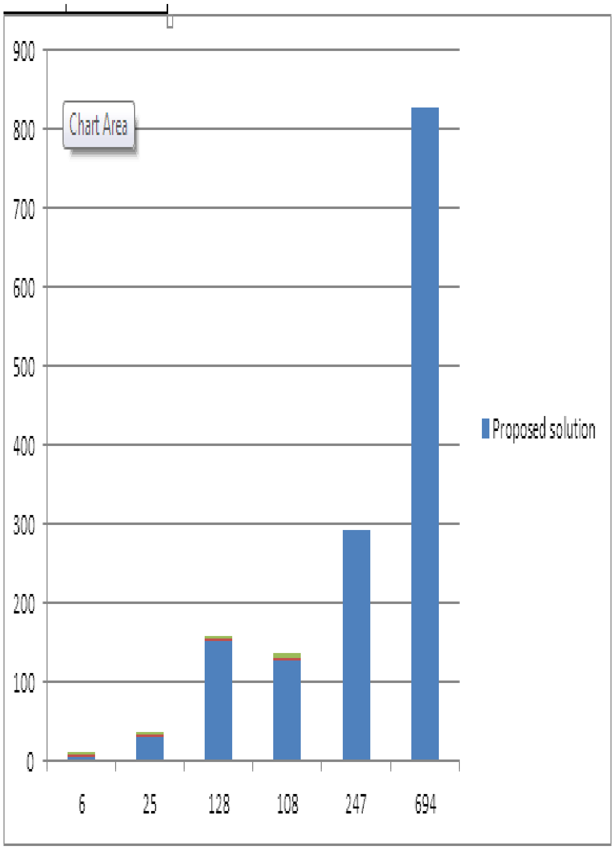


Figure6: Graph for Proposed Work

Table3: Table comparison graph shows computation time is reduced in the proposed work as

File Size(KB)	**AES Computation Time micro sec**	**Hybrid Computation Time micro sec**
6	1000	6.27
25	850	28.81
108	2500	128
128	250	152.91
247	76	294.25
694	142	829.12

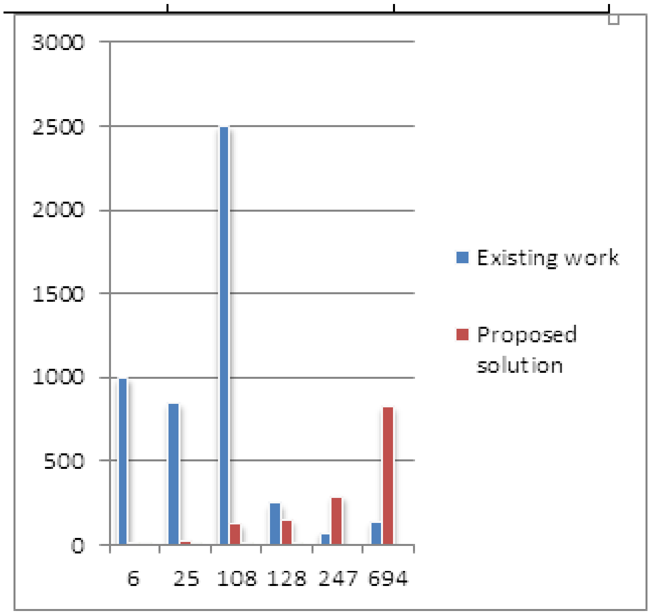


Figure 7: Comparison Graph for Proposed Work and Existing Work

VII CONCLUSION

Cloud stores files in a file system with reliable storage of file on the basis of local file system. This storage of file is stored in different computers and thus called as servers which can be accessible to other computers, these are clients.

Proposed work achieves user's trust and improves trust on cloud service provider. Architecture for security service is implemented for secure and safe storage of data using web services and technologies. The demand of security in cloud based architecture is always wanted and analysis is performed in our work also to achieve it. In this activity the security feature which is mainly cantered is confidentiality.

REFERENCES:

[1]. Babitha.M.P and K.R. Ramesh Babu," Secure Cloud Storage Using AES Encryption" published in International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT),International Institute of Information Technology (I²IT), Pune 2016.

[2]. Prof. Vishwanath S. Mahalle, "Implementing RSA encryption algorithm to enhance the data security of cloud in cloud computing", International journal of pure &amp; applied research in engineering and technology, 2013, volume (8):220-227, ISSN-2319- 507X IJPRET.

[3]. (U.S.) Nicholas. Carr, fresh Yan Yu, &quot;IT is no longer important: the Internet great change of the high ground - cloud computing,&quot; The Big Switch:Rewining the World, from Edison to Google, CITIC Publishing House, October 2008

[4]. Jin-Mook Kim and Jeong-KyungMoon," Secure Cloud Storage Using AES Encryption" published in International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT),International Institute of Information Technology (I²IT), Pune 2016.

Authors Profile

Mr Arpit Agrawal acknowledged his B.E degree in 2006 and M.E degree in 2011 both in Computer Engineering.At present he is Sr lecturer in Computer Engg department at IET-DAVV university.His research interest comprises Information Security and Machine Learning.

Mrs. Sakshi Joshi received the B.E. degree in 2016 from Institute of Engineering & Technology DAVV, Indore, M.P. and M.E.(Information Technology) wih Specialization Information Security in 2018from IET DAVV, Indore.