International Journal for Rapid Research in Engineering Technology & Applied Science
Vol 6 Issue 10 October 2019
ISSN Online: (2455-4723)

Hybrid Security Model for Secure Communication in Cloud Environment

Aaradhana Sonakiya*
Student
BM college of technology
Indore, M.P.
aaradhanasonakiya@gmail.com

Mohit Jain**
Assistant Professor
BM college of Technology and Science
Indore, M.P.
bmctmohitcs@gmail.com

Abstract

Cloud computing is probably the best developed technology to cater services & resources in every possible corner. Applications are delivered to users with easy of access & at very low cost. The vulnerability of such applications are high, as they are placed on public servers and uses open infrastructure, making them prone to fabricate or leak information to hackers. To main authenticity of services & information, security is the primary requirement. In this research paper, we will focus on the weak status of security in cloud computing system and concentrate on enhancing safety & privacy within the application, come up with a security model which reduce the security overhead too. To ensure integrity, MD5 algorithm has been deployed with a combination of RC6 & ECC, which separately provides confidentiality over communication. A cloud-based application is kept under test on internal cloud server to investigate this whole research work. The proposed solution is checked on the parameters of computation time so that the performance can be evaluated. This work discusses about the common issues and compare the different already existing solutions.

Keywords: RC6, ECC, Cloud Computing Application

1. Introduction

Cloud computing is a platform technology which configures various resources and share them around all the corners via internet. Server capabilities are enhanced in terms of storage and computation. In simple language, cloud computing creates a pool of resources which distributes and share services with desired multiple

computing machines powered with hardware & software. Due to the nature of shareability, cloud computing is always ready to expand as per convenience, change as per trend & very cost effective.

Security is a feel of freedom, freedom from all the potential threats and possible hacks going around. Most of the time, attackers hit where the security is less, let it be at sender level, or at storage or during the communication. To keep the hackers off and avoid the unauthorized access, security best practices and algorithms are been used. This research paper discusses about how to enhance both performance & security of the cloud computing system, and for that we have proposed a security model. This work is tested on the basis of computation time & implemented using Java applications. To provide an even better data safety during communication, this work uses two different encryption approach.

2. Cloud Computing

There are 4 ways in which the cloud computing can be distributed, and those are:

1. **Public Cloud:** This kind of cloud system is the most in-use thing of today's world. Best thing about this technique is that this is accessible both from outside and inside the premises, even you can enjoy full access no matter where you are situated or roaming, all you need is an internet connection. Internet connection is the basic requirement for the communication between the cloud users & cloud servers. Being situated on a public platform and using open infrastructure, this technique is prone to get attacked easily by the cyber-hackers, who can fabricate or leak private data by exploiting the public network vulnerabilities. The lack of security leads to potential danger for users and surely is a privacy concern.
2. **Private Cloud:** This cloud is designed to serve only a particular organization or business, that means no outsider can share data or access services on this cloud at any point. It surely keeps the data security better than public cloud, but the demerit of this technique is that it takes whole lot of efforts to alter scalability. Also, this is purely in-house system, which makes it low in use.
3. **Hybrid Cloud:** It is a fusion of private & public cloud and accessible from both outside and inside as per the requirement.
4. **Community Cloud:** This particular cloud is framed for developer's community especially but widely used for social use as well.

Cloud computing applications are developed to be shared and used at every corner. The pyramid of cloud computing is distributed into 3 parts top to bottom, and those are as follow:

1. **Infrastructure as a Service [IaaS]:** This service model integrates various small hardware machines and make them act like a single powerful machine. This structure shares storage, services and computation from the hardware to all deployed applications according to decided policies and protocols.

2. **Platform as a Service [PaaS]:** Server software turns shareable with full access to all the machines and operating systems through this service model.

3. **Software as a Service [SaaS]:** With the help of Restful web service of SOAP services, application software are made shareable and by using this SaaS service model, all famous mobile and web applications are been developed in the market.

A block diagram for demonstrating complete deployment and service model is shown in figure A.

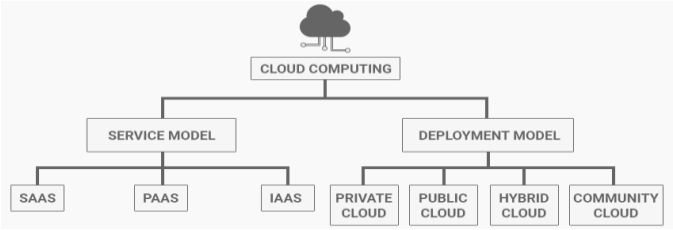

Fig. 1: Cloud Computing Deployment and Service Model

3. Data Security

Both cloud service and security threats go hand in hand. Cloud computing can turn into prey for reasons like eavesdropping, illegal invasion, and denial of service attack. Below are some data security threats:

1. **Confidentiality:** While public communication, confidentiality is the primary and most needed factor for the user to ensure them that their data is safe from fabrication and unauthorized usage. The data is converted from human readable content to non-readable by human format with the help of data encryption & decryption, this whole concept is called cryptography. Overhead is the main demerit of this technique. The size plain text is increased too much which consume extra time to convert plain text into cipher one.

2. **Authentication:** This principle is introduced to allow the access only to the authorized user and deny any unauthorized attempt of access in the system, but the only demerit of this technique is that it takes validation time. We are already known to the fact that authentication needs some extra time to validate the access, hence this increases the starting time.

3. **Access Control:** This separates between the users and allow access only till the specific user is given permission. Majorly it classifies according to the role of the user and providing them the access only till there where they are assigned. In simple words, it keeps the record "**who can access what**".

4. **Integrity:** This feature ensures that the data coming from the sender end to the receiver end is original and not fabricated or got modified somewhere during the communication. It uses Integrity algorithms i.e. SHA-1 & MD5 to estimate the value of original content received from the sender end.

4. Existing System

Mahavir Jain et al. In [1] by using IDEA & DES proposed hybrid cryptography solution. To provide double level of security, they used symmetric key cryptographic technique.

P Shaikh et al. In [2] used a combination of blowfish & AES algorithm and proposed a hybrid approach to achieve confidentiality in data. Performance of algorithm is measured by using encryption & decryption time.

DivyaPrathana Timothy et al. In [3] chose RSA and blowfish algorithm, and proposed a common architecture based on them. It has been observed that the existing system claims to help in achieve confidentiality & integrity in the system, but it also increases unwanted overhead. Author used a secure hash algorithm to bring data integrity. Encryption & decryption, both steps are been followed in the existing work. Below is how the complete system work:

1. To provide safety & privacy at the time of transmission, the proposed solution uses encryption algorithm.

2. A secret key is taken in use to encrypt the plain text into cipher text.

3. For blowfish algorithm, a vast range of keys from 448bits to 1024bits are used in the work.

- For selected file encryption via secret key, Blowfish algorithm is taken in use.

- RSA encryption technique is applied to keep the secret key safe.

- To ensure safety of secret key and integrity of plain text, Secure Hash Algorithm (SHA) is used.

The complete work is demonstrated in figure B.

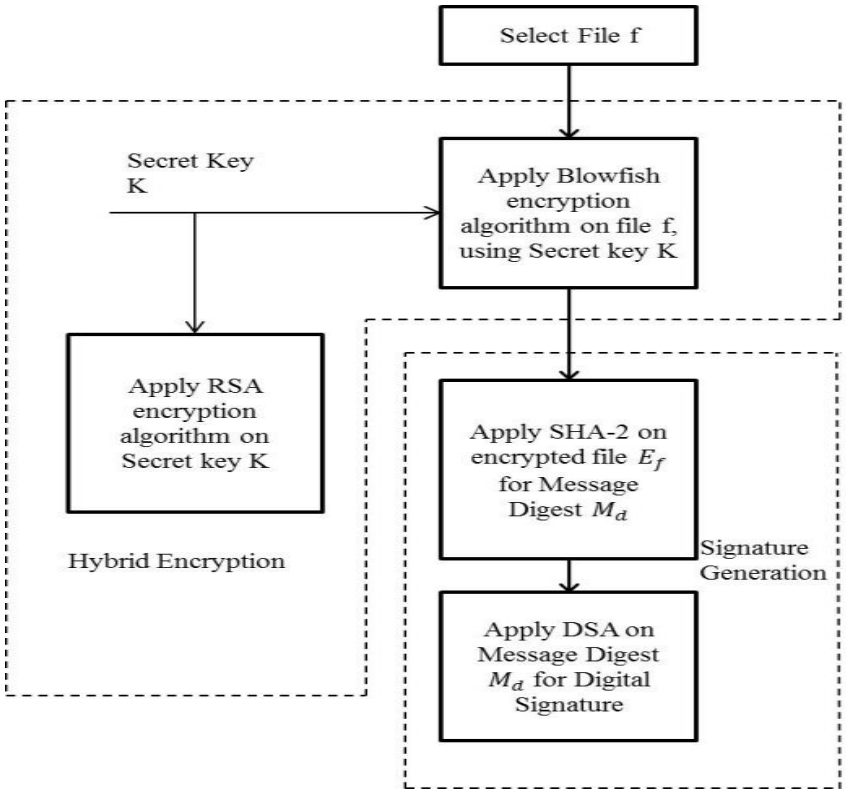

Fig. 2: Encryption Process of Existing Solution

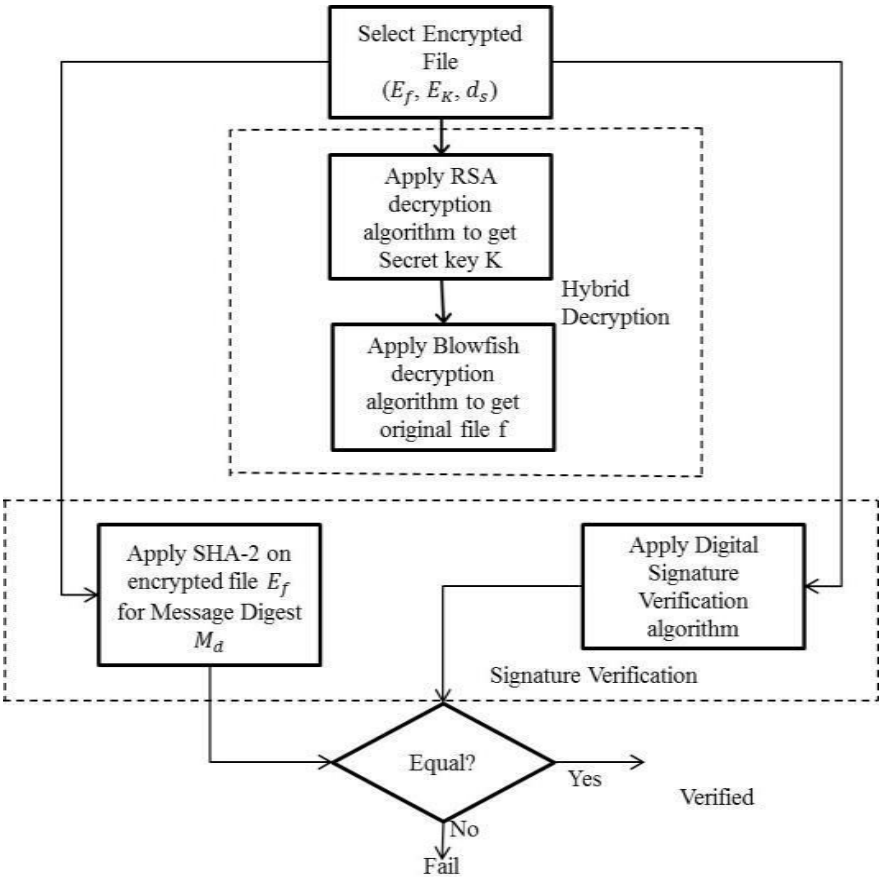

Fig. 3: Decryption Process of Existing Solution

5. Problem Statement

Cloud computing is all about taking the applications to the public network, where the user with granted access can make the use. The open nature of storage and usage of public infrastructure makes the whole system vulnerable to cyber-attacks. The same issue is been addressed in the existing work too. Multiple problems has been observed when studies were done on various related works, those are as under:

1. Low overhead & security is claimed by the symmetric key cryptographic algorithm but the issue of weak security is the major concern here.
2. In comparison to symmetric cryptographic technique, Asymmetric key cryptographic algorithm provides much better security, but it rapidly increases the overhead during communication.

3. The communication and encryption time is raised too much in the existing solution, as it uses DES, RC4, RSA and other such high computation time consuming algorithms.
4. As we talk about ensuring security for cloud computing, there is no web defined model introduced yet.
5. Single cryptographic algorithms are single layer protection only, which is not enough in itself and can be compromised.

6. Proposed Solution

This study of various existing solutions suggests that there the whole system is craving for a security model which is capable of providing all forms of security like integrity, access control & authentication, and not just encryption. The proposed solution design of security model is discussed under:

Security Principles	Security Algorithm
Confidentiality	ECC & RC6
Authentication	User Authentication
Integrity	SHA-1
Access Control	Role based access control

Table 1: Proposed Security model

Figure 4 has been designed to explain the complete process of encryption and decryption.

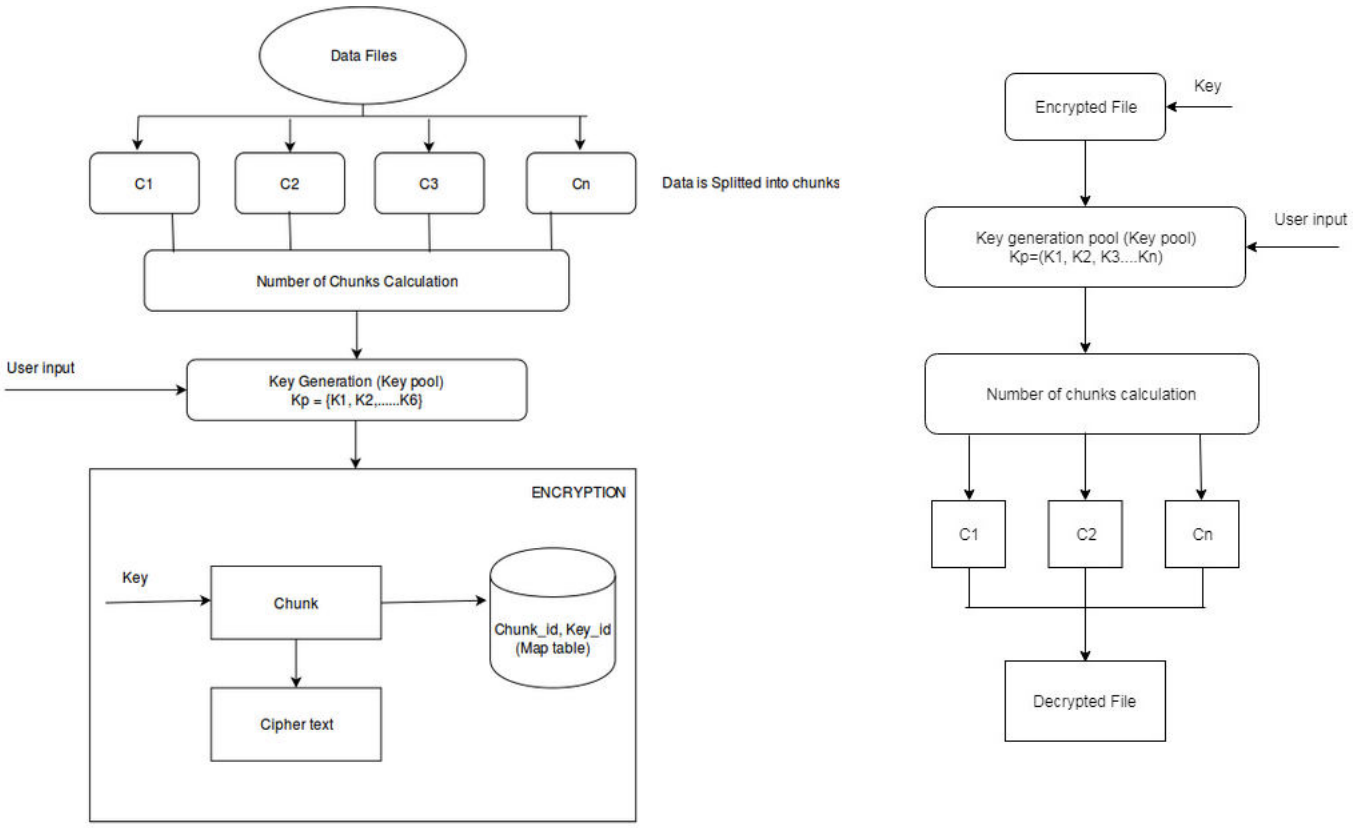

Fig. 4: Encryption and Decryption Process of Proposed Security Model

With the use of ECC, the proposed solution overcomes the limitation of base work. ECC eliminates all the complications in key management, and also reduces computation time & memory overheads, hence ECC replaced RSA. To increase the ease of access and storage capacity, Chunking has been added. Similarly, to enhance security level, RC6 is introduced too in the work.

7. Experimental Analysis

To evaluate the performance of proposed structure & in existing system, the proposed solution is been implemented as cloud application. Various RestAPI were developed to implement Software as a Service (SaaS) model and fixed in AWS instance. To achieve Internet as a Service (IaaS), the Amazon free instance was used with 1 GB RAM & 2 core processor, also to store data, MYSql database were setup. To evaluate the performance in different conditions, multiple data sizes were taken in use and complete work was evaluated based on time taken by computation. Comparison graph shows the complete work:

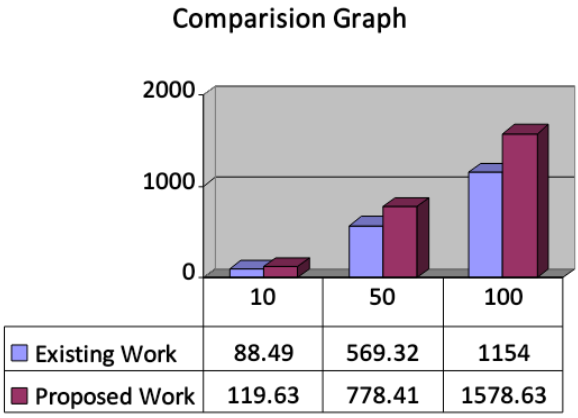

Fig. 5: Comparison of Existing Solution with Proposed Work in Total Computation Time

8. Conclusion

This study observes that to maintain authenticity of information and trust in services, security is very important. An attempt to investigate the security issues and develop a model which is capable of providing enhanced level of safety and privacy within the application, which eventually lower down the security overhead is taken in this research paper. The proposed solution measures computation time to evaluate the performance of the security model. The complete evaluation concludes that the proposed solution of security model is capable of decreasing the overhead issue, provide desired level of integrity and authentication and is much better alternative to the existing solution.

References

[1]. Mahavir Jain, and Arpit Agrawal, “Implementation of Hybrid Cryptography Algorithm”, International journal of Core Engineering & Management, Volume 1, Issue 3, pp. 1-8, June 2014.

[2]. P Shaikh, and V. Kaul, “Enhanced Security Algorithm using Hybrid Encryption and ECC”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 3, pp. 80-85, May-June 2014.

[3]. DivyaPrathana Timothy, Ajit Kumar Santra, "A Hybrid Cryptography Algorithm for Cloud Computing Security". International conference on Microelectronic devices, circuits and systems (ICMDCS), 2017, IEEE.

[4]. Ali E.TakiEl_Deen, "Design and Implementation of Hybrid Encryption Algorithm", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, pp. 669 673, December-2013.

[5]. R. K. Seth, RimmyChuchra and Simran, "TBDS – A New Data Security Algorithm in Cloud Computing", International Journal of Computer Science and Information Technology, Vol. 5, Issue

[6]. Jan Mohammad Najar, and Shahid Bashir Dar, "A New Design of a Hybrid Encryption Algorithm", International Journal of Engineering and Computer Science, Volume 3, Issue 11, pp. 9169 9171, November 2014.

[7]. Sherif El-etriby, Hatem S. Abdul-kader, and Eman M. Mohamed, "Modern Encryption Techniques for Cloud Computing", ICCIT, pp. 800-805, 2012.

[8]. HanumanthaRao.Galli and Dr.P.Padmanabham, "Data Security in Cloud using Hybrid Encryption and Decryption", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, pp. 494-497, October-2013.

[9]. Balkees Mohamed Shereek, ZaitonMuda, and Sharifah Yasin "Improve cloud computing security using RSA encryption with Fermat's little theorem", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 4, Issue 2, pp. 1-8, February-2014.

[10]. Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Vol. 1. Issue 2, pp. 06 12, December-2011.

[11]. Dr. NanditaSengupta, "Designing of Hybrid RSA Encryption Algorithm for Cloud Security", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 5, pp. 4146- 4152, May-2015.

[12]. Piyush Gupta and Sandeep Kumar, "A Comparative Analysis of SHA and MD5 Algorithm", International Journal of Computer Science and Information Technologies, Vol. 5, Issue 3, pp. 4492-4495, 2014.

[13]. K. S. Suresh and Prof K. V. Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 10, pp. 110-114, October-2012.