A Survey to Evaluate Need of Security in Cloud Applications

Pratibha[1], Megha Singh[2]
[1]Research Scholar- COE-CSE, [2]Asst. Professor-COE-CSE
[12]Dr. APJ Abdul Kalam University Indore

Abstract- Cloud computing is a widely popular technology in IT industry and in the field of computer science. With the movement of technology toward cloud, organizations are globally expanding with low cost infrastructure. Organizations uses cloud which reduces the hardware and software infrastructure. Although, the vital need and concern is security which may be risky in terms of privacy and is a great barrier. Even geographically service provider can handle the migrated organizations. This paper review on security in cloud with emphasizing security issues like access control, data leakage, confidentiality, integrity and reliability. In it technique is multi key RC6 with ECC, which implements double encryption with addressing cloud security.

Keyword- Cloud computing, security, RC6, ECC, authentication

I. INTRODUCTION

Contribution of cloud computing in providing services, resources, sharing, processing and storage is vast and impact. Demand of internet on the basis of services and technology is increasing. Cloud does not require any knowledge to use it, it has to be used on the basis of pay per use. Consumption of resources on the basis of clients requirement is justified and abstracted. Clients can simply and easily access services and resources from cloud with the use of internet and quality of services like scalability and reliability with power computing. Self service is demanded by cloud because user requires on-demand services with wide network and maintenance, enhanced with speed and elasticity. Cloud is characterized on the basis of its service model and deployment model. Software-as-a-service, Platform-as-a-service, Infrastructure-as-service are the service models of cloud. Whereas, private cloud, public cloud, hybrid cloud and community cloud are the deployment model of cloud. These service and deployment model of cloud offers comfort with high quality storage service by the mean of internet.

SERIVCE MODEL OF CLOUD:

1. Software-as-a-service: Software-as-service offers on demand software application to there customers over an internet. It runs on cloud infrastructure from where user can access any machine and service according to his/her requirement. Services like database, network, server, data space, softwares etc. are expanded by service providers of cloud.

2. Platform-as-a-service: Platform-as-a-service offers layer of application which are encapsulated with softwares and with developing environment. Through PAAS, user can build his own application which runs on high level infrastructure. It also serves with different features like supporting multiple hosting, scaling and extensibility.

3. Infrastructure-as-service: Infrastructure-as-service offers complete infrastructure and distribution of resources with the capability of storage and computing with using virtualization technology. Vital computing resources like network, storage system and servers are provided by user.

DEPLOYMENT MODEL OF CLOUD:

1. Public Cloud: Third party providers like service providers manage and operate public cloud. Service provider can control the physical infrastructure of public cloud with assigning location to data centers.

2. Private Cloud: Only organization can handle private cloud and after it, they made them available for user to use. Third party can also manage private cloud but after owing it. Private cloud becomes

B. Private Cloud: Private cloud infrastructures are generally handled through an organization and made available to specific set of users. The private cloud can also managed by third party. In this deployment model, it makes sure that no additional security policy, official necessities or bandwidth obstructions since it offers greater control and configurability of the infrastructure and security.

C. Hybrid Cloud: Hybrid cloud is the blending of both two previous cloud models which lets greater flexibility for business and more data deployment models. It helps to perform diverse functions within same organization. Hybrid cloud provides secure services such as receiving customer payments, secondary business processes such as employee payroll processing. [4]

D. Community Cloud: Community cloud has mutual analyze include security, strategies, etc, among organization and communities in the Cloud infrastructure. Third party service provider manages the shared scheme of infrastructure which is allotted by several organizations.

II. RELATED WORK

A. Study of Base Paper with Diagram:

Divya Prathana Timothy et al. In[1] designed a hybrid cryptographic system using both symmetric and asymmetric algorithm. Blowfish is a symmetric algorithm which is used for maintaining confidentiality of data and RSA is a asymmetric algorithm which is used for the purpose of authentication. To achieve data integrity, author used secure hash algorithm

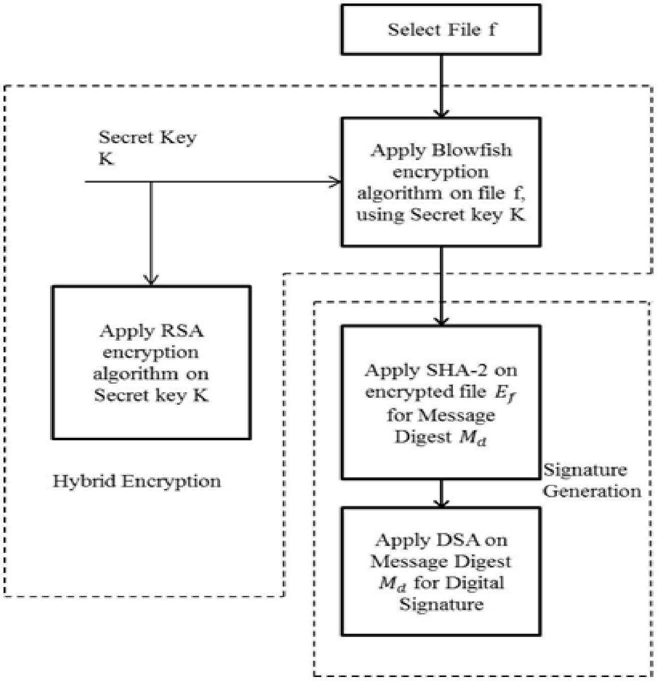
Select File f
Secret Key K
Apply Blowfish encryption algorithm on file f, using Secret key K
Apply RSA encryption algorithm on Secret key K
Hybrid Encryption
Apply SHA-2 on encrypted file E_f for Message Digest M_d
Signature Generation
Apply DSA on Message Digest M_d for Digital Signature

Fig.1: Encryption process in existing work

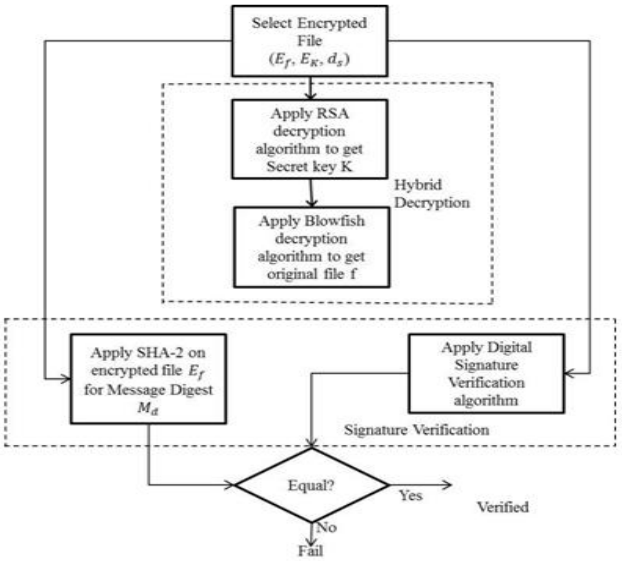
Select Encrypted File (E_f, E_K, d_s)
Apply RSA decryption algorithm to get Secret key K
Hybrid Decryption
Apply Blowfish decryption algorithm to get original file f
Apply SHA-2 on encrypted file E_f for Message Digest M_d
Apply Digital Signature Verification algorithm
Signature Verification
Equal?
Yes
Verified
No
Fail

Fig.2: Decryption process in existing work

Mahavir Jain et al. In[2] proposed hybrid cryptographic algorithm using symmetric cryptographic techniques DES and IDEA. Data encryption standard is used to strengthen encryption algorithm. Author mainly focused on security of data so that sensitive data can be kept secure at the time of transmission of data over insecure network.

P Shaikh et al. In[3] implemented a hybrid approach using AES and blowfish algorithm for the purpose of data confidentiality. Also evaluated performance of used algorithm on the basis of encryption/decryption time.

R. K. Seth et al. In[4] introduces security of data at the time of transmission so as to protect data from intruders. Author proposed a methodology, where token id is generated for every person automatically. Digital signature is produced with token id which decreases security threats to achieve data confidentiality.

III. PROBLEM STATEMENT

Cloud serves with many advantages but with many of the benefits cloud also faces disadvantages too. And these challenges needs to be overcome. Cloud faces security issues like identity management, risk management, access control, confidentiality etc. if any of the organization is outsourcing there data on cloud then they need to provide there data to service provider. It leads to the probability of handing sensitive data to wrong person, which increases risk of data protection in cloud. Cloud services can be easily accessible and available for all the users. This is the case, which evolves risk and any organizations does not want there data to be in risky hands. Therefore, security issues needs to be resolve in cloud computing.

Users personal information needs to be protect, otherwise transmission of data may lead to leakage of personal information like contacts and e-mail. Many technology and security algorithms are applied to protect data. Many of the ideas are also used with solving issues of cloud computing.

Limitations of existing work:

1. RSA deals with key size which is divided by 8 to generate plain text. Which results in more chunking of data.
2. With the increase in chunking data, computation time and memory overhead increases.
3. RSA faces issue of memory overhead and computation time overhead.
4. With the increase in number of user, complications in key management increases.

IV. PROPOSED SOLUTION

Proposed solution deals with security and privacy concept. Multi key RC6 with ECC is used in this work.

Firstly data files are divided into number of chunks by splitting data. Number of chunks are calculated after it keys are generated through key pool using multi key RC6 and these key pools are as K1, K2, K3.....Kn. Then the data is stored in Map table with there Chunk_id and key_id. In the encryption process, data is encrypted using ECC.

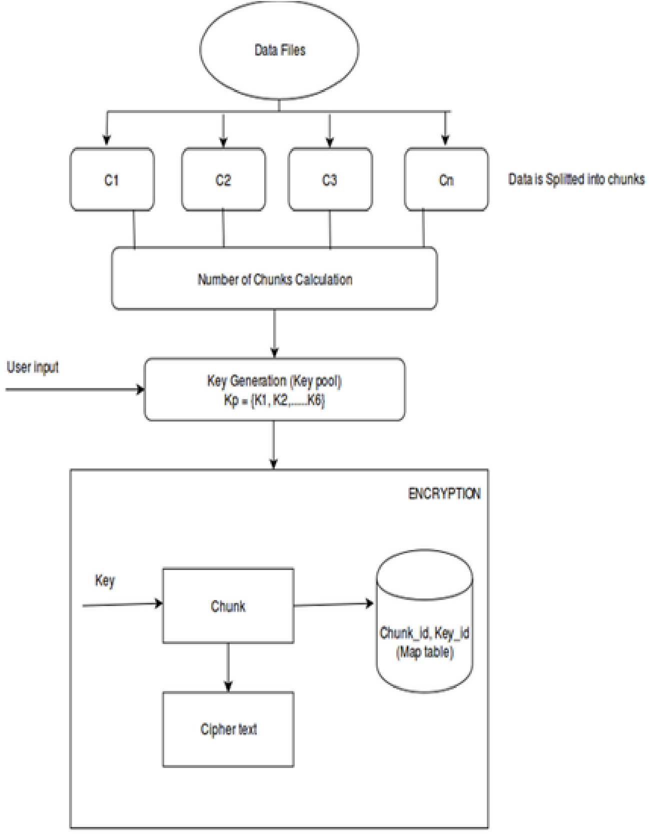

Fig.3: System Architecture

Limitation of base work is overcome in this proposed solution by using ECC. RSA is replaced by ECC because ECC reduces memory overheads and computation time with also elimination complications in key management.

V. CONCLUSION

Cloud faces security issues like identity management, risk management, access control, confidentiality etc. If any of the organization is outsourcing there data on cloud then they need to provide there data to service provider. In it technique is multi key RC6 with ECC, which implements double encryption with addressing cloud security.

VI. REFERENCES

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

[2]. 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.

[3]. 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.

[4]. R. K. Seth, Rimmy Chuchra and Simran, "TBDS – A New Data Security Algorithm in Cloud Computing", International Journal of Computer Science and Information Technology, Vol. 5, Issue 3, pp. 2703-2706, 2014.