Framework to Enhance Security of Data in Private Cloud using Multiple Algorithms in AWS

Miss. Dhara A. Mehta[1], Mr. Kaushik K. Rana[2]
[1, 2] Department of Computer Engineering
[1] GEC, Modasa
[2] VGEC,Ahmedabad

Abstract- *Cloud computing is emerging technology which is a new standard of large-scale distributed computing and parallel computing. It is a shared pool of virtualized resources as a new concept. It provides shared resources, information, software packages and other resources as per client requirements at specific time. As cloud computing is growing rapidly and more users are attracted towards utility computing, better and fast service needs to be provided.*

Keywords- Cloud Computing ,data security,RSA,AES,AWS

I. INTRODUCTION

Cloud Computing provides organizations with an efficient, flexible and cost effective alternative to hosting their own computing resources. However, hackers, attackers and security researchers have shown that this model can be compromised and is not 100% secured. In a Cloud, security is shared between the Cloud provider and the Cloud user. Both entities need to trust each other and complement wherever there is scope for improving security. There are many security threats which emerge inside or outside of Cloud providers/consumer‟s environment and these can be broadly classified as Insider threats, outsider malicious attacks, data loss, issues related to multi-tenancy, loss of control, and service disruption.

II. EXISTING WORK

There are many different security frameworks are available in Cloud Computing environment. For private Clouds here the authentication, authorization and access controls for data are still current issues. In research paper they shows strong data security when stored in cloud at upload and download times using hybrid algorithms (RSA/AES) and Amazon S3 service. But the problem is in this case only less than 5 MB data can be stored easily due to settings of Amazon S3, for data which contains more than 5MB data that also should be stored in cloud with this strong security.

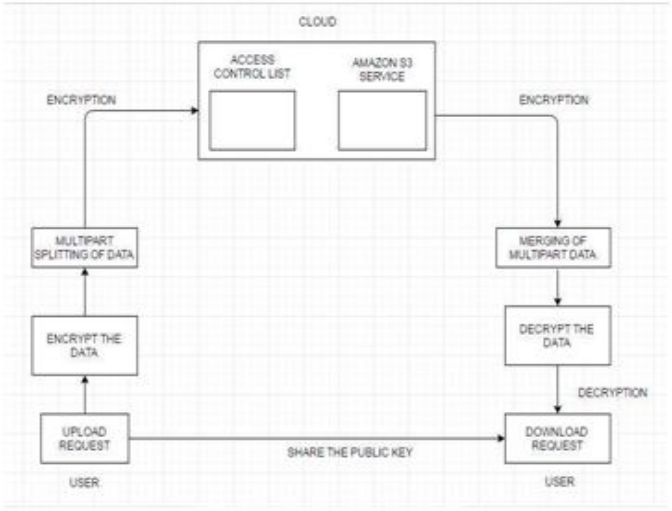
In data security frameworks, when any user authorized or unauthorized download or upload data in private Cloud the malignancy of data is not well checked. Here I would like to improve this same scenario and want to store larger data by applying extra strategies with encryption algorithms, access control and splitting the data.

III. PROPOSED WORK

There are several issues related to security we can see nowadays in cloud services. The existing work can be enhanced by taking some access controls, Amazon S3 as an intermediate storage between user and private cloud and hybrid enhanced encryption scheme of RSA and AES algorithms for large data.

My approach tries to enhance the security of data stored in private cloud by using different parameters like RSA and AES algorithms and Amazon S3 services as secure cloud storage. For password encryption, I have used RSA algorithm and for Data encryption AES algorithm. All encryption will be done at the agent application stored on Client system. So Cloud will get only exposer to the encrypted data not the real data. The uploading of data which will be encrypted that will be splitted into multi parts also before storing in Cloud which can give immense security to the data of the user. All security concerns like Confidentiality, Privacy, Authenticity and Access permissions are implied strongly in this work. For cloud storage I am using Amazon Simple Storage Service as a cloud which is faster and secured.

Proposed algorithm



The proposed algorithm which I have created is including hybrid algorithms like combination of AES and RSA algorithm.

Uploading Files :

1) RSA key pair input : Public and Private key
2) Select file for upload + Enter Password
3) Enc File = Password + AES + File
4) Split the data in multipart
5) Enc(Password) = Password + Private Key
6) Store Enc(file) + Enc(password) to S3 service storage in cloud

Downloading Files :

1) Download Multiparts of Enc(File) + Enc (Pass)
2) Provide Public key
3) Dec (Pass) ← Public Key
4) Dec(Pass) + AES + Enc(File) = Dec (File)
5) Download file

I have used Apache Tomcat server ,Java development tool, and Amazon Web Services here for storage of private cloud. The file data will be divided into multi-parts and will be encrypted and stored into Amazon web service storage and when decryption takes place the divided parts will be merged and a requested data will be sent to authenticated user only.

VI. CONCLUSION

The large data encryption and decryption with strong security in private cloud can be done as dividing the data into multi parts for encryption before storing into cloud and when authenticated user asks for that data then merged data in decrypted structure available.

REFERENCES

[1] Shuai Zhang, Shufen Zhang, "Cloud Computing Research and Development Trend", 2010 Second International Conference on Future Networks.

[2] Mladen A.Vouk," Cloud Computing – Issues, Research and Implementations", Proceedings of the ITI 2008 30th Int. Conf. on Information Technology Interfaces, June 23-26, 2008, Cavtat, Croatia.

[3] Victor Delgado. Exploring the limits of cloud computing. In Master of Science Thesis Stockholm, Sweden 2010.

[4] Pankaj Arora* Rubal Chaudhry WadhawanEr. Satinder Pal Ahuja,"Cloud Computing Security Issues in Infrastructure as a Service", Volume 2, Issue 1, January 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[5] AkhilBehl, Emerging Security Challenges in Cloud Computing, Centre of Excellence, Advance Services Cisco System, New Delhi, India.

[6] Meiko Jensen, J¨orgSchwenk, Nils Gruschka, Luigi Lo Iacono, On Technical Security Issues in Cloud Computing, 2009 IEEE International Conference on Cloud Computing.

[7] Chang-Lung Tsai Uei-Chin Lin Allen Y. Chang Chun-Jung Chen, Information Security Issue of Enterprises Adopting the Application of Cloud Computing. Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on

[8] Yue Tong, Student Member, IEEE, Jinyuan Sun, Member, IEEE, Sherman S. M. Chow, and Pan Li, Member, IEEE ,Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability, IEEE Journal of Biomedical and Health Informatics (Volume:18 , Issue: 2).

[9] Lo'ai Tawalbeh,1,3 Raad S. Al-Qassas,2 Nour S. Darwazeh,2 Yaser Jararweh,3 and Fahd AlDosari1, Secure and Efficient Cloud Computing Framework[11],Cloud and Autonomic Computing (ICCAC), 2015 International Conference on

[10] Sunita Rani, AmbrishGangal ,Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints[12], Sunita Rani et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4302 – 4304.

[11] Mohammed Faez Al-Jaberi and Anazida Zainal Data integrity and Privacy model in Cloud Computing , IEEE

2014 International Symposium on Biometrics and Security Technologies (ISBAST)

[12] Mr. Krunal Patel, Mr. Navneet Singh, Mr.Kushang Parikh, Prof. Sendhil Kumar K.S, Dr.Jaisankar N., Data Security and Privacy using Data Partition and Centric key management in Cloud, Information Communication and Embedded Systems (ICICES), 2014 International Conference on

[13] RandeepKaur1 ,Supriya Kinger2, Analysis of Security Algorithms in Cloud Computing[, International Journal of Application or Innovation in Engineering & Management (IJAIEM)