International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 4, Special Issue 3 (March '2018)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

SECURE FILE SHARING AND ACCESS IN CLOUD USING AES AND RSA

K.Sundar,
Assistant Professor,
Department of Computer Science and Engineering,
Velammal Engineering College,
Chennai, Tamilnadu,India.

S.Faizur Rahuman,
Student,
Department of Computer Science and Engineering,
Velammal Engineering College,
Chennai, Tamilnadu,India.

R.Depak kumar,
Student,
Department of Computer Science and Engineering,
Velammal Engineering College,
Chennai, Tamilnadu,India.

M.Vinoth,
Student,
Department of Computer Science and Engineering,
Velammal Engineering College,
Chennai, Tamilnadu,India.

Abstract: In cloud computing distributed resources are shared via network in open environment. Hence user can easily access their data from anywhere. At the same time there exist privacy and security issues due to many reasons. First one is dramatic development in network technologies. Another is increased demand for computing resources, which make many organizations to outsource their data storage. So there is a need for secure cloud storage service in public cloud environment where the provider is not a trusted one. In the existing system the owner uploads the file in the cloud using AES encryption it is easily attackable and it is not more secured so if anyone has know the file was encrypted using AES algorithm so they can able to crack that file using some techniques. To overcome this problem we are going to propose a double encryption using AES and RSA algorithm. It was more secured and it is not possible to decrypt a file by someone. Along with this we are adding some features such as Time scheduling and Group sharing .We are using FIFO method in Time scheduling for request and response. Group sharing is when the owner of the file wants to share the file to a particular group of peoples, he can use this technique to share the file to the group he wanted. No other person other than the group members cannot able to access, view or modify the file.

Keywords: CRF (Conditional Random Fields), Thresholding, SVM (Support Vector Machines) Classifier.

I.INTRODUCTION

One of the main characteristics of cloud computing is to use the cloud services in a pay-as-you-go manner.Also cloud offers an infinite storage space for client to store their data. Thus cloud storage provides the way for remote data backup, so that user can able to retrieve the data at any time using the cloud services. Cloud also reduces the financial overload of enterprises and organizations in maintaining their data.

There are more case studies that are related to cloud storage for remote data backup . Also individuals can store their personal data to the cloud using Google Drive etc. Nowadays more number of peoples are using tools like to store their data in cloud. However, we need to consider the security concerns in storing the sensitive data in cloud which is maintained by third party cloud services.

In our proposed work, two security issues are considered particularly. First, we need to ensure that only authorized parties have access to the outsourced data in cloud through efficient key distribution mechanism and access policy. Second, to guarantee secure data access we need to implement cryptography schemes for providing security when users upload/download data from cloud services. In this paper, we used RSA and AES algorithm for achieving the proposed issues.

We also perform several cryptography key operations to protect the data which is accessed from the cloud. The proposed protocol is applicable for general storage backups where upload/download of data takes place with the help of backend interface.

II.LITERATURE SURVEY

The popular press has recently promoted grid and cloud computing as two of the most promising trends in IT. Grid computing debuted first, in the early 1990s. Arising from the need for more computational power than clusters can provide, researchers soon found that distributed high-performance computing in virtual organizations could help them deal with large amounts of data. Research projects soon started all over the world, funded by governments as well as industry, in an attempt to fully exploit grid computing's computational advantages. Lately, however, a new computing paradigm has emerged: cloud computing. Just as with the buzz around grid computing, this topic has generated a lot of discussion among scientists and researchers. But how does it differ from grid computing? Is it simply a new name for current technology, or does it pave the way for the commercial widespread use of large-scale IT resources? In this article, we'll examine what cloud computing really is and introduce a new ontology for describing the different applications and business models for compute clouds. This ontology provides a clear framework to characterize and classify cloud offerings and application scenarios[1].

With the significant advances in Information and Communications Technology (ICT) over the last half

century, there is an increasingly perceived vision that computing will one day be the 5th utility (after water, electricity, gas, and telephony). This computing utility, like all other four existing utilities, will provide the basic level of computing service that is considered essential to meet the everyday needs of the general community. To deliver this vision, a number of computing paradigms have been proposed, of which the latest one is known as Cloud computing. Hence, in this paper, we define Cloud computing and provide the architecture for creating Clouds with market-oriented resource allocation by leveraging technologies such as Virtual Machines (VMs). We also provide insights on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain Service Level Agreement (SLA)-oriented resource allocation. In addition, we reveal our early thoughts on interconnecting Clouds for dynamically creating global Cloud exchanges and markets. Then, we present some representative Cloud platforms, especially those developed in industries along with our current work towards realizing market-oriented resource allocation of Clouds as realized in Aneka enterprise Cloud technology. Furthermore, we highlight the difference between High Performance Computing (HPC) workload and Internet-based services workload. We also describe a meta-negotiation infrastructure to establish global Cloud exchanges and markets, and illustrate a case study of harnessing 'Storage Clouds' for high performance content delivery. Finally, we conclude with the need for convergence of competing IT paradigms to deliver our 21st century vision[2].

We describe two algorithms, based on dynamic programming logic, for optimally solving the discrete time/cost trade-off problem (DTCTP) in deterministic activity-on-arc networks of the CPM type, where the duration of each activity is a discrete, nonincreasing function of the amount of a single nonrenewable resource committed to it. The first algorithm is based on a procedure proposed by Bein, Kamburowski and Stallmann for finding the minimal number of reductions necessary to transform a general network to a series-parallel network. The second algorithm minimizes the estimated number of possibilities that need to be considered during the solution procedure. Both procedures have been programmed in C and tested on a large set of representative networks to give a good indication of their performance, and indicate the circumstances in which either algorithm performs best[3].

III.MODULE DESCRIPTION OF SECURED FILE UPLOAD:

Our application consists of 5 modules. The 5 modules are User interface Design, Generation of Key and Encryption Files, View, Analysis and Deliver Request, Key Distribution with Time Scheduling and View and Download

3.1 User Interface Design:

In this user interface design, this is the initial module of our project. User Interface Login Page Design plays an important role for the user to interact with login page to client page or user page. This module has been created for user authentication purpose. In this login page, Authorized users can login with their valid credentials otherwise they have to register with their details like providing Work with Their Number number...Etc. details. So, thereafter registered details will be stored into database and will be authenticate while logging time. It will verify each and every user information details. If those details are doesn't matches with database details then it will gives an error message and it will shows the registration page automatically. So, here we are skipping the illegal users and providing more surveillance for our application.

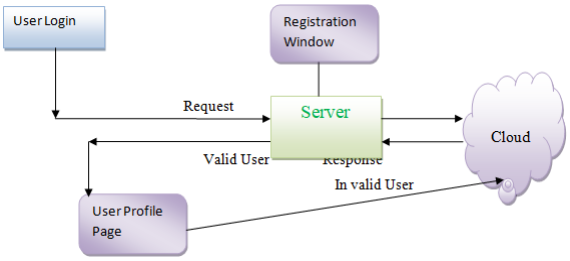

FIGURE: 3.1

3.2 Generation of key and Encrypting files:

Generating the key and encrypt the files using AES algorithm and again Encrypt previous Encrypted Content.

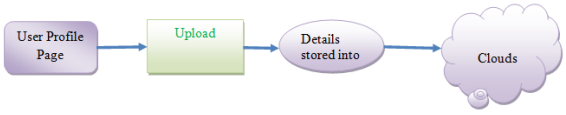

FIGURE: 3.2

3.3 View, Analysis and Deliver request:

In this third Module my project will be view the uploaded files list in my project for confirmation and analysis use. If the process of the fully analysis by the user and the fully uploaded data. In this finally request the wanted own file from the uploaded file.

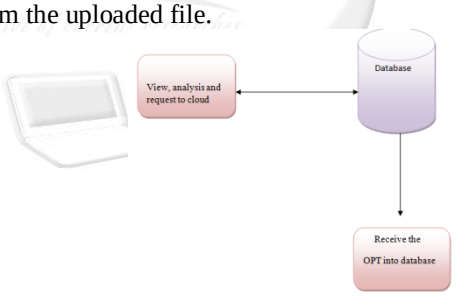

FIGURE: 3.3

3.4 Key distribution WITH Time Scheduling:

This is the fourth module in our project; in this module here we are going to allocate the resources for users which are processed after scheduling process. Here, we are implementing the make spam & monitoring cost of the process which involves in dynamic process. By using the strategy profile of the user process we will allocate the time based on the tasks which are performed by the user. Here, we will also introducing to going to involve reverse mechanism to the user for his choices depends.

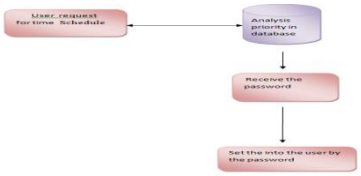

FIGURE: 3.4

3.5 View and Download:

This is the final module of our project. In this module we deliver the product to the customer, when the key condition will be satisfying file backup will be downloaded. The delivery phase is the last module in our project.

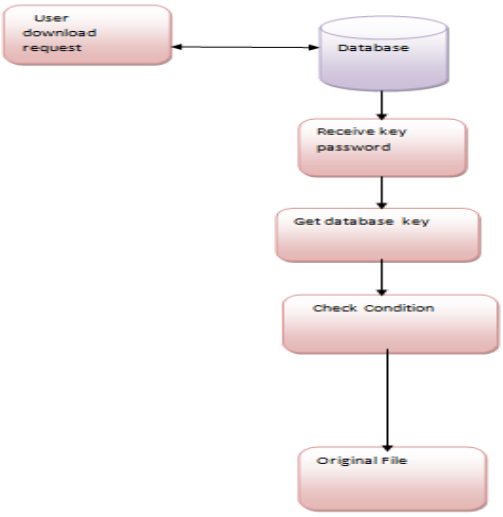

FIGURE:3.5

IV.PROCESS OF FILE UPLOAD

The following are the process of the File upload.

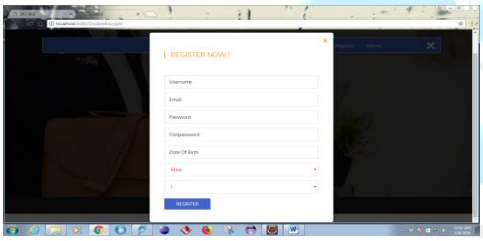

FIGURE:4.1: Registration form for user who are going to upload file.

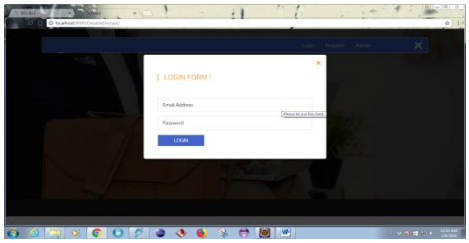

FIGURE:4.2: This is the pop up box of login form.

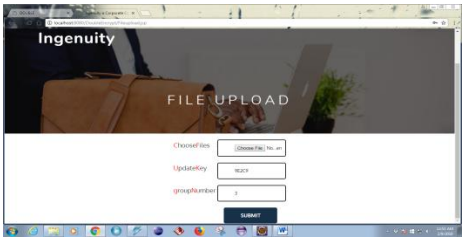

FIGURE:4.2: This page shows user to upload a file.

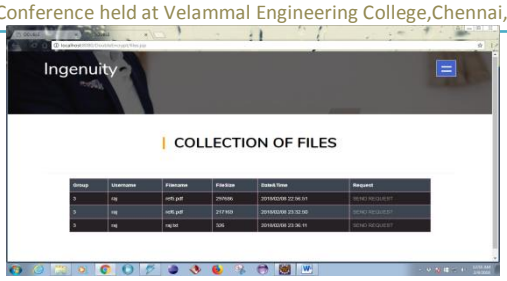

FIGURE:4.3:User can see collection of files and can send request to the file that the user want.

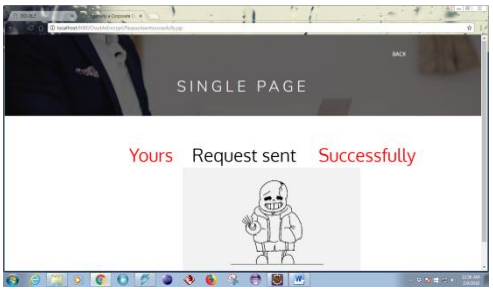

FIGURE:4.4:Request has been sent to the Admin.

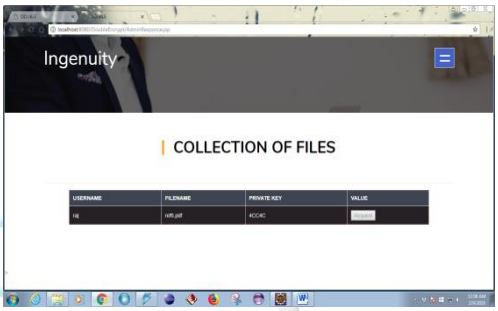

FIGURE:4.5: Generation of private key to the user after.

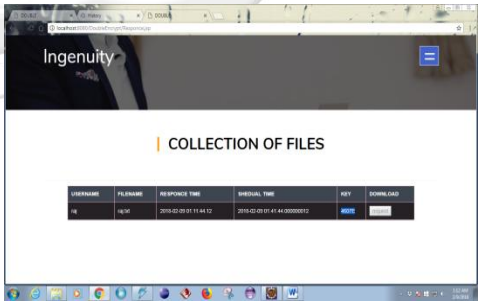

FIGURE:4.6 Admin gives a key to the user to download file.

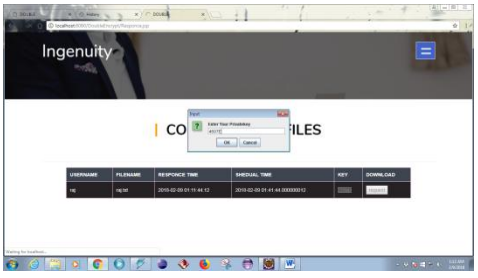

FIGURE:4.7 User have to enter key that has been given by admin to download.

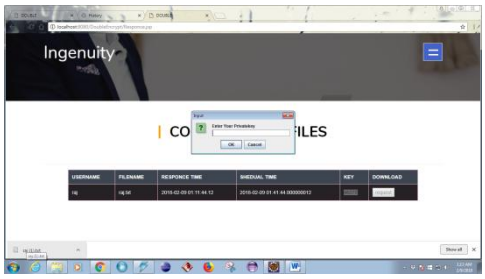

FIGURE:4.8 Pop up box to enter a private key that has sent to the user.

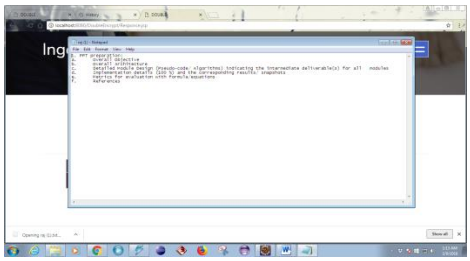

FIGURE: 4.9File gets download and user can see a decrypted original file.

V.CONCLUSION

We proposed a secure sharing of data using RSA and AES algorithm to maintain security within cloud server. KDM will be responsible for all key generation and key distribution process in our proposed scheme. The performance is evaluated and the results are obtained based on RSA key generation and AES encryption process. From the result, it is noticed that our proposed method will be applicable for sharing data in cloud securely. We use policy based access mechanism to provide security with the data in cloud and also to provide authentication. In future we can use multiple KDM to handle the data with different access policies to avoid insider attacks.

VI.REFERENCES

[1]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing." Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010. https://doi.org/10.1145/1721654.1721672

[2]. Amazon, "Case Studies," http://aws.amazon.com/solutions/ casestudies/# backup, 2012.

[3]. Dropbox, http://www.dropbox.com, 2010.

[4]. Google Drive, http://www.drive.google.com, 2012

[5]. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, 2010. https://doi.org/10.1007/978-3-642-14992-4_13

[6]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010. https://doi.org/10.1109/infcom.2010.5462173