A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture

Kawser Wazed Nafi[1,2], Tonny Shekha Kar[2], Sayed Anisul Hoque[3], Dr. M. M. A Hashem[4]
[1]Lecturer, Stamford University, Bangladesh
[2]Khulna University of Engineering and Technology
[3]Chittagong University of Engineering and Technology
[4]Professor, Khulna University of Engineering and Technology

***Abstract*— The cloud computing platform gives people the opportunity for sharing resources, services and information among the people of the whole world. In private cloud system, information is shared among the persons who are in that cloud. For this, security or personal information hiding process hampers. In this paper we have proposed new security architecture for cloud computing platform. This ensures secure communication system and hiding information from others. AES based file encryption system and asynchronous key system for exchanging information or data is included in this model. This structure can be easily applied with main cloud computing features, e.g. PaaS, SaaS and IaaS. This model also includes onetime password system for user authentication process. Our work mainly deals with the security system of the whole cloud computing platform.**

Keywords- Cloud Computing; Security architecture; AES; RSA; onetime password; MD5 Hashing; Hardwire database encryption.

I. INTRODUCTION

At the present world of networking system, Cloud computing [1] is one the most important and developing concept for both the developers and the users. Persons who are interrelated with the networking environment, cloud computing is a preferable platform for them. Therefore in recent days providing security has become a major challenging issue in cloud computing.

In the cloud environment, resources are shared among all of the servers, users and individuals. As a result files or data stored in the cloud become open to all. Therefore, data or files of an individual can be handled by all other users of the cloud. [2, 3] Thus the data or files become more vulnerable to attack. As a result it is very easy for an intruder to access, misuse and destroy the original form of data. An intruder can also interrupt the communication. Besides, cloud service providers provide different types of applications which are of very critical nature. Hence, it is extremely essential for the cloud to be secure [4]. Another problem with the cloud system is that an individual may not have control over the place where the data needed to be stored. A cloud user has to use the resource allocation and scheduling, provided by the cloud service provider. Thus, it is also necessary to protect the data or files in the midst of unsecured processing. In order to solve this problem we need to apply security in cloud computing platforms. In our proposed security model we have tried to take into account the various security breaches as much as possible.

At present, in the area of cloud computing different security models and algorithms are applied. But, these models have failed to solve all most all the security threats. [5, 6, 7] Moreover for E-commerce [8] and different types of online business, we need to imply high capacity security models in cloud computing fields. Security models that are developed and currently used in the cloud computing environments are mainly used for providing security for a file and not for the communication system [9]. Moreover present security models are sometimes uses secured channel for communication [10]. But, this is not cost effective process. Again, it is rare to find a combined work of main server security, transaction between them and so on. Some models attempt on discussing about all of these, but are completely dependent on user approach. The models usually fail to use machine intelligence for generating key and newer proposed model. Some models have proposed about hardware encryption system for secured communication system [11]. The idea is usually straightforward, but the implementation is relatively difficult. Besides, hardware encryption is helpful only for the database system, not for other security issues. Authenticated user detection technique is currently very important thing. But, this technique is rarely discussed in the recently used models for ensuring security in cloud computing.

In this paper we have proposed new security architecture for cloud computing platform. In this model high ranked security algorithms are used for giving secured communication process. Here files are encrypted with AES algorithm in which keys are generated randomly by the system. In our proposed model distributive server concept is used, thus ensuring higher security. This model also helps to solve main security issues like malicious intruders, hacking, etc. in cloud computing platform. The RSA algorithm is used for secured communication between the users and the servers.

This paper is formatted in the following way: - section II describes related work of this paper work, section III describes proposed architecture and its working steps, section IV describes the experimental environment, results in different