A Newer Secure Communication, File Encryption and User Identification based Cloud Security Architecture

Tonny Shekha Kar[1], M. A. Parvez Mahmud[2] ,Shahjadi Hisan Farjana[3] ,Kawser Wazed Nafi[1], and Bikash Chandra Karmokar[1]
Department of Computer Science and Engineering[1]
Department of Electrical and Electronic Engineering[2]
Department of Mechanical Engineering[3]
Khulna University of Engineering and Technology, Khulna, Bangladesh

ABSTRACT
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. Because of this, different security related problems have grown in this platform. This paper work has proposed newer security architecture for cloud computing platform, which ensures secured communication system and hiding information from others. DES based file encryption system and asynchronous key system for exchanging information or data is included in this model. This structure is easily applicable with main cloud computing features, e.g. PaaS, SaaS and IaaS. This model also includes unique encryption key for user authentication process. El Gamal has been proposed in this paper for secured communication between users and cloud storage system. This paper work mainly deals with providing security for files stored in cloud computing archtecture.

Keywords
Cloud Computing, Security architecture, DES, El Gamal Cryptosystem.

1. 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 of the present world cloud computing is a preferable platform for them. Therefore in recent days providing security has become a major challenging issue in cloud computing.

In 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] 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. For this it is also very much essential for the cloud to be secure [4]. Another problem with cloud is that an individual may not have control over the place where the data have to be stored. Because a cloud user have to use the resource allocation and scheduling provided by the cloud service provider. For this it is also necessary to protect the data or files in the midst of unsecured processes. In order to solve this problem we need to apply security in cloud computing platforms. In our proposed security structure we have tried to take into account security breaches as much as possible.

At present, different security models and algorithms are applied in the field of cloud computing. But, these models have failed to solve all 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 environment are mainly used for providing security for a file and not for the whole communication system [9]. Moreover present security models are sometimes using 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 though try to discuss about all of these, they are fully dependent on user approach and failed to use machine intelligence for generating key and newer proposed model. Some models have proposed about hardwire encryption system for secured communication system [11]. It is easy to thinking, but hard to implement. Besides, hardwire encryption is helpful only for database system, not for other security issues. Again, authenticated user detection is now a day very important thing, which is rarely discussed in the recently used models for ensuring security in cloud computing.

In this paper we are going to show a newer security architecture for cloud computing platform. Here files are encrypted with DES algorithm in which keys are generated randomly by the system. For one file, only one key is generated. Two servers, means distributed server concepts are used here for ensuring high security. This model also helps to solve main security issues like malicious intruders, hacking, etc of cloud computing platform. El Gamal algorithm is used for secured communication between the users and the companies' servers.

The paper is organized in following way :- section 2 describes the related cloud computing security architectures and models; section 3 describes briefly the proposed cloud computing storage architecture; section 4 describes the step-by-step execution process of proposed architecture; section 5 discusses on the results of the proposed model got from different experiments with users in lab and finally, section 6 discusses on our achievements and future plans.

2. RELATED WORK
Various researches on security in cloud computing have already completed now a day. Identification based cloud computing security model was worked out by different researchers [12]. But only identify the actual user does not all times give relief from data hacking or intruding data or information saved in the database of cloud environment. Yao's Garbled Circuit is used for secure data saving in cloud