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 Kormokar[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
tulip0707051@yahoo.com, piash117@gmail.com, shahjadisynthy@yahoo.com, kwnafi@yahoo.com, bikash_kuet@yahoo.com

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 servers [13, 14]. But it is also an identification based work. It does not work with ensuring security in whole cloud computing platform. Researches related with ensuring security in whole cloud computing environment have already worked out in different structures and shaped. AES based file encryption system is used in some of these worked out models [15, 16]. DES based file encryption system is also researched out [17]. But these models keep both the encryption key and encrypted file in one database server. So, only tried and become successful to hack one of the servers can give the hacker all information about the file, which is not desirable. Some other models and secured architecture are proposed for ensuring security in cloud computing environment [18, 19]. Though these model ensures secured communication between users and servers, but these models doesn't encrypt the loaded information. But for best security ensuring process the uploaded information needs to be encrypted so that none can know the information. Some other precious secured models for cloud computing environment are also researched out [20, 21]. But, these models also fails to ensure all criteria of cloud computing security issues [22].

3. PROPOSED MODEL

The Proposed Model mainly works with the following security algorithms:

1. El Gamal [23, 24, 25]
2. DES Encryption algorithm [26]

During the time of working with proposed model, we developed and worked with the cloud-computing scenario shown in Figure 1.

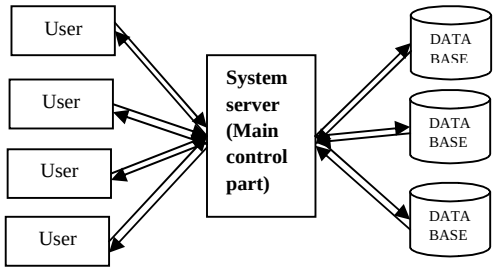

Fig 1: Cloud Architecture (Working Scenario)

In this scenario, we can see that all the users need to contact with the main server and with the help of this computer users can communicate with databases for uploading or downloading their files. Every time the system server serves the users. It takes files from the users, keeps these files in different databases, which are connected with it and retrieve files from the databases to specific users whenever needed. As there is no other connection between the system server and the databases, these connections are not secured. No security algorithm is applied here. Between users and the system server, El Gamal cryptosystem is used. Public and private keys between the users and the system may be distributed with the help of KDC or a third party computer/ server, which may be installed by the cloud system. Here, at the time of uploading a file, the file is encrypted with the public key of the cloud system, mainly with the public key of the system server. At the time of downloading a file, a user first sends his/her request of his/her file, which he/she has already uploaded before, in an encrypted format. The system server decrypts it and processes the request. System server then encrypts the requested file, which is retrieved from the database, with the public key of the user (searched out or request KDC for the public key of the user) and sends it to that user. For this reason, only the specific user can decrypt the file and work with it. Again, El Gamal is probabilistic. One file can be encrypted is several ways. So, it becomes hard for one to understand the keys. For this reason, no one can easily interrupt in the communication between the users and cloud storage system.

When a user uploads his/her file to cloud storage system, the system server first encrypts it with the help of DES algorithm. DES algorithm uses 64-bit long key for encryption process and 16 cycles, which includes substitution and transaction. This makes the file unreadable to the outsiders. This encryption key is generated by the system. When a user uploads his/her file to cloud system, the system server first generates randomly a 64-bit key and encrypt the file. Then, the system sends the key to the user's email address, who has uploaded the file. Then, the system randomly selects one database, attached with the system server and uploads the file to that selected database server. The system server maintains a table where it entries the server no accompanying with user name and file name. Because email no of user is used by the proposed cloud storage system as user name, it is unique and both of file name and user name can give a unique representation of an uploaded file. So, it becomes easy for the system server to upload file to a database and retrieve the file easily whenever needed. If a database server is busy in uploading file when the system server wants to upload another file in that database server, the system server again randomly selects another database server except the previous one and uploads the file. If the system server tries to upload a file to the database server, which is larger than the free size of that database server, the system again selects randomly another database server except the present one and uploads the file. The 64-bit file encryption key is also helpful for authenticate the user. Because this encryption key is sent to users' email accounts, only authenticate users' can open their uploaded files. At the time of downloading that file, the system server asks the encryption key to the user. For this reason, no other person except the actual one can open and access the files. Again, if anyone wants to hack files from the communication channels between the system server and database servers, no one can do it easily because everything operation is done through the system server. Accidently, if anyone gets a file, it will become useless to him. Because only encrypted files are sends from system server to database servers and no copy of key is kept in memory. This proposed cloud security model works with not only file encryption system based security model but also with authentication based system security model. So, the proposed cloud security model architectures looks like as shown in Figure 2

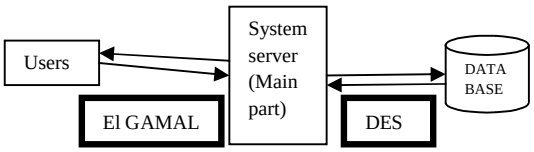

Fig 2: Proposed Cloud Security Architecture

4. EXPERIMENTAL SETUP

The model shown in figure 2 has worked out in the lab with the following configuration:-

1. Processor Core 2 duo 2.6 GHz
2. RAM 2 GB
3. Windows 7
4. Combination of ASP.Net and C#

At first public and private keys with the help of EL Gamal are generated with a computer. Then, they are distributed to the users and main system server. Users use the public key of the cloud storage system for encrypting the file ready uploading by the users. Cloud storage system uses public key of the specific users for encrypting the retrieved files and sends them to users. Figure: 3 shows step by step process of secured transactions between a user and the system server:-

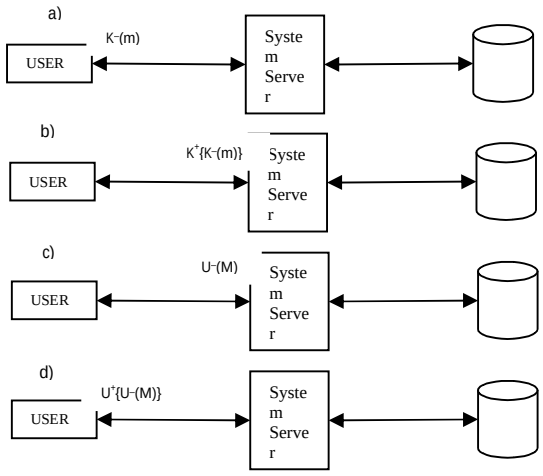

Fig 3: Step by Step El Gamal Transactions

Here, from Figure 3 we see that, at first, message m is encrypted by key k^-, which is the public key of the cloud storage system. This public key is generated by El Gamal cryptosystem process [27]. After receiving the files, system server decrypts it with private key K^+. at that time the message or file is accessible by the system server. For sending something to users, system server encrypts the files or message with public key of that user, U^-. After getting these files, users open it with their own private key, U^+. Then it becomes readable and accessible to users.

After getting the files from the users, the main server starts its works. First of all it randomly generates a 64 bit key. After that, the system server encrypts the files and sends the encryption keys to specific users email addresses. Files are then uploaded by the system server to database servers (One file in one database server). When users want to download files, only with the help of encryption keys, the files can be opened and readable by the users. Figure 4 shows the whole file encryption processes pictorially.

From Figure 4 we see that at first of all transactions, users first upload files. Each user can upload one file at a time. System server then generates encryption keys (K), encrypts file, inserts file, database server information in table, and sends the keys to specific users. Next time, when user wants to download a file, he needs to send his encryption key (K) to the system main server. System server than retrieves that file from database by searching out specific database server according to the information in system server (same as Table 1).

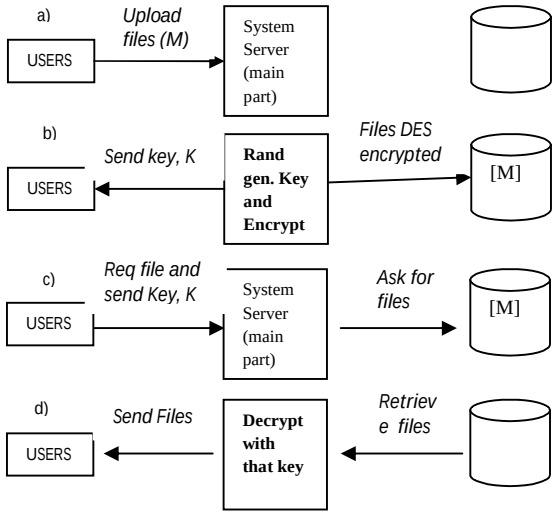

Fig 4: Step by Step Files Encryption process

After the completion of the download process, the files are no more in database and keys become useless. If one wants to upload the same file again, a new key will be sent by the system server to his/her mail account.

Table 1. Table Maintained in System Server for Users, Files and Database Servers Information

User Account	File Name	Server Number
abc@yahoo.com	Abcd.txt	1
bddf@gmail.com	Asdfasd.dat	2
……	…….	……
asdfa@hotmail.com	Ppoip.extension	1

5. EXPERIMENTAL RESULTS

Experimental results of the proposed model are taken in two phases. Here time required for the completion of each phase is taken under consideration. The full experimental work has taken 40 people reviews for getting results of the proposed model.

Phase 1: 40 people have worked with the El Gamal encryption and decryption technique for communicating with the main server (system server) of the cloud storage system. Times required for sending request and files from users side to system server and after processing downloading request, times required for sending files from system server to users side are shown in Table 2. Though the experiment is completed with 40 people, 10 people's results are shown here.

Table 2. Resulting Time for Transactions between Users and Cloud Storage System Server

Number of People	Time required from user side to system	Time required from system server to that user	Number of People	Time required from user side to system	Time required from system server to that user
1	2 sec	2 sec	6	3 sec	3 sec
2	3 sec	3 sec	7	2 sec	2 sec
3	2 sec	3 sec	8	2 sec	2 sec
4	2 sec	2 sec	9	3 sec	2 sec

5	3 sec	3 sec	10	2 sec	2 sec

From the data of Table 2 we can see that transactions from users side to system or from system side to users take averagely 2-3 seconds. The range of files size, which are used by the users to communicate with the proposed model are laid between 5 KB to 50 KB.

Phase 2: 40 people have worked with DES file encryption and decryption technique for uploading files from system server to database server (the file storage device). Times required for uploading files from system server to database servers and for processing downloading request, after searching out files, times required for transferring searched files from storage devices to system server are shown in Table 3. Again, 10 people's results are shown here.

Table 3. Resulting Time for Transactions between System Server and File Storage Servers

Number of People	Time required from system server to database	Time required from database to system server	Number of People	Time required from system server to database	Time required from database to system server
1	1 sec	2 sec	6	1 sec	2 sec
2	1.5 sec	2.5 sec	7	1 sec	2 sec
3	1 sec	2 sec	8	1.5 sec	2.5 sec
4	1 sec	1.5 sec	9	1 sec	2 sec
5	1.5 sec	3 sec	10	1 sec	2 sec

From Table 3 we can see that transactions for DES encryption process take averagely 1-2 sec.

The proposed cloud storage security architecture has solved different security problems for cloud computing platform. It solves user authentication problem, many user interruption problems, file hacking problems, etc. The advantages of the proposed model on different points are discussed in Table 4.

Table 4. Advantages of the Proposed Model Over Different Present Models

Points for discussion	Identification Based Models	File encryption based Models	Secured channel using models	Proposed Model
Ways of ensuring security	Only identify the authorized person,	Key and file both remains in one server. So, getting access on one server helps to get all information	Intruder cant access the data, but uploaded file is not secured	Both identify people and Encrypt Files for make secure form intruders
Information leakage probability	Medium	Medium	Medium	Low
Complexity	Low	Medium	Low	Low
Ensuring User Authentication	Main theme	If key is chosen by user, then slightly authenticate users	Probably not maintained	One encryption key for one file. So, each user has unique encryption key, which authenticates him/her
Execution time	Small	Medium	Small	Small
Security Breaking probability	Medium	Medium	Medium	Probably Low than others
Cloud Architecture	Easy to establish	Easy to establish	Easy to establish	Easy to establish
Security Level	Medium	Medium	Medium	Higher than other models

6. Conclusion

In this paper we have proposed a newer security structure for cloud computing environment which includes DES file encryption system and EL Gamal cryptosystem for secure communication This model ensures security for uploaded files in cloud, authenticate users. Here, execution time is lower because of lightweight security ensuring algorithms. Here, user authentication system with the help of unique encryption key helps to ensure proper user interaction. Again, each algorithm is executed individually in each single server and the results of these algorithms are then transmitted from one side to other. For this reason decision taking is easy here for each server, like authenticate user, give access on file, etc.

In proposed model El Gamal cryptosystem is used which is probabilistic. In future we want to work with ensuring higher secure communication system between users and system with help of other security algorithms, user to user. We also want to work with different encryption algorithms to find out more secure encryption system for solving problems related with DES file encryption system.

7. ACKNOWLEDGMENTS

The Authors are willing to express their profound gratitude and heartiest thanks to all the researchers in the field of cloud computing architecture's security, specially to the developers of DES and El Gamal data security algorithms, who have made their research work easy to accomplish.

8. REFERENCES

[1]. Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", *International Journal of Computer Science Emerging Technology*, Vol-2 No 5 October, 2011 , 316-322

[2]. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011

[3]. Mladen A. Vouk, "Cloud Computing – Issues, Research and Implementations", *Journal of Computing and Information Technology* - CIT 16, 2008, 4, 235–246

[4]. Ye Hu, Johnny Wong, Gabriel Iszlai, Marin Litoiu, "Resource Provisioning for Cloud Computing", *IBM Canada Ltd*., 2009

[5]. Daniele Catteddu, Giles Hogben, "Cloud Computing:- Benefits, risks and recommendations for information security", November, 2009

[6]. "Cloud Computing: Silver Lining or Storm Ahead?", Volume 13 Number 2, Spring 2010

[7]. NGONGANG GUY MOLLET, "CLOUD COMPUTING SECURITY" , Thesis Paper, April 11, 2011

[8]. Gunasekar Kumar, Anirudh Chelikani, "Analysis of security issues in cloud based e-learning", Master's thesis, 2011

[9]. Jiyi Wu, Qianli Shen, Tong Wang, Ji Zhu, Jianlin Zhang "Recent Advances in Cloud Security", *JOURNAL OF COMPUTERS*, VOL. 6, NO. 10, OCTOBER 2011

[10]. Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy, "Token - Based Cloud Computing Secure Outsourcing of Data and Arbitrary Computations with Lower Latency", TRUST 2010, LNCS6101, pp . 417–429, 2010.

[11]. Trusted Computing Group, "Solving the Data Security Dilemma with Self-Encrypting Drives", May 2010

[12]. Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, "Identity-Based Authentication for Cloud Computing", Cloud Com 2009, LNCS 5931, pp. 157–166, 2009

[13]. Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, "Twin Clouds: Secure Cloud Computing with Low Latency", CASED, Germany, 2011

[14]. Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, "Twin Clouds: Secure Cloud Computing with Low Latency"- Extended Abstract, CASED, Germany, 2011

[15]. Luis M. Vaquero, Luis Rodero-Merino, Daniel Morán, "Locking the sky: a survey on IaaS cloud security", Computing (2011) 91:93–118

[16]. Yang Tang, Patrick P. C. Lee, John C. S. Lui, and Radia Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion", 2010

[17]. Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security", *VSRD-IJCSIT, Vol. 2 (4), 2012*, pg: 316-321

[18]. Thuy D. Nguyen, Mark A. Gondree, David J. Shifflett, Jean Khosalim, Timothy E. Levin, Cynthia E. Irvine, "A Cloud-Oriented Cross-Domain Security Architecture", *The 2010 Military Communications Conference*, U.S. Govt.

[19]. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", US National Science Foundation under grant CNS-0831963, CNS-0626601, CNS-0716306, and CNS-0831628, 2009

[20]. Vaibhav Khadilkar, Anuj Gupta, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Secure Data Storage and Retrieval in the Cloud", University of Texas, 2011

[21]. John Harauz, Lori M. Kaufman, Bruce Potter, "data Security in the World of Cloud Computing", The IEEE Computer SOCIETIES, August, 2009

[22]. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for cloud computing", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010

[23]. Taher ElGamal, "A public key cryptosystem and a signature scheme based discrete logarithms", *HP labs*, 1985.

[24]. AndreasV.Meier, "The ElGamal Cryptosystem", 2005.

[25]. Melissa Helgeson, "Security and Applications of ElGamal's Encryption Algorithm", Google Scholar,

[26]. Raymond G. Kammer, William M. Daley, "DATA ENCRYPTION STANDARD (DES)", *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION*, FIPS PUB 46-3, 1999

[27]. Marco Bodrato, "Public key cryptography. ElGamal, hints on implementation", Tokyo University of Science - March 18th, 2008