# A Robust Information Security Model for Cloud Computing Based on the Scrambling Algorithm and Multi-Level Encryption

Dr. Mohammad V. Malakooti
Faculty and Head of Department of Computer Engineering
Islamic Azad University, UAE branch, Dubai, UAE
malakooti@iau.ae

Nilofar Mansourzadeh
Student of Department of Computer Engineering
Islamic Azad University, UAE branch, Dubai, UAE
n_mansourzadeh@yahoo.com

**ABSTRACT:** Many companies use cloud computing for their storage purposes to get benefit of using cloud environment to decrease the cost and accessibility of the data. When we store our data over the cloud environment, to obtain the low cost storage, we will lose the control over our data and certain type of security as well as different levels of security should be applied depend upon the type of data. The applied security will protect our data from intruder and hacker even though they obtained our data accidentally or intentionally. There are various forms of security algorithm and models that can be used to protect our stored data over distributed networks and cloud environment.
The method that we have proposed is based on the scrambling algorithm and multilevel encryptions. We have designed, implemented, and tested our security model on the image type of information that is going to be stored on the cloud environment.
Our model can be modified and expanded to apply security on the multimedia information, real time video and movies that are going to be stored on the cloud servers. In addition, we have presented a new model based on multi-cloud distributed system, in which the specified information will be divided in to N different segments and each segment will be stored on one cloud server to prevent hacker from accessing the entire information. This process will apply higher level of security even the information is already scrambled and encrypted.

**Keywords**: cloud computing, data security, data integrity and availability, depsky model,Bioemtric

## I. INTRODUCTION

We have issues in cloud computing such as security of data, file system, backup, network traffic, and host security [1-2]. There are some important policy problems in cloud computing which include issues of privacy, security, namelessness, trustworthiness, and responsibility. The most important issues regarding to cloud computing is the security of information stored inside the cloud servers as well as the implementation of the well-designed cloud architecture over the distrusted networks. The security issue is a general term and it all depends upon the user's points of view and types of security required for their resource and applications software [3].

Although, the cloud computing is intended to be efficient, reliable, and cost effecting but several problems exist regarding to the storage of data and information over the cloud networks. Since many companies store their information and even their software applications over the cloud environment these information may become vulnerable and goes under some changes. Thus, a special type of security required to be applied before this information are carried and stored over the cloud environment.
We have presented a robust information security model based on the scrambling and multi-level encryption. Our paper is organized as following:
In section II we discuss about cloud data security and other issues. In section III we talk about related works and problems exist in the cloud data security. In section IV we focus on the proposed information security model. In section V, the paper is concluded and future works is presented.

## II. DATA SECURITY AND ORHER ISSUES IN CLOUD COMPUTING

Cloud computing can be considered as the next generation of IT architecture because in the traditional data storage facilities the data are located on the physical or logical devices that are controlled by the users [4]. But, in cloud computing environment the application software, general services, and databases are distributed and stored over the cloud networks and the users have no idea about physical location of the data or any services. The lack knowledge about the physical location data or services makes the cloud environment unreliable, unsafe, and vulnerable to many attacks by intruder illegal users.
Thus, the user can not have a full trust for their stored data on the cloud environment and their information

must be secured by some algorithm before it has been stored on the cloud environment.

Time, cost and innovation are the most important factors of cloud computing but the security problems still need to be considered and taken into account for the cloud environment [5]. Beside the security problem there are some other issues that need to be considered before we have stored our data over the cloud environment. The most important issues are as following:

1- **Data Integrity**
**2- Data Availability**
**3- Data Location and Relocation**
**4- Data Storage Backup and Recovery**
**5--Privacy and Confidentiality**
**6- Multi-Cloud Platform Support**

**1-Data Integrity**: The cloud service provider is responsible for establishing some type of reliable mechanism to assure the integrity of the stored data and service as well as ability to analyze the physical location of datasets and certain database on the cloud environment.

In addition, the user must be aware of the physical location of the data or services on the cloud and know what particular dataset are on each host on the cloud. Data integrity and the ability to know that what type data are located on the public cloud is the main requirement to have prior information and advanced knowledge to prevent the tampering and vulnerability of the stored data [4].

**2-Data availability**: In cloud computing the data normally are divided into several different segments and each segment will be stored on different servers or even in different clouds. Thus, the data availability is another critical issue of the cloud computing during the demand time.

In addition to the data storage capability of the cloud environment the application software as well as the other services are stored and located on the distributed networks and cloud computing environments. Since, the clients and users have almost the same access right and they can simultaneously demand the execution of one service or application software, the heavy traffic on the cloud environment may cause the delay or interruption of the required service. Thus, clod providers are urged to implement some type of architecture to work along with the load sharing to increase the speed and efficiency of the data availability and prevent the interruption of the requested services.

**3-Data Location and Relocation**: As we mentioned before, the data will be divided into several pieces and to be stored on different locations on the cloud environment. The mobility of data over the cloud environment is another critical issue and clients may prefer to store their data on particular location. Thus, it must be some type of agreements between the clients and cloud providers in which defines the location of the specific data on the cloud environment

We have a high level of data mobility in cloud computing environment. Users of cloud computing do not know the location of their data, but maybe want to know its exact location or want to store their data on the preferred storage location. Thus, we need to have an agreement between the cloud provider and users of the cloud. In addition, it is suggested that cloud provider implement the strong authentication procedures to protect the client's stored information.

**4- Data Storage Backup, and Recovery**: Before our data are ready to be stored on the cloud environment, we must ensure that cloud provider has the reliable backup system and ability to return the original data back to the clients without any damages.

A simple backup system might be appropriate to be used for the data storage and recover of the cloud environment without any natural and manmade disasters.

In case of natural disaster such as earthquake, volcano eruption, flood, and tsunami the simple backup system might not be appropriate and backup system and recovery could be damaged. The level of damage also would be high when we have the manmade disasters.

To obtain a reliable backup system with robust recovery we have to design and implement a complex architecture for the cloud computing based on several cloud environments.

**5-Privacy and Confidentiality**: Although the cloud computing has several advantage over the tradition system but there are some disadvantages when the clients are going to store the sensitive data in the cloud environments. In addition to the security issues in cloud computing the data privacy and confidentiality are another issue that must be considered. When the data are stored on the cloud environment the users have no control over the data but the service providers and government authorities can easily access the user's data without obtaining any permission. There should be some kind of agreement between the users and cloud providers that only authorized users can access the data stored on cloud environment and confidentiality and security of the data are guaranteed by the cloud providers.

**6-Multi-Cloud Platform Support:** The main issue of the IT companies and enterprises are how to merges the cloud services stored on the different

cloud environments, with different operation systems. With the multi-cloud platform we can mix, the public clouds, private clouds, and even the virtualized environments to obtain the architecture that meets our cloud requirements and strategies. The cloud providers are responsible to provide the required software and hardware to support the communication between different cloud environments with different hardware and different operation systems.

## III. REALATED WORKS

The emergence of the cloud computing environment makes it possible for the software vendors to distribute their software over the virtual machines and virtual servers rather than physical servers. The cloud environment makes a simple interface between the user and software vendor. Thus, the software vendors only focus on the software development rather than being worried about the platform.

In traditional data center the security is measured on the edge of hardware platform but in cloud computing the processes of data storage and service storages can be done through the virtual servers, in which each virtual server belongs to different logic groups. This mutual relationship and communication between the logical servers make it possible to create a lot of security threats on these servers that may damage the integrity of the data stored on the cloud environment [5].

Dai Yuefa, et al [5] presented a data security model based on three-level defense system structure, in which each level of defense system is responsible for one type of operation related to the security of data in the cloud environment. The first level of operation is responsible for the user authentication. The second level is dedicated to the user's data encryption, and the third level of operation is for the fast data recovery.

In this model if the attacker can bypass the authentication stage or the authentication system is deceived by some type of operation, the attacker is not able to capture the original data because the data in the second level of security system are already encrypted and intruder or attacker is unable to obtain effective access to vital information, such as business secret information. The rapid restoration of files in the third level by using fast algorithm makes it possible to obtain the user data with the maximum recovery rate even in case of some damages [5]. Although this method looks like an ideal model but it has its own weakness and limitation.

This model is based on the user's private matrix, M, which can be captured by the intruder during the transmission process. In addition, the encryption process in second stage is slow and time consuming.

K. Govinda, Yannnik Ngabirano [6] and Mohit Marwaha, Rajeev Bedi [7] has applied the encryption algorithm to analyze the feasibility of the data encryption on data security and privacy in cloud environment. In [6], the base key obtained by extracting the client biometric features to generate public required for the RSA algorithm.

Alysson Bessani , Miguel Correia, et al [8] presented a new multi-cloud model called DEPSKY, and indicated that this model is dependable and secure for the data storage on the cloud environment. They mentioned that changing from single cloud to multi cloud environment can solve the issues exist in the service availability and security attack of single cloud environment. There are several cloud providers that provide three main categories of the cloud services, Infrastructure as a Service (IaaS) or Hardware as Service, Software as a Service (SaaS), and Platform as Services (PaaS).We have mention the name of some cloud provider and their services as following:

1) Amazon S3, Microsoft SkyDrive and Nirvanix cloudNAS for cloud storages which allow users to access data.
2) Amazon EC2 for providing computation resources.
3) Google Apps supplies online cooperation tools

DEPSKY provides a virtual storage based on the cloud system that includes four different cloud providers and two different agents. The main task of DEPSKY is to increase the availability and the confidentiality of data by using multi-clouds providers, joining Byzantine quorum system protocols, cryptographic secret sharing and erasure code. Each cloud provider has its own interface and the encryption algorithm is placed on agents. So there is no need to execute code on the cloud providers [9].

We have presented a new data security model based on the scrambling and multi-level encryption for the cloud environment, called Malakooti-Mansourzadeh Multi-cloud Information Security Model (MMMDSM) which is the combination and modification of two models, data security using Biometric features [7] and DEPSKY[8].

## IV. PROPOSED MMMISM MODEL

In this paper we just focused on the security of the stored images on the cloud environment but it can be applied on other type of information such as, voice, text, multimedia, and even movies. First we have selected four images and merged them to obtain a group image to be able to implement our model on the group image and compare its result with the DESKY model. Once the group image is formed, then three levels of securities are applied to obtain a highly secure stored image on the cloud as following:

1- Layer One of Securities: In this layer we have applied our scrambling algorithm on the group image.
2- Layer Two of Securities: Once the group image is scrambled we have applied the XOR operations on the elements of the Scrambled Group Image (SGI) with the elements of Malakooti Transform (MT) Algorithm used as the General Key (GK) Matrix, to implement additional security on the stored images.
3- Layer Three of Securities: In this layer we have applied more complex algorithm, based on the combination of, Malakooti Randomized Key Generator (MKG), and Malakooti Polynomial Algorithm (MPA), to generate four Individual keys(IK) required for the third level of securities.

**Fig. 1-** Merging the four different images into one image

## Scramble Algorithm:

Our proposed scrambling algorithm is designed and implemented on the square images with the image size M, where M is power of two, $M=2^N$. This algorithm can be applied on any type of non-square images with the different image sizes.
In this algorithm the color RGB images will be converted into three matrices of Red, Green, and Blue. The algorithm then applied on each matrix and then the scrambled matrices will be combined to form the scrambled image. The algorithm works as follows:
First the elements of main diagonal in each image matrix will be move into its corresponding temporary array. Then, the elements of the upper diagonal and lower diagonal will be moved to the end of temporary array. This operation will be continued until all elements of the upper diagonal and lower diagonal are moved into the end of temporary array.
Once all elements of image matrix(R, G, B) are moved into the corresponding temporary array then these elements will move back into corresponding scrambled image matrix(R,G,B). These three matrices will be combined to form the RGB color space scrambled image, as shown in Figure 2.

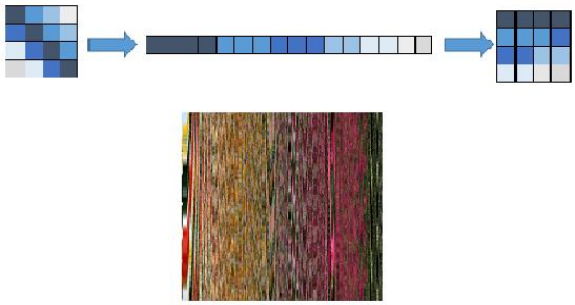

**Fig. 2-** Scrambled group image

### IV.A- Generation of the General Key matrix

We have generated the elements of the GK matrix and applied the XOR operation on the elements of the scrambled group image with the elements of the GK matrix as following:

**Generate Malakooti Transform matrix:**

1) Enter two integer numbers, a and b, i.e., a=1, b=2.
2) Let $M_0=1$ (5-1)
3) $M[0,0]= M_0$ (5-2)
4) $$M_k = \begin{bmatrix} a\,M_{k-1} & ab\,M_{k-1} \\ ab\,M_{k-1} & a\,M_{k-1} \end{bmatrix}$$ (5-3)
5) Apply XOR operations on the elements SGI and GK Matrices

$$EncImg[i, j]= ImgSc[i, j] \text{ XOR } M [i, j] \quad (5\text{-}4)$$

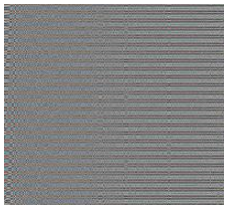

**Fig. 3 -** Encrypted image applying XOR on SGI and GK matrices

### IV.B- Generation of the Individual Key

We have divided the scrambled and encrypted group imaged into four sub-images, the same size as the original individual images. We also generated four individual keys to be applied on the scrambled and encrypted sub- images as following:

1) Generate the MT: The generation of Malakooti Transform is the same as IV.A but with different values as before, a=1,b=1.
2) Generate the Malakooti Randomized keys (MRK).
   A. Enter two large prime numbers to start the key gen algorithm.
   B. Enter the block size to stop the key gen algorithm.

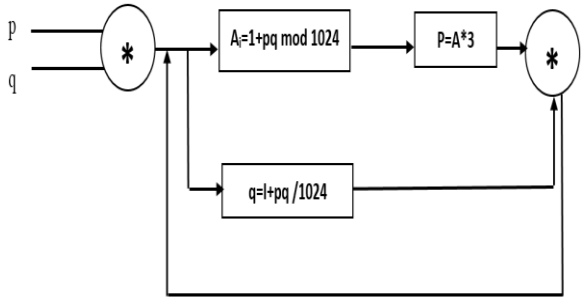


**Fig. 4**- Generation of Randomized Keys

3) Generate the polynomial Weight Functions:

$$W = [1 \; X \; X^2 \; X^3] \qquad (5\text{-}5)$$

4) Generate the Malakooti Polynomial Coefficients, P:

$$P_i = M_i \, W^t \qquad (5\text{-}6)$$

5) Generate Four Individual Keys:

$$\begin{aligned} IK(1) &= A_{1,1}P_1(x) + A_{1,2}P_2(x) + A_{1,3}P_3(x) + A_{1,4}P_4(x) \\ IK(2) &= A_{2,1}P_1(x) + A_{2,2}P_2(x) + A_{2,3}P_3(x) + A_{2,4}P_4(x) \\ IK(3) &= A_{3,1}P_1(x) + A_{3,2}P_2(x) + A_{3,3}P_3(x) + A_{3,4}P_4(x) \\ IK(4) &= A_{4,1}P_1(x) + A_{4,2}P_2(x) + A_{4,3}P_3(x) + A_{4,4}P_4(x) \end{aligned} \qquad (5\text{-}7)$$

Where $A_{i,j}$ are the elements of the MRK and $P_i$ are the elements of Malakooti Polynomial coefficients.
We finally apply the XOR operations the elements of each scrambled and encrypted sub-image with its corresponding individual key to implement the third level of security on the images that are going to be stored on the cloud environment. We can apply our algorithms on two different scenarios:

**Scenario 1:**
In this scenario the group image is scrambled and encrypted based on our proposed algorithm as already explained. Thus, the scrambled and encrypted image will be divided into four sections and each section will be XOR with its corresponding individual key. Once, the individual keys are applied on the corresponding sub-images they will be combined to form one image that will be stored into four different cloud environments for the sake of security, data availability and accessibly.

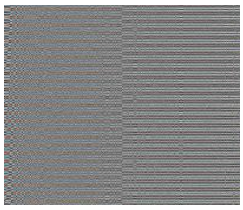

**Fig. 5**- encrypted image by 4 different keys

**Scrambled Matrix /XOR with Gen and Individual Keys**

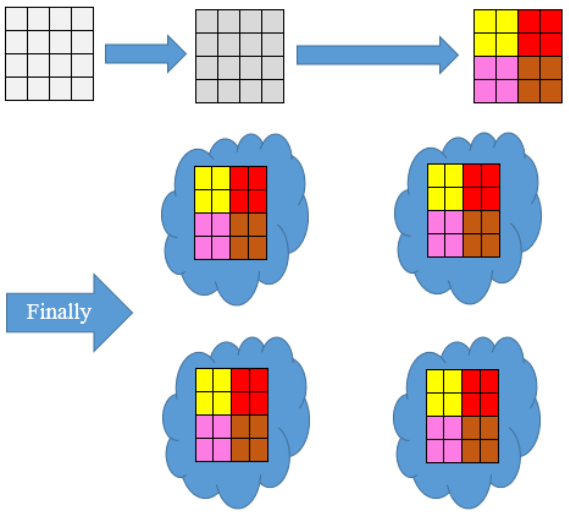


**Fig. 6**- Store the scrambled and encrypted image into four different cloud providers

In this scenario we have four copies of coded and stored image and can retrieve the original image just from any cloud provider. The cost of storing four copies of coded image would be high but the security is very high too.

**Scenario 2:**
The first two steps of this scenario are the same as scenario 1. Once, the group image is scrambled and encrypted then it will be divided into four part and each parts will be XOR with the individual keys. After the individual keys are applied on the corresponding sub-images the four coded images will not be combined but the combination two parts will be stored into four cloud providers(AD,BC,CB,DA) or six cloud providers(AD,BC,CB,DA,BC,AD) depend upon the type of the stored data, where A,B,C, and D are representative of 4-sub images.

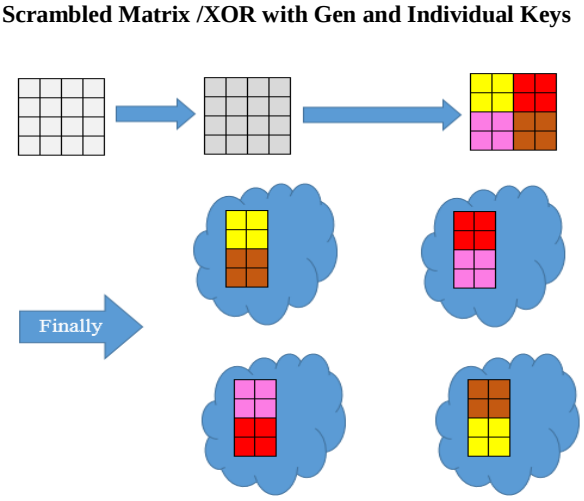


**Fig. 7**- Divide the image and distribute the parts into Four cloud providers

In the scenario-2, Figure 7, if the cloud providers' numbers 2 and 3 have failed simultaneously or are inaccessible then we will lose 50% of our image information. To solve this problem we have stored image parts BC and AD into two other cloud providers, totally six cloud providers to provide the high degree of security, availability, and accessibility.

## V. CONCLUSIONS AND FUTURE WORK

Cloud Computing has solved the problem of data storage and service availability but still has its own security problem. When data are stored on the cloud environment the user's data are no longer under his control. In addition to the security issues in cloud computing the data privacy and confidentiality are another issue that must be considered and govern authority and cloud provider can easily get access to the data without getting any permission.

We have a robust Security Model for Cloud Computing Based on the Scrambling Algorithm and Multi-Level Encryption to provide high level security on the stored data on cloud environment. Our Algorithm highly secured because three level of security are applied on the data before stored on the cloud. In addition, to our security algorithm we have applied two different scenarios similar to DESSKY to increase the viability as well as accessibility. Our algorithm has better performance than DEPSKY because addition scrambled algorithm is applied before the encryption and also we have use a complex but fast symmetric encryption as oppose to time consuming RSA algorithm. Finally, we have used the Malakooti Polynomial coefficient to generate the individual key and we have suggestion that these coefficients will be replaced with biometric features obtained from the Finger print, face, or even the user Iris.

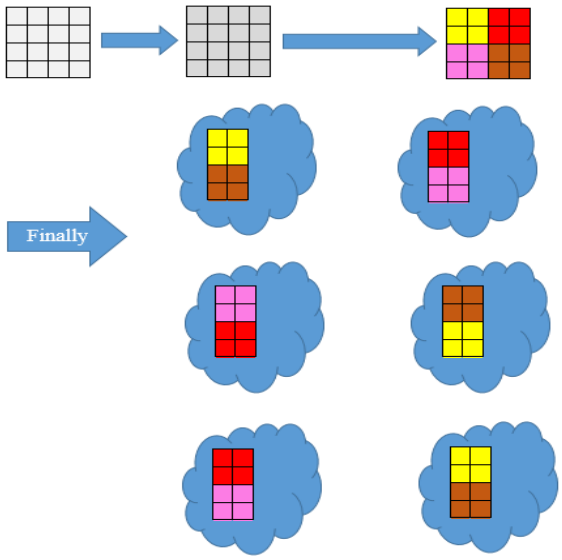


**Fig. 8**- Divide the image and distribute the parts into Six cloud providers

## VI. REFRENCES

[1] Neha Jain, Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security", VSRD-IJCSIT, Vol. 2, 2012,

[2] K.S.Suresh, K.V.Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 10, 2012

[3] Mandeep Kaur, Manish Mahajan," Implementing various encryption algorithms to enhance the data security of cloud in cloud computing", VSRD International Journal of Computer Science & Information Technology, Vol. 2 No. 10, October 2012

[4] Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[5] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing, , "Data Security Model for Cloud Computing", Proceeding of IWISA 2009, Nov. 2009, P.141-144,*Qingdao, China.*

[6] K. Govinda, Yannnik Ngabirano, , " Secure Data Storage in Cloud Computing Using Biometric", IJARCSSE, Vol. 2, Issue 5, May 2012,P. 11-16.

[7] Mohit Marwaha, Rajeev Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, P. 367-370, January 2013

[8] Alysson Bessani, Miguel Correia, Bruno Quaresma Fernando Andr´e Paulo Sousa, "DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds", University of Lisbon, Faculty of Sciences, Portugal.