Cloud Data Security in Database using Kernel Convolution Encryption Model

J.Kingsleen Solomon Doss

Research Scholar

VISTAS

Chennai, India

Dr. R.Varalakshmi

Associate Professor

VISTAS

Chennai, India

ABSTRACT*:* In this paper, a secure Cloud Data Security Data is proposed using Kernel Convolution Encryption Model (KCEM). The secure data provided by cloud with the ability to store encrypted convolution format to a powerful cloud data without providing the model or revealing source safe data in cloud. To this end, a real data is secured in KCEM by using a data to store in cloud. Additionally, a convolutional encryption is designed and added in the framework. Experimentally, the model was trained for Cloud Data's. This encrypted cloud data shows secured results for all classification in cloud which is compared against an unencrypted data's.

Keywords: Cloud; Kernal; Convolution; Encryption Security.

I.INTRODUCTION

Today we are in the era of cloud computing. We are also using the concept of distributed computing over the internet which is called cloud computing. In this Cloud Data Security is used widely in the internet or intranet and central remote servers to maintain the secure data and applications. Cloud data collects all information from the users and computing resources and manages them automatically by using various software.

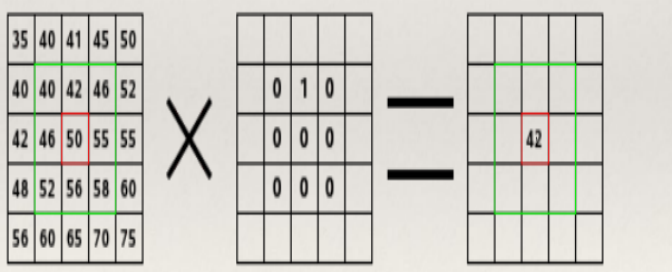
Cloud encryption is a service offered by cloud storage providers whereby data, or text, is transformed using encryption algorithms and is then placed on a storage cloud. Let's take a look at how your cloud data can be potentially compromised and how you can add another layer of protection by encrypting. Data stored in the cloud is nearly always stored in an encrypted form that would need to be cracked before an intruder hacks the data. I recently tried to store data by byte and convolute methods. As a special I did a small homework which can encrypt an entire byte array by twisting the data. With my methods it is portable and the data is stored very efficiently with secure. Cloud data security through KCEM is new technique which many data's wants to store in order to secure their way of storing in cloud.

II.KERNEL CONVOLUTION ENCRYPTION MODEL

A. What is Kernel

The kernel is the central module of an operating system which we already known but in another method for Image Processing kernel is used. A kernel is a (usually) small matrix of numbers. The kernel connects the system hardware to the application software in operating system. Every operating system has a kernel. Likewise for Processing the Data in secure way in cloud i used the concept of kernel.

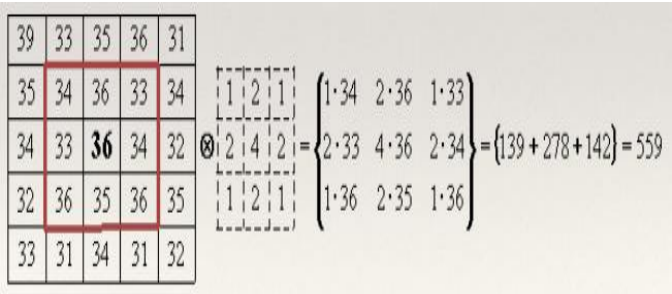
Figure shows you the sample Kernel processing



B. Convolution

This is loosely related to a form of mathematical convolution. It should be noted that the matrix operation, convolution, is not traditional matrix multiplication, even though it is, typically, denoted by *. In words convolution is: given two three-by-three matrices.

Figure shows you the sample Convolution processing



III.KMEC TECHNIQUE

*C. **Description of the this Technique***

Kernels are an automatic method to linearly separate the input data so that we can train linear algorithms on it. Feature spaces with kernel methods are different. First the feature space is not handcrafted. Instead it is determined by the selection of a kernel. Different kernels implicitly indicate different feature spaces. Second, the feature space is usually of a much higher dimensionality so that the data is more easily linearly separable

The performance of kernel methods depends on how easy it is to linearly separate the data and also the algorithm employed to learn the separation. The choice of the right kernel for a particular data distribution is crucial in making the data linearly separable. There is a different approach to computing the kernel function that speeds up computation time considerably

D. ***MCET Main Concept by Pictorial Representation***

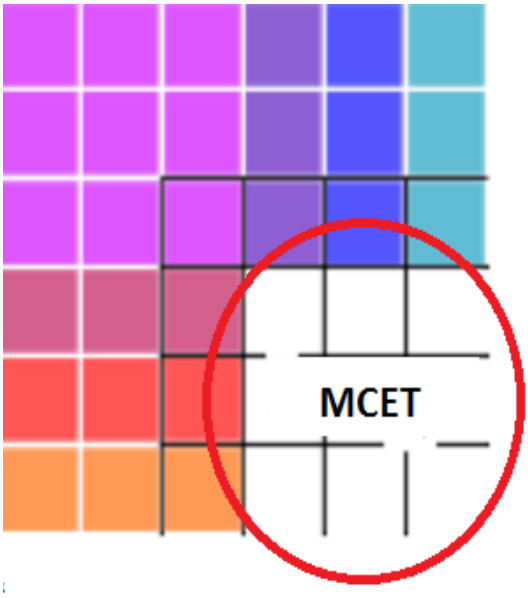


Figure 1. MCET

E. ***Matrix Swapping from byte array***

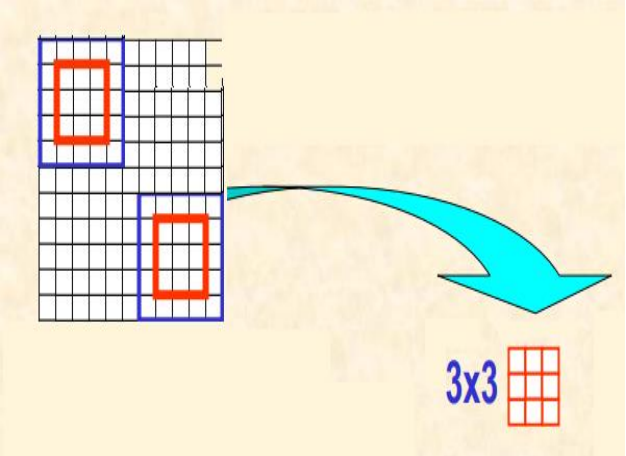
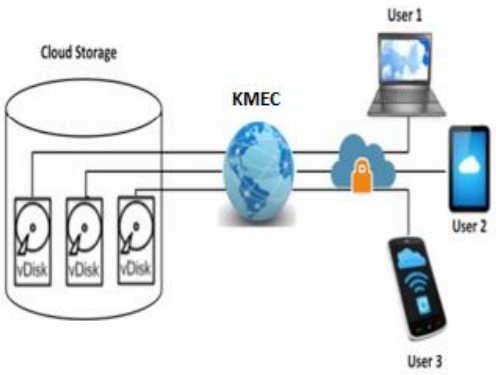


Figure 2. Bytes Swapping Method

F. *Main Diagram for KMEC*



IV.ADVANTAGES OF USING KCEM

After the encryption completed, the data is ready for the implementation. The Main Advantages of using this KCEM is as follows.

G. KCEM ADVANTAGES

a) The KCEM approach has underlying advantages.

b) Data secures using encryption even cloud admin does not knows the data for every respective respondent.

c) It performs on all security data,this method twist data in all kinds so that data wont get loss.

d) This process is very easy and need nothing ,just required couple of things a file containg data and a routine to generate KCEM encryption method. The is quite simple.

e) This process could be applied on a selected sets of one (or more) data fields.

f) The most important and popular cloud service is data storage. In order to preserve the privacy of data holders, data are often stored in cloud in an encrypted form. Our Encryption values are expected to be changed continuously for all data. mostly data security are less expected to be changing for the intruder and have a few chances to be altered during convolution encryption.

g) The process is not restricted or limited only. Care must be taken while applying kcem method in cloud; otherwise *the usefulness of the data will be destroyed and it loses true and correct information*.

*H. **Encryption algorithm Followings are the steps in proposed encryption algorithm.***

Step 1

Any Data will be converted into byte array with user defined encryption.

Step 2

Get the 3x3 Matrix for the last string array from the byte array.

Step 3

Get the 3x3 Matrix for the first string array from the byte array.

Step 4

Twist the value from last to first in each data which is converted.

Step 5

Each matrix use three different key K=K1, K2, K3 for encryption.

Step 6

Apply the encrypted value into the first and last matrix in the same order.

Step 7

Save the data in the cloud. Repeat it vice-versa for decryption

I. KCEM FIGURES

The main principle objective is to Secure the Data using Kernal Convolution Method. Accordingly, in order to achieve this objective, detail as-sessment on this is reference model, threat and attacks for securing data.

TABLE I.

S. No	Kernel Convolution Encryption Model	
	Advantages	***Disadvantages***
1	Data Security	Nil
2	Data Integrity	Nil
3	Data Manipulation	Nil

Tablulation of Advantage and Disadvantage of MCET

Figure 1: A function that takes as its inputs vectors in the original space and returns the dot product of the vectors in the feature space is called a kernel function.

J. Characteristics of KCEM Techniques

Elasticity: it is one of the most essential characteristics of our vision of Cloud. It defines the ability of a given infrastructure to dynamically adapt to a scale.

Ability to adapt: This provide a set of automatization allowing it self-management. Its administration should require a minimum human intervention.

Quality of Service: is another key aspect of Encryption Technique, using metrics such as time response, the number of operations in a second; the service provides guarantees to its users. It no longer belongs to the user having to decide what resources to deploy but rather to define terminals that the service should meet.

High Availability: playing on replicated data in different data centers, the Cloud must provide reliable, not sensitive to the failure of an instance or a data center.

Cost reduction: Pay Per Use, means that the user only pays for the service based on its utilization.

Overview of our approach

My goal is to build up a model to facilitate the data security and sharing across cloud along with preservation of data confidentiality. For this we will be using an encryption technique to provide data security on cloud data.

CONCLUSION

This method States Kernel Convolution Encryption Method is one such method that can provide safe and secure data to user in cloud and if the user have control over encryption and decryptions of data that will be confidence and secure for more people to cloud platform.

REFERENCES

[1] Sachida Nanda Barik, “Data Swapping In Cloud Computing”INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH, VOL 3, ISSUE 04 145, ISSN 2347-4289 (2015).

[2] Manisha R. Shinde and Rahul D. Taur, “Encryption Algorithm for Data Security and Privacy in Cloud Storage” Available at http://www.imedpub.com/articles/internet-capabilities-for-effective-learningand-research-a-review.pdf, 2015.

[3] Jensen, Meiko, et al. "On technical security issues in cloud computing." Cloud Computing, 2009. CLOUD'09. IEEE International Conference on. IEEE, 2009.

[4] Shlomo, Natalie, Caroline Tudor, and Paul Groom. "Data swapping for protecting census tables." Privacy in statistical databases. Springer Berlin Heidelberg, 2010..

[6] Fienberg, Stephen E., and Julie McIntyre. "Data swapping: Variations on a theme by dalenius and reiss." Privacy in statistical databases. Springer Berlin Heidelberg, 2004.

[7] Sean Carlin, Kevin Curran, “Cloud Computing Technologies”, International Journal of Cloud Computing and Services Science (IJ-CLOSER), Vol.1, No.2, pp. 59~65, June 2012.

[8] Prof. T. R. Shinde, Prof. M. U. Sanap, Prof. N. M. Karolia, "Survey On Kernel Level Encryption", Volume: 05Issue:02,Feb-2018.