Secure Cloud Architecture based on YAK and ECC

Ankit Kumar Singh
M.tech Student Computer Science Department
Babu Banarasi Das University
Lucknow U.P India

Saroj Kumar
Assistant Professor Computer Science Department
Babu Banarasi Das
N.I.T.M Lucknow U.P India

Abhishek Rai
M.tech Student Computer Science Department
Babu Banarasi Das University
Lucknow U.P India

ABSTRACT
In the present scenario security is biggest issue over internet cloud computing acronym is served everywhere in fast and growing computer generation. So security over the cloud is prime concern .In this paper YAK and ECC are security measures use over the cloud YAK is an asymmetric key cryptography. Whereas ECC is an encryption algorithm. So using YAK and ECC over the cloud network administrator can enhance the security measures. As per concerned of security measures these algorithms can fulfill requirements over the cloud In this paper cloud model is proposed on the basis of cloud architecture where YAK and ECC are imposed in cloud architecture for enhancement of security measures

General Terms
Cloud Security, Use cases and actors, Encryption algorithms, Security features, Cloud, Cloud services

Keywords
CIA (confidentiality integrity availability), YAK [6], ECC (elliptical curve cryptography)[5].

1. INTRODUCTION
Cloud computing is the perfect platform for delivering any kind of services over pay per use model. It delivers the resources (hardware and software) as a service over the internet. It provides applications and performance of information technology via services. It is a model of arranging of IT services provided through a catalog that replies to the requirements of the user in a adjustable and easiest way. The billing of this model is based upon the usage made by the consumers. Cloud platforms emanate as systematic options to conventional computer centers. They shows a systematic way over the acquisition and maintenance of the computer centers through virtualization. Cloud computing has fascinated a great deal of attention in the education sector as a way of delivering more efficient, feasible, and decisive education services.
In present, most of the traditional education firms are enhancing not being relevant for necessity of educational development and not being capable to snap up with the transformation of learning demands in time. Thus cloud computing have brought eventuality for it. However, in common web-based e-learning mode, system development and preservation are established in interior of educational firms, which concludes in a lot of complication existed, such as a lot of financing required. Cloud computing is becoming a provocative technology due to its dynamic flexibility and effective usage of the computing resources; it can be promoted under any conditions where the feasibility of resources is limited.

2. CLOUD SERVICES
Cloud provides a common platform on which each user can implement its own architectures which is based on different services. It mainly provides three service models.

2.1 IaaS (Infrastructure as a service)
In Iaas cloud provides a virtual infrastructure so that service consumers and developers can extent up and down computing resources demand vigorously. IaaS provides virtualization over data centers and offers it as a service. Examples Amazon EC2, Windows Azure Platform.

2.2 SaaS (Software as a service)
In this software is presented to service consumers as a service on their appeal. It saves the user form the predicament of software deployment and its maintenance. Software are usually presented in a web browser as a service. Billing is based upon the usage of the software. Examples Microsoft Dynamic CRM online, Google Apps, Sales force**.**

2.3 PaaS (Platform as a service)
It provides a evolution stage with a set of services to support application design, development, testing on the cloud. Example Google Compute Engine, AWS Elastic Beanstalk and Microsoft Azure.

2.4 Service Oriented Architecture (SOA)
Service-Oriented Architecture (SOA) is a way of designing, establishing, expanding, and managing systems that are characterized by coarsened services and end users. The services represent reusable business functionality. In standard interfaces of SOA, service consumers compose applications and systems uses those services. SOA can meet these predictions, various conditions and standards have been recommended and conceived, and middleware things are becoming more powerful.

Service oriented Architecture provides a relation model based on three basic units.

1. Service Consumer
2. Service Provider
3. Service Developer

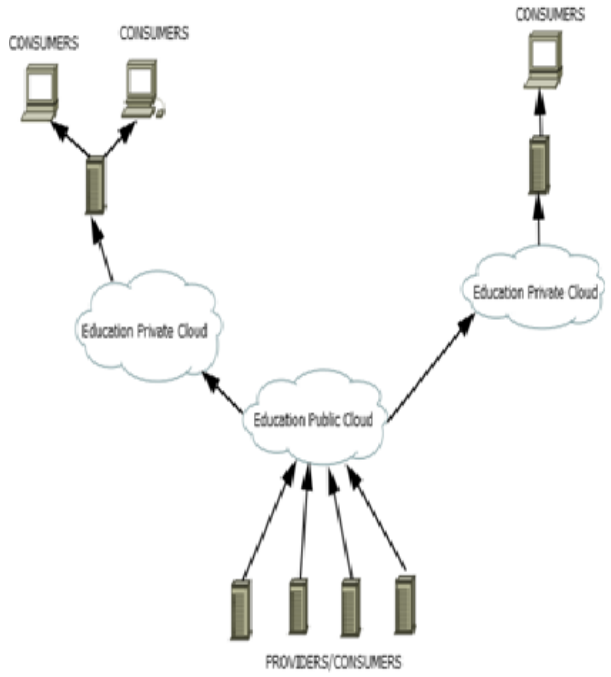

Fig.1 Secure Education System Model

In this paper a secure cloud model for education system is proposed. In this architecture Cloud Service Providers provide all the educational resources on public cloud which is accessed by anyone. The educational institutions which required the resources send request to their private cloud which is dedicated to their institutions. All Educational private cloud forward their requests to public cloud. thus public cloud provides all the essential resources to private cloud and private cloud forwards the resources to their consumers.

3. CLOUD ACTORS AND USE CASES

3.1 Actors

Actors define all the entities (person or program) that interact with the system.

3.2 Use Case

Use Cases define how group of service consumers and their resources may interact with one another cloud computing system to achieve specific goals.

Table 1 Cloud Actors Vs Use Cases

Use Cases\ Cloud Actors	
User	Any entity in world that is identified by a secure id and has a permission to access any data.
Cloud Subscriber	Any identified user that maintains a business relationship with a cloud.
Cloud Subscriber user(Developer)	Any identified user who works both as service provider and service consumer. In this way he works as a developer and consumer both.
Cloud User(Private Cloud)	They are consumers which interacts with public cloud based upon the requirements of end consumers
Payment Broker	Any financial broker that charges cloud subscriber based upon its service usage.
Cloud Service Provider	Cloud service provider are those who provide services over the network and take charge from the cloud subscriber including end users based upon the service usage .

4. ISSUES IN CLOUD SECURITY

Cloud security [1] is the one of difficult task due to third party authentication, dynamic distribution, flexibility and scalability. The three basic goals of cloud security of confidentiality, availability and integrity, known as CIA triad.

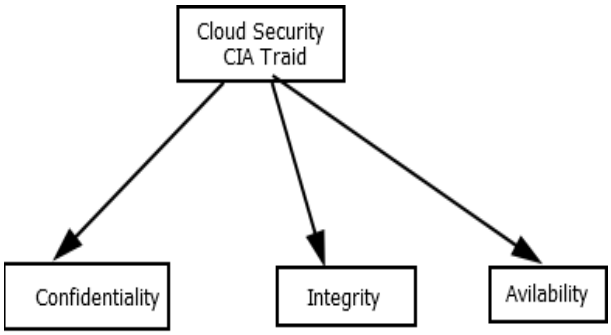

Fig.2 Cloud Security

4.1 Confidentiality

It is also known as security from unauthorized access. Confidentiality not only applies to the storage of the information, it also applies to the transmission of information. In cloud architecture it is assured by various things like encryption techniques, authentication methods, security protocols.

4.2 Integrity

Integrity means that changes need to be done only by authorized entities and through authorized mechanisms. Integrity violation is not necessarily the result of a malicious act; an interruption in the system, such as a power surge, may also create unwanted changes in some information. In cloud it is assured by the help of IDS and firewalls.

4.3 Availability

Availability ensures that all the resources should be available to all authorized entities .In cloud architectures it is assured by the help of Fault mechanisms, tolerance authentication, authorization, access control and network security.

5. PROBLEM STATEMENT

The security of educational resources of the consumers is the essential liability of cloud service provider. So for the adequate data security, system needs a mechanism that provides security against the different eve attacks and secure data transmission techniques. This paper focuses on security for education system including all security goals.

6. PURPOSED SYSTEM

In this introduced Architecture's aim is to remove security threats by the help of two methods as follows

6.1 Encryption Algorithm.

6.2 Security Features.

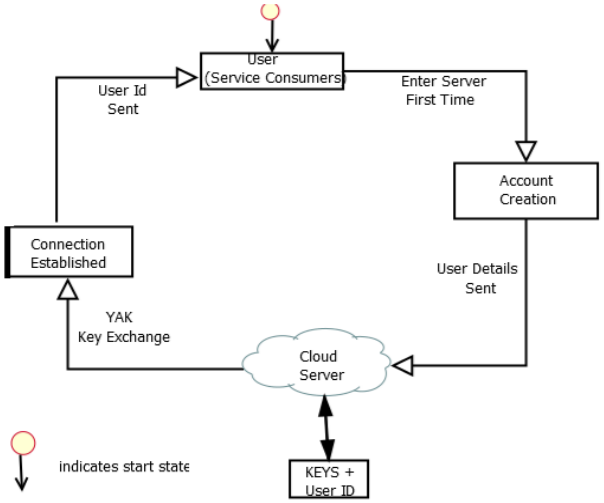

Fig.3 Account Creation

In this way a secure architecture provides reliability and security over cloud servers also. Provided corresponding model involves following steps

6.1.1. Connection Establishment

When Service Consumer logs in first time in he has to create the account in the system. The Basic connection is established over session secure layer protocol and secure hyper text transfer protocol.

6.1.2. Creation of account

When secured connections established then the service consumer is asked to fill the account details in the form provided by the cloud Server. After that the filled form is forwarded to the server for the account creation. Then the connection is established by YAK protocol. The server generates a user id as unique identification, its YAK equivalent stream, required public and private key for ECC encryption. User id is sent to end consumer over secure channel which is used as device for re authentication.

6.1.3. Authentication

When the user logs, SSL connection is created. As the account is accessed the service consumer is asked to provide all the essential details including user id. The cloud server checks the legitimacy of the end user by finding out YAK equivalent of the user id from server depository. When the keys matched, then the connection is maintained by this protocol and the user is logged into the server. At the background its private key and ECC algorithm is send for the data encryption.

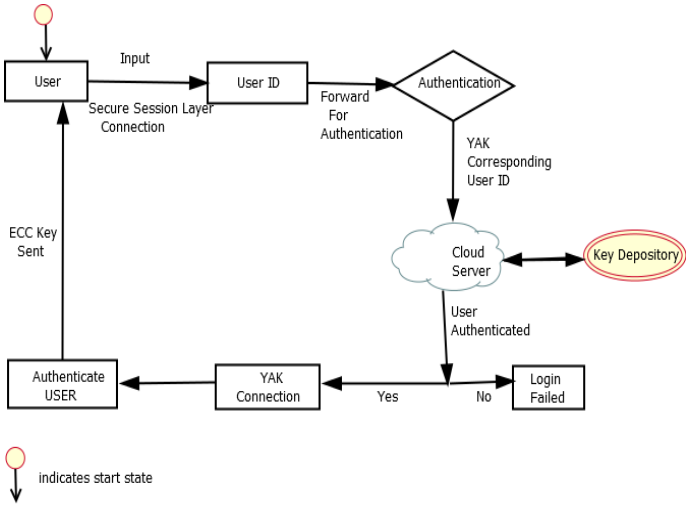

Fig.4 User Authentication

6.1.4. Data Exchange.

Data is transferred in two methods:

6.1.4.1. The client side

The client Query is transformed in a form of a file and encrypted using his public key. The encrypted data is forwarded to the server for processing.

6.1.4.2. The Server Side

The Sever decrypts the encrypted by its private key and processes the data. After that it encrypts the data using his public key and responses to the client.

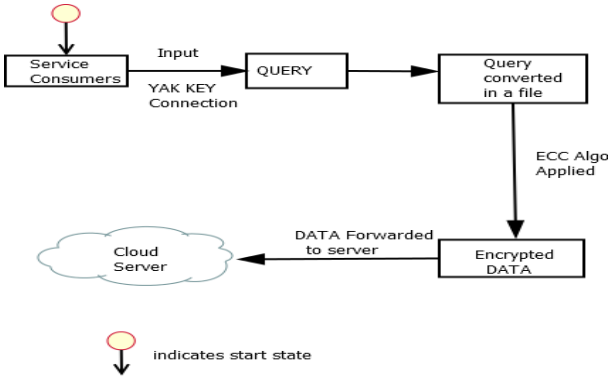

Fig.5 Data transfer from Client Side

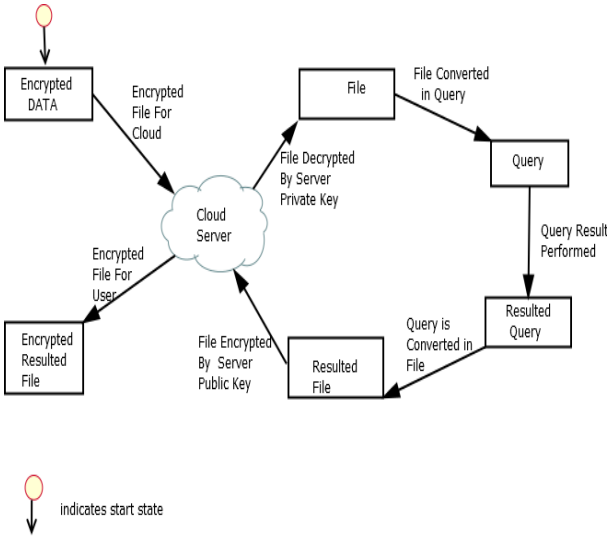

Fig.6 Data transfer from Server Side

7. SECURITY FEATURES

Security features identities the actions performed by the cloud actors on the educational resources. Each actor has a accessibly mode which is defined as following. So that the integrity of the data is maintained because no actor can perform any operations without any accessibility.

Mode Security features involves basic three actions which are performed by any actor:-

7.1 Access

It involves accessing, viewing of educational data.

7.2 Process

It involves modifying, updating and deleting of educational data.

7.3 Store

It involves storing or copying educational data.

Table2:- Function Vs Cloud Actors

Functions\ Cloud Actors	Access	Process	Store
User	Y		Y
Cloud Subscriber	Y	Y	
Cloud Subscriber user(Developer)	Y	Y	Y
Cloud User(Private Cloud)	Y	Y	Y
Payment Broker	Y		
Cloud Service Provider	Y	Y	Y

Table3:- Function Vs Information Life Cycle.

	Create	Store	Use	Share	Achieve	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

8. CONCLUSION

This paper proposed secure cloud architecture by using YAK and ECC. As in cloud computing security is major concern. Under YAK and ECC Algorithm given cloud architecture provide fast and secure accessibility to the user over the resource utilization. Cloud computing is a future of inherit resource utilization over the network. As security, speed and accuracy are the major concerns for resource migration over cloud computing. So proposed architecture which is incorporated with YAK and ECC is an one attempt of provide secure resource utilization and this will be base for many other algorithms related to security over the cloud model.

9. REFERENCES

[1] M.Joshi, YS Moudgil "SECURE CLOUD STOARGE" International Journal of Computer Science 2011, ijcscn.com.

[2] M.Premkumar "A SECURE CLOUD STORAGE SYSTEM WITH INCREASE AVALIABILTY AN ROBUSTNESS" 2012, ijeres.org.

[3] Dr. Chander Kant, Yogesh Sharma "ENHANCED SECURITY ARCHITECTURE FOR CLOUD DATA SECURITY" DCSA Kurukshetra University,ISSN: 2277128X,ijarcsse.com.

[4] Arjun Kumar, Byung Gook Lee,Hoonjae Lee,Anu. "SECURE STORAGE AND ACCESS OF DATA IN CLOUD COMPUTING " IEEE 2012 P.336339.

[5] Veerraju Gampala, Sri Lakshmi Inuganti, Satish Muppidi. "DATA SECURITY IN CLOUD COMPUTING WITH ELLIPTIC CURVE CRYPTOGRAPHY" Vol. 2 Isscue 3,july 2012 ijsce.com ISSN: 2231-2307.

[6] F. Hao."ON ROBUST KEY AGREEMENT BASED ON PUBLIC KEY AUTHENTICATION." Proceedings of the 14th International Conference on Financial Cryptography and Data Security, Tenerife, Spain, LNCS 6052, pp. 383-390, Jan, 2010

[7] Sven Bugiel1, Stefan Nurnberger1, Ahmad-Reza Sadeghi1, Thomas Schneider2 "TWIN CLOUDS: AN ARCHITECTURE FOR SECURE CLOUD COMPUTING" 1center of advanced security Germany. fsven.bugiel@trust.cased.de,stefan.nuernberger@trust.cased.de,ahmad.sadeghig@trust.cased.de. 2System Security Lab, Ruhr-University Bochum, Germany. thomas.schneider@trust.rub.de.

[8] Kawser Wazed Nafi1, Tonny Shekha Kar2, Sayed Anisul Hoque1, Dr. M. M. A Hashem2 "A NEWER USER AUTHENTICATION, FILE ENCRYPTION AND DISTRIBUTED SERVER BASED CLOUD COMPUTING SERCURITY ARCHITECTURE" 1Lecturer Stamford University Bangladesh.2 Khulna University of engineering and technology.

[9] Ren, Kui, Cong Wang, and Qian Wang. "SECURITY CHALLENGES FOR THE PUBLIC CLOUD." Internet Computing, IEEE 16.1 (2012): 69-73.

[10] Kaufman, Lori M. "CAN PUBLIC-CLOUD SECURITY MEET ITS UNIQUE CHALLENGES?."Security & Privacy, IEEE 8.4 (2010): 55-57.

[11] Sosinsky B, Cloud Computing Bible. 1st ed. Wiley; 2011.

[12] Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144.

[13] C. Cachin, I. Keidar and A. Shraer, "TRUSTING THE CLOUD", ACM SIGACT News, 40, 2009, pp. 81-86.