I.J. Engineering and Manufacturing, **2017, 6, 12-26**
Published Online November 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijem.2017.06.02

Available online at http://www.mecs-press.net/ijem

EduCloud: A Dynamic Three Stage Authentication Framework to Enhance Security in Public Cloud

G. Kumaresan[a,*], N.P. Gopalan[a]

[a] *Department of Computer Applications, National Institute of Technology, Tiruchirappalli - 620015, India*

Received: 25 August 2015; Accepted: 11 September 2017; Published: 08 November 2017

Abstract

Now-a-days, one of the most exciting technology is cloud computing. Accessing dynamically virtualized resources through internet is called as cloud computing. Security and confidentiality are the major concerns in public cloud. Though EduCloud (Educational Cloud) uses public cloud, moving data from one location to another location may lead to risk. Information related to staff, student and management or admin that can be shared in EduCloud, are to be secured in public educational cloud environment. In this scenario, data security is the most critical issue in cloud. But present authentication system available does not provide enough security in public EduCloud. Hence, we propose new authentication framework to enhance security in public educational cloud. The features of various authentication techniques are discussed in this paper and a novel framework is proposed for pubic EduCloud, which provides not only security but also improves the response time. The developed software tool is best suited and provably a secured solution to the public educational cloud environment.

Index Terms: Cloud Computing, EduCloud, Cloud Service Provider, Security, Authentication.

1. Introduction

Cloud computing is an internet based computing service which is dynamically accessible, virtualized and resources are delivered as a service across the internet. Cloud brings a lot of gains especially in ubiquitous services, in which everyone can access computing services provided over internet. These services using internet technologies, accessed through web browsers by the staff, students and management. According to the NIST definition [1], "cloud computing is a delivery model that enables convenient instant network access to a pool of

* Corresponding author.
E-mail address: kumareshtce@gmail.com

shared configurable computing resources that can be quickly provisioned and released with minimal management effort or service provider interaction".

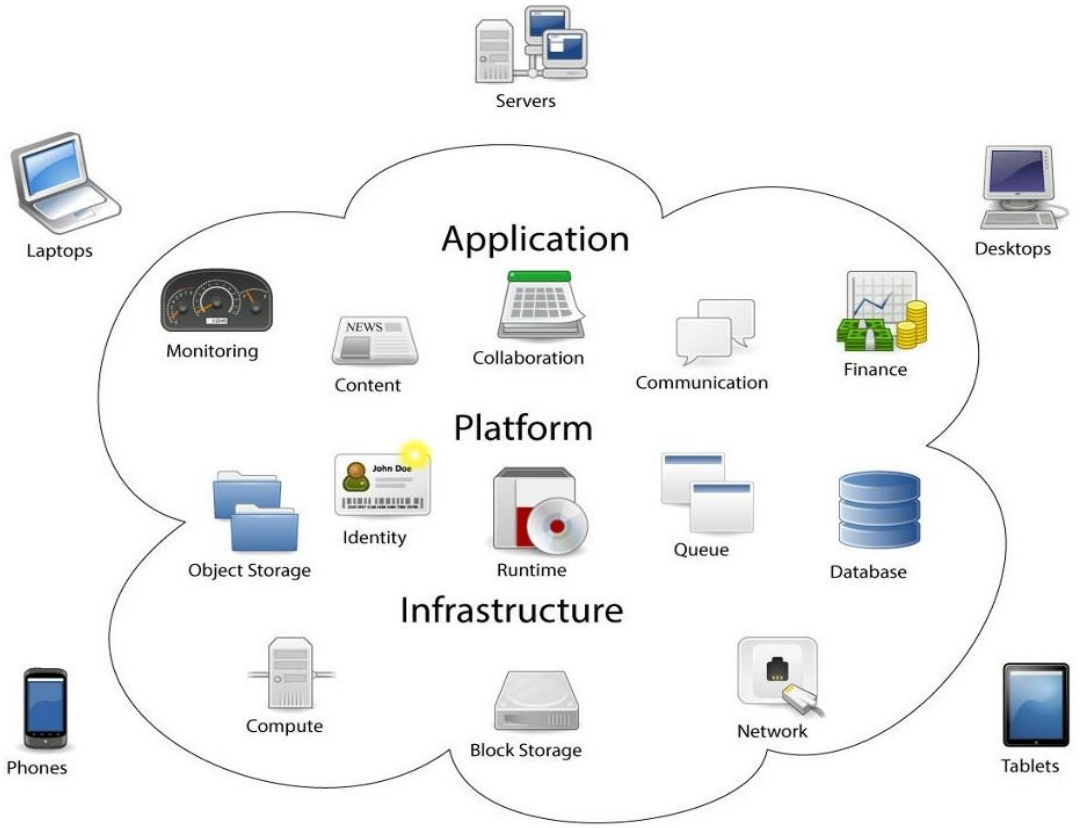

Fig.1. Cloud Computing

Cloud computing provides various services across internet such as data storage and virtualization [2], [3]. Cloud service provider applications and computing resources can be accessed anywhere, anytime using smartphone and personnel computers [4]. Cloud computing is an internet based computing, in which more than one computer is connected in the distributed environment for instant network access or data access to a collective group of computing resources as shows in Fig.1. Cloud environment decreases the need of installing and running the applications on the user's personal computer [5], [6] and [7]. Cloud service providers take responsibility to provide high security for their customer's information. They can help its customers via many services such as instant access to their data from anywhere, anytime and anyplace [8]. Cloud services include scalability, pay-per-use, data storage, data recovery and prevent against attackers.

1.1. Essential Characteristics

1.1.1. On-Demand Self-Service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

1.1.2. Broad Network Access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.

1.1.3. Resource Pooling: The service provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction.

1.1.4. Rapid Elasticity: Capabilities can be elastically provisioned and released, in some cases automatically to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

1.1.5. Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilized service.

1.2. Service Models

1.2.1. Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities with the possible exception of limited user specific application configuration settings.

1.2.2. Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage but has control over the deployed applications and possibly configuration settings for the application hosting environment.

1.2.3. Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and other fundamental computing resources where the consumer is able to deploy and run arbitrary software which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly limited control of select networking components.

1.3. Deployment Models

1.3.1. Private Cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers. It may be owned, managed, and operated by the organization a third party or some combination of them and it may exist on or off premises.

1.3.2. Community Cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns. It may be owned managed and operated by one or more of the organizations in the community a third party or some combination of them and it may exist on or off premises.

1.3.3. Public Cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned managed and operated by a business, academic or government organizations or some

combination of them. It exists on the premises of the cloud provider.

1.3.4. Hybrid Cloud: The cloud infrastructure [9] is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

1.4. Security Issues in Public EduCloud

Today, education is completely associated with the information technology for content delivery, communication and collaboration. The need for servers, storages and software is in high demand in the universities, colleges and schools. Cloud computing is the perfect technology to resolve this problem. However, security of data and breach of confidentiality are the major concerns in public cloud. Institutions may not worry about the security of their data, if it is hosted within the institutions [10]. Moving data from one location to another location without the control of the institution and the location, may lead to risk [11], [12]. One of the main benefits of cloud computing is high service availability, there is a chance that mostly high profile providers are at more risk such as denial of service attacks, rainbow attacks and phishing attacks [13]. In addition, the data may be sold to some third parties, without the knowledge of the users. In these circumstances, data security is the most critical issue. Hence, there is a need for an efficient security framework in public educational cloud.

1.5. Problem Definition

Confidential data of staff, student and management are to be secured in public educational cloud. Authentication is a key technique for data security, which is a technique to find proof of individualities to access any system. It is usually based on username and password. Traditional password authentication systems do not provide enough security for data in educational cloud environment. Hence, enhanced authentication techniques and framework should be proposed for public educational cloud to secure saved data.

The rest of the paper is organized as follows: In section 2, we give a brief review of previous work for authentication framework. In section 3, we present the details of the proposed authentication framework. We present its implementation in section 4. In section 5, we discuss the performance of the proposed authentication framework. Finally, we conclude the paper in section 6.

2. Related Works

This research work is focused on providing security for public Educational cloud environment. In this regard, we propose a new framework to enhance security in the public EduCloud. Security is the key factor for any cloud service providers. Therefore, we studied the literature of previous works to enhance the security in cloud from different perspective. Many researchers had presented different methods to enhance security in cloud environment. Prachi Soni *et al.* proposed a framework for multi-factor authentication based on educational cloud computing [14]. It analyzes the concept of educational cloud and describes the multi-factor authentication framework. The authors stated that the old-style authentication system doesn't provide sufficient security in public educational cloud. Hence, they proposed a well-organized authentication framework and a secure solution in public cloud environment. Later, an architecture was proposed [15] by Chander Kant *et al.* to enhance security in cloud computing environment where they introduced configured samba storage in cloud architecture and followed encryption and decryption mechanisms. The samba storage deployed with cloud architecture and used in particular operating system for three attribute values such as user or owner, group and global. Then, this cloud architecture mapped with cryptographic operations such as encryption and decryption. Paolo Cemim *et al.* proposed an academic cloud tool that provided a simple environment to realize and test cloud computing concepts [16]. It can be easily deployed, without the demand for additional hardware or access to external resources. It allowed the deployment of a private cloud tool using heterogeneous resources by common hardware.

It performs the various jobs associated to the management of a cloud structure. The proposed architecture of EduCloud (Educational Cloud) is divided into five primary components such as user interface, API controller, centralized storage, cloud controller and node controller. Rajesh *et al.* discussed [17] an optimized and secured EduCloud (Educational Cloud) virtualizations.

They analyzed various components and characteristics for cloud computing, which provides well defined cloud services to end users. Cloud uses virtualization which provides minimum cost services through internet. The authors also described about various security issues and then provided some guidelines to develop cloud computing for education. Finally, they stated that cloud computing is a correct technology to adopt for all educational institutions. A new multi-factor authentication framework was proposed by Rohitash Kumar Banyal *et al.* [18] for cloud computing. The proposed framework is helpful to verify cloud access management based on multiple factors and users are verified and accessed. The authors suggested that arithmetic captcha is an innovating factor for authentication to provide security in cloud computing environment. Bariah Aljebreen *et al.* discussed a higher educational resource sharing and cloud services [19]. Cloud computing can access anywhere, anytime to share with anyone; it is a big advantages for communication, collaboration and content delivery, as key parts in higher educational institutions.

The authors also surveyed many case studies, related frameworks, architectures and supporting tools that are related in migration of institution resources and management resources into cloud environment. Omondi John Opala *et al.* proposed [20] a work for an exploratory analysis of information security and its adoption into cloud. It has to improve the scalability approach for large organization, how data can be delivered as a service. Cloud computing is not a new one instead of a new type of approach in distributed environment. A survey was conducted by authors and the result showed that top management perception of cost effectiveness was more significantly related to their security. Hence, cloud security has the influence in educational institutions. Benjamin Fabian *et al.* discussed topological analysis of cloud service connectivity [21]. The authors focused on the network reachability of cloud services. Topological analysis was done by authors with the help of graph based measures. This article described the connection between the autonomous systems in the form of internet backbone. The authors approach can be used by cloud service providers directly involved and connect the internet; this will reduce the time and internet outages. Cloud service providers can use it to resolve the problems. Ashish Kumar Singh *et al.* proposed [22] a comprehensive approach to enhance security in proposed model called CAESAR cloud.

The authors stated that, now-a-days many companies are interested to migrate services into cloud, especially amazon and salsesforce by providing cloud hosting and cloud storage. Security is the major problem in cloud computing. So, they mainly focus on data security, especially malicious attacks such as denial of service attack. So they proposed CAESAR cloud mechanism to enhance security in public cloud. A.M. Mansuri *et al.* discussed [23] advantages of cloud computing while educational institutions and online marketing strategies using this service. In educational institutions, Staff, student and management or admin has opportunity to quickly access the resources from the cloud. Reducing the storage space and cost are the main benefits in cloud computing environment. Cloud is an important role in educational institutions, where online marketing has to provide data to the students, faculty, management and its customers. Ali Shahbazi *et al.* proposed security architecture for private cloud in a distributed key environment [24]. They presented the "Treasure Island security framework" to enhance security in private cloud. They proposed framework based on a distributed key in hadoop and google file system. The author's methodology utilized the sequential addressing and distributed key to provide more security in private cloud. When compared to the previous security mechanism, the results showed by authors have more security. A conceptual framework was proposed [25] by Mary Jane *et al.* by deploying cloud infrastructure as a service in higher educational institutions in the African continent. Here, they conducted a survey and the final results showed that, the possibility of deploying infrastructure as a service is enough to implement throughout the African continent. After that, Shanto *et al.* discussed [26] four module approach to secure cloud from denial of service attack in virtual machine. Cloud has great potential but still dangerous because of different type of attacks, such as denial of service. Hence, they proposed a four stage model to prevent the malicious attacks. Later, Kumaresan *et al.* proposed [27] a novel framework for two factor

authentication in public educational cloud. In their system prevents from malicious attacks and improves the response time. However, there are many techniques are analyzed [28] and it has been found that, with large number of technically advanced attackers out, there is a skill to launch a successful attack against any security system. Hence, there is a need for an efficient security framework to protect our high sensitive information in public cloud.

3. Proposed Work

The research work aims to propose new authentication framework to public educational cloud. Our model contains two phases, namely registration phase and authentication phase which are shown in Fig.2.

3.1. Registration Phase

Fig.2. shows the registration phase. The term user refers to the staff, students, and management. These users can register themselves using personal computer, laptop, and tablet or even with a smartphone. The details of the user will be registered and correspondingly monitored by the cloud service provider who is an admin. The admin takes the responsibility to generate a unique identification number for a particular user from the user details. This unique identification number is strictly accessible only by cloud service provider. All the registered details are stored and maintained in local database server by cloud service provider. After successful registration, an acknowledgement will be sent to the user via email or short message service.

3.2. Authentication Phase

Fig.2. shows the authentication phase. The proposed framework provides access to the registered users only. Correspondingly, a three stage selection process is proposed to enhance the security of the framework. Lists of standard algorithms are stored in the stack.

3.2.1. *User Select Stage:* In the proposed framework, the first stage is done by user, which gives an option for selecting an algorithm in the present stack.

3.2.2. *CSP Machine Select Stage:* In this stage, the cloud service provider (CSP) machine selects an algorithm randomly from the stack using a random generator. Both of the selected algorithms are compressed into a single file and stored in the memory buffer.

3.2.3. *CSP Person Select Stage:* The third stage is made by cloud service provider, by selecting an algorithm from the stack and the selected algorithm is computed with previously compressed algorithm.

3.3. Working Methodology

This result is captured at the end of encryption technique. The encrypted file will be decrypted with the help of standard decryption algorithm, which should match the unique identification number for the respective user in replica of the local server database. This signals a successful authentication message to the cloud service provider, which leads for next stage of access through their services.

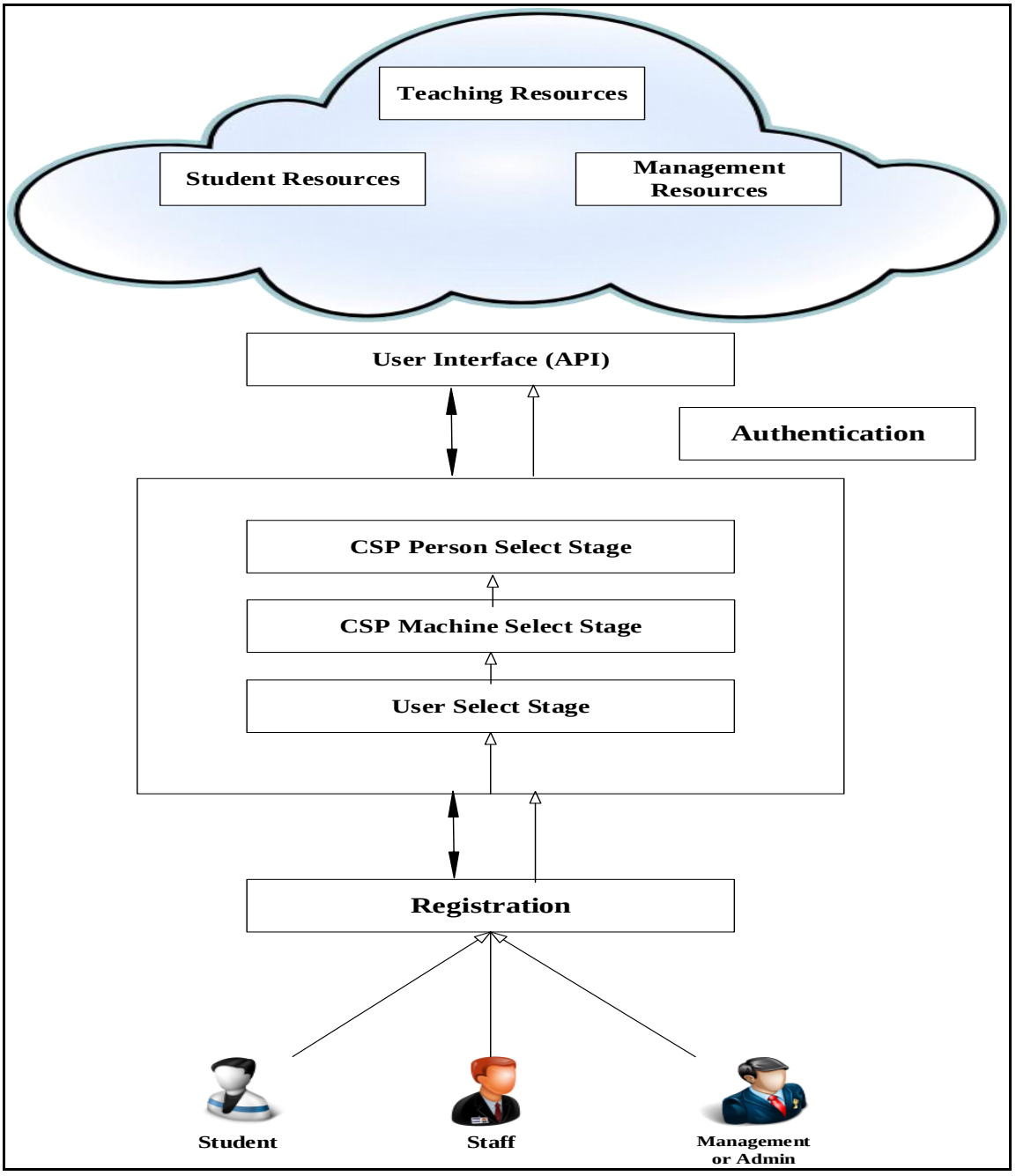

Fig.2. Framework for Dynamic Three Stage Authentication Selection in EduCloud

3.4. Pseudo Code for the Proposed Model

```
STEP 1:  registration()            //Module for Registration Phase
{                                  //CSP-Cloud Service Provider
        if ( login = = new user) {   //UID-Unique Identification Number
Get the details from new user;
Store the user details into CSP local server database;
Generate UID number for a particular user;
Confirm message sent to the user via email or sms;
Go To STEP 2;    } else
 {   Access Denied;
 }
                    }
STEP 2:  authentication()        //Module for Authentication Phase
{
 if ( login = = existing user)
{
System ask user to select one algorithm from the stack;
CSP machine randomly select one algorithm from the stack;
System ask CSP person to select one algorithm from the stack;
if (FinalId = = UID)
{   Access the cloud services;
 }
else {    Access Denied;  }
Go To STEP 2;   }
      }
```

3.5. User Interface(API)

User interface acts as a bridge between the user and cloud service provider. It mainly identifies what type of

user (i.e. student, staff and management etc.) can access the cloud resources in public educational environment. When compared to the previous model, the three stage model is highly reliable. Based on the proposed model, a software tool is developed for authentication in public educational cloud environment. This tool will be best suitable for securing high sensitive information in public educational cloud environment.

4. Implementation

We have implemented the above pseudo code on a personal computer (Dell with an i3-4005U CPU@1.70 GHZ Processor, 4GB Ram memory and the window 8 operating system) using the net beans environment. In our experiments, the personal computer and the database are the user and server respectively. The response time of those operations is listed in Table. 1. This paper deals with enhancing the security in public educational cloud. In this section, the developed authentication framework software tool has been implemented in EduCloud to resolve the issue such as

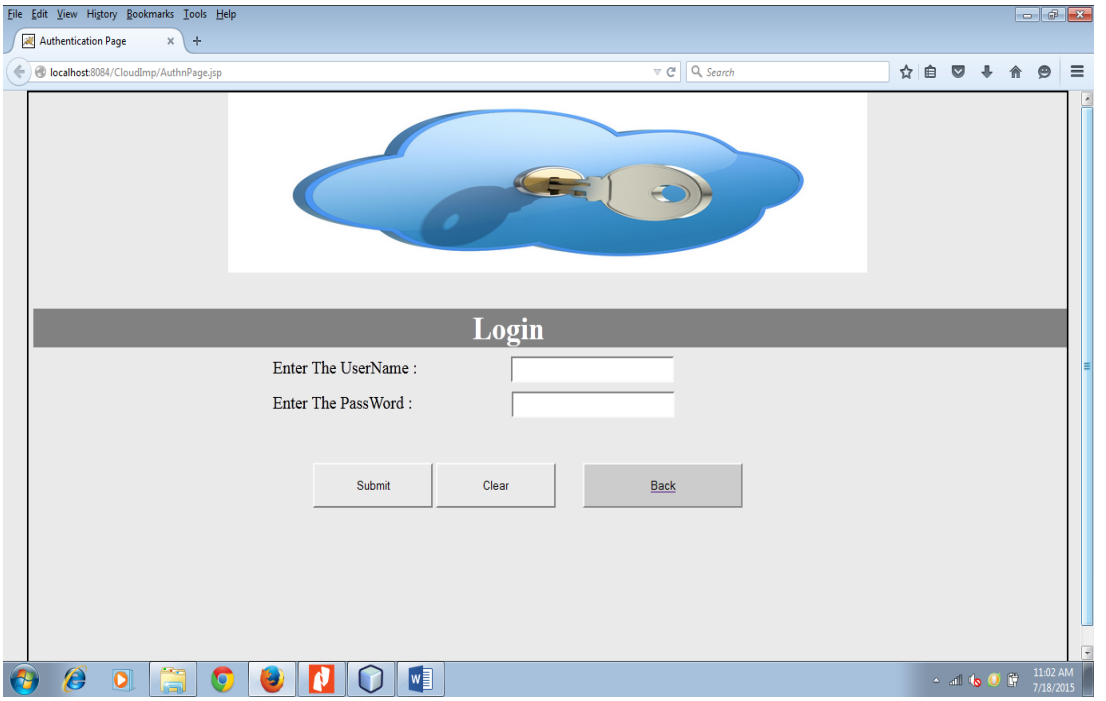

Fig.3. User Login Page

denial of service attacks, rainbow table attacks and phishing attacks. The main objective is to provide high security in public educational cloud. Legitimate users (such as student, staff and management or admin) can access the respective cloud resources. To access this cloud resources, user can sign into the cloud and get the acknowledge message from cloud service provider admin. Only, the authenticated users can strictly access these cloud services. Fig.3. shows the user login in which users (e.g. staff, student and management or admin) can enter their username and password.

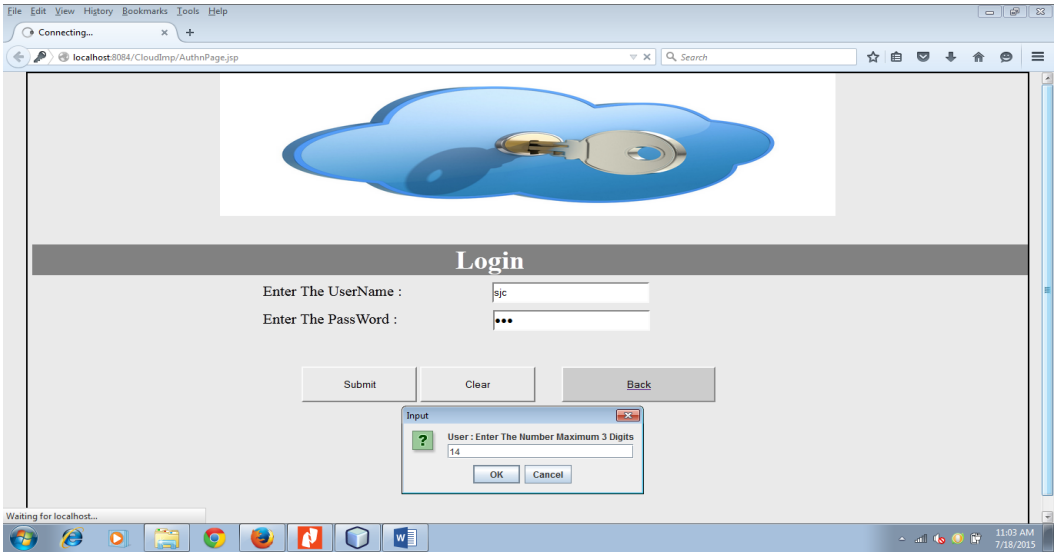

Fig.4. First Stage Authentication Page

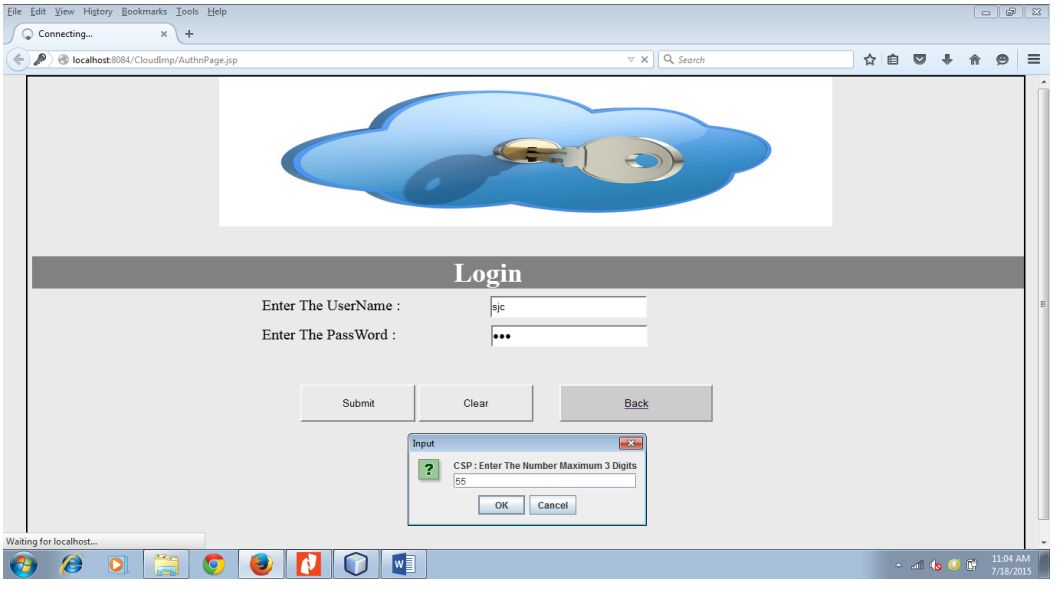

Fig.5. Third Stage Authentication Page

Fig.4. shows the first stage authentication, in which user needs to enter a number having one to three digits (1-999) into the field and submit the form. As the second stage is machine dependent, Fig.5. shows the third stage of authentication in which the cloud service provider person needs to enter the digit from one to three digits into the fields and submit the form. After successful authentication, it takes to next stage of access through their services. Fig.6. shows the cloud service. After successful authentication, the users access the respective resources in public educational cloud environment.

Fig.6. Cloud Service Page

5. Result and Discussion

Proposed authentication framework has been analyzed in public educational cloud environment. This work enhances security and also maintains the integrity of data. The response time are computed in accordance to the varying database records. These results are compared with earlier authentication techniques such as three factor and four factor authentications. The calculated results are compared based on their response time. Then, the improved speed up percentage can be measured using below formula.

$$Speed(\%) = \frac{ETF - PF}{ETF} \times 100, \tag{1}$$

where *ETF* represents the existing three factor authentication and *PF* denotes proposed factor. Table 1. shows that the number of records has been compared between existing three factor authentication, four factor authentication and our proposed factor authentication.

Table 1. Response Time for Varying Database Records

Number of Records (n)	Response Time (Sec)			Improvement in Speedup (%) From (1)
	Three Factor (ETF)	Four Factor (EFF)	Proposed Factor (PF)	
19	16.7	20.2	15.1	0.09
14	12.4	14.2	10.5	0.15
10	11.1	12.5	9.9	0.10
6	6.3	9.7	5.8	0.07
2	5.6	7.8	4.4	0.21

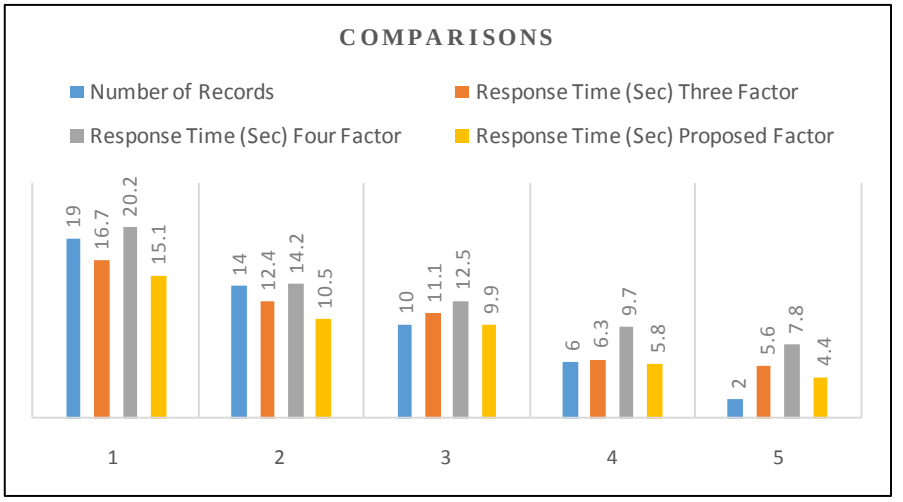

Fig.7. Comparison of Response Time

Fig.7. shows the comparison of response time for three and four factor authentication and our proposed authentication technique. It has been noticed that, depending upon the number of records, we achieve an improvement in speed up percentage. This can be seen in Fig.8. Hence, the response time is successfully executed from Fig.8. It is understood that, as the number of records increase, the improved speed up percentage decreases, and vice versa. Finally, it resists the attacks like denial of service, rainbow table etc., and also improves the execution time.

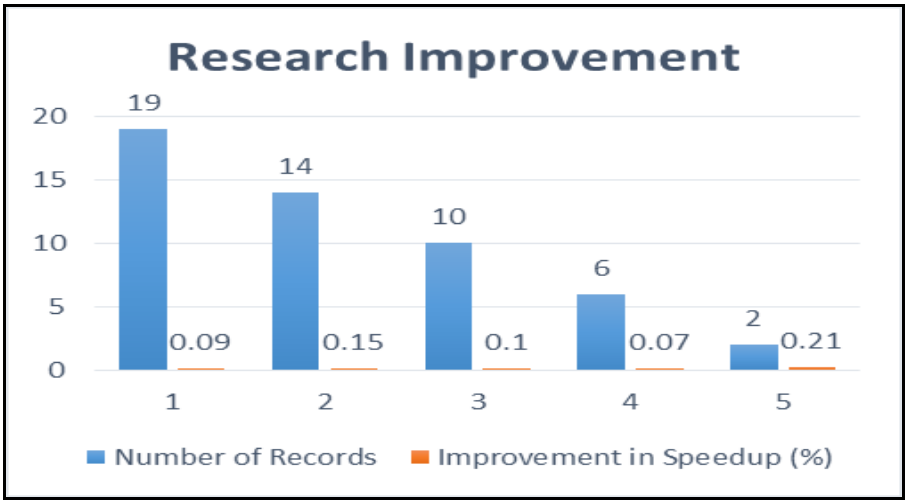

Fig.8. Speedup Percentage

6. Conclusion

Cloud technology users are increasing rapidly. Security of data is the major concern in public cloud. Hence, in

this paper, trusted security framework is presented for public educational cloud environment. It not only provides security but also improves the response time. In this framework, the users (i.e. staff, student, management or admin) are prevented from the attacks like denial of service, rainbow attacks and phishing attacks. This framework provides security in the public educational cloud and makes the cloud as a reliable one.

Acknowledgements

This work was supported by the University Grants Commission in India under Rajiv Gandhi National Fellowship (Award Letter Number: F1-17.1/2015-16/RGNF-2015-17-SC-TAM-4667).

References

[1] P. Mell T. Grance, "The NIST definition of cloud computing version 15 technical report," Computer and information Sciences, 53(6), 2009, pp.1-10.
[2] P. Jain, R. Agrawal, "An improved pre-copy approach for transferring the VM data during the virtual machine migration for the cloud environment," International journal of engineering and manufacturing, 2016, volume 6, no. 6, pp. 51-60.
[3] S. Jain, V. Sharma, "Enhanced load balancing approach to optimize the performance of the cloud service using virtual machine migration," International journal of engineering and manufacturing, 2017, volume 7, no. 1, pp. 41-48.
[4] N.A. Yekini, U.I. Vdoh and F. Doherty, "Open educational resources (OER) for sustainable development using automatic cloud computing system," International journal of engineering and manufacturing, 2016, volume 6, no. 6, pp. 60-68.
[5] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds toward a cloud definition," ACM sigcomm computer communication review, 39, 2009, pp.50-55.
[6] Buyya. R, Yeo, C and Vengopal, S, "Market oriented cloud computing vision, hype, and reality for delivering IT services as computing utilities," proceedings of the 10th IEEE international conference on high performance computing and communications, 2008, pp.5-13.
[7] R. Buyya, C. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms vision hype and reality for delivering computing as the 5th utility," Further generation computer systems, 25, 2009, pp.599-616.
[8] S. Subashini, V. Kavitha, "A survery on security issues in service delivery models of cloud computing," Journal of network and computer applications, 2011, pp.1-11.
[9] Lee Badger, Robert Bohn, Shilong Chu, Mike Hogan, Fang Liu, Viktor Kaufmann and Jian, "Useful information for cloud adopters," NIST cloud computing program, 2(1), 2011, pp.1-73.
[10] J. Viega, "Cloud computing and common man," Computer, 42(8), 2009, pp.106-08.
[11] C. Wang, et al., "Ensuring data storage security in cloud computing," Proceedings of the 2009 17th International Workshop on Quality of Service (IEEE), 2009, pp.1-9.
[12] E. Michael whitman et al., "In defense of the realm: Understanding the threats to information security," International Journal of Information Management, 24, 2004, pp. 43-57.
[13] Dimitrios Zissis , Dimitrios Lekkas, "Addressing cloud com-putting security issues," Future Generation Computer Systems, 28, 2012, pp.583-592.
[14] Prachi Soni, Monali Sahoo, "Multi Factor Authentication Security Framework in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering, January 2015, volume 5, issue 1, pp. 1065-1071.
[15] Chander Kant, Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security," International Journal of Advanced Research in Computer Science and Software Engineering, May 2013, volume 3,

issue 5, pp. 570-575.
[16] Paolo Cemim et al., "EduCloud: A Private Cloud Tool for Academic Environment," IEEE Latin America Conference on Cloud Computing and Communications, 2012, pp. 66-71.
[17] Rajesh R, Jaya Lakshmi A, "Optimized and Secured EduClouds by Implementing Virtualization," International Journal of Electronics and Computer Science Engineering, 2014, volume 1, pp. 2404-2408.
[18] Rohitash Kumar Banyal, Pragya Jain, Vijendra Kumar Jain, "Multi factor authentication framework for cloud computing," in 5th international conference on computational intelligence, modelling and simulation 2013, pp.105-110.
[19] Bariah Aljebreen, Ajantha Dahanayake and Liyakathunisa Syed, "Advances in higher educational resource sharing and cloud services," International journal of computer science and engineering, June 2015, volume 6, no. 3, pp. 27-42.
[20] Omondi John Opala, Syed M. Rahman, "An Exploratory Analysis of the influence of information security on the Adoption of cloud computing," IEEE international conference on system of system engineering, June 2013, pp. 165-170.
[21] Benjamin Fabian, Annika Baumann and Jessika Lackner, " Topological analysis of cloud service connectivity," International journal of computers and industrial engineering, June 2015, pp. 1-34.
[22] Ashishkumar Singh et al., "CAESAR CLOUD: A comprehensive approach for enhancing security and service availability based on reputation for cloud user environment," International journal of network security and its applications, 2014, pp. 2164-2175.
[23] A.M. Mansuri, Pradeep laxkar and Manish verma, "Benefit of cloud computing for educational institutions and online marketing," Information security and computer fraud, 2014, volume 2, no. 1, pp. 5-9.
[24] Ali Shahbazi et al., "A distributed key based security framework for private clouds," International journal of advanced computer science and applications, 2013, volume 4, no. 9, pp. 79-83.
[25] Mary jane sule, "A conceptual framework of deploying cloud IaaS in higher educational institutions," IEEE international conference on cloud computing technology and science, 2011, pp. 489-493.
[26] Shanto, Mahmud Hossain, "Security threats in cloud computing: A four module approach to secure cloud from DOS attacks in virtual machine," 2014, pp. 21-25.
[27] G. Kumaresan, N. Veeraragavan and L. Arockiam, "A dynamic two stage authentication framework to enhance security in public educloud," International journal of applied engineering research, 2015, volume 10, no. 82, pp. 126-131.
[28] G. Kumaresan, N. Veeraragavan and L. Arockiam, "A study of user authentication techniques in cloud computing ," Journal of emerging technologies and innovative research, 2015, volume 2, no. 8, pp. 3309-3314.

Authors' Profiles

G. Kumaresan: Research Scholar at Department of Computer Applications, National Institute of Technology Tiruchirappalli, Tamil Nadu, India. He received MCA from Thiagarajar College of Engineering, Madurai, India. M.Tech from Bharathidasan University, Tiruchirappalli, India and M.Phil. from St.Joseph College, Tiruchirappalli, India. His areas of interest include Cellular Automata based Cryptography and Cloud Security.

N.P. Gopalan: Professor at Department of Computer Applications, National Institute of Technology, Tiruchirappalli, Tamil Nadu, India. He obtained his PhD from Indian Institute of Science, Bangalore, India. Interested in Data Mining, Distributed Computing, Cellular Automata, Theoretical Computer Science and Cryptography.

How to cite this paper: G. Kumaresan, N.P. Gopalan,"EduCloud: A Dynamic Three Stage Authentication Framework to Enhance Security in Public Cloud", International Journal of Engineering and Manufacturing(IJEM), Vol.7, No.6, pp.12-26, 2017.DOI: 10.5815/ijem.2017.06.02