User Authentication Mechanism for Sharing E-resource in Educational Clouds

I.Arulmani, L.Arockiam, and N.Veeraragavan

Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India

Summary
Cloud computing is a computing environment centre on clients and to access the programs or documents stored correspondingly in servers. In this paper we have discussed mainly on cloud computing environment in educational system. The educational learning, utilising e-resources can be done between two or more educational institutions with community cloud computing. The authentication should not depend (or) should not matter where the user is all over the world. It should be noted only the user can use the methodology anywhere in the world by the communication. We used latest criteria for authentication process like communication between user and server with highly secured two levels security model. Global Positioning System (GPS) and Mobile Tracking Software (MTS) were used main resources. With the help of mobile phone and internet, the password is transferred in two level processes. Community cloud computing is focussed in order to make use of two or more users can be provided the cloud services.

Key words:
Authentication, security, Global Positioning System (GPS), Mobile Tracking Software (MTS), Educational Learning, Community Cloud, e-resource

1. Introduction

Cloud computing is the internet based computing. The cloud computing is spread widely and it has used by small, medium and large scale companies [1]. In cloud computing the user and service provider's use the resource in low cost without owning the resource needed [2]. Users store their files and most important backups, by creating their environments in it [3]. The services are provided with the internet with massive scale services by many users [4]. The development of cloud computing security is still facing many challenges from unauthorized users and leakages [5]. In order to improve the efficiency and security of cloud computing, the different services with distributed networks in various places are installed and implemented [6].

This paper discuss about the user authentication for cloud computing. Authentication is the process of finding the individual using security identity. Cloud provides high security to the user authentication. It should be done in a few clicks with high security. User authentication is the method of identify whether the user is accessing a secure and restricted service and verifying the same. The user must be identified with respect to his/her identity created by his own. The service provider gives the users own ID for authentication process. The cloud computing services are used only with the ID given for users and the authentication method.

As authentication are more important criteria in cloud computing. Along with the technology improvements, mobile phones are quite normal for the usage in all the level of the people. Now-a-days a mobile phone itself acting as a mini computer for various applications.

The service of community cloud is enormously used in education system. The two level password security mobile phone signals tracking with high speed using GPS is the latest trend introduced in this paper. The educational field is also not missed by the computers and its latest inventions. The day to day innovations, finding of new technology, hardware, software is not only used in business level but also practised in educational field. The cloud computing combining with latest innovation of mobile phones and computer technology is today's major focused demand in IT sector [7].

The main architecture such as service layer for repository, composition and execution, resource layer for computation, persistence, bandwidth, currency, coordination layer for virtual machine, Identity, Networking transactions are the main layers which motivated to develop a project in user authentication in community cloud computing. The educational system is demanding the cloud system for it various usage and technologies to be migrated [8]. It is focusing on World Wide Web (WWW) for web services [9]. Using the internet protocol hypertext Transfer Protocol (HTTP), the educational area is well utilised by accessing Google, Amazon, Wikipedia etc. The user authentication used in community cloud for educational system is highly reliable and security which is not used in previous educational systems.

2. Related work

The common user authentication security process is used in following papers which is explained for related works:

Manuscript received August 5, 2013
Manuscript revised August 20, 2013

2.1 Trusted Computing Technology (TCP)

Zhidong Shen et al [6] are proposed for the trusted computing technology is used in the cloud computing environment in order to obtain the requirements and fulfil it for the need of cloud computing. In TCP approach, the cloud computing system was provided by the security functions, like authentication, communication security and data protection. It serves as hardware base for the cloud computing system. In this design TCP is based on Trusted Platform Module (TPM). TCP will improve the security and provide authentication, confidentiality and integrity in cloud computing for the users.

TCP is based on hardware modules, and it is used for the process of cryptographic computation. The Trust Security Services (TSS) is used in the TPM module in order to make the security function more easily. Latency of the encryption and decryption is the main limitation faced in TCP. If the time interval of encryption of the data and decryption of the data is increased may tends to unsecured communication.

2.2 Hierarchical Identity Based Cryptography

Liang Yan et al [10] are proposed for the use of federated identity management. With this proposal, the server and user have their own unique identity. The identity key is allowed by system hierarchal. By the use of unique identity and hierarchical identity, the simplified form of key distribution and mutual authentication is attained. In identity based cryptography, the master public key and master private key were created by Public Key Cryptography (PKG). The master pubic key is published to all the users who are all interested. The user creates their own public key for them.

The private key is if needed by the user, then the user should contact with PKG with his/her identity. The private key was generated in Federal Hierarchical Identity Based Cryptography (HIBC) by PKG's. They are the intermediates between users and service providers. They may create their own digital signature without the knowledge of the user (or) server. Here the user authentication lacked with this escrow problem. The knowledge of the username and password of sub level PKG's known to main PKG, which motivation will lead to unsecure of data between user sub PKG's and cloud computing services.

2.3 Secure Access Mechanism for Cloud Storage

Danny Harnik et al [11] are proposed to the secure access mechanism analysis the secure access to objects in a storage cloud. It checks the performance and security level of storage cloud. The contribution of this is the security manager was requested by the client for a credential and using it for access data in secures.

The security policy manager be acting as interlink between user and cloud server. The key used for validation can be known to the security policy manager. The security policy manager may make use of the key and make the user to believe without the knowledge of service provider. The secret data is communicated between security policy manager and user but not with server.

2.4 Cloud Based One Time Password (OTP) Token

Fred Cheng [12] is proposed to two factor authentication system. A leading password technology is OTP token automatically generate a dynamic session password. Due to high cost, difficulty in carrying and support expenses, the Rubbing Encryption Algorithm (REAL) is used. REAL has secure encrypting for it unique strength and fast scramble algorithm to hide the OTP numeric code in a large equiprobable matrix. Even with the public internet kiosk, the data is transmitted in secure to the remote Personal computer (PC). The REAL encryption key is given in the hardware token.

The OTP token authentication is due to Trojan problem. It stays in the PC of the user. It will redirect the user to fraudulent website to collect user's data and again redirects the user to the genuine website after the data collection. This type of new attack is really challenges to entire network. The hardware token kept secure and should not get lost by the user in order to encrypt and decrypt the REAL image.

2.5 The Trust and Security in Cloud Computing

Mahbub Ahmed et al [13] are proposed to the requirements of security property such as information or data confidentiality with line security, the cloud computing proposed a common protocol among different protocols and analysing it. The exchange of data with hamper confidentiality and integrity between Information Owner (INO) and Cloud Service Provider (CSP) is done by Cloud Computing Environment (CCE) by the successful elimination of dangling pitfalls. By knowing the value of password and offline password guessing attack is possible. Hijack and spoof of exchange is possible in data transmission without cryptographic protection.

2.6 User Authentication Platform Using Provisioning in Cloud

Hyosik Ahn et al [14] are proposed to the user's ID/password, Time, Position and place were analyzed by the cloud and allow the user to authenticate. The user's current status was analyzed and monitored. The change of user status also monitored recorded in the user profile database. The change in position was also asked by the cloud computing whenever the user enters for authentication process.

All the above mentioned limitations are major criteria in today's trend. In the education learning with community cloud is completely made by resolved of above mentioned issues. There is no intermediation like security policy manager is available. The main PKG's like master level user with sub users are not used here. The low time level is get improved by using MTS and GPS as supporting software for communicating and tracing the user's location.

3. Components in Framework

The cloud service provider should provide their services in less cost as compared to other areas. Since the students were mainly are considered as users, it is to be done with low cost. The service should be user friendly as any persons with less knowledge of system can get the service completely. By the usage of the software MTS, the user can authenticate at any location. Reliability is for the institutions having trust on the cloud by long standing trend. So, the above important criteria's, the educational latest technology to compare with cost for the user is comparatively less and it can be used by the teachers, faculty and other staffs in additional to the students.There are three types of techniques were doing this model are as follows:

3.1 Basic Access Authentication (BAA)

It is the simplest user authentication technology. In BAA, the client recognizes themselves with a username and password. Initially the cloud was accessed by the client using this method. Whenever the user using the username and password, the cloud services verify and allow the user to use the service.

3.2 Cell Phone Tracing (CPT)

CPT means knowing current location of the mobile phone. After receiving the username and password the cloud asks for the user's personal mobile number current tower signal name. User enters the current location and it was verified by the cloud using GPS. Most of the cell phones accessible in the market have the GPS technology. GPS has become easy to trace the mobile phone location. Since the cell phones are already use radio signals to communicate with cell towers, GPS simply carries onward that signal to satellites determining the location of that cell phone. A GPS device establishes a connection with three or more satellite to there an accurate location.

Currently GPS easy to trace the cell phone location. Global Positioning System determines the position to uses satellites. The position can be of an individual, a fleet, a vehicle or of a device. At first intended to aid the military, global positioning system was additional unlimited for civilian use as well. GPS uses the time, latitude and longitude to determine the exact position.

3.3 One Time Password (OTP)

Cloud verifies the BAA and CPT then check for OTP. The system generates a random number. The cloud service providers send an OTP to the user's registered mail ID. The cloud allows the user to progress provided the random number is correct. In this OTP method every communication from client to user or user to cloud is only one of its kinds, and hacker using an earlier message would fail to access the system. In addition, the OTP authentication system defers from nearly all people to another person for a password.

Most of the people understand a password to be selected by the user to be significant and can be use again and again. The importance of OTP however is the single-use nature of the password. By this way the security is satisfied. Abstractly it can be hack by hackers who use the data in the message to log into the service as the user or to use wrongly.

4. User Authentication Framework

Fig. 1 shows the secure framework for the community cloud. There are various steps involved in the education based user authentication algorithm as follows:

(i) Step 1. The user logging in by using his username and password. After receiving the username and password cloud checks for double security entry.
(ii) Step 2. The cloud asking for the user's personal mobile number's current tower signal name which can be shown in cell info display.
(iii) Step 3. User response the cloud request.
(iv) Step 4. The cloud verifies it using GPS. The cloud traces the user's mobile number location by MTS installed in the cloud system. By entering the user's mobile number in MTS, the exact location of the particular mobile number was traced and the same was shown in the cloud's system by GPS direct wireless connection through satellite. If the data is correct, then
(v) Step 5. The cloud sends a Random Number to the user's Personal mail id.

(vi) Step 6. The cloud will allow the user to progress by entering the random number correctly.

This method is very secure as the double security was used by cloud and user.

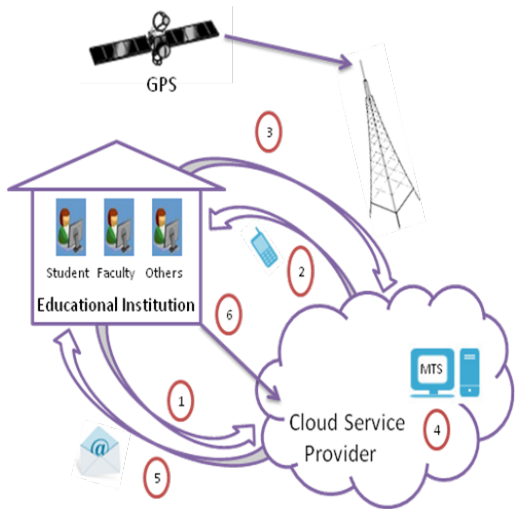

Fig. 1 User Authentication for Community Cloud

5. Performance Analysis

Performance comparisons between related work issue and proposed model in above technique is shown below [4]:

5.1 Communication Cost

The comparison of communication cost between the related issues and proposed model is shown in Table 1.

Table 1: Comparison of Communication Cost

Issue	Cost	Proposed Model	Cost
OTP Token Device	2	OTP send E-mail	1

Reference [12] shows that communication cost of OTP Token device due to high cost, difficulty in carrying and support expenses. So, the communication cost is 2. In this proposed model the CSP send an OTP to the user's registered mail ID. However, the communication cost is 1 on the internet connection for accessing mail.

5.2 Computation Cost

The comparison of computation cost between the related issues and proposed model is shown in Table 2.

Table 2: Comparison of Computation Cost

Issue	Cost	Proposed Model	Cost
TC hardware in the boot ROM	2	E-mail & Location	1

Reference [6] shows that computation cost of the cryptographic hash code is computed by TC hardware in the boot ROM. Each chunk of code is added to log the hash of the next chunk that loads. So, the computation cost is 2 and its take more time to compute OTP. In this proposed model OTP send E-mail and Mobile location, so user within a second to view the email and mobile location to get OTP. However, the planned model computation cost is fewer of 1.

5.3 Result and Analysis

The results confirm that the communication cost and computation cost of proposed model is less and the authentication time is shorter as shown in Fig. 2 & Fig. 3.

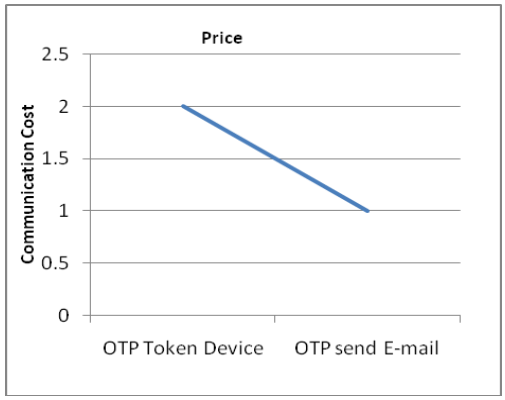

Fig. 2 Comparison of communication cost

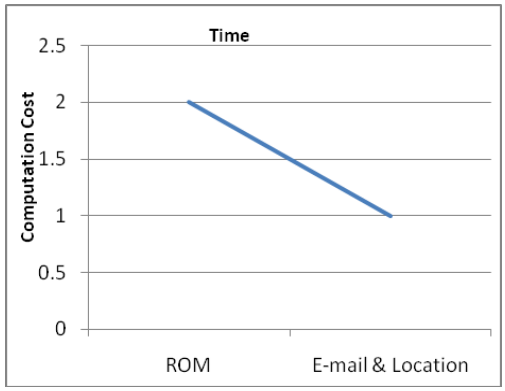

Fig. 3 Comparison of computation time

6. Conclusion

The problems faced in various publications were discussed and its issues were resolved with their user authentication technique to improve high standard of security level and usage of the cloud services. Here in this paper discuss about the user authentication process with the model of community cloud in emerging trend. The latest updating and new upcoming can be introduced to this technique which certainly help to solve the educational related issues to the students faculty, other staffs etc. The high security,

password protection in two level modes and user friendly were achieved by the authentication process used in education system.

The two level security, one is through mobile phone tower deducting and the second is using mail id (personal) can help the user/institutions to have secure accessing. All the information's stored regarding the user which helps in improvement along with their academic developments. The improvement of this model along with the changes in cloud computing technologies and various user authentication techniques will rapidly improve the education system as high priority for upcoming generation. In the nearby future, the framework can be used for community cloud. Therefore, it can be used by any different cloud service provider for implementation. The proposed model framework is used by phone and email. The technology can be get hijacked. The use biometrics technology becomes more secure in future.

References

[1]. G.A.Patil and S.B.Patil,"Data Security Mechanism for Cloud", International Journal of Computer Application, pp. 24-27, 2011.

[2]. Hyokyung Chang and Euiin Choi, "User Authentication in Cloud Computing", Communications in Computer and Information Science, vol. 151, pp. 338-342, 2011.

[3]. Joao Paulo Barraca, Alfredo Matos and Rui L.Aguiar," User Centric Community Clouds", Wireless Personal Communications, Vol. 48, no. 1, pp. 31-48, Jul 2011.

[4]. Hongwei Li, Yuanshun Dai and Ling Tian , Haomiao Yang," Identity-Based Authentication for Cloud Computing", International Conference on Cloud Computing, vol. 5931, pp.157-166, 2009.

[5]. Jin-Song Xu, Ru-Cheng Huang and Wan-Ming Huang, Geng Yang, " Secure Document Service for Cloud Computing", International Conference on Cloud, vol. 5931, pp.541-546, 2009.

[6]. Zhidong Shen and Qiang Tong, "The security of Cloud Computing System enabled by Trusted Computing Technology", International Conference on Signal Processing Systems, pp. 11-15, 2010.

[7]. Shalini Gupta,"Cloud Computing in Education in Current Financial Crisis", International Conference on Technology and Business Management, pp. 325-330, March 26-28, 2012.

[8]. Xiao Laisheng and Wang Zhengxia," Cloud Computing: a New Business Paradigm for E-learning", International Conference on Measuring Technology and Mechatronics Automation, pp. 716-719, 2011.

[9]. Mohssen M.Alabbadi, "Cloud Computing for Education and Learning: Education and Learning as a Service (ELaaS)", International Conference on Interactive Collaborative Learning, pp. 589-594, 2011.

[10]. Liang Yan, Chunming Rong and Gansen Zhao," Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical identity-Based Cryptography", International Conference on Cloud Computing, vol. 5931, pp.167-177, 2009.

[11]. Danny Harnik, Elliot K.Kolodner, Shahar Ronen, Julian Satran, Alexandra Shulman-Peleg and Sivan Tal," Secure Access Mechanism for Cloud Storage", Scientific International Journal Parallel and Distributed Computing, Vol. 12, pp. 317-336, 2011.

[12]. Fred Cheng," Security Attack Safe Mobile and Cloud-based One-time Password Tokens Using Rubbing Encryption Algorithm", Journal Mobile Networks and Applications, vol. 16, pp. 304-336, 2011.

[13]. Mahbub Ahmed, Yang Xiang and Shawkat Ali," Above the Trust and Security in Cloud Computing: A Notion towards Innovation", International Conference on Embedded and Ubiquitous Computing, pp. 723-730, 2010.

[14]. Hyosik Ahn, Hyokyung Chang, Changbok Jang and Euiin Choi, "User Authentication Platform using Provisioning in Cloud Computing Environment", Communications in computer and information science,vol.199, pp. 132-138, 2011.

I. Arulmani she had completed her under graduation, B.Sc physics in Tranquebar Bishop Manickam Lutheran College, Porayar and her post graduation, M.C.A. in Krishnasamy College of Engineering & Technology, Cuddalore. She is doing M.Phil (Computer science) in St.Joseph's College (Autonomous), Trichy. Her research interest includes the mechanism of user authentication in educational clouds by sharing the E-resources. E-mail, mobile phone, GPS network and their applications were the main sources used in her research.

L. Arockiam has been working as an Associate Professor in the Department of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 23 years of experience in teaching and 16 years of experience in research. He has published 109 research articles in the International / National Conferences and Journals. He has also presented research articles in the Software Measurement European Forum in Rome, Italy and in the International conference on Computational Intelligence and Cognitive Informatics in Bali, Indonesia. He has chaired many technical sessions and delivered invited talks in National and International Conferences. 'Success through Soft Skills' is the name of the book authored by him. His research interest includes Software Measurement, Cognitive Aspects in Programming, Web Service, Mobile Networks, Data mining and Cloud Computing.

N. Veeraraghavan has completed his M.Sc., B.Ed., M.Phil., degrees and has been working as an Assistant Professor in the Department of Computer Science, St.Joseph'sCollege (Autonomous), Tiruchirappalli, Tamil Nadu, India.