IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol-6, Special Issue-8, Oct 2018 E-ISSN: 2347-2693

Data Privacy Using Dynamic Multi-Layer Authentication Mechanism in Open Learning Environment

[1*]R. Anuratha, [2]M. Ganaga Durga

[1,2]Mannar Thirumalai Naicker College, Govt. Arts College for Women, Sivagangai Tamil Nadu, India

Available online at: www.ijcseonline.org

Abstract- Cloud computing, delivers abundant services between Cloud Service Providers (CSP) and Cloud Users (CU) on a demand basis in metered service without having the underlying infrastructure with the help of Internet. This ease will increase the cloud users day by day to adopt cloud model. Technological advancements, specially Information Communication Technology (ICT) and cloud computing, transform traditional teaching and learning practices into blended learning. Due to the fabulous development of Massive Open Online Courses (MOOC) and Open Educational Resources (OER), more attention and efforts are crucial to the security procedures for massive open online courses. Authentication of the users to the cloud service is mandatory, because it eliminates the risks and attacks found in the cloud services.

Password is widely used for user authentication because of its simplicity. Frequently changing password is a tedious work. Simple passwords are easily hacked, but complicated one is hard to memorize. To overcome this, we suggest Personally Identifiable Information (PII) for the purpose of Authentication. *In this paper, we propose a security model using Dynamic Multi-Layer Authentication Mechanism, which is based on user's personally identifiable information.*

Keyword- Authentication, Access Control, Massive Open Online Course, Open Educational Resource, Responsive Open Learning Environment, Self-Regulated Learning.

I. INTRODUCTION

The amazing growth of online learning brings digital advancement in higher education. Emerging digital technologies such as wikis, blogs, and social software are gradually being combined into online courses. The web-based learning environments which eliminates time and location, commonly make temptation to join online courses. This will increase the Internet usage and also the importance to secure data during communication in the network. Confidentiality (to prevent unauthorized reading), Integrity (to prevent unauthorized writing) and Availability (to make available to authorized persons) is the key concern for the security of the information.

Cryptography, Access Control and Security Protocols are the solutions to make comfort in protecting the network. Cryptography deals with encrypting information in unreadable (meaningless) format and decrypting by the recipient only [1]. Access control deals with authentication and authorization. Security protocols are the communication rules followed in a security application.

Authentication is required for protecting any computing resources. It is widely used for its simplicity and efficiency in the remote host login system. The key concern of an authentication is to provide the assurance between the communicating parties that they are the true personalities. The rest of the paper is ordered as follows: Section II reviews the related research work regarding Authentication. Section III describes our proposed Dynamic Multilayer Authentication Mechanism. Section IV analyses the simulation of the model and Section V concludes the paper.

II RELATED RESEARCH WORK

a. Authentication

Authentication is a process of identifying the genuine user in the way that what he/she knows (password), what he/she has (token), what he/she is (behaviour) and what he/she recognises from unauthorised persons. authentication protocols were classified according to the freshness of the protocol run using timestamps or nonces, Secret key generation by the trusted server, by only one of the clients or by the participation of both clients and Authentication (key distribution) only or authentication with hand- shake (key distribution and key confirmation). Also, the efficiency of an authentication protocol was measured against two metrics that the total number of messages exchanges in a successful protocol run and the total number of rounds in a successful

run. A round is set of message exchanges between participating entities that can occur simultaneously.

Authentication techniques are classified into textual password, graphical passwords, smart cards and biometric schemes like fingerprint, voice recognition, iris scanning and face recognition. Now-a-days dynamic authentication protocols are used for enhancing security. Authentication process includes two steps that identifies and verifies the genuine user.

Fig 1 shows the simple Authentication mechanism to a remote server. Multi-Layer Authentication must deliver the high power of security in the public cloud environment, where the diverse nature of data level [2]. After analysing the related work, we suggest the Dynamic Authentication Mechanism which provides efficient security in future.

In 2004, Das et al. described a Dynamic ID-based scheme to solve user tracking problems [5]. In 2005, Liao et al. pointed out that Das et al.'s scheme can't protect against guessing attacks [6]. In 2006, Yang *et al*. suggested a password-based user authentication and key exchange protocol using two-server architecture [7]. Here, the front-end server only communicates directly with the users and a control server does not interact with the users directly. The concept of distributing the password verification information and authentication functionality into two servers requires additional efforts from an attacker to compromise two servers to launch successful offline dictionary attack. In 2008, Tsai recommended a multi-server authentication protocol using smart cards based on the nonce and one-way hash function [8]. The recommended authentication protocol is efficient as compared to other such related protocols because it does not use any symmetric and asymmetric encryption algorithm for its implementation.

In 2009, Liao and Wang proposed a new authentication scheme with anonymity for a multi- server environment that uses one-way hash functions to improve efficiency [9]. But Hsiang and Shih pointed out Liao and Wang's scheme can't withstand insider attacks, masquerade attacks, server spoofing attacks, and registration center spoofing attacks [10]. To overcome the weaknesses of Liao and Wang's scheme, Hsiang and Shih proposed their scheme. Yet, in 2011, Lee et al. found Hsiang and Shih's scheme still could not overcome masquerade attacks, and server spoofing attacks [11]..

b. Access Control

Generally, Access control systems accomplish authorization, identification, authentication, access approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys. Access control being the first line of Défense. If not implemented with utmost care itself suffers from severe security risks that hamper the privacy and confidentiality of user's personal information or a specific group's data.

We assure that, hybrid model which consists of combination of any two access control models (merging rule and role-based access control) ensures the data security; which is stored in the Cloud server [3].

Fig: 1 Simple Authentication Model for a Remote Server Login System

c. Massive Open Online Course (MOOC)

MOOC are a flexible and open form of self-directed, online learning designed for massive participants. MOOC platforms provide course materials with the help of institution using Cloud-based hosting environments. The learners can access course material at free of cost. MOOC offer certificates after completing their e-assessment at a cost. The 5R (Retain, Reuse, Revise, Remix and Redistribute) open content provide quality assurance and best practices.

d. Open Educational Resource (OER)

OER are openly available licensed text, media, and other digital assets that are useful for teaching, learning, and assessing for research purposes all over the world freely. Most of the OER sites and repositories do not have any log-in procedure leads to security breaches.

e. Responsive Open Learning Environment (ROLE)

ROLE aims to exploit web-based tools and technologies to empower learners to construct their own personal learning environments [4]. The overall goal is to create flexible, web-based open technologies for the federation and mash-up of learning services on a personal level. The vision of ROLE is to empower the learner to build their own responsive learning environment. Responsiveness is defined as the ability to react to the learner needs and reflect upon her own learning process [4]. PLE takes a more natural and learner-centric approach and is characterised by

the use of a set of services and tools that are controlled and carefully chosen by individual learners.

f. Self-Regulated Learning (SRL)

According to Ernesto Panadero, SRL includes the cognitive, metacognitive, behavioural, motivational, and emotional/affective aspects of learning. Barry Zimmerman describes that "Self-regulation is not a mental ability or an academic performance skill; rather it is the self-directive process by which learners transform their mental abilities into academic skills." Also, Students are seldom given a choice regarding academic tasks to pursue, methods for carrying out complex assignments, or study partners.

Past research confirms that online learning providers and practitioners have not considered security as a top priority

III. PROPOSED MODEL

a. Overview

SMAC (Social Media, Mobile Computing, Analytics and Cloud Computing) bring Virtual Learning Environment into the institutions realizing that technologies were essential for paving a new way to the Teaching and Learning environments. Most of the MOOC, OER sites have not considered security as a top priority. For this, we recommend an Effectual, Simple and Secure Authentication model to the Open Learning Environment.

b. The Main contribution of the proposed work includes:

The proposed work has planned in three main classes:
Register PII: Contains PII and graphical password.
Authentication: Contains Security Index Questionnaire and graphical password information.
Change PII: Contains updating the PII.

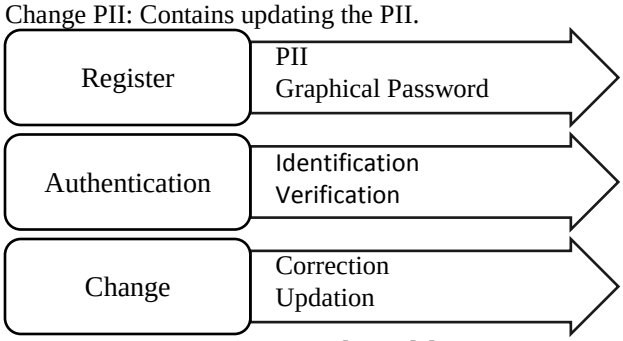

Fig 2: Work Model

i. Register PII (Personally Identifiable Information) Phase

Personal Identifying or Personally Identifiable Information (PII), which is "the information pertaining to any living person which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person)" [12]. PII is simply the attributes of a person, such as: their hair colour, sound of their voice, height, name, qualifications, past actions, reputation, medical records, etc.
Layer 1 – PII Registration.
Layer 2 – Graphical User Authentication.
Layer 3 – Unique ID Generation for each user.

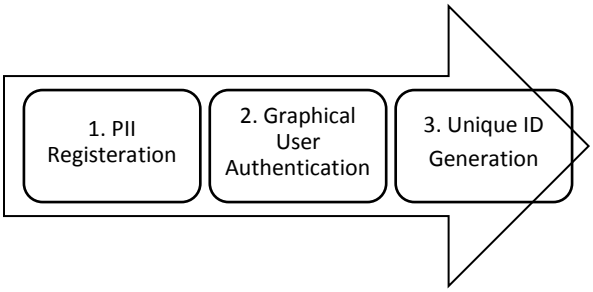

Fig 3: Register PII Phase

ii. Authentication Phase

After successful completion of registration user can get access to that environment through login or sign in. Authentication phase does identification and verification of the user. A valid user only get access to the cloud resources.
Layer 1 – Login must be done with ID and OTP. OTP is generated first time login process for validating the mobile number. Other wise ID is enough for the login process.
Layer 2 – User will be asked to answer to the randomized question selected from PII. Only two choices are allowed to prove their identity. If not, the user access is denied.
Layer 3 – Graphical Password must be chosen. The order and the Point of Interest (POI) can be enforced for stronger authentication.

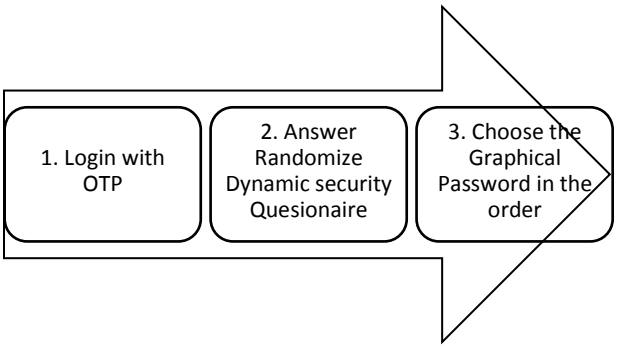

Fig 4: Authentication Phase

iii. Change PII (Personally Identifiable Information) Phase

Smart devices are often stolen or damaged. To avoid this; Change PII phase helps us to change the information or update the information.

IV SIMULATION

In higher education teaching and learning process pave a way to the integration of Information and Communication Technology. The tremendous growth in Online Courses

ensures the proper Authentication mechanism. The proposed system model has three modules:
Administrator
User
Highest privileged User
Lowest privileged User
Highest Credential Functions

Administrator
Administrator has the power to control entire system. If any anonymous is found in the activities of the user, the user has denied the access to the resource and the information is also sent to the admin. Admin takes charge for the group generation, setting roles (Student, Faculty) and access (like read, write, upload, download, transfer, copy and alter).

Highest privileged User
Faculty who is registered in the group can store data and share it to the registered students. Faculty follows up the activities of the students. Faculty restricts the time to submit assignment and appear for test.

Lowest privileged User
Student who is registered in the group has the limited power. Student can access the data within the given time period. Any unwanted activities are found the access is denied.

Highest Credential Functions
Data alteration/Deletion require additional verification. The user must prove their original identity for the highest credentials functions. In future Biometric authentication like Fingerprint, face recognition may be used for the highest privileges of the task.

V. CONCLUSION

Regardless of geographic location one can easily access online resources simply with a few clicks; become critical today in securing access to the online resources. At the same time, more and more of these accesses are made from handheld devices. Cloud Computing is eminently suitable for offering dynamic provisioning of computing resources. Authentication of the users to the cloud service is mandatory, because this way it eliminates the attacks of risks to enter into the Cloud services.

In this paper, we suggest that the Dynamic Authentication Mechanism (DAM) obtains high-level Security in low-cost and confirms the successful result.

ACKNOWLEDGEMENT

I take this privilege to express my gratitude and respect to the Principal, Management of Mannar Thirumalai Naicker College, Bharathiar University and my special thanks to my Supervisor.

REFERENCES

[1] Pranav Vyas, Dr. Bhushan Trivedi, An Analysis of Session Key Exchange protocols, International Journal of Engineering Research and Applications, Vol. 2, Issue 4, June-July 2012, pp.658-663, ISSN: 2248-9622, available at www.ijera.com.
[2] Anuratha. R, Dr. Ganaga durga. M, "Authentication – A part of Identification in the Cloud Environment", International Journal of Advance Research in Science and Engineering, vol. 07, Special Issue 01, January 2018, ISSN 2319-83554, pp. 25-34
[3] Anuratha. R, Dr. Ganaga durga. M, "Analysis of Data Security in Cloud Computing Using Access Control Technique", International Conference on Global Talent Management in the Digital Era, ISBN: 978-93-86537-95-9, September, 2017.
[4] Sten Govaerts, Katrien Verbert, C. Delgado Kloos et al. (Eds.), Towards Responsive Open Learning Environments: The ROLE Interoperability Framework, EC-TEL 2011, LNCS 6964, pp. 125–138, 2011. Springer-Verlag Berlin Heidelberg 2011.
[5] L. Das, A. Saxena, and V. P. Gulati, "A Dynamic ID-Based Remote User Authentication Scheme," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629 - 631, 2004.
[6] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang, "Security Enhancement for a Dynamic ID-Based Remote User Authentication Scheme," In Proceeding of International Conference on Next Generation Web Services Practices, 2005 (NWeSP 2005), pp. 437-40 , 2005.
[7] Y. Yang, R. H. Deng and F. Bao, "A Practical Password- Based Two-Server Authentication and Key Exchange System," IEEE Transactions on Dependable and Secure Computing, Vol. 3, No. 2, 2006, pp. 105-114. doi:10.1109/TDSC.2006.16
[8] J. L. Tsai, "Efficient Multi-Server Authentication Scheme Based on One-Way Hash Function without Verification Table," Computers & Security, Vol. 27, No. 3-4, 2008, pp. 115-121. doi:1 0.1016/j.cose.2008.04.001
[9] Yi-Pin Liao and Shuenn-Shyang Wang, "A Secure Dynamic ID-Based Remote User Authen- tication Scheme for Multi-Server Environment," Computer Standards & Interfaces, vol. 31, no. 1, pp. 24-29, 2009, available at www.sciencedirect.com.
[10] Han-Cheng Hsiang and Wei-Kuan Shih, "Improvement of the Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment," Computer Standards & Interfaces, vol. 31, no. 6, pp. 1118-1123, 2009.
[11] Cheng-Chi Lee, Tsung-Hung Lin, and Rui-Xiang Chang, "A Secure Dynamic ID Based Re- mote User Authentication Scheme for Multi-Server Environment Using Smart Cards," Expert Systems with Applications, vol. 38, no. 11, pp. 13863-13870, 2011.
[12] N.S Chauhan and A.Saxena, "Energy Analysis of Security for Cloud Application," in Proc. Annual IEEE India Conference, pp. 1-6, 2011.

