IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

Dynamic Query Updation for User Authentication in cloud Environment

Gaurav Shrivastava[1], Dr. S. Prabakaran [2]

[1] Research Scholar, Department of Computer Science, SRM University, Kattankulathur, Tamilnadu, India

[2] Professor, Department of Computer Science, SRM University, Kattankulathur, Tamilnadu, India

Abstract

Cloud computing is a network-based computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources. It is cost efficient, provide almost unlimited storage and better backup and recovery services. Also, it facilitates automatic software integration and easy access to information.These all is possible through successful authentication. There are so many existing authentication methods based on static approaches like password and PIN based authentication. Drawback of these static authentication approaches is that they are susceptible to more cyber-attacks, data leakage, IP theft etc. Hence there is a need of more robust authentication technique. In this work, a robust and dynamic authentication approach based on query updation for cloud environment is proposed. The proposed system appears to be more secure against the traditional approaches.

Keywords: ***cloud authentication, Ip theft, cyber-attacks.***

1. Introduction

1.1 Basic Cloud Architecture

Cloud computing is an evolution of grid computing. Cloud offers great benefits to the users as well as the IT infrastructure by breaking the physical boundaries between them due to openness of accessible information and data relying on trust between cloud provider and users. Threats due to heightened security must be overcome in order to benefit fully from this new computing exemplar. Cloud technology is helping organizations build a smarter business infrastructure with immense flexibility and scalability. Cloud-based systems have brought a new, scalable application delivery service model to the market. They can help clients save money and increase flexibility. Cloud computing provides the remote services to the Cloud utilizers through a network services. Cloud uses resource in minimized way and gives the maximum capability of computing. The end user needs only minimum hardware requirements in order to use these facilities. Cloud computing can dynamically deploy, allocate or reallocate computing resources and also used to monitor the usage of resources at all times. Cloud provides some of the management mechanisms and also provides services to the millions of users simultaneously. Cloud service mainly gives these essential characteristics. 1. On-demand self-service, 2. Broad network access, 3.Resource pooling, 4.Rapid elasticity and 5.Measured service. Cloud mainly provides three types of services to the all cloud utilizers and they are 1. IaaS (Infrastructure as a Service), 2.PaaS (Platform as a Service), 3.SaaS (Software as a Service) and collectively *aaS (Everything as a Service) all of which means a service-oriented architecture. One of the benefit of the cloud computing is that it reduces cost of hardware that could have been used at user end. In cloud computing there is no need to store data at user's end because the data are already stored at some other location. Although there are so many advantages of cloud computing, there are few disadvantages of cloud computing like Technical Issues, Prone to Attack, and Security in the Cloud. So we will discuss how to resolve the security issues, for this we need to have a robust and dynamic authentication approach based on query updation for cloud environment is proposed in this paper.

1.2 Authentication

Authentication is an important aspect to consider while accessing any information. For the authentication purpose user is provided with a login id and password to prove his access rights and identity. However, this type of authentication can be circumvented by hackers. Some of the common existing authentication approaches like Password and PIN based authentication, SMS based authentication, Symmetric-key authentication, Public-key authentication, Biometric authentication.

1.3 Design Objective

1. Integrity: Integrity means the assurance that the information can only be either accessed or modified by the authorized user. It also termed as protecting the data from any unauthorized party.

ISSN 2348 – 7968

2. Confidentiality: It defines set of rules or a promise that limits access or places restrictions on certain types of information.
3. Scalability
4. Storage Efficiency
5. High Reliability Cloud uses data fault tolerant to ensure the high reliability of the service.

The paper is organized as follows: Section II discusses about the Existing Authentication System. The Dynamic Query Updation proposed method briefly discussed in Section III. Related Work defined over Section IV and finally conclusion is on Section V.

2. Existing System

2.1. Introduction to Authentication system in Cloud Computing.

In order to ensure the authorized user in cloud computing, the authentication system plays vital role in it. Information Assurance (IA) mainly contains five pillars of process where Authentication is one of the important process in it. The other processes are integrity, availability, confidentiality and non repudiation. When the user tries to access any information from the system, Authentication begins at that moment. While User tries to log in into the system, User has to give the User Name and Password for authentication purpose. These types of login credentials are assigned to the user already and which can also be spread over hackers. Hackers may use these credentials to login into the authorized user's system. Hence these credentials cannot be shared with any others because it contains sensitive information. Previously some mechanisms were used for this authentication purpose. They are discussed below.

2.2 Existing Authentication Method

1. Password and PIN based authentication

This authentication method is one of the common mechanism which uses password or Personal Identification Number (PIN) to login. One of the example of this mechanism is use of password to login HK public library system for book reservation.

2. SMS based authentication

In this method, the Information System generates One-Time Password (OTP) which is delivered to the user through SMS. In order to complete authentication process user uses the password which he received through message in cell phone. Nowadays in Internet banking system SMS-based authentication is used.

3. Symmetric-key authentication

One of the unique key is shared among the user and authentication server, where user randomly generates the message which is encrypted using the secret key and sends it to the authentication server. In the other end the authentication server decrypts the message with shared secret key and matches it, and authenticates the user. One slight variation of this approach is the use of OTP tokens, which generate the OTP on user side for matching with that generated on server side. In Internet banking system this OTP are used for the authentication.

4. Public-key authentication

In this method some key pairs are used which contains the user's private key and group's public key. Private Key is kept secretly by the user, while the corresponding public key is commonly embedded in a certificate digitally signed by a certification authority. The certificate is shared among all the users. In Registration and Electoral Office, this authentication is used to change the address of the registered voter.

5. Biometric authentication

In this Biometrics method a person's authentication information is generated by digitizing measurements of a physiological or behavioral characteristic. Biometric authentication verifies user's claimed identity by comparing an encoded value with a stored value of the concerned biometric characteristic. For example this biometric authentication used in HK Immigration passenger e-channel where fingerprints are used.

3. Proposed Method

The proposed method mainly discusses about the three modules. They are 1. Registration Module, 2. Log-In Module, and 3. Log-Out Module.

ISSN 2348 – 7968

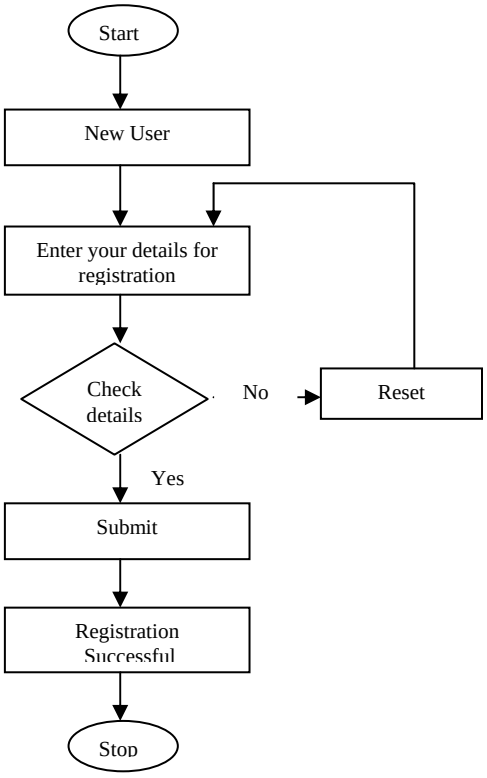

Fig. 1 Registration Module

Fig. 1 shows the Registration module for the proposed system. First the User can be of two type that 1. New User and 2. Registered User. If the New User comes to the system he has to provide details for the upcoming authentication process. Registration Form asks the usual question from user like user name, password, email id etc. The data will be validated and then user will successfully complete the registration. After the Successful Registration each user has to give the question and answers for the authentication purpose.

Fig. 2 shows the Log-In module for the proposed method where the already registered user wants to log in into the system and tries to utilize resources. User has to first give the credentials of user name and password. When they are validated successfully User moves to the next phase of validation process. In next phase user has to answer for the two questions which he already entered while registration and also the user's IP address will be validated which is already defined one for each user. When this phase completes successfully, User can work with cloud resources. If some unauthorized person tries to login with same credentials and with answers with different IP address the authorized person will immediately get one email notification for password change process. This password could be any random system generated value. Hence in this way the system data can be protected from any unwanted user.

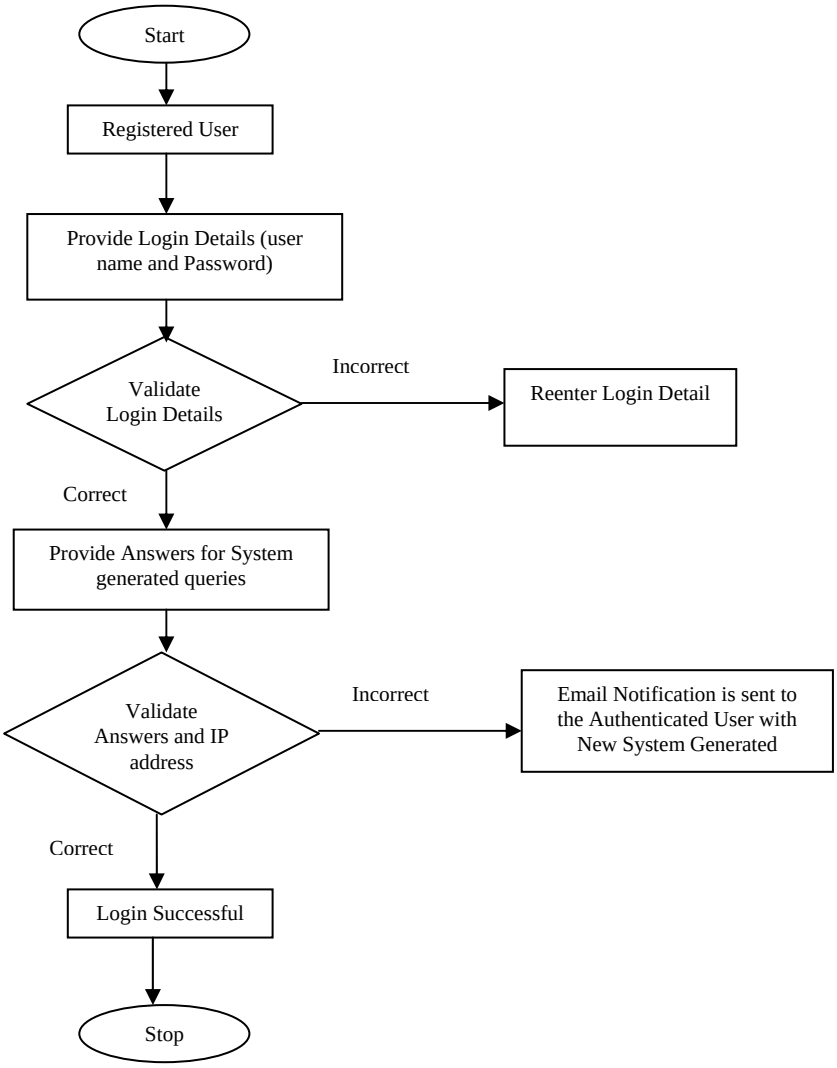

Fig. 2 Log-In Module

Fig. 3 shows the Log-Out Module for the proposed method which come into play when user completes all his work over cloud. After completion of his work User presses the Log-Out button which will lead the user to the query form, where the user need to give two new queries and answers for them. This two queries will be replaced with the two existing queries which the system has generated during Log-In module. Hence In this way the system storage space effectively utilized.

Proposed system provides the scalability option also where any number of user can add into the system and also their data will dynamically maintained. All the Design goals will be achieved through this proposed method where confidentiality, Reliability and Integrity increased.

ISSN 2348 – 7968

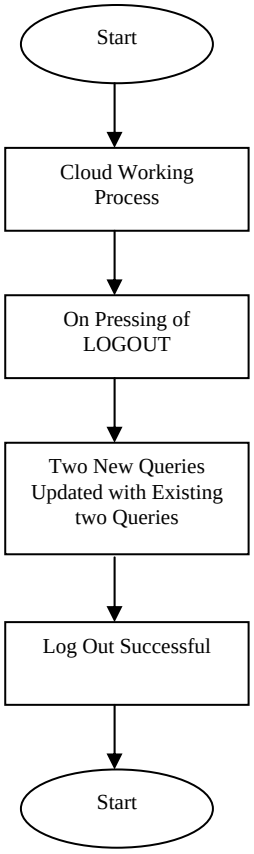

Fig. 3 Log-Out Module

4. Related Work

Yassin*etal* proposed a method for authentication using anonymous Password authentication [APA] which is mainly used for the Privacy Authentication. This system guaranteed two factors that 1. Private Information Retrieval [PIR]. 2-Factor Authentication (2FA). It has mainly two benefits that 1. There is no need for storing the password on the server 2. Server side authentication is done [1]. Banyal*etal* proposed Cloud Access Management system for an authentication based on three factors: Arithmetic Captcha Expression, Multi-Level Authentication, and Secret Splitting of Authentication Factor. For cloud computing environment these secret-splitting and encrypted value of arithmetic captcha are innovative factor. The user also authenticated dynamically using multi Secret key, One Time Password and IMEI number. This framework provides a feasible and efficient solution by combining the traditional user id and password based authentication [2]. Jivanadham *et al* proposed an authentication system known as cloud cognitive authentication (CCA). This method uses the concept of one round zero knowledge proof (ZKP) and Advance Encryption Standard (AES) to enhance the security in public, private, hybrid cloud [3]. Rouzbehetal proposed an authentication mechanism in which they introduced two techniques those were Client-Based User Authentication Agent (CUA), Modified Diffie-Hellman Agent (MDHA). In CUA agent had been introduced to confirm identity of the user in client side before accessing to cloud servers. CUA provides a secure user authentication for personal and registered devices. However, for accessing to cloud servers with un-registered devices another process of authentication seems to be necessary. Accordingly, MDHA is introduced based on ZKP Diffie-Hellman to increase the rate of reliability in process of user authentication by un-registered devices. By using MDHA, temporary access permission has been provided for users for accessing from un-registered device [4]. Jyoti Choudhury et al proposed an authentication schemes in which an extra OOB (out of band) factor which undoubtedly provided better security over two factor authentication. This scheme consisted of three phases: registration phase, login phase and authentication phase and one activity, called password change. The proposed framework provides identity management, mutual authentication, session key establishment between the users and the cloud server. A user could change his/her password, whenever demanded [5].

5. Conclusion

The proposed method mainly describes about the modules which are present in the Dynamic Query Updation Authentication system. In existing mechanism this query related authentication was not used. But in Proposed System the user has to give queries and answers and each time the old queries will be replaced by the new queries. Hence the Storage space will be effectively utilized and also the efficiency improved in terms of security, scalability, and integrity. This mechanism will become more trust-worthy for the users who use and share confidential data over cloud.

Reference

[1] **Ali A. Yassin, Haijin, and AyadIbrahim "**A Practical privacy-preserving password authentication scheme for cloud computing", **IEEE 26th International Parallel and Distributed Processing Symposium , 2012**

ISSN 2348 – 7968

[2] **Rohitash Kumar Banyal, Pragya Jain**, "Multifactor Authentication Framework for cloud computing", **Fifth International Conference on Computational Intelligence, Modeling and Simulation , 2013**

[3] **L.B Jivanadham, yoshiakin katayamma, "**Authenticating the cloud environment by Cloud cognitive authenticator (CCA)", **2013**

[4]**SohrabRouzbeh ,NimaMorabAlibeigi., "**A Scalable and Efficient user Authentication scheme for cloud computing environments"**, 2014**

[5] **AmlanJyotiChoudhury, Pardeep Kumar,** "A Strong User Authentication Framework for Cloud Computing", **2014**

[6] **M. Peyravian, Zunic, N**,"Methods for Protecting Password Transmission," Computers & Security , **vol. 19, pp. 466-469, 2012.**