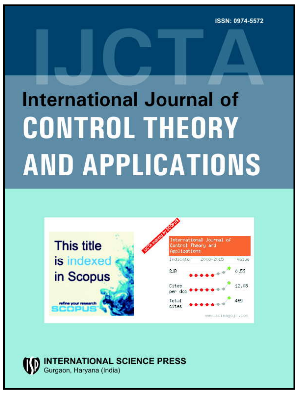

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 14 • 2017

Multi-Tier Authentication Model for Cloud Computing: "Security as a Service"

Ayushi Pathak[1] and Deepak Motwani[1]

[1] *Department of Computer Science Engineering ITM University, Gwalior, M.P., India,*
Emails: er.ayushi.pathak@gmail.com, dmotwani20005@gmail.com

Abstract: In the late years, cloud computing has become a best option for an industry, because it offers scalability, cost efficiency, multi-tendency and fault tolerance. On the other hand, cloud computing is still facing difficulties, researcher are trying to overcome it. User authentication in cloud computing is one of the major problem. Currently, the private information has been leaked through a high - degree system such as- phishing beyond snatching the user ID and Password. User authentication is one of the basic procedures to ensure the standard and quality of any product in the market. In this paper we suggest a model whereby the application in the advance cell phone decrypts the captured coded image and sends it all the way through the Cloud Data Management Interface for authentication. The message is sent to product manufacturer's data center and the response received from the cloud allows the consumer to decide on the products authenticity. After successful authentication, OTP is send to registered number which prevent user from replay attack.

Keywords: One-time Password, QR Code, User Authentication

1. INTRODUCTION

In this paper, authentication method for sensitive cloud framework is proposed. Cloud network which may available greater convenience and security to user for sensitive information through authentication method i.e. 32 bit encrypted code, mobile and password OTP with the QR-code. Once the user contain 32 bit encrypted password matches with the users' original password then it goes QR code authentication, whenever he login to his account it time. The problem occurred mainly because of improper authentication system to find whether the product is an original one. Cloud computing is the commoditization of data storage along with computing time through standardized technologies. It has noteworthy advantages over conventional physical distribution [5]. QR code has become a medium of advertising strategy, since it provides a method to access a website more quickly than by physically entering a URL address. It also reduces the chance of error while entering URL, because single change in letter may leads to wrong website. QR codes can be utilized to sign in into sites: a QR code is appeared on the login page on a PC screen, and when an enrolled client read it with a checked verified smart phone, they will be directly signed in. Authentication is performed by the advanced cell phone which contacts the server [6]. One Time Passwords (OTP) is passwords which are legal only for the session to authenticate the user within a particular amount to time. Hence for each session the user will be validated using new OTP. They are also caring in preventing replay phishing attacks, and other attacks on basic static passwords. Also there are they offer another characteristics like extensity, portability, anonymity and enables to keep the information from being leaked. SomeOTP transmission is done by text messages through gateway; web based systems, propriety tokens, grid file and secure code machines. The most current grid file maintains a hash type file of confirm the user's authentication request also improvement the risk to tampering. But all to them deal with text based methods which may be identified in infinite time.

The rest of the paper is organized as follows. Literature Survey is explained in section II. Cloud Authentication is discussed in section III. Architecture of Proposed System is presented in section IV. Concluding remarks are given in section V.

2. LITERATURE SURVEY

Markus Jocobsson et al proposed a scheme in which authentication is done on the basis of client behavior. Authentication score is checked against a specific limit. Consequently a best outcome rely on upon application[1]. The word Cloud Computing comprises of three things: "application" "storage" and "connectivity". Many of the users and cloud vendors are attracted towards cloud computing, because it facilitates various important characteristics available in the cloud system [7]. Traditional authentication procedure generally requires a password and id to authenticate the identity to user. By nature, user is in that case looking for a password that is easy to secure and remembers from any attack. However, remembering lots of difficult passwords, especially when user have various accounts, is not an easy target. Earlier two factor verification technique is common in use. OTPs are converted into the form to an image which makes this complex for intruder to find the presence to secured information. OTP is send to the concerned user through an email message. In that case two factor verification personally may be identified through his password and username. If the password and username is matched with the device then process to authentication is complete and user may be control the data. But in this technique anyone may hack access and password information. In many cases, users' passwords are collected in plain-text form onto the server machine. A person who can access server's database has access to adequate information to impersonate any authenticable user. In cases in which users' passwords are data collected in encrypted form on the server system, plain-text passwords are still sent across a possibly-insecure network from the client to the server. Each separate system must carry that's own copy of each user's authentication information. As a result, users must retain passwords at every method to which they authenticate, and so are likely of prefer less-than-secure passwords for ease. Knowledge based authentication uses undisclosed information. When user available few information of authenticate himself as a legitimate user, the method processes this suggests and information whether the user is legitimate or not. Amlan Jyoti choudhury et al proposed a scheme which offers Session key agreement, Mutual authentication, Identity management. Proposed approach verifies smart card and password from local system, which cause leakage of information [2]. H. A. Dinesha et al proposed scheme where central system distribute credential for authentication purpose. Credentials were distributed by central system, thus if central server is hacked then entire system fails[3]. Hua-Hung Zhu et al proposed algorithm which make the voice print information invertible. Size of database depends on users, hence number of user increase the overhead is more[4].

3. CLOUD AUTHENTICATION

In First step we create a program which is generate 32 bit keyed-hash message authentication code encrypted code, this program continuously generated 32 bit code in specific time interval. This code then embed into cloud URL having user login id and address. After a specific time span the generated code is expire and new code is generated. Each time when key changed a Specific QR Code is generated for client which offers very high security to client. Thus authentication of Cloud can be done with the QR codes it is printed on the mobile page, webpage, authentication card etc. It is captured as an image through the camera attached with the mobile phone. The image is then opened with the QR code reading application to extract the data from the code and is sent to the central web server as an SMS an OTP is generated by service provider to user which consist of encrypted password. The web server is attached to the cloud with through internet; the web server on receiving the SMS sends the data to the corresponding service provider in the cloud. The service provider using a searching algorithm looks for the encrypted password given by user in the Corresponding database. If the encrypted password is found, a reply is sent to the central server stating that the user is authorized to enter in could and if the corresponding record is not found then the service provider sends a message to the central server stating that the user is unauthenticated.

4. ARCHITECTURE OF PROPOSED SYSTEM

Cloud computing has nowadays come into the mobile world as ‾Mobile Cloud Computing , the cloud computing offers general applications online which can be accessed by a web browser while all the software and data resides in the server and the client can access those applications and data without the total knowledge about the infrastructure.. The cloud computing has five essential characteristics: On demand self-service, Broad network access, Resource pooling, Rapid elasticity and Measured service. The authentication system uses SMS to transmit the data from the mobile phone to the server in the cloud. The data is transferred through the wireless medium using the Signaling System No 7 protocol. This protocol is used to send the MMS, SMS from the mobile phone to any other phone. Attacking the transmitted signal is considerably increased in the recent years. So there is a high probability of hacking the data sent through the SMS and modify it to show that the product scanned is original by the hacker. To avoid such attacks the system should also be able to resist the intrusion. The system is made more secure with the help of applying an encryption algorithm to it. The algorithm used is a normal public key encryption algorithm which uses the same key to decrypt and encrypt and the message. With the help of this encryption system the message is encrypted before sending from the mobile and in the server after receiving the message from the mobile it is decrypted to get the actual message. The QR code with an encryption algorithm increases the security of the whole system which makes it more difficult to attack the system and get the data transmitted. The Algorithm Generate32SecretCode() below illustrates the encryption and decryption process in the system.

The various steps followed in the process of authenticating the products are as follows. First the QR code is read with the camera connected to the mobile device and the captured image is then encoded with the decode () function. Then the encoded data is then move to the central server in the cloud through SMS

```
Generate32SecretCode()
    set sb = null
        Random random = new SecureRandom()
        set i = 0
         Repeat step (i) to (iii) while i< 16
        i)set val = random.nextInt(32);
        ii)if (val< 26) then
                sb.append((char) ('A' + val));
            else
                sb.append((char) ('2' + (val - 26)));
            [End of id statement]
     iii) set i = i+1
     [end of while loop]
    return sb.toString();
```

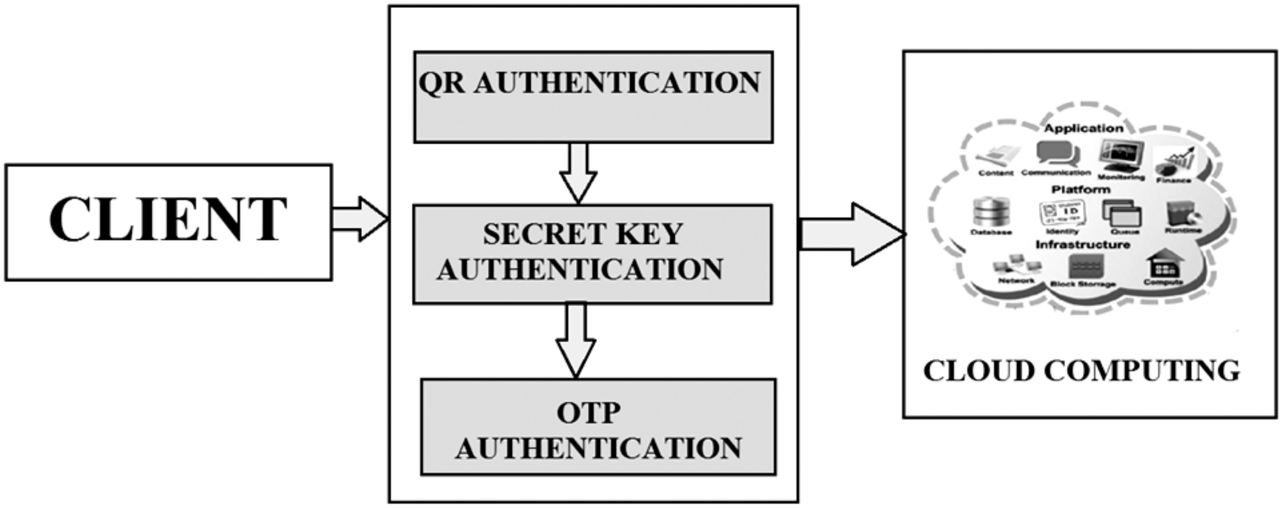

Figure 1: Proposed MTA Model for Cloud Computing

with the help of the send Encoded() function. The central server on receiving the data from the mobile searches the respective server and checks for the record. The reply is then transmitted to the central server and then the server sends the reply to the mobile device. The architecture of proposed MTA model is shown in fig .

In the proposed methods the user have to register. The user registration phase required users login password and name is kept in the database at that time of the registration. As well as in these times to registration user run a program which generate a 32 bit encrypted password which stored on server database. The user registration require personnel information of user. When this information is fill then user account will be created. This password may regularly changed after the specific interval. Each time a password changed a new QR-Code is generated for user for Authentication. When user scan the generated QR-Code with Mobile an authenticated screen show on mobile and an OTP message generated which consist of encrypted password. Given below algorithm generate the URL for QR-Code with secure password.

```
QRPictorialUrl(keyId,secret)
Sets b = new String Builder(128);
sb.append("https://chart.googleapis.com/chart");
sb.append("?chs=200x200&cht=qr&chl=200x200&chld
=M|0&cht=qr&chl=");
sb.append("http://").append(keyId).append("%3Fsecret%3
D").append(secret);
returnsb.toString();
[end of algorithim]
```

When user enter the password and press submit button the control move to the cloud database and check the password given by user if password is correct the user entered into the could.

Figure shows the first stage of proposed approach where 32-bit secret key is generated and which is active for a short period of time.

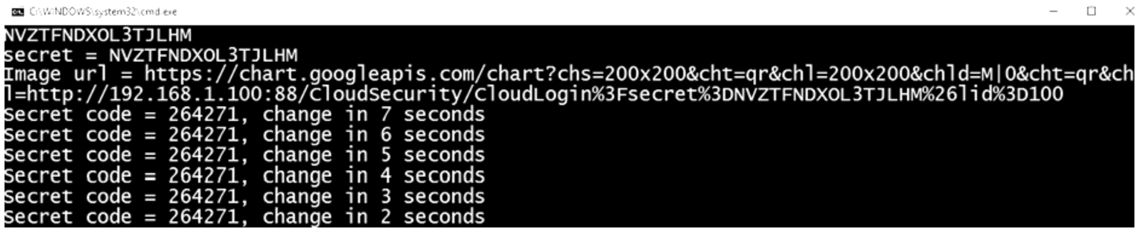

Figure 2: 32-bit Secret Key

Figure 3: QR Image for website

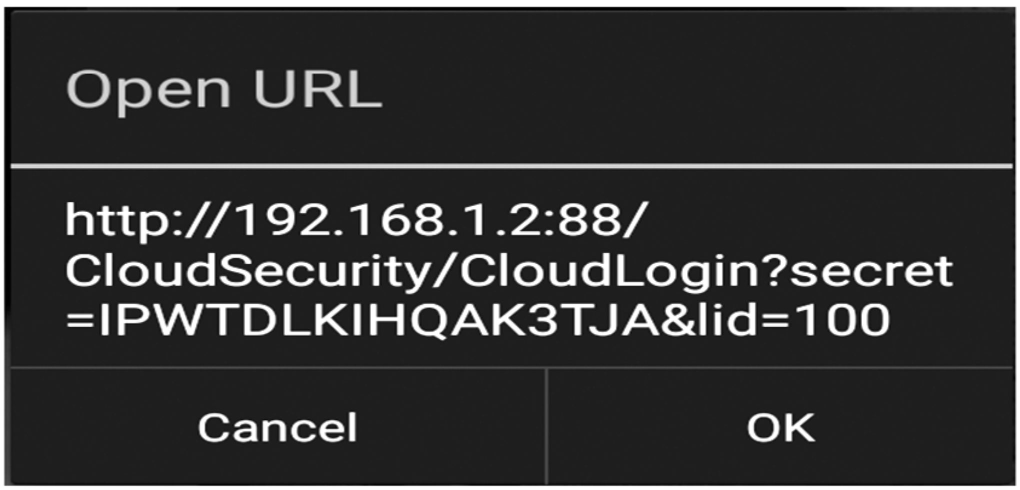

Figure 4: URL Generated From QR Image

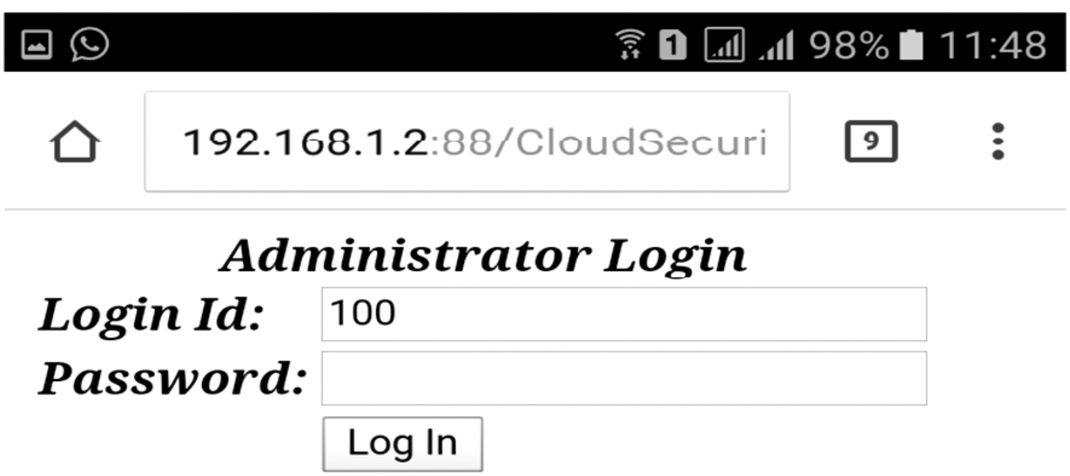

Figure 5: Login Page

After key phase, QR image will be generated which is more easier way for entering into a website. The QR redirect user to a website through URL address.

The proposed system is more protect than the other authentication method at the time to login. If in there are user entered password and username is accurate then he moves from chessboard otherwise he display the message incorrect username or password. After completion to a chessboard user goes to a QR code environment in that environment user requires an OTP. When this password is right then user have a permission to do their workon cloud using a hadoop framework.

5. CONCLUSION

Proposed MTA model is known as Safe Three layer password protection; in this we provide various verification system step by step (one level after other level). Our technique available the authentication or security for sensitive data as the hacker will have to goes by three stage of authentication in which the complexity level growing's at every step. We thus conclude our proposed model saying that this will be a most safe Cloud Authentication System and can be implemented for safe and secure login .In this paper we have proposed a novel authentication scheme for cloud by QR code based OTPs. In recent years there has been the precipitous improvement in the number of cloud users. Hence the proposed method satisfies the high protect requirements to the cloud systems and protects them against various security attacks. Also the system does not need any technical pre-requisite and this creates it very user-friendly. Hence QR code proves to be versatile at the same time beneficial for both the customers in terms of security and vendors in terms of increasing their efficiency. Hence it is most widely used to advertise and market the products by most businesses.

REFERENCES

[1] Chow, Markus Jocobsson, Ryusuke Masuoka, Jesus Molina, Yuan Niu, Elaine Shi, Zhexuan Song, "Authentication in the Clouds, 2010.A Framework and its Application to Mobile Users. CCSW 10, October 8, 2010, Chicago, Illinois, USA.

[2] Amlan Jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim, Hoon Jae-Lee, 2011. "A Strong User Authentication Framework for Cloud Computing", *Asia - Pacific Services Computing Conference*, *IEEE*, 2011.

[3] Dinesha H A, 2012. "Multi-level Authentication Technique for Accessing Cloud Services", *International Conference on Computing, Communication and Applications (ICCCA), IEEE*, 22-24 February 2012, pp 1-4.

[4] Hua-Hong Zhu, Qian-Hua He, Hua-Hong Zhu, Hong Tang, Wei-Hua Cao,"Voiceprint-Biometric Template Design and Authentication Based on Cloud Computing Security", *IEEE international Conference on Cloud and Service Computing*, 2011

[5] Ayushi Pathak and Deepak Motwani, "Enhancing BigData Security in Cloud", in*Proceedings of ICCCS-2016,* September 2016

[6] Google testing login authentication via QR codes,2012

[7] Mohiuddin Ahmed, Abu Sina Md. Raju Chowdhury, Mustaq Ahmed, Md. Mahmudul Hasan Rafee, "An Advanced Survey on Cloud Computing and State-of-the-art Research Issues", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012.

[8] Prof. Sonkar S.K.; Dr. Ghungrad S.B., "Minimum Space and Huge Security in 3D Password Scheme",*International Journal ofComputer Applications* (0975- 8887), Volume 29-No.4, September 2011.

[9] Cloud Computing: A Practical Approach Anthony T. VelteToby J. Velte, Ph.D. Robert Elsenpeter.

[10] Kuan-Chieh Liao, Wei-Hsun Lee, Min-Hsuan Sung, Ting-Ching Lin, "A One-Time Password Scheme with QR-Code Based on Mobile Phone", *Fifth International Joint Conference on INC, IMS and IDC,* 2009, pp 2069-2071

[11] Sang-Il Cho, HoonJae Lee, Hyo-Taek Lim, Sang-Gon Lee, "OTP Authentication Protocol Using Stream Cipher with Clock-Counter", October, 2009.

[12] R.Buyya, C.S.Yeo, S.Venugopal, J.Broberg, and I.Brandic. Cloud Computing and Emerging IT platforms : Vision, Hype and Reality for Delivering Computing as the 5thUtility. Future Generation Computer Systems, 25(6):599-616,*Elsevier*, June 2009.