www.ijiarec.com

ISSN: 2348-2079

MAY-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

# CLOUD BASED MULTIFACTOR AUTHENTICATION FOR PERSONAL HEALTH RECORD

[1]S.Roobini, [1]V.Shivaganeshan, [1]B.Swathi, [2]Mrs.S.Vidya

## ABSTRACT

Cloud-based services are increasingly becoming extensively adopted by healthcare organizations. The past year alone has seen a rush of attention concerning the prospective of cloud computing with many vendors set to start moving healthcare-related applications across to cloud platforms. Healthcare clouds put forward new possibilities, such as straightforward and everywhere access to medical data, and opportunities for new business models. Still, they also put up with new risks and elevate challenges with respect to security and privacy. Traditional way is to provide security to PHR is Authentication to the data stored in the database. To make more secure, various Authentication techniques are used. In existing system two factors Authentication is performed based on the OTP which is randomly generated and sent through mobile phones as a Short Message Service (SMS). The proposed model describes about a Multifactor Authentication which includes Color Scheme, Graphical Password and One Time Password (OTP) is generated.

**KEYWORDS:** Personal Health Record, Cloud Computing, Multifactor Authentication, Color Scheme, One Time Password

## INTRODUCTION

Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices are used to handle the data. In cloud computing, the word cloud means “the Internet," so the phrase Cloud computing means “Internet-based computing,"[6].PHR grants patients access to a wide range of health information sources from anywhere at any time. PHR plays a predominant role in healthcare and important since because of increasing health issue in the modern world. The information in PHR is accurate and updated periodically. The patients control over their own privacy using homomorphic encryption has been done with data auditing to check the correctness of PHRs stored in cloud server [7].

Authentication is the process to establish the identity. Passwords are used as one of the authentication to control the data access. To make secure, Authentication is provided to the data’s stored in the cloud database. Access Control is normally based on the User’s identity which requests an access to a resource, Authentication is important to Security [4].

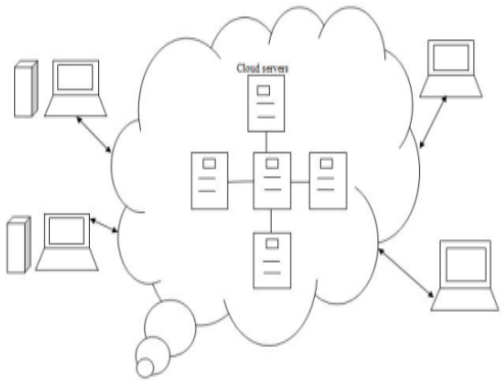



**Figure 1. Structure of Cloud Computing**

Two factors Authentication implements the above methods by using several mechanisms. Multifactor Authentication uses more than one form of authentication to verify user’s credentials. The goal of this project is to access personal health record which is stored in Cloud database and implementation of Multifactor authentication.

**Author for Correspondence:**

[1]B.E-Final Year, Department of Computer Science and Engineering, SNS College Of Technology, TN, India.

[2]AP/ Department of Computer Science and Engineering, SNS College Of Technology, TN, India.

## RELATED WORK

The related descriptions with its ideas and several articles convey the following.

### ONLINE-BASED ACCESS

The accessing and sharing geospatial data issue, online services called Open Geospatial Consortium Web Services (OGC Web Services) was introduce to enhance interoperability among heterogeneous data. Web services established a single point of access called Ocean Data Portal (ODP) to improve seamless access to oceanographic data. Medical system called as Telemon, facilitate ease access to critical patient data during emergency situations and patient history [4].

### BIOMETRIC-BASED ACCESS

The commonly used Biometrics such as face recognition, fingerprint, hand geometry, iris or retina-scan, voice- recognition and keystroke scan. These provide ease access only for authorized personnel to certain information or infrastructure of a building, protect the network facilities, systems [4].

### TOOL-BASED ACCESS

The most commonly used Tool-based Accesses are smart card, smart-tag, co tag to authenticate the identity of user before granting the access of particular information. Another alternative data accessibility method is barcodes, QR codes to store the data or links which can be used via mobile devices [4].

### TEXT-BASED AUTHENTICATION

In Text-based authentication, the user ID and a text password is needed to have access to the cloud services [1].

### HYBRID TEXT-IMAGE BASED AUTHENTICATION

In this type of authentication, this combines the images with text to ensure a strong authentication scheme against brute force attacks. Image-based authentication provides the best solution and can be done at both the cloud client level and also at the application level [1].

### ABE FOR FINE-GRAINED DATA ACCESS CONTROL

Attribute Based Encryption (ABE) used to secure Electronic Healthcare Records (EHR) which can be encrypted using a broadcast variant of cipher text policy CP-ABE that allows direct revocation. In this the owner has to upload ABE-encrypted PHR files to the server. Each owner's PHR files are encrypted both under a certain fine-grained and role- based access policy for users and a selected set of data attributes that allows access from users. Only authorized users can decrypt the PHR files, except the server [8].

### MA-ABE IN THE PUBLIC DOMAIN

Multi authority ABE (MA-ABE) to increase the security and avoid key escrow problem. Our framework delegates the key management functions to multiple attribute authorities. In favour of achieve stronger privacy guarantee for data owners, the Chase-Chow (CC) MA-ABE scheme is used and each authority governs a disjoint set of attribute distributive. The enhanced MA-ABE scheme facilitates the data confidentiality of the PHR data against unauthorized users [8].

## EXISTING SYSTEM

The existing model so far focuses on two factors Authentication. Authentication types which exist today are of three categories. It is based on what we know, what we have, what we are. Passwords come under what we know. These passwords can be easily revealed to others and it is hard to remember. Traditional authentication is usage of text password system suffers from problems like eves dropping, dictionary attack and shoulder surfing. Security issues are predominant in this system because of weak authentication. Smart cards and tokens fall under what we have or possess. These smart cards and tokens can be easily stolen and lost. This kind of authentication using smart cards and tokens are expensive and also hard to manage [2]. Two factor authentications are used with smart cards and tokens but they are not efficient because of its disadvantages. Biometric authentication is the third type which exists and it is based on what we have. Fingerprint scanning, IRIS scanning are the examples for biometric authentication. Biometric authentication is not extensively used because it is expensive and it is not applicable to everyone [9]. One time passwords (OTP) are used to decrypt the data. One time passwords used with smart card and tokens are not efficient. Two factor authentications are also used with mobile phones. SMS based Onetime passwords is generated to decrypt the users data. This symmetric key is used to carry out transaction in secured manner. It has some drawbacks such as

it requires more storage, cost of maintenance is high and if this key is hacked then there is no use in OTP generation.

The main drawback in existing method is asymmetric based key exchange so using public key the confidential information can be easily taken by the third party.

## PROBLEM FORMULATION

The Problem identified is Authentication provided to ensure Security. On accessing the data, it should provide those integrity based information in a secured manner. Two factor Authentication technique in which generation of OTP and sending through mobiles leads to breach of information. Less efficient Authentication mechanisms does not provide Confidentiality while accessing the data. Stronger Authentication is required during accessibility of data from cloud server.The usage of lengthy passwords will be secure but the remembrance is difficult and short passwords can be easily remembered but easy to crack.

## PROPOSED SYSTEM

Proposed system includes Multifactor Authentication Scheme. Multiple stages of authentications include User-name password, Graphical password, Color scheme. One time passwords (OTP) can be generated using color scheme authentication which acts as a decryption key for access. This access key is sent to users mail account. Multiple stages of authentication functionalities are as follows

### GRAPHICAL PASSWORD AUTHENTICATION

Graphical password authentication is an image based authentication. Multiple hotspots are fixed in image that acts as password. Hot spot fixing is done at the time of registration. Admin must login by clicking on correct hotspots given at the time of registration or else has to retry. Methodology used is Peruasive Discretization. The hotspots are fixed in an image based on the discretization to a particular viewport in an image. The Peruasive Discretization algorithm is a client-server model which displays the images and authenticates the admin to access their PHR. Every points needs to be accurate and it is computed based on the |xoriginal − xcurrent| and |yoriginal − ycurrent|.During login phase the password must match the database which is provided at that time of registration.

### COLOR SCHEME AUTHENTICATION

Color scheme authentication is mainly to provide strong Authentication. The users rates the colors from 1 to 8 during registration phase as shown in figure2.Same rating can also be given to different colors. The colors can be remembered in the order as “RLYOBGIP”. During login, an interface is displayed which contains 8x8 grids because it has the combination of those colors randomly distributed. A pair of color is used in which it has 4 pairs. The first color is considered as row and the other is column with its intersection, password is provided. At this phase, an interface is displayed as shown in figure 3.The strips of colors are considered in the interface

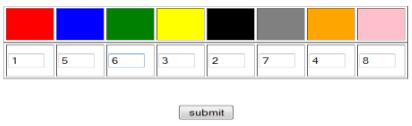



**Figure 2. Rating of colors**

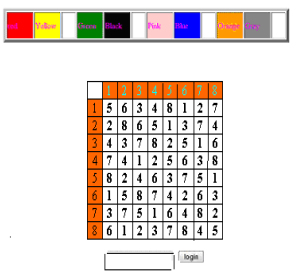



**Figure 3. Pairing of colors and interface**

**ONE-TIME PASSWORD (OTP)**

The generation of OTP is done using special algorithms to provide randomness. The randomness of algorithm is required because without any randomness there is a chance to predict the future by analysing the past OTP's.

By using several mathematical algorithms, the server has to provide a key for transmogrification which can be done only by sending OTP as mails.

**ENCRYPTION ALGORITHM**

The Algorithm selected for encryption is Advanced Encryption Standard (AES). The Advanced Encryption Standard or AES is a symmetric The Cipher is said to be encrypted text, after the transmogrification of plain text, the resulted text is said to be Cipher text. Cipher blocks which operates on the fixed length group of bits called as blocks. Rijndael Algorithm uses triple discreet invertible uniform transformations. Encryption algorithm includes layers as Linear Mix Transform; Non-linear Transform and Key Addition. During login phase, username and password is provided. Then, in graphical password the hotspot is used as a password. An interface of color grid is displayed, in which password is generated based on the rated colors. This generated password is mainly used as an OTP to decrypt the data stored in cloud server. The patients can view their details of PHR and can access it in a secured manner. The modules present in our proposed system:

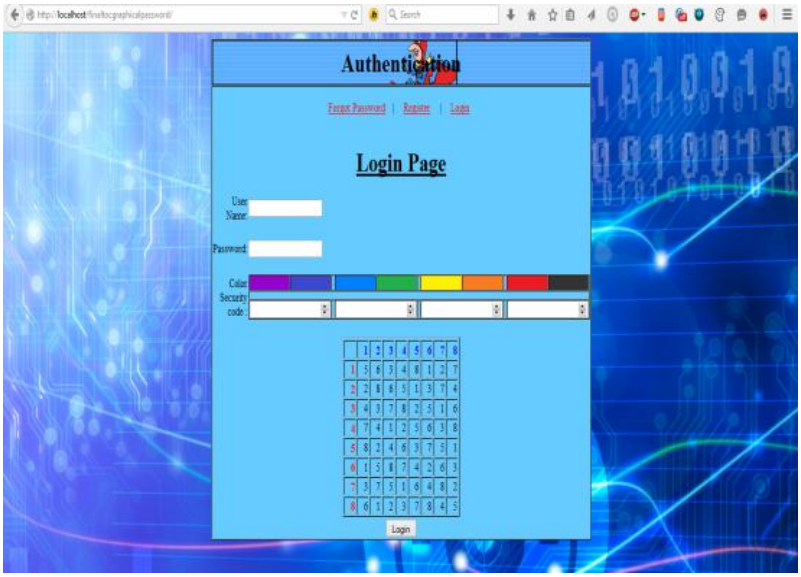
- **CLOUD USER AND CONSUL**
  Cloud users register by providing their credentials. Users login to access PHR by using credentials that was specified at the time of registration. Admin logs into the system using his account to view encrypted data of users and keeps an overall control. Admin approves valid users after verification.

- **TRANSMOGRIFICATION AND REDEEM**
  Encryption of data to provide secured access.Advanced encryption scheme (AES) is used. Rijndael algorithm is used to handle additional block sizes that were not adopted in AES.

- **GRAPHICAL PASSWORD AUTHENTICATION**
  Authentication based on images by fixing hotspots. Multiple hotspots are fixed at the time of registration. Users authenticated when they locate correct hotspots. Incorrect location of hotspots results in authentication failure and users are requested to retry. In figure5, the image has four hotspots.

- **COLOR SCHEME AUTHENTICATION**
  Color ratings provided at the time of registration. Session passwords created based on color ratings. User authentication is failed in case of change in color ratings and users are requested to reattempt. In figure 4, authentication is provided based on ratings

**Figure 4. Color based Sign in**



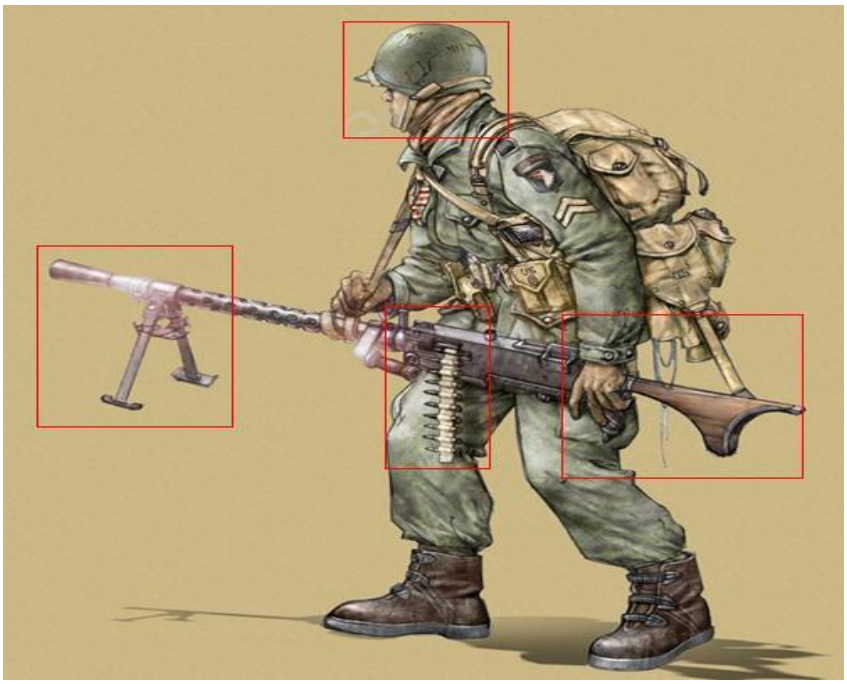


**Figure 5. Hotspot based sign in**

## CONCLUSION AND FUTURE WORK

Multifactor Authentication includes Username and Password pair, as well as graphical password and color scheme Authentication with OTP. This new system is more beneficial and ensures secured accessing of data by including encryption algorithm. In future record migration can takes place with the help of Administrator in a confidential manner and the system can be further enhanced by integrating an emergency rule access.

## ACKNOWLEDGEMENT

The completion of project depends upon cooperation, coordination and combined efforts of several sources of knowledge. We would like to thank our Department of Computer science and engineering for providing immense guidance for our project.

## REFERENCES

[1]. AlinaMadalinaLonea, Daniela Elena Popescu,"An Hybrid Text-Image Based Authentication for Cloud Services" Faculty of Electrical Engineering and Information Technology, University of Oradea Romania, 410087 Oradea, 1, ArmateiRomaneStr, INT J COMPUT COMMUN, ISSN 1841-9836 8(2):263-274, April, 2013.

[2]. Anu Varghese, Deepthy Mathews. Er, "Securing SMS-based approach for two factor authentication" International Journal of Research in IJRCCT Computer and communication technology Computer Science Department Christ Knowledge City Ernakulam, India, 2014.

[3]. Dussa Manasa1, K. Rajesh Khanna M.Tech in CSE Dept, Associate Professor in CSE Dept, Vaagdevi Engineering College, Warangal, Andhra Pradesh, India "Sharing of PHR's in Cloud Computing", International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 2, Issue 4, pp: (201-208), October - December 2014.

[4]. Fathin N. M.Leza, Mohd. Khanapi A. Ghani , Nurul A. Emran, , "Review Of Data Accessibility Methods In Healthcare" Centre for Advanced Computing Technology(C-Act), International Symposium on Research in Innovation and Sustainability 2014 (ISoRIS '14)University Teknikal Malaysia Melak, October 2014.

[5]. Gagandeep Singh. Er, HarpreetSingh, MadhuBahl.Er , "Securing Data Storage on Public Cloud by Encryption Based 2-Way Authentication", International Journal of Emerging Research in Management &Technology. ISSN: 2278-

9359 Volume-3, Issue-7, Chandigarh Engineering College, Landran, India, July -2014.

[6]. HeeDongYang[3],KangchanLee[1],Seungyun Lee[2],"Towardson Cloud Computing Standardization",[1]ETRI, [2]ETRI, [3]Ewha Womans University, International Journal of Multimedia and Ubiquitous Engineering Vol.9, No.2,pp.169-176, 2014.

[7]. Vidya.S[1,] Vani.K[2] Kavin Priya.D[3],"Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing", ISSN: 2278-0181, Vol. 1 Issue 10, December-2012.

[8]. Murali N.S. [*1], Dr.D.Thilagavathy[2], PGScholar, HOD, Department of CSE, "Authenticated Sharing of Personal Health Records in Cloud" IJERST International Journal Of Engineering Sciences & Research Technology Adhiyamaan College of Engineering, Hosur, India ISSN: 2277-9655 Impact Factor: 1.852, January 2014.

[9]. Ying Luo, "Efficient Anonymous Biometric Matching in Privacy-Aware Environments" University of Kentucky, 2014.