ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 7, pp. 18259-18263, July, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

SECURE TWO-TIER USER AUTHENTICATION MECHANISM FOR IOT ENABLED SMART HEALTHCARE SYSTEM

Shantha Mary Joshitta R* and Arockiam L

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

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0807.0478

ARTICLE INFO

Article History:

Received 16th April, 2017
Received in revised form 25th May, 2017
Accepted 23rd June, 2017
Published online 28th July, 2017

Key Words:

User_Auth; IoT; Smart Healthcare System; User Authentication Mechanism; Security

ABSTRACT

Internet of Things (IoT) is a paradigm that links real world physical objects with the virtual world providing any time and any where connectivity with one another over the internet. Integration of this technology with smart devices in healthcare domain will cause great impact on saving life. Now-a-days, the healthcare experts are started using the benefits of this technology in their field, thus generating a noteworthy improvement in healthcare communication and sharing of medical information. But the secure communication and sharing of medical information brings many issues in security and leads to privacy violation. Thus, this paper introduces a two-tier authentication mechanism for authenticating the users of the medical information. It checks the identity and legitimacy of the users using random image patterns and secret code provided by the authentication server.

INTRODUCTION

Due to the rapid advancement of new-fangled technologies of the twenty first century, connecting anything with anybody over internet is made possible and easier. Internet of Things (IoT) is one among such new technologies which improves sharing of information with others over the internet. It made everything around us to be smart using data-gathering sensors and machine-to-machine communication. This technology saves many lives when it is integrated with healthcare sector but brings many threats to the security of the personal information and privacy of the people. The types of medical information collected, the place of storage of such collected information and the users of the stored medical information are the questions of the hour and not yet answered clearly.

In this situation, authenticating remote users of the healthcare system plays a vital role in IoT enabled smart healthcare system. It has to confirm the identity of the users but also has to prove the legitimacy of the users over the internet irrespective of the users' place and the device they use. To resolve this issue, this paper proposes a two-tier mechanism for authenticating users of a medical system in an IoT enabled healthcare system. Random image patterns are used to identify the users and a secret code is used to prove the legitimacy of the users. This two-tier mechanism improves the security of the medical users and resilient to many attacks.

The organization of the paper is as follows. In Section 2 the reviews of previous works have been done. Sections 3 and 4 brief the motivation and design goals respectively. Section 5 details the proposed two-tier mechanism followed by conclusion in Section 6. References are listed at the end of the paper.

RELATED WORKS

Kameswara Rao *et al* (2016) presented a shoulder-surfing resistant pair based graphical password scheme to authenticate a user. Key aspects of the proposed scheme were discussed and security analysis of the method was evaluated. User password was processed as pass-characters one pair at a time until the last pass-character forms the first element in the pair. The authors proposed to facilitate the scheme with touch screens and planned to extend it using three color password characters (red, green, and blue) thereby increasing the password space by 282 characters.

Anto Kumar *et al* (2015) designed a new methodology called CaRP (Captcha as gRaphical Password) based on hard AI problems. CaRP was both captcha and graphical password scheme and overcame diverse attacks such as online guessing

Corresponding author:* **Shantha Mary Joshitta R
Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India

attacks, shoulder surfing attacks and rely attacks. CaRP addressed the image hotspot problem in graphical password systems such as pass points. CaRP also offered security and usability and thus improved online security.

Ashraf Aboshosha *et al* (2015) proposed a onetime password (OTP) based authentication protocol over a multi-channels architecture. The proposed protocol employed the RC4-EA encryption method to encrypt the plain-OTP to cipher-OTP. The Quick Response (QR) code was used as a data container to hide the cipher-OTP. The protocol was integrated in a web based application to communicate with the remote user over a multi-channels authentication scheme. It offered high security to prevent the OTP from eavesdropping attack. By integrating Web-based application and mobile-based technology, the proposed protocol overcame many attacks such as replay attack, man-in-the-middle (MITM) attack, DoS attack, real-time phishing (RTP) and other malware attacks.

Masafumi Kosugi *et al* (2016) evaluated the image-based user authentication method for touch screen devices proposed by Takahashi and Uchida. Though the proposed authentication method of Takahashi and Uchida was resistant to smudge attacks, but the security strength was low. The authors proposed an image-based user authentication method called SWIPASS for touch screen devices. The security strength was improved without any change in either the resistance to smudge attacks or the users' burden of memorizing.

Biswas Gurung *et al* (2015) proposed a hybrid-based authentication scheme termed as Enhanced Virtual Password Authentication (EVPA). It was resistant to the shoulder surfing attacks. The proposed method used a system generated random value. Mathematical functional value was obtained by secret mathematical operation against the pre-selected secret number. Several experiments were conducted and proved its resilience to password attacks and usable for day-to-day purposes.

Cecil Donal *et al* (2016) introduced a Pattern Based User Authentication (PBUA) mechanism to identify and authenticate the users in MobiCloud environment. The authentication process was divided into identification and authentication phases. Dynamic patterns were generated using random mathematical function and the experimental results proved that the proposed PBUA was resistant against shoulder surfing attack. The time taken for pattern matching was very less and the complexity of the algorithm was also reduced drastically and the efficiency was improved.

Chien-Cheng Lin *et al* (2015) adopted histogram features from smart phone sensors to build authentication models. The authors adopted touch screen and orientation sensor to evaluate the feasibility of the system. Sixteen touch-based features and thirty-three orientation-based features were used to construct the two authentication models. The results showed that the histogram features of the adopted two sensors were feasible for authentication purpose. Ching-Nung Yang *et al* (2016) developed a visual cryptography scheme (VCS) for authenticating smart phones . The proposed method dealt with gray-scale images and color images that could enhance the image quality of VCS. The proposed authentication scheme avoided the inconvenience of using password everywhere, and also resisted attacks from hackers and the man-in-middle attack.

Hsueh-Fan Lee *et al* (2015) proposed a skeleton and gesture based user authentication system using depth cameras. The system captured a user's skeleton and gesture information when a new user registered and store it into the database. When authenticating a user, the proposed system captured the user's skeleton and gesture information and compared it with the already stored data. Experimental results showed that the combined use of skeleton and behavioral information improved the accuracy of user authentication.

Patrick Lacharme *et al* (2016) proposed a new protocol combining protected biometric data and a classical synchronous one time password. It enhanced the security of user authentication while preserving usability and privacy. Behavioral biometrics were used to provide a fast and a usable solution for users. It proposed the generalization of the synchronous one time passwords by adding a biometric feature which is protected by a biometric template protection scheme. Bio-hashing algorithm was used in the protocol. Experiments were carried out on a homemade benchmark dataset.

MOTIVATION

There are six different stakeholders in an IoT enabled smart healthcare environment. They are doctors who medicate a patient, nurses who are in-charge of the patient, and relatives to whom the healthcare information of the patients can be discussed, the other medical stakeholders such as medical researchers, medical insurance providers and drug designers. The first three come under the category of Privileged Users and the remaining can be called as Ordinary Users. The Privileged Users can take immediate action to the medical information which they received or monitored. But the later one can use the medical data for some research oriented purposes and should not use them for business purposes. These users will not be provided the personal information of the patient for privacy purposes. These users will use their laptops, desktops, tablets or mobile phones to access or receive medical information of a particular patient. Moreover, the chances for security attacks such as shoulder surfing, brute force and online password guessing attacks are high.

In such a situation, the proposed user authentication mechanism should authenticate the user irrespective of the device they use and must provide higher level of security during the communication channel between the cloud storage and the medical users.

DESIGN GOALS

The aim of this paper is to propose a user authentication mechanism for accessing medical data from the dedicated central cloud server in an IoT enabled smart healthcare system. Therefore, the following goals should be guaranteed in the proposed authentication of the user. The security requirements include:

1. Secure user authentication and key agreement
2. Resistance to various attacks.

To obtain the goal (i), all the user must be authenticated irrespective of the system they used by the Authentication Server. After successful authentication, the secure communication channel should be established between the user devices and the authentication server.

For goal (ii), user devices should be resilient to the security attacks such as shoulder surfing, brute force and online password guessing attacks.

THE PROPOSED MECHANISM

There are six major phases namely, Registration, Login, Authentication, Mail-address change, Mobile number change and Password change in the authentication process of the proposed mechanism. These phases will be explained in the following sessions. The framework of the proposed authentication mechanism is presented in Figure 1.

Figure 1 The Proposed User_Auth Mechanism

The notations used in the proposed mechanism are depicted in Table 1.

Table 1 Notations used in the User_Auth mechanism

Notation	Explanation
U_i	User of the IoT enabled Smart Healthcare System
AS_i	Authentication Server
MS_i	Medical Server
CID_i	Citizen Unique Identification Number
$MCID_i$	Modified CID computed for requesting registration
PW_i	Password selected by $User_i$
U_Data_i	User Personal data used for registration
h(.)	Modified Neeva - One way hash function (Khushboo Bussi *et al*, 2016)
UY_i	Intermediate variable in User Registration Phase
UX_i	Intermediate variable in User Registration Phase
E[.]	Simeck lightweight block cipher (Gangqiang Yang *et al*, 2015)
||	Concatenation Operation
SK_i	Session Key for U_i

Registration Phase

The registration process collects the details of the user who are using the medical data from the medical server which resides in the cloud storage. It is a one-time process and normally carried out by the Authentication Server (AS). The user selects a username and password for him and provides his mobile number and email address during the registration process. The authentication server creates a user id (UID) for him and stores it for further references. The inputs used in the mechanism are explained below:

1. Citizen Identification Number (CID): It is a proposed unique identification number for every human on the global. It can be Aadhaar number in India, Social Status Number (SSN) in USA and National Identification Number (NIN) in many other African countries.
2. Password (PW): Password is selected by the user according to his wish but its length should be more than 8 characters. A numeric and a special character should present in the password.
3. Mobile number (Mble_no): It is a 10 digit mobile number.
4. E-Mail address (Mail_id): The e-mail id of the user.

The processes involved in the registration phase are given in Figure 2.

Figure 2 User Registration Phase

The steps involved in registration phase are explained below.

Step 1. User U_i enters his / her CID_i , PW_i , $Mail\_id_i$ and $Mble\_no_i$

Step 2. User computes $MCID_i = E_{AS}[CID_i \,||\, PW_i]$ and $U\_Data_i = E_{AS}[Mble\_no_i \,||\, Mail\_id_i]$

Step 3. U_i sends $MCID_i$ and U_Data_i to the AS for registration

Step 4. After receiving the message from U_i, AS computes $UX_i = D_{AS}[E_{AS}[MCID_i]]$, $UY_i = D_{AS}[E_{AS}[U\_Data_i]]$

Step 5. AS computes CID_i=substring $(UX_i,0,96)$ and $Mble\_no_i$=substring $(UY_i,0,10)$

Step 6. AS computes user code UID. $UID_i = h(CID_i \,||\, Mble\_no_i)$

Step 7. AS displays random image pattern to the user

Step 8. User selects random image patterns of his choice

Step 9. AS sends CID_i, PW_i, $Mail\_id_i$, $Mble\_no_i$ and UID_i to the User_Reg_Tab and Pattern selected by the user in User_Pattern_Tab

Step 10. AS sends ACK_i to U_i.

The User_Reg_Tab and the User_Pattern_Tab are presented in Table 2 and Table 3 respectively.

Table 2 User_Reg_Tab

CID_1	PW_1	$Mail\_id_1$	$Mble\_no_1$	UID_1
CID_2	PW_2	$Mail\_id_2$	$Mble\_no_2$	UID_2
CID_3	PW_3	$Mail\_id_3$	$Mble\_no_3$	UID_3
..	..	..	..	..
..	..	..	..	..
CID_n	PW_n	$Mail\_id_n$	$Mble\_no_n$	UID_n

Table 3 User_Pattern_Tab

UID_1	UIP_{11}	UIP_{12}	UIP_{13}	..	..	UIP_{1n}
UID_2	UIP_{21}	UIP_{22}	UIP_{23}	..	..	UIP_{2n}
UID_3	UIP_{31}	UIP_{32}	UIP_{33}	..	..	UIP_{3n}
..	..	..	..	..	..	..
..	..	..	..	..	..	..
UID_n	UIP_{n1}	UIP_{n2}	UIP_{n3}	..	..	UIP_{nn}

The flow diagram of the registration process is presented in figure 3.

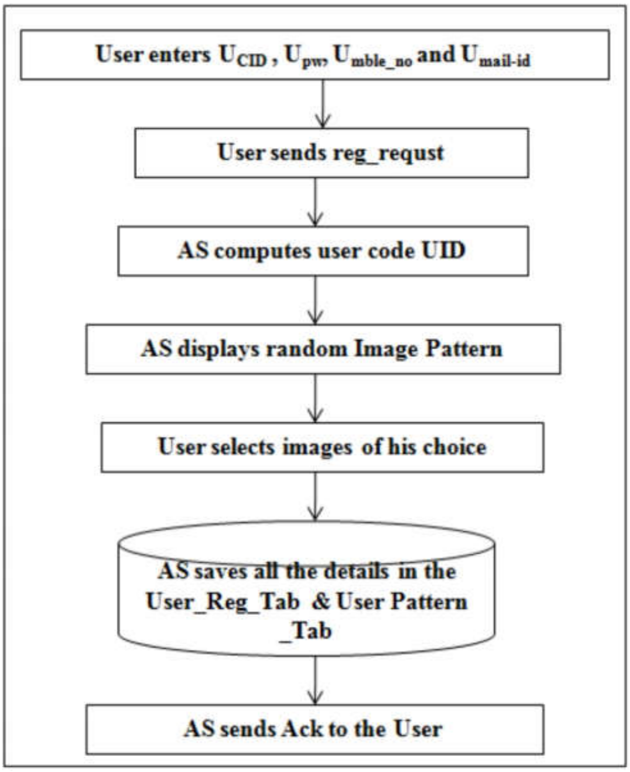

Figure 3 User Registration Process

Login and Authentication Phase

Before authentication starts, the users have to login for checking their legitimacy. If the verification holds success, it proceeds further to the authentication phase by providing two-tier security checks. First, the Authentication server displays a list of random patterns to the user among which the patterns he has selected during the registration phase is available. After the successful completion of this check, the AS sends a part of the secret code it generated for the user to his mobile number which is registered during registration. If it holds success, it provides the session key SK for accessing the medical data of the patient. Otherwise, it forwards the login request to the registration phase and an authentication failed message is sent to the User.

Secret Code: it is nothing but a 12 digit code having two parts, Server part and User part. It is generated to verify the legitimacy of the user. The server part has 8 digits and the user part is of 4 digits. The user part of the secret code will be sent to the user as a verification message. When the user inputs his part user code within a time interval, the final verification of the secret code will be carried out by the AS and if verification holds, the session key SK for accessing the medical data of the patient will be sent to the user.

The login and authentication steps are explained below.

Step 1. User U_i enters his / her CID_i and PWi and computes $MCID_i = E_{AS}[CID_i \| PW_i]$
Step 2. U_i sends $MCID_i$ to the AS as login request
Step 3. After receiving the message from U_i, AS computes $UX_i = D_{AS}[E_{AS}[MCID_i]]$, CID_i=substring $(UX_i, 0, 96)$
Step 4. AS validates whether CID_i is equal to the stored CID_i in the User_Reg_Tab. If validation occurs, AS collects the Mble_noi from the User_Reg_Tab and computes user code UID. $UID_i = h(CID_i \| Mble\_no_i)$
Step 5. AS displays random image pattern to the user
Step 6. User selects random image patterns which of them are selected by him in the registration phase
Step 7. AS validates these image patterns with the User_Pattern_Tab. If match occurs, AS computes secret code for the user
Step 8. AS sends the user part of the secret code to the user Mble_no which is active for 30 seconds.
Step 9. User enters his part secret code
Step 10. AS validates the secret code and sends the session key SK_i as a token to access data from the cloud medical server.
Step 11. If validation does not hold, the AS forwards the login request to the Registration Phase.

The processes involved are depicted in Figure 4.

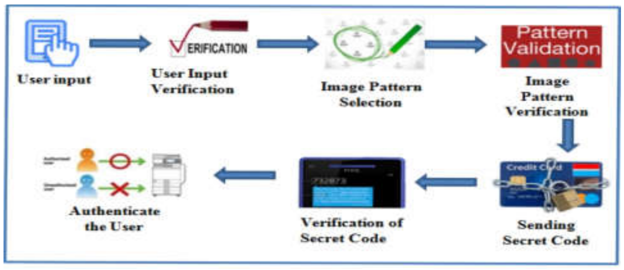

Figure 4 User Login and Authentication Process

The Login and Authentication phase of the proposed Mechanism is presented in Figure 5.

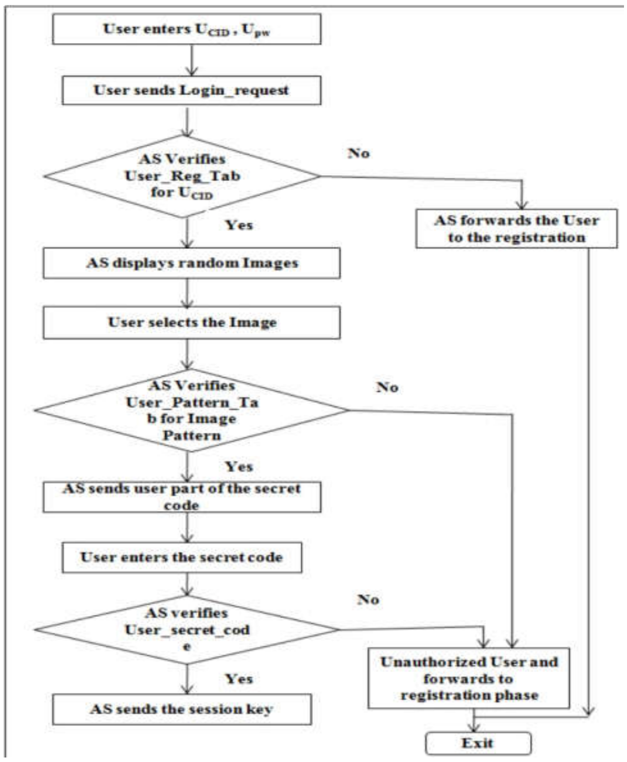

Figure 5 User Login and Authentication Processes

Mail-address change Phase: Because of the practical problem, any user may need to change his mail-address in course of time.

Mobile number change Phase: There are chances for losing his mobile or in-activation of user mobile number. So, the user may need to change his mobile number which he registered during the registration phase.

Password change Phase: The password of the user can be changed using the following procedure.

The steps involved in these phases are given below.

Step 1. User U_i enters his / her CID_i and PW_i and computes $MCID_i= E_{AS}[CID_i \| PW_i]$

Step 2. U_i sends $MCID_i$ to the AS as login request

Step 3. After receiving the message from U_i, AS computes $UX_i=D_{AS}[E_{AS}[MCID_i]]$, CID_i=substring (UX_i,0,96)

Step 4. AS validates whether CID_i is equal to the stored CID_i in the User_Reg_Tab. If validation occurs, AS collects the type of change the user opt for. (Mail_id, Mble_no and PW)

Step 5. If change type ='Mail_id' then

AS collect the mail_id_old and the mail_id_new from the User

AS verifies the mail_id of the CID in the User_Reg_Tab .if verification holds, it ask for a confirmation from the User

If the user confirm to change the mail_id, it replaces the Mail_id_old by the Mail_id_New

AS sends intimation to the user Mble_no as a confirmation message

Step 6. Else if change type ='Mble_no' then

AS collect the Mble_no_old and the Mble_no_new from the User

AS verifies the Mble_no of the CID in the User_Reg_Tab .if verification holds, it ask for a confirmation from the User

If the user confirm to change the Mble_no, it replaces the Mble_no_old by the Mble_no_New

AS sends intimation to the user Mail_id as a confirmation message

Step 7. Else

AS collect the PW_old and the PW_new from the User

AS verifies the PW of the CID in the User_Reg_Tab .if verification holds, it ask for a confirmation from the User

If the user confirm to change the PW, it replaces the PW_old by the PW_New

AS sends intimation to the user Mail_id as a confirmation message

Step 8. End if

CONCLUSION

This paper presents a two-tier user authentication mechanism, User_Auth for authenticating the remote users of the IoT enabled smart healthcare system. The proposed work ensures the authenticity of the remote user of the system. Two different techniques are used to authenticate the user in the proposed mechanism. It uses random image patterns to identify the users of the system and provide a secret code to prove their legitimacy. After proving the users' identity and legitimacy, it sends the session key SK for accessing the medical information of a particular user. Thus, the security of the medical data in the central cloud server is managed using this two-tier mechanism.

References

M. Kameswara Rao, Ch. Vidya Pravallika, G. Priyanka and Mani Kumar. 2016. A Shoulder-Surfing Resistant Graphical Password Authentication Scheme. Innovations in Computer Science and Engineering, Advances in Intelligent Systems and Computing, Springer, Vol. 413, pp. 105 - 111.

R.P. Anto Kumar, R. Sivakumar and S.S. Aalin Grace. 2015. A New Implementation of Graphical Password Scheme for Captcha Based Security System. *Middle-East Journal of Scientific Research*, Vol. 23, No.7, pp. 1353-1357.

Ashraf Aboshosha, Kamal A. ElDahshan, Eman K. Elsayed and Ahmed A. Elngar. 2015. Multi-Channel User Authentication Protocol based on Encrypted Hidden OTP. *International Journal of Computer Science and Information Security*, Vol. 13, No. 6, pp. 14-19

Masafumi Kosugi, Tsuyoshi Suzuki, Osamu Uchida and Hiroaki Kikuchi. 2016. SWIPASS: Image-Based User Authentication for Touch Screen Devices. *Journal of Information Processing*, Vol. 24, No. 2, pp. 227-236.

Biswas Gurung, P.W.C. Prasad, Abeer Alsadoon, Amr Elchouemi. 2015. Enhanced Virtual Password Authentication Scheme Resistant to Shoulder Surfing. Proc of the IEEE Second International Conference on Soft Computing and Machine Intelligence, pp.134-139.

Cecil Donald A. and L. Arockiam. 2016. PBUA: A Dynamic User Authentication Mechanism for Secure MobiCloud Environment. *Indian Journal of Science and Technology*, Vol. 9, No. 35, pp. 1-6,

Chien-Cheng Lin, Chin-Chun Chang , Deron Liang. 2015. An Approach for Authenticating Smartphone Users based on Histogram Features. Proc. of the IEEE International Conference on Software Quality, Reliability and Security, pp. 125- 130.

Ching-Nung Yang, Jung-Kuo Liao, Fu-Heng Wu and Yasushi Yamaguchi. 2016. Developing Visual Cryptography for Authentication on Smart phones. Industrial IoT 2016, LNICST 173, pp. 189-200.

Hsueh-Fan Lee, Yi-Shu Lu, Jiun-Long Huang. 2015. A Skeleton and Gesture Based User Authentication System. Proc of the 8th International Conference on Ubi-Media Computing (UMEDIA), pp. 254-258.

Patrick Lacharme and Christophe Rosenberger. 2016. Synchronous One Time Biometrics With Pattern Based Authentication. Proc of the International Conference on Availability, Reliability and Security (ARES), pp. 1-7.

Khushboo Bussi, Dhananjoy Dey, Manoj Kumar and B.K. Dass. 2016. Neeva: A Lightweight Hash Function. Cryptology ePrint Archive, Report 2016/042, pp.1-14.

Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang Gong. 2015. The Simeck Family of Lightweight Block Ciphers. IACR, Springer-Verlag, June 2015.

****