International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-7, Issue-5, 2020 Regular Edition E-ISSN: 2349-7084

Secure Authentication Mechanism in IoT Based Healthcare System

Anita Chaudhari[1], Janice Rodrigues[2], Aparna Vattamparambil[3], Revati Warang[4], Vidya More[5]

Information Technology, St. John College of Engineering and Management, Mumbai University, India
E-mail: anitac@sjcem.edu.in , jan99.icer@gmail.com , aparnaraju218@gmail.com , revatiwarang@gmail.com , vidyamore1998@gmail.com
**Corresponding Author: anitac@sjcem.edu.in*
Available online at https://www.ijcert.org

Received: 24/05/2020, Revised: 26/05/2020, Accepted: 07/06/2020, Published: 12/06/2020

Abstract: In today's world, security is the most significant concern. We produce tons of data that must be unbroken secure. Be it our data or data associated with a transnational company. The data can be protected with the usage of authentication and authorization. Authentication and authorization help to verify and validate a user's identification. Applications in today's society are swaying towards IoT concepts as this delivers them agility, competency, conventionality, and future-proof. However, this winds up into a higher security risk. The projected system proposes a multi-factor authentication methodology or, in simple terms, presents a 3-way authentication. This constitutes the well-known authentication levels that are the password and OTP but mainly focuses on the third step signifying the most protected method of authentication that's the challenge-response pair mechanism. The generated challenge is exclusive to each user, and therefore, the gadget.

Keywords: Information security; Authentication; Healthcare; IoT; OTP; CRP Mechanism.

---

1. Introduction

Today, security matters are surging in all sectors such as banks, governmental applications, healthcare industry, military organizations, educational institutions, etc. Government organizations are establishing standards, passing laws, and are demanding organizations and agencies to comply with these standards with non-compliance being met with wide-ranging outcomes [1]. In wireless networks, reliable wireless communication over vulnerable communication channels is a huge challenge. Therefore, user authentication and secret key distribution have become a vital security aid for wireless communication networks [2].

Presently, three globally acknowledged philosophy is used for digital identification: what we know (i.e., password), what we have (i.e., Tokens and cards) and universal identity (i.e., Biometric characteristics) [3]. Numerous challenges have occurred, chiefly related to connectivity, power consumption, and security. Indeed, security is necessary for IoT devices: being an abundance of distributed nodes, the surface that is exposed to attacks is exceptionally vast and hard to protect [15]. Health is one of the various challenges for humanity. Internet of things (IoT) is the new criterion where an object is equipped with features, senses, and processes. High security against the current perils with scarcer computational expenses is an essential requirement in remote health care monitoring through the WMSN [13]. These objects communicate with each other through the internet. Nowadays, the medical field is evolving swiftly due to the alterations in the lifestyle of the people and their food habits. The primary challenge is to provide round-the-clock healthcare assistance to those patients who require it via wearable wireless medical devices [19].

Also, the medical reports & records are a primary concern. These records require to be kept protected to guard the privacy of the patients. Medical records hold sensitive and personal data that should not fall in the hands of an unauthorized person. Only sanctioned people should be able to view the medical report.

 https://doi.org/10.22362/ijcert/2020/v7/i05/v7i0503

Hospitals have begun using IoT devices. Internet of Medical Things has been allowed the use of medical machines and applications to gather data and knowledge, over a wireless arrangement, with the healthcare IT operation. The accelerated development of IoMT, however, has meant that the security and privacy of these IoMT-based healthcare systems often have experienced insufficient attention. The outcomes of poor security in IoMT healthcare systems can be, for instance, compromised patients 'privacy due to eavesdropping, and delayed detection of life-threatening episodes due to the disruption of normal operations of IoMT devices caused by Denial of Service (DoS) attacks [20].

With the growing rate of IoT devices, various types of attacks have increased. Thus authentication and authorization are necessitated when it comes to protecting the Internet of Medical Things. Multi-factor authentication is a methodology that utilizes a couple of more authentication methods, simultaneously including the password method. Thus we propose a secured healthcare system that assures to efficiently operate and maintain patient health data in an effective manner.

2. Related Work

By definition, authentication is the use of one or more mechanisms to verify that you are who you claim to be. Once the identification of the human or machine is approved, access is granted [1]. Password-based authentication is a vulnerable solution and is no longer sufficient. The user chooses a static password, which is straightforward to guess and remember pertinent information, or general for all authentication processes. This simplicity makes inadequate authentication schemes; as so far, static passwords are known as the most uncomplicated target for attackers [3].

The medical department is developing swiftly and consequently is the medical records. These records need to be secure to provide privacy to patients. Medical records contain sensitive data and should not fall in the hands of unauthorized people. But, the progressing technologies such as cloud computing and wireless networks make this data vulnerable to fall prey to cyber-attacks. To avert a replay attack, a CRP should not be used more than once. However, this requires a broad set of CRPs to authenticate a device a notable number of times before the CRP set is exhausted [14]. The Healthcare industry has perpetually been on the lead in the adoption and utilization of knowledge and intelligence technologies for useful healthcare guidance and practice. Hospitals have started using IoT devices. Internet of Medical Things (IoMT) has expanded to collect data and interact, beyond a wireless arrangement, with the healthcare IT operations.

Amidst the expanding rate of IoT devices, the number of attacks has grown. Thus, authentication is a must when it comes to protecting these IoMT devices. Our method is determined to be an answer to manage the safety of the healthcare enterprise. In the prevailing systems, authentication is done based upon token, biometrics, OTP, etc. Token-based authentication is a defense technique that validates the users who strive to log in to a server or another reliable system utilizing a token granted by the server. Biometric authentication is a security process that relies on unique biological characters like iris, fingerprint, voice, keystroke, odor, etc., of an individual to verify that he/she is someone that they claim to be. OTP is further reliable than a static password, particularly a user-created password. OTPs may reinstate authentication login data or may be practiced in an attachment to it, to append an extra tier of safety. OTP tokens frequently present a number that is uncommon to both the user and the machine. The utmost of the authentication tools necessitates the usage of Bluetooth and WLAN. They are not compatible with changes in the environment.

There is a drawback that others can impersonate these systems (attackers). There might be difficulty in identifying the user if his/her appearance changes. Issues such as reliability and low-security problems, low computation, storage, and communication overhead also exist. If the authentication is based on passwords, there is a huge possibility that the password can be forgotten. Passwords can be easily hacked by either guesswork or using any password cracking Algorithm. If the authentication is based on biometrics, there is a tendency for biometrics to be mimicked. Keeping in mind all these vulnerabilities from the existing system, we have proposed an additional level of security to overcome these vulnerabilities.

3. Methodology

Our system provides authentication with three levels of security. Firstly, the input is taken as a patient parameter like pulse rate, ECG, temperature, etc. This parameter is transferred as an analog signal to the ADC module, which converts it into a digital signal. This process will take place within the raspberry pi. The information of the patient parameter is saved in the database. Furthermore, we will go through the working of the 3-way authentication mechanism.

 https://doi.org/10.22362/ijcert/2020/v7/i05/v7i0501

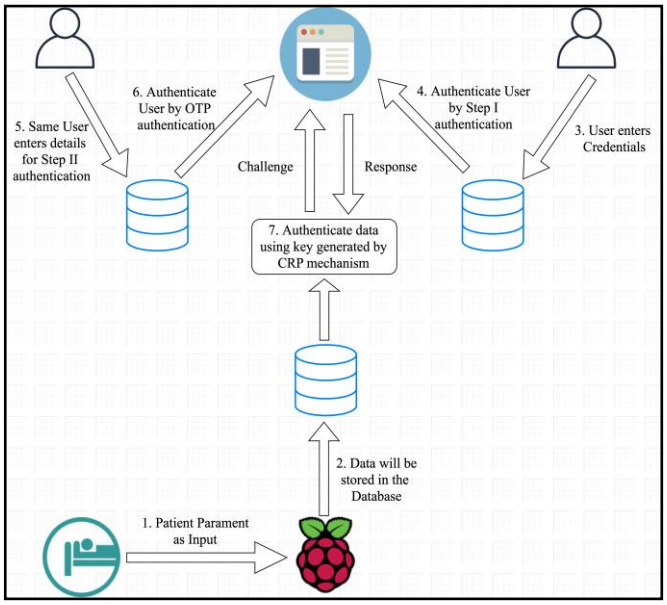

Figure 1. Methodology

Step I: The user opens the webpage on a browser using a mobile phone or a personal computer. He/She logs in to the website by entering their credentials. Their credentials are verified in the database. When the credentials entered match the one in the database, the user is validated by Step I authentication.

Step II: Once the user is approved, by the Step I authentication, he/she is taken to the next page for Step II authentication. When the user initially registers to the website, he/she provides a valid email address. This email address is used for the Step II authentication. An OTP will be sent to this email address to verify the user. To secure the operation, the provided OTP must be arduous to presume, reclaim, or pursue by hackers. Thus, it is notably crucial to utilize a reliable OTP generating algorithm.

Step III: Step I and Step II authentication are the primary authentication mechanisms that most of the systems employ. To strengthen the security and defend the system more beneficially, we propose Step III authentication, i.e., the Challenge-Response Pair mechanism. To view patient details, Step III authentication is executed. A challenge is assigned to the user, and the user proffers in response to this challenge. The method known to solve this challenge is only apprehended to the user because, during registration, he/she attained this method. The user is authenticated by verifying the key generated by the CRP mechanism.

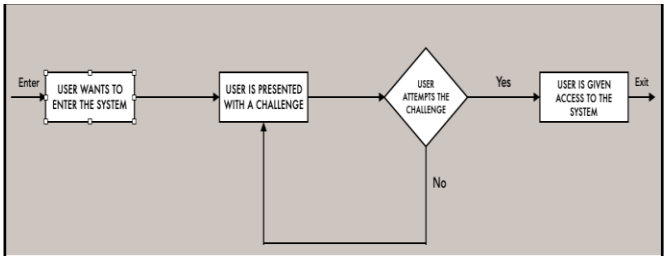

Figure 2. Working of CRP

Working of CRP Mechanism: When the user needs to view the details of the patient, he/ she will be given a challenge. The approach to solve this challenge is only known to the user. The user has to solve the challenge to be verified by the system. Once the user attempts the challenge, he/she is permitted to access the details of the patient.

During user registration, the user keeps a password for Step I authentication and a challenge along with a response for Step III authentication. This user passwords and responses are saved in separate databases. The user passwords are encrypted using an inbuilt MD5 algorithm. The RC4 Algorithm first encrypts the responses, then by MD5 and finally by Salt SHA 512 algorithm - which is considered the most secure encryption algorithm. Since the passwords and the responses are encrypted and then saved in the databases, the system entirely grows even more secure. Salt SHA 512 algorithm is complex to decrypt, thus, making it one of the most effective and most protected encryption algorithms.

Proposed Algorithm: **Encryption and Decryption using RC4 Algorithm:- 1) Key-Scheduling Algorithm** - *Initialization:*

- Create an Initial Vector P[0] to P[255]
- Create a temporary vector ' R ' If len(key) == 256 bytes then the key is specified to R vector else the key recurs multiple times, needed to fill R

-For initial permutation of P, Let, d=0

```
 for c=0 to 255 do
 {
 d = (d + P[c] + R[c] ) mod 256;
swap( P[c], P[d] );
}
```

So, here we perceive a distinct initial vector P.

***2*) Pseudo-Random Generation Algorithm –**

- Once this vector P is initialized, the input key will not be utilized.
- Here, from new initial vector P, for each P[c] swap it with P[d]

```
Let c, d = 0 while(True)
c = ( c + 1 ) mod 256;
d = ( d + P[c] ) mod 256;
```


swap(P[c], P[d]);
r = (P[c] + P[d]) mod 256;
a = P[r]

3) Encrypt and Decrypt using XOR( ) - - Encryption and decryption is done using XOR( ).

Explanation:

Firstly a temporary vector' P' will be created of some specific size. For example, P = [1 2 3 4]. When the user enters the password, it will be stored in the database as a key. Temporary' R' vector will be created of a size equal to the' P' vector, and key values will be entered in the' R' vector. Initial permutation of S is performed until a new initial vector' P' is obtained. The new initial vector' P' will be used as a key. By the use of this value, furthermore swapping function will be implied. After the swapping function is implemented, we will get a new key value. This key value will be encrypted using XOR(). It can be decrypted using the same.

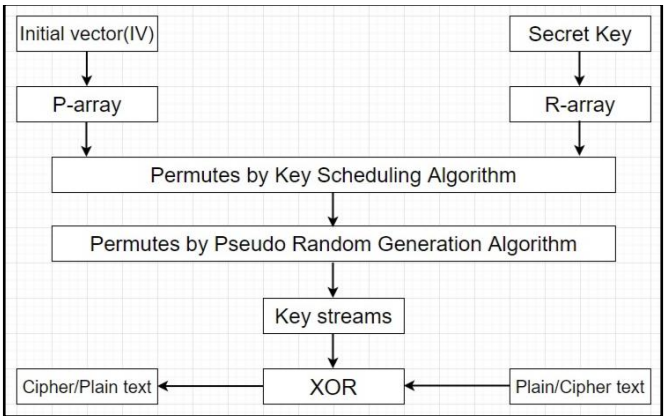

Figure 3. Encryption Flowchart

4. Results and Discussion

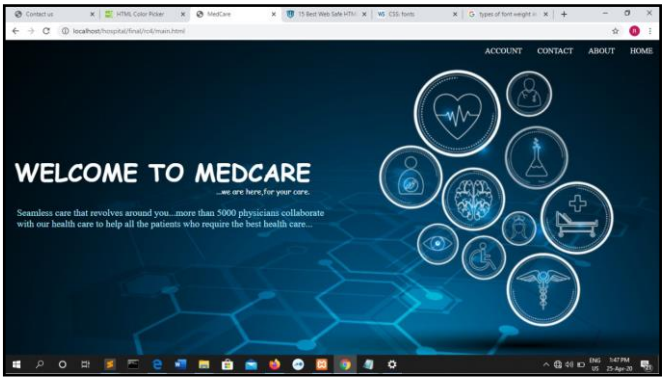

Figure 4. Web Portal for Healthcare System

Figure 4 shows the homepage of our website MedCare. This will be the first page the user will see when he/she visit our website. From this page, the user will get an impression of our website.

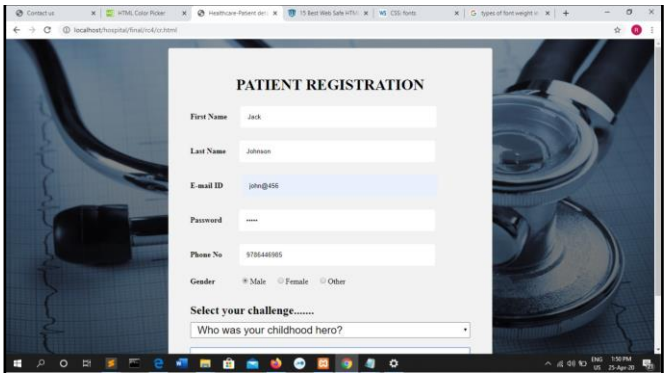

Figure 5. User Registration Form for New Users

Figure 5 shows the enrolment page of our website. If the user is new to the website, he/she has to register. The necessary details are to be filled by the user. The user also has to select a challenge that will be used for Step III authentication. Once the user has successfully registered on the website, he/she has to log in. This is Step I authentication consisting of the basic level of authentication, i.e., email id and password.

Figure 6. OTP generation

Here the user has to enter their registered email address. The OTP will be sent on this particular email address only. This is the Step II authentication. The OTP sent is unique to the user as well as the system. OTP will be received via the email address given by the user.

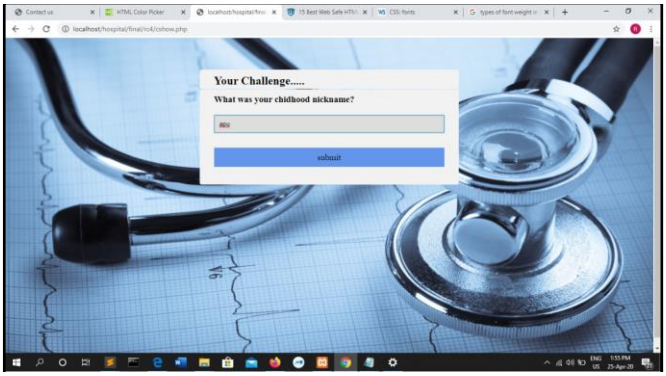

Figure 7. CRP Mechanism

This is the Step III authentication of our system. This is the final step of our authentication process. This level of authentication is used to view the patient details. Without the CRP mechanism, the user will not be able to view the patient details. The user needs to respond to the challenge, which was introduced during registration.

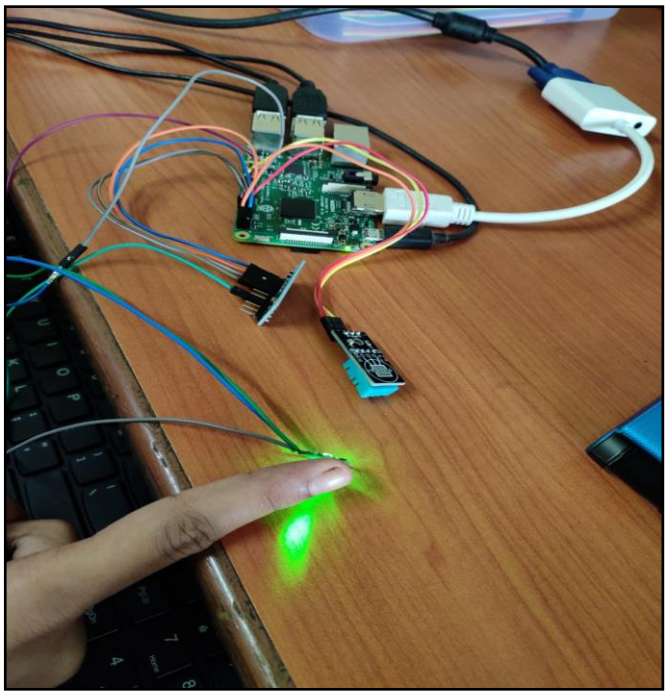

Figure 8. IoT devises Setup

The sensor takes the patient's input parameter and uploads it to the cloud so the doctor can be notified with the patient's details. It also stores the patient's information in the database. The readings are displayed continuously as long as the patient's finger is on the sensor. All the data recorded and stored by the sensor can be accessed through the website by patient and doctor after completing the authentication process anywhere and anytime.

5. Conclusion and Future Scope

We have momentarily agreed that security is undoubtedly the essential element in our society. We need to make sure that our data is protected in such a way that even if an attack takes place, the damage must be minimal. Thus, we have successfully analyzed the above literature papers on authentication. Our system secures the patient's medical information from the outside world. In our system, we employ the two most certain forms of authentication, along with the third most reliable method that is the CRP mechanism. We have been able to protect the patient's details with the use of the CRP mechanism. Only when the challenge is solved, the verified user is allowed to view the details, thus, providing security and privacy to the patient's details. Even the database administrator cannot view the data. So there's no chance of data breach from the admin side. We can explicitly denominate our system the most protected because we are encrypting the response thrice before storing it in the database. Using one of the strongest hashing algorithms in our system makes the system more protected. This system can be used in any field. We have decided on the medical department because of the evolution of technology in this department. Furthermore, many other sensors can be added. This system can be made more compatible and can be used on a large scale.

References

1. Two Factor Authentication Using Mobile Phones" by Fadi Aloul, Syed Zahidi, Wassim El-Hajj, IEEE, 2016.
2. "A Security-Enhanced Authentication and Key Distribution Protocol for Wireless Networks" by Chao Lv, Maode Ma, Hui Li and Jianfeng Ma, IEEE, 2010.
3. "Token Based Authentication using Mobile Phone" by Parekh Tanvi, Gawshinde Sonal, Sharma Mayank Kumar, IEEE, 2011.
4. "A survey on Biometric Based Authentication in cloud computing" by P. Padma and Dr. S. Srinivasan, IEEE, 2016.
5. "Password Security system with 2-way authentication" by Subhradeep Biswas and Sudipa Biswas, IEEE, 2017.
6. "Secure Authentication with Dynamic Password" by Zubayr Khalid, Pritam Paul, Soummyo Priyo Chattopadhyay, Anik Naha Biswas, IEEE, 2016.
7. "Overview of PUF - Based Hardware Security Solutions for Internet of Things" by Basel Halak, Mark Zwolinski and M. Syafiq Mispan, IEEE, 2016.
8. "Performance Evaluation of Cryptographic Ciphers on IoT Devices" by Kedar Deshpande and Praneet Singh.
9. "Secure Medical Data Transmission Model for IoT-based Healthcare Systems" by Mohamed Elhoseny, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Shihab A. Shawkat, Arunkumar N, Ahmed Farouk, IEEE, 2018.

 https://doi.org/10.22362/ijcert/2020/v7/i05/v7i0501

10. "A PHY-Aided Secure IoT Healthcare System With Collaboration of Social Networks" by Peng Hao and Xianbin Wang, IEEE, 2017.
11. "Device Authentication Mechanism for IoT Enabled Healthcare System" by Shantha Mary Joshitta. R and Arockiam L.
12. "Design of a secure medical data sharing system via an authorized mechanism" by Chin-Ling Chen, Jin-Xin Hu, Chun-Long Fan and Kun-hao Wang, IEEE, 2016.
13. "A Comprehensive Survey of Security Mechanisms in Healthcare Applications" by Mr. D. Stalin David and Dr. A. Jeyachandran.
14. "A Robust Physical Unclonable Function with Enhanced Challenge-Response Set" by Abhranil Maiti, Inyoung Kim, and Patrick Schaumont, IEEE, 2012.
15. "Authenticating IoT Devices with Physically Unclonable Functions Models" by Mario Barbareschi, Pierpaolo Bagnasco, Antonino Mazzeo, IEEE, 2015.
16. "Lightweight PUF-Based Authentication Protocol for IoT Devices" by Yildiran Yilmaz, Steve R. Gunn, Basel Halak, IEEE, 2018.
17. "E-Healthcare: Remote Monitoring, Privacy, and Security" by Olga Boric-Lubecke, Xiaomeng Gao, Ehsan Yavari, Mehran Baboli, Aditya Singh, and Victor M Lubecke, IEEE, 2014.
18. "System Level Design of a Secure Healthcare Smart Card System" by Merve Oksar and Berna Ors and Gokay Saldamli, IEEE, 2011.
19. "Monitoring Patients Via A Secure And Mobile Healthcare System" By Yonglin Ren, Richard Werner Nelem Pazzi, And Azzedine Boukerche, Ieee, 2010.
20. "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey" by YINGNAN SUN , FRANK P.-W. LO , AND BENNY LO, IEEE, 2019

