International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

# Continuous Authentication using Smart Health Monitoring System

**Pavithra D R, Supritha R**

***Abstract*: The main security issue in most of the computer is user identification and authentication. In traditional authentication schemes, the user is only validated during initial login which provides low security for the system. Hence continuous authentication has to be done to resolve the security issue. With increase in the number of smartphone users, continuous validation of the authenticated user is important. Continuous authentication mechanism can be made using two behavioral traits: app usage and touch based. There is a worldwide increase in the usage of apps that works on touchscreen, hence both can be used for authentication. Hence, the continuous authentication will be based on app usage and touch screen based which provide high security. In this paper, smart health monitoring system is used for continuous authentication. The data which is collected from wearable biomedical sensors for continuous health monitoring can also be used for continuous authentication. Although the biomedical signals are not highly discriminative a robust machine learning to obtain high accuracy levels is used. An android app is developed to gather data and send to cloud for data storage. The user is validated based on the decisions from the classifiers. The proposed work does not need any extra model for data collection as it uses the data gathered for health monitoring purpose, it can be used for low cost applications.***

***Index Terms*: Authentication, wearable biomedical sensors, machine learning, security.**

## I. INTRODUCTION

Authentication is the procedure or action of validating user identity. Since computers store important information, it should be protected from invaders [1]. Tradition user validation method is password inquiry at the initial login. The user is validated only when he enters the correct password. One-time authentication request the user to enter the password only at the initial login. Hence anyone can access the system resources if the user leaves the workstation without logging out properly. Hence there is need for the system to constantly supervise and validate the user after first login session [2]. Recently, wearable health care monitoring system have gained a lot of attention. The wearable health monitoring system have ability to change healthcare by providing low cost solutions. In Figure 1.1 shows a collective health care model [12].

**Manuscript published on 30 June 2019.**
***** Correspondence Author (s)
**Pavithra D R**, Department of Bachelor of Engineering in Electronics and Communication, Sri Jayachamarajendra College of Engineering, Mysuru (Karnataka), India.
**Supritha R,** Department of Bachelor of Engineering in Electronics and Communication, has received her Bachelor of Engineering in Electronics and Communication, Vidyavardhaka College of Engineering, Mysuru (Karnataka), India.



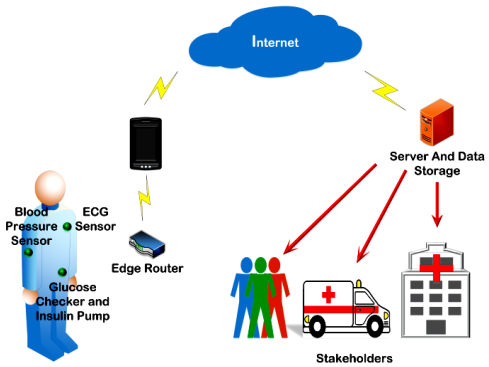



**Figure 1.1: Collective-Healthcare Model**

Since biomedical signals are collected for health monitoring, we propose a method where it can also be used for continuous authentication. The biomedical signals for continuous authentication is useful because of these three reasons.

1) Continuous authentication system does not require an extra model since they are collected for biomedical.
2) The information is collected with minimal user involvement.
3) The biomedical signals collected is accessible whenever the user is wearing WMSs.

Our objectives are as follows:

1) To design the architecture for continuous authentication system.
2) Sensitive data from sensors connected to user's body should be sent to the server through the user smartphone.
3) The received data from the sensors is to be stored on cloud so that it can be used anywhere and at any time for authentication.

## II. REALATED WORK

The significant advantage of continuous authentication is that user is validated for every fixed interval of time so that there is no leakage of important information to any unauthorized person. Various technologies already exist for continuous authentication including Face ID, iris and fingerprint in smartphones. The survey done for the various continuous authentication system suggests that the keystroke dynamics can replace already existing traditional authentication system [1].They are two types of biometrics i.e. Hard biometrics which include Face, Hand shape, Fingerprint, Iris and Soft biometrics refers to physical and behavioral traits such as Keystroke, Voice, Color of the clothing, Facial color etc. which are not unique but helpful for identification and verification of specific individuals [2],[3].

A single biometric is not sufficient for the continuous validation of the user as there might be some loss of information. Hence, to resolve the limitations multimodal biometrics is considered. The work includes Multimodal biometric traits like Sclera and Fingerprint for continuous user validation [4]. Continuous authentication using soft biometrics allows the user to login using face color and color of the clothing. The system is efficient as it does not change with the user's posture. Hence high security can be provided by using both hard and soft biometrics for continuous authentication schemes [5].Other biometric authentication framework include keystroke dynamics. Keystroke dynamics refers to the typing behavior of an individual. Since, it is unique it can be used for authentication process [6]. The proposed system was evaluated by conducting a field study by taking samples from 52 participants in 30 days [7]. Mouse dynamics validates the users based on their mouse operating peculiarity of an individual. This study extracts the mouse operating characteristics using pattern growth mining method for continuous authentication by using only one classifier. The work showed that mouse dynamics was significant enhancement for the traditional authentication systems [8]. An individual computer user has a unique behavioral hand movements while texting, this is named as "Typing behavior". Webcam was used to record video streams pointing towards the keyboard. Database of 63 unique static text and free text of multiple sessions was demonstrated. For one typing video, the typing behavior are segmented in each frame and an unique descriptor was used to extract based on the shape and position of hands [9]. To address the issues of security privacy, many researchers have proposed various continuous authentication schemes based on behavioral traits. The paper has done a survey on various continuous authentication schemes and compared the results based on different perspectives [10]. Although biometrics have their own set of drawbacks, it is still used because it is unchangeable. The proposed work uses biomedical signals generated from the human body for continuous authentication [11].

## III. PROPOSED METHODOLOGY

Internet of Things (IoT) contains enormous number of smart devices connected through internet for communicating with each other. IoT devices are used to collect data like temperature, blood pressure for smart health monitoring system. IoT based health monitoring system is used to collect the data using Arduino device. Figure 3.1 illustrates various biomedical signals connected to the Arduino device in continuous authentication system. Data gathered from the sensors are processed by Arduino microcontroller. All data are received through the serial input of HC-06 Bluetooth module. When the module receives data, it is sent out through the serial interface. This data is received by the Bluetooth of mobile. Through app installed in mobile the data is sent to cloud. The data is stored in SQL database and it is used in user authentication phase to take decision if the user is authenticated or not. The working of the proposed system is divided into two phases (i) enrollment phase in which mobile application is developed for the user in order to collect data from sensors and sent to cloud server and also user can read the data anywhere and at any time and (ii) user authentication phase in which decision is taken whether the user is authenticated or not based on the classifiers.

***1) Enrollment phase*** : In the enrollment phase, user has to login using unique id and password which will be provided during registration of the android app. The user can view their personal details and report anywhere and at any time. The data is collected from the sensors which is connected to the user body and sent to app developed through Bluetooth. The data is transmitted from mobile app to cloud server is stored in SQL database.

***2) User authentication phase*:** In this phase, the decision is made whether the user is authenticated or not based on the database stored in cloud server using classifiers. The user has to be authenticated at regular intervals in continuous authentication system. During authentication process, the smartphone will sent request to cloud server where user data is collected and stored. Therefore the system has no need to wait to gather the information as in the case of other authentication systems like keyboard or mouse. The information will be already gathered for health monitoring purpose. Figure 3.2 illustrates how user authentication is done.

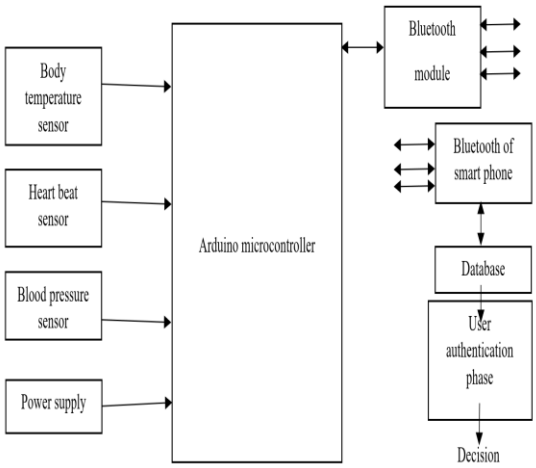



**Figure 3.1: Block diagram of Continuous authentication system using WMSs**

In a single verification attempt

1. The smartphone will be sent request to cloud server.
2. The dedicated classifier processes the information and outputs a binary decision.

The two well-known binary classification methods:

**1) *SVM***: A Support Vector Machine (SVM) is a discriminative classifier for dividing a plane in two parts by fixing a threshold value. The threshold values are fixed based on the normal range of the biomedical signals of an individual.

**2) *AdaBoost:*** Although SVM has been commonly used for continuous authentication systems, since the biomedical signals from the sensors are slightly discriminative which leads to weak classifier. We decided to include AdaBoost as well in order to build a highly reliable classifier by adding many weak classifiers.


*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication (BEIESP)*

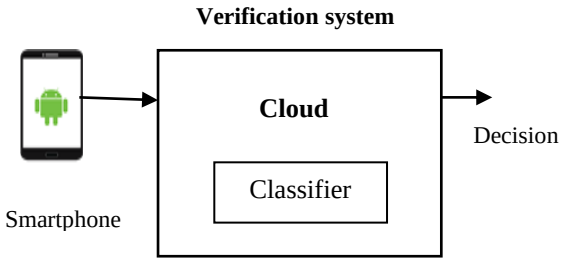



**Figure 3.2: User authentication phase**

Figure 3.3 illustrates the flowchart of the proposed system. The user will login in to android app using unique user id and password. Then the information are gathered from the wearable sensors and sent to mobile app. From app the data is sent to cloud where previous data of the user will be stored. The data is compared with the normal range and present received data. If it is in normal range then the person is authenticated otherwise message is sent to resend the data from the sensors again. There might be changes in the data of an authenticated user due to running or other actions. After 3 minutes the user condition will come to normal and again data is sent. Again it is compared with the normal range. If it is in the prescribed range then the user is authenticated otherwise the user is not authenticated message is sent. In many cases after 3 minutes the authenticated user might have health issues, hence the intruders may take advantage of this situation. The proposed provides high security by providing the condition that after 3 minutes also if the user is authenticated but the data is not in normal range then the message is given as not authenticated.

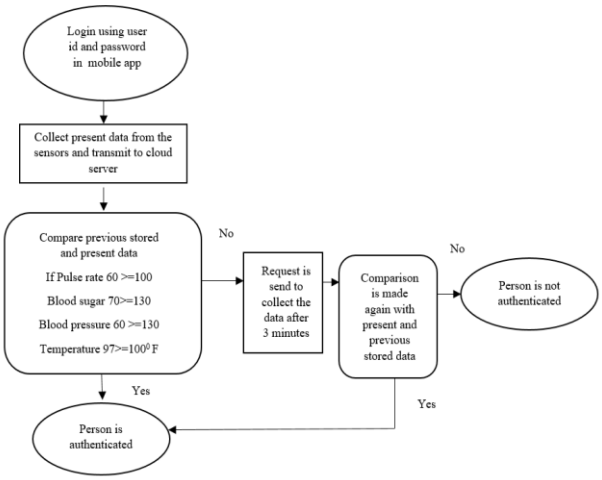



**Figure 3.3: Flow chart of proposed system**

## IV. IMPLEMENTATION

### A. *Hardware Setup*

AVR microcontroller is used to process the information sent by sensors. Figure 4.1 shows the hardware connection of wearable biomedical sensors. The different sensors required for implementation of the proposed work are as follows:

1) ***Body temperature sensor*** : **LM35** is temperature sensor whose output is proportional to the temperature (in degree Celsius).

2) ***Heart beat sensor****:* Pulse Sensor uses a transmission mode PPG probe (HRM-2511E) sensor, which uses an infrared light source to illuminate the finger on one side, and a photodetector on the other side to measure small variations in the transmitted light intensity due to changes in blood volume inside the tissue.

3) ***Blood pressure sensor****:* Blood pressure monitor measures the mean arterial pressure (MAP) and approximates the systolic and diastolic pressures.

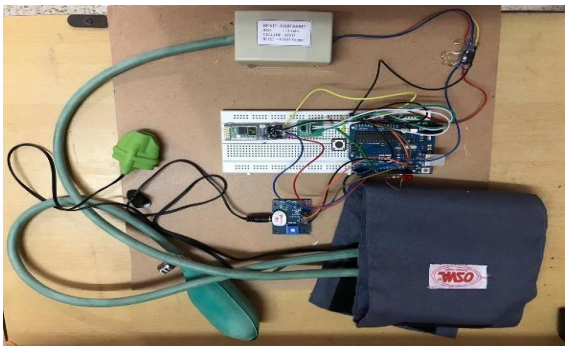


**Figure 4.1: Hardware setup**

### B. *Android App Development*

The app will allow the user to give unique id and password during registration. User can view their personal details and report. User can anytime view their report. XAMPP software is used as server. HeidiSQL is used to store database which is sent to server from user android application. The different pages developed for the mobile app are as follows:

***Login Credentials*****:** User will require 2 credentials for login: 1) user Id 2) Password. The user should give same user id and password as given during registration process. Figure 4.2 shows login page.

***Registration Credentials*****:** User need to fill their personal details like: Name, Age, Address, Mobile, Email, Username, Password, Emergency number. Figure 4.2 shows registration page of app.

***User Interface*****:** After successful login the user can view personal information, send and receive report and logout from the app. Figure 4.2 shows the user interface page of app.

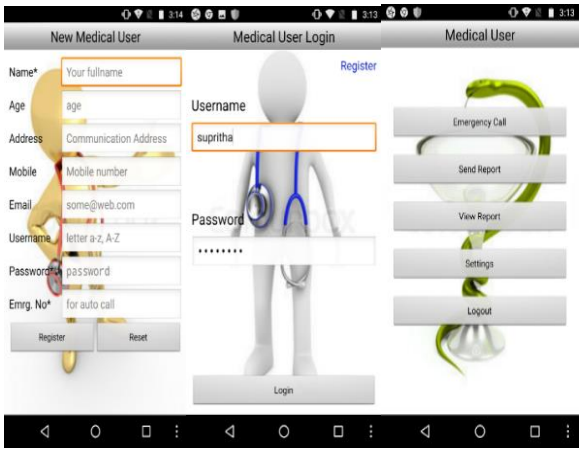



**Figure 4.2: Login page, Registration page and User interface page respectively.**


Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

### C. *Cloud Server*

The collected data from the biomedical sensors is transmitted to a cloud server so that the data is available anywhere through the Internet. The cloud server is used for data storage, data investigation, and data envisage which can be accessed and manipulated. The data stored in the cloud server is used to take decision whether the user is authenticated or not.

**XAMPP**: XAMPP software is used as web server for the proposed system that work across multiple types of platforms or operating environments. Server login page created using XAMPP software is as shown in below Figure 4.3 where user name and password has to be given in order to login to the home page and Figure 4.4 shows home page where sensor data sent to the cloud is visible and decision is made if the user is authenticated or not.


Figure 4.3: Server Login Page

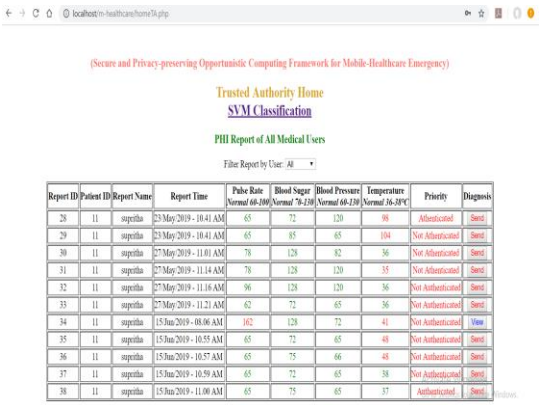



Figure 4.4: Home page

**HeidiSQL:** HeidiSQL is a free administration tool used for server connection, server host and to store databases. Figure 4.5 shows database stored in SQL. The different user's registration details, login id and password are stored as well as the data sent through the cloud from the mobile app are also stored.

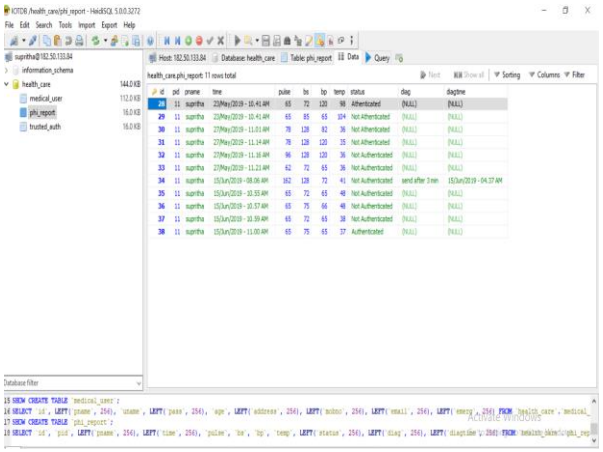
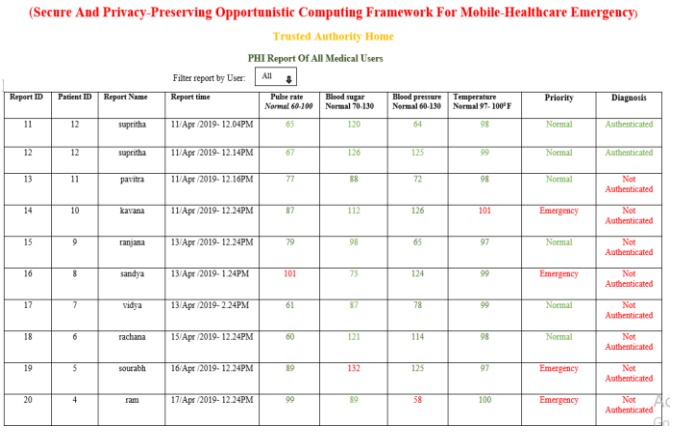


**Figure 4.5: Database stored in SQL**

## V. EXPERIMENTAL RESULTS

The user should login using user id and password through mobile app. The data from the sensors connected to the user body is transmitted using Bluetooth module HC-06. The data is received by mobile app through Bluetooth of mobile which is paired with Bluetooth module connected with the sensors. The data is updated in server and decision is made whether the user is authenticated or not using two classifiers SVM and AdaBoost. The threshold values for the classifiers is determined based on the user's historical health information. Figure 5.1 shows the previous stored data and present sent data by the sensors is same then message pops as authenticated.

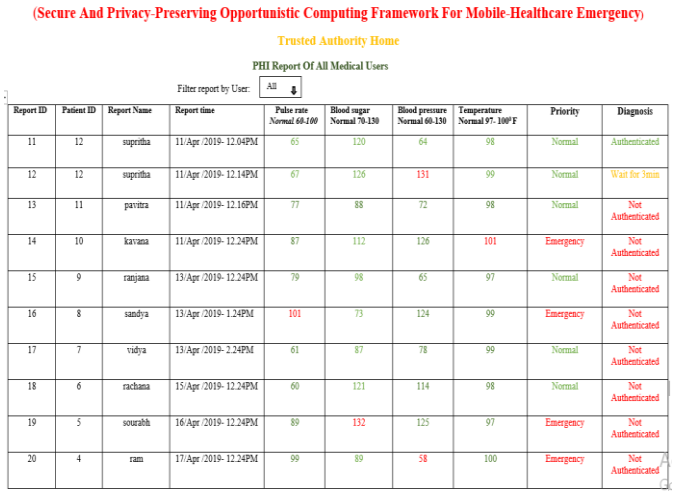



| Report ID | Patient ID | Report Name | Report time | Pulse rate Normal 60-100 | Blood sugar Normal 70-130 | Blood pressure Normal 60-130 | Temperature Normal 97- 100°F | Priority | Diagnosis |
|---|---|---|---|---|---|---|---|---|---|
| 11 | 12 | supritha | 11/Apr /2019- 12.04PM | 65 | 120 | 64 | 98 | Normal | Authenticated |
| 12 | 12 | supritha | 11/Apr /2019- 12.14PM | 67 | 126 | 125 | 99 | Normal | Authenticated |
| 13 | 11 | pavitra | 11/Apr /2019- 12.16PM | 77 | 88 | 72 | 98 | Normal | Not Authenticated |
| 14 | 10 | kavana | 11/Apr /2019- 12.24PM | 87 | 112 | 126 | 101 | Emergency | Not Authenticated |
| 15 | 9 | ranjana | 13/Apr /2019- 12.24PM | 79 | 98 | 65 | 97 | Normal | Not Authenticated |
| 16 | 8 | sandya | 13/Apr /2019- 1.24PM | 101 | 73 | 124 | 99 | Emergency | Not Authenticated |
| 17 | 7 | vidya | 13/Apr /2019- 2.24PM | 61 | 87 | 78 | 99 | Normal | Not Authenticated |
| 18 | 6 | rachana | 15/Apr /2019- 12.24PM | 60 | 121 | 114 | 98 | Normal | Not Authenticated |
| 19 | 5 | sourabh | 16/Apr /2019- 12.24PM | 89 | 132 | 125 | 97 | Emergency | Not Authenticated |
| 20 | 4 | ram | 17/Apr /2019- 12.24PM | 99 | 89 | 58 | 100 | Emergency | Not Authenticated |

**Figure 5.1: Results for authenticated user who is in normal healthy condition.**

If the certified user is not in normal condition means there might be variation in data because of running, jumping and walking then the message will pop as wait for 3 minutes so that authenticated user will become normal. The Figure 5.2 shows results for the authenticated user who is not in normal condition.


*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication (BEIESP)*


(Secure And Privacy-Preserving Opportunistic Computing Framework For Mobile-Healthcare Emergency)

Trusted Authority Home

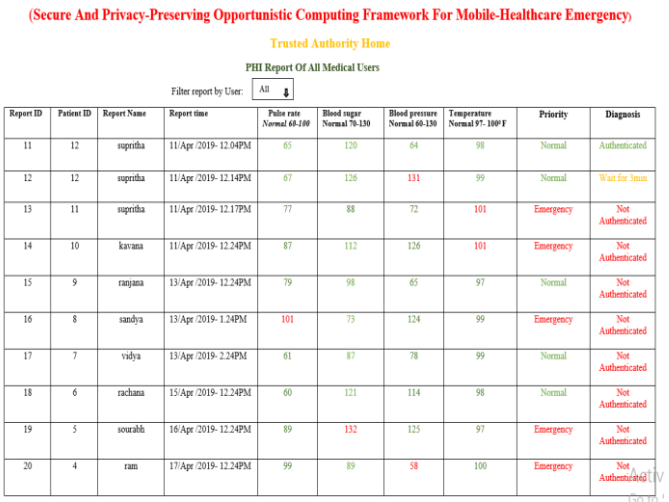
PHI Report Of All Medical Users

Filter report by User: All

| Report ID | Patient ID | Report Name | Report time | Pulse rate *Normal 60-100* | Blood sugar Normal 70-130 | Blood pressure Normal 60-130 | Temperature Normal 97- 100°F | Priority | Diagnosis |
|---|---|---|---|---|---|---|---|---|---|
| 11 | 12 | supritha | 11/Apr /2019- 12.04PM | 65 | 120 | 64 | 98 | Normal | Authenticated |
| 12 | 12 | supritha | 11/Apr /2019- 12.14PM | 67 | 126 | 131 | 99 | Normal | Wait for 3min |
| 13 | 11 | pavitra | 11/Apr /2019- 12.16PM | 77 | 88 | 72 | 98 | Normal | Not Authenticated |
| 14 | 10 | kavana | 11/Apr /2019- 12.24PM | 87 | 112 | 126 | 101 | Emergency | Not Authenticated |
| 15 | 9 | ranjana | 13/Apr /2019- 12.24PM | 79 | 98 | 65 | 97 | Normal | Not Authenticated |
| 16 | 8 | sandya | 13/Apr /2019- 1.24PM | 101 | 73 | 124 | 99 | Emergency | Not Authenticated |
| 17 | 7 | vidya | 13/Apr /2019- 2.24PM | 61 | 87 | 78 | 99 | Normal | Not Authenticated |
| 18 | 6 | rachana | 15/Apr /2019- 12.24PM | 60 | 121 | 114 | 98 | Normal | Not Authenticated |
| 19 | 5 | sourabh | 16/Apr /2019- 12.24PM | 89 | 132 | 125 | 97 | Emergency | Not Authenticated |
| 20 | 4 | ram | 17/Apr /2019- 12.24PM | 99 | 89 | 58 | 100 | Emergency | Not Authenticated |

**Figure 5.2: Results for authenticated user who is in not in normal healthy condition**

If in case the data sent again after 3 minutes is also not same as the previous stored data then message pops as the user is not authenticated. Figure 5.3 shows the results for person who is not in normal condition. Otherwise the authenticated user might be in emergency condition and further actions need to be taken.


(Secure And Privacy-Preserving Opportunistic Computing Framework For Mobile-Healthcare Emergency)

Trusted Authority Home

PHI Report Of All Medical Users

Filter report by User: All

| Report ID | Patient ID | Report Name | Report time | Pulse rate *Normal 60-100* | Blood sugar Normal 70-130 | Blood pressure Normal 60-130 | Temperature Normal 97- 100°F | Priority | Diagnosis |
|---|---|---|---|---|---|---|---|---|---|
| 11 | 12 | supritha | 11/Apr /2019- 12.04PM | 65 | 120 | 64 | 98 | Normal | Authenticated |
| 12 | 12 | supritha | 11/Apr /2019- 12.14PM | 67 | 126 | 131 | 99 | Normal | Wait for 3min |
| 13 | 11 | supritha | 11/Apr /2019- 12.17PM | 77 | 88 | 72 | 101 | Emergency | Not Authenticated |
| 14 | 10 | kavana | 11/Apr /2019- 12.24PM | 87 | 112 | 126 | 101 | Emergency | Not Authenticated |
| 15 | 9 | ranjana | 13/Apr /2019- 12.24PM | 79 | 98 | 65 | 97 | Normal | Not Authenticated |
| 16 | 8 | sandya | 13/Apr /2019- 1.24PM | 101 | 73 | 124 | 99 | Emergency | Not Authenticated |
| 17 | 7 | vidya | 13/Apr /2019- 2.24PM | 61 | 87 | 78 | 99 | Normal | Not Authenticated |
| 18 | 6 | rachana | 15/Apr /2019- 12.24PM | 60 | 121 | 114 | 98 | Normal | Not Authenticated |
| 19 | 5 | sourabh | 16/Apr /2019- 12.24PM | 89 | 132 | 125 | 97 | Emergency | Not Authenticated |
| 20 | 4 | ram | 17/Apr /2019- 12.24PM | 99 | 89 | 58 | 100 | Emergency | Not Authenticated |

**Figure 5.3: Results for the user who is in not in normal healthy condition after 3min**

Hence, the experimental results for different conditions can be concluded as shown in Table 5.1.

**Table 5.1: Experimental Results**

| User | Condition | Decision |
|---|---|---|
| Certified | Normal | Authenticated |
| | Emergency | Wait for 3 minutes |
| | Emergency(After 3 minutes) | Not Authenticated |
| Invaders | Normal | Not Authenticated |
| | Emergency | Not Authenticated |

## VI. CONCLUSION AND FUTURE RESEARCH

The initial one-time login authentication is insufficient to provide high security. In this paper, an IOT based health monitoring system is used for continuous authentication. The data which is collected from wearable biomedical sensors for continuous health monitoring can also be used for continuous authentication. Although the biomedical signals are not highly discriminative a robust machine learning by combining two classifiers SVM and AdaBoost is used in order to obtain high accuracy levels. An android app is developed to gather data and send to cloud for data storage. The collected data is communicated to a cloud server so that the data is available anywhere through the Internet. Hence, the proposed work involves less user involvement and the data is accessible whenever the user is wearing WMSs. The proposed work provides high security by continuously validated the user.

Our future work will include the authenticated user to login mobile app using the fingerprint so that high security can be provided for the proposed work.

## REFERENCES

1. P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," The Scientific World Journal, vol. 2013, 2013.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
2. A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to bio-metric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1,pp. 4–20, Jan. 2004.
3. A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp.125–143, Jun. 2006.
4. T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687–700, 2007.
5. K. Niinuma, U. Park, and A. K. Jain, "Soft biometric traits for continuous user authentication," IEEE Trans. Information Forensics and Security, vol. 5, no. 4, pp. 771–780, 2010.
6. S. P. Banerjee and D. L. Woodard, "Biometric authentication and identification using keystroke dynamics: A survey," J. Pattern Recognition Research, vol. 7, no. 1, pp. 116–139, 2012.
7. S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D.Wagner, "Are you ready to lock?" in Proc. ACM Conf. Computer and Communications Security, 2014, pp. 750–761.
8. C. Shen, Z. Cai, and X. Guan, "Continuous authentication for mouse dynamics: A pattern-growth approach," in Proc. IEEE Int. Conf. Dependable Systems and Networks, 2012, pp. 1–12.
9. J. Roth, X. Liu, and D. Metaxas, "On continuous user authentication via typing behavior," IEEE Trans. Image Processing, vol. 23, no. 10, pp. 4611–4624, 2014.
10. I. Deutschmann, P. Nordstrom, and L. Nilsson, "Continuous authentication using behavioral biometrics," IEEE IT Professional, vol. 15, no. 4, pp. 12–15, 2013.
11. A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensorbased systems for health monitoring and prognosis," IEEE Trans. Systems, Man, and Cybernetics, vol. 40, no. 1, pp. 1–12, 2010.
12. Abideen, Zain Ul, and Munam Ali Shah. "An IoT based robust healthcare model for continuous health monitoring." 2017 23rd International Conference on Automation and Computing (ICAC). IEEE, 2017.

## AUTHORS PROFILE

**Pavithra D R** has received her Bachelor of Engineering in Electronics and Communication from Sri Jayachamarajendra College of Engineering, Mysuru, affiliated to Visvesvaraya Technological University, Belagavi, Karnataka in the year 2004, and M.Tech. in the area of Computer Networks and Engineering from National Institute of Engineering, Mysore affiliated to Visvesvaraya Technological University, Belagavi, Karnataka in the year 2010 and now pursuing her Ph.D. in the area of digital Image signal processing from Visvesvaraya Technological University, Belagavi. Her areas of interest include Signal Processing, Digital Image Processing.

**Supritha R** has received her Bachelor of Engineering in Electronics and Communication from Vidyavardhaka College of Engineering, Mysuru, affiliated to Visvesvaraya Technological University, Belagavi, Karnataka in the year 2017 and now pursuing her M.Tech. in Industrial Electronics from Sri Jayachamarajendra College of Engineering, Mysuru, affiliated to Visvesvaraya Technological University, Belagavi, Karnataka. Her areas of interest include Signal processing, Automotive Electronics and Internet of things.