ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 6, June 2019

A High Security System Based On Bioaura

Ammus Sivanandhan[1], Ashlin P Eldhose[2], Jitha Shajan[3], Mercy George[4], Robin George[5]

UG Students, Dept. of ECE, Mar Baselios Institute of Technology and Science, Nellimattom, Ernakulam, Kerala, India[1,2,3]

Dept. of ECE, Mar Baselios Institute of Technology and Science, Nellimattom, Ernakulam, Kerala, India[4,5]

ABSTRACT: In most of the computer systems only one time initial authentication is possible which can lead to security concerns. So here we are proposing a system with more security services ie, BioAura. The three parameters here we are considering are: temperature measurement, pulse rate and the distance between the eyelashes.And also an OTP is also used for high verification. CABA authenticates users based on their BioAura, an ensemble of biomedical signal streams that can be collected continuously and non-invasively using wearable medical devices. While each such signal may not be highly discriminative by itself, we demonstrate that a collection of such signals, along with robust machine learning, can provide high accuracy levels.

I. INTRODUCTION

Authentication refers to the process of verifying a user based on certain credentials, before granting access to a secure system, resource, or area. Traditionally, authentication is only performed when the user initially interacts with the system. In these scenarios, the user faces a knowledge based authentication challenge, e.g., a password inquiry, and the user is authenticated only if he offers the correct answer, e.g., the password. Although one-time authentication has been the dominant authentication mechanism for decades, several issues spanning user inconvenience to security flaws have been investigated by researchers. For example, the user has to focus on several authentication steps when he tries to unlock a smartphone based on a password/pattern-based authentication method. This may lead to safety risks, e.g.,distraction when the user is driving. A serious security flaw of one-time authentication is its inability to detect intruders after initial authentication has been performed. For example, an unauthorized user can access private resources of the authorized user if the latter leaves his authenticated device unattended, or forgets to log out.

II. IMPLEMENTATION

BIOAURA

In this section, we first briefly describe how Biostreams can be collected using the sensors. Then, we discuss which Biostreams constitute the BioAura. As mentioned earlier, BioAura is an ensemble of Biostreams, which are gathered by sensors for medical diagnosis and continuous health monitoring. The most widelyused scheme for continuous health monitoring consists of two classes of components: (i) sensors and (ii) a base station . All sensors transmit their data to the base station either for system can perform simple preprocessing to extract values of some important features from the data, and transmit those values. In CABA, the system first executes a very simple feature extraction function that computes the average value of the samples in each Biostream over the last one minute time frame of data. Then, it only transmits a feature vector that contains these average values. Further processing or long-term storage. In recent years, systems have become the dominant base station since they are powerful and ubiquitous, and their energy resources are less limited relative to sensors. Simple continuous authentication system that consists of several small lightweight sensors, which transmit their biomedical data to the basestation over a python software with the expected widespread use of the sensors, CABA can be used to provide a continuous authentication system as a side benefit of continuous health monitoring systems. Our proposed BioAura consists of Biostreams that are essential for routine continuous secure authentication, and the biostreams are pulse rate, temperature measurement and the distance between the eyelashes and their collection needs minimum user involvement. And after sensing these parameters an OTP verification is also there for login to the webpage created. Such Biostreams are expected to be included in long-term continuous secure authentication systems.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 6, June 2019

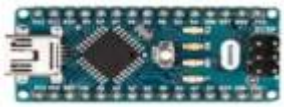
III. SCOPE OF APPLICATIONS

In this section, we describe the possible applications of CABA. The concept of continuous authentication based on BioAura can be used to protect (i) personal computing devices and servers, (ii) software applications, and (iii) restricted physical spaces. Next, we conceptually describe how CABA can be used to protect each domain. Computing devices, e.g., personal computers, laptops, tablets, and cell phones, or servers can employ two different approaches to utilize CABA: (i) they can use their own computing resources to implement a stand-alone version of CABA, or (ii) they can simply use decisions made by a version of the scheme implemented on a trusted server. We investigate both approaches. For example: Suppose the user wants to login to his personal computer, the computer has enough computational power and energy capacity to implement a stand-alone version of CABA. This case is similar to the one in Example 1, except that there is no need for a trusted server. Similarly, CABA has the potential to provide continuous authentication for applications that need strong authentication, e.g., e-commerce applications. Its authentication decisions can be made on the same device that runs the application or on a powerful trusted server and then transmitted to the device that runs the application.

IV. COMPONENTS REQUIRED

Arduino Nano

Fig 1 Arduino Nano



Arduino Nano is a small, compatible, flexible and breadboard friendly Microcontroller board, developed by Arduino.cc in Italy, based on ATmega328p (Arduino Nano V3.x) / Atmega168 (Arduino Nano V3.x). It comes with exactly the same functionality as in Arduino UNO but quite in small size. It comes with an operating voltage of 5V, however, the input voltage can vary from 7 to 12V. **Arduino Nano Pinout** contains 14 digital pins, 8 analog Pins, 2 Reset Pins & 6 Power Pins. Each of these Digital & Analog Pins are assigned with multiple functions but their main function is to be configured as input or output. They are acted as input pins when they are interfaced with sensors, but if you are driving some load then use them as output. Functions like pinMode() and digitalWrite() are used to control the operations of digital pins while analogRead() is used to control analog pins. The analog pins come with a total resolution of 10bits which measure the value from zero to 5V. Arduino Nano comes with a crystal oscillator of frequency 16 MHz. It is used to produce a clock of precise frequency using constant voltage. There is one limitation using Arduino Nano i.e. it doesn't come with DC power jack, means you can not supply external power source through a battery. This board doesn't use standard USB for connection with a computer, instead, it comes with Mini USB support.

Temperature Sensor

The temperature sensor here we are using is water proof sensor. Its a one wire bus communication since it uses one port for communication and has 3 pins: red, black, yellow. It always give digital output because it has inbuilt ADC and we also providing a 4k pull up resistor. In the working of this sensor firstly it senses the temperature, and threshlod temperature is between -55 degree celsius to 125 degree celsius. After senses the temperature it converts the analog data into digital data. While converting it transmit 1 and after converted the value it transmit 0. And thus we get the digital output.

Fig 2 Tempreature sensor

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 6, June 2019

Pulse Sensor

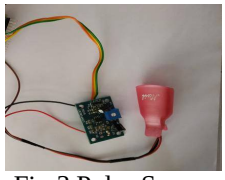


Fig 3 Pulse Sensor

The Pulse Sensor is a plug-and-play heart-rate sensor for Arduino. It can be used by students, artists, athletes, makers, and game & mobile developers who want to easily incorporate live heart-rate data into their projects. Essence it is an integrated optical amplifying circuit and noise eliminating circuit sensor. Clip the Pulse Sensor to your earlobe or finger tip and plug it into your Arduino, you can ready to read heart rate.
The Pulse Sensor can be connected to arduino, or plugged into a breadboard.. On the front you see a small round hole, which is where the LED shines through from the back, and there is also a little square just under the LED. The square is an ambient light sensor, exactly like the one used in cellphones, tablets, and laptops, to adjust the screen brightness in different light conditions. The LED shines light into the fingertip or earlobe, or other capillary tissue, and sensor reads the light that bounces back. The back of the sensor is where the rest of the parts are mounted. The main specifications of pulse sensor are Operating voltage: 3.3V – 5V, Current: 4mA, Indicator LED.

PCB

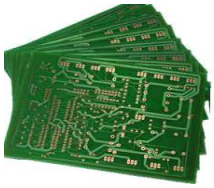


Fig 4. PCB

Aprinted circuit board (PCB) mechanically supports and electrically connects electronic components or electrical components using conductive tracks, pads and other features etched from one or more sheet layers of copper laminated onto and/or between sheet layers of a non-conductive substrate. Components are generally soldered onto the PCB to both electrically connect and mechanically fasten them to it.

LCD

Fig 5. LCD

A liquid-crystal display (LCD) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in color or monochrome. LCDs are availableto display arbitrary images (asin a general-purpose computer display) or fixed images with low information content, which can be displayed or hidden, such as preset words, digits, and seven-segment displays, as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements. LCDs can either be normally on (positive) or off (negative), depending on the polarizer arrangement.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 6, June 2019

V1. IMPLEMENTATION

Prototype Implementation

Similar to other authentication systems, CABA has two operating phases:

1)Enrollment phase in which CABA builds machine learning-based models for each user, given the training data.

2)User authentication phase in which the system continuously authenticates the user. The description of the two phases is presented next.

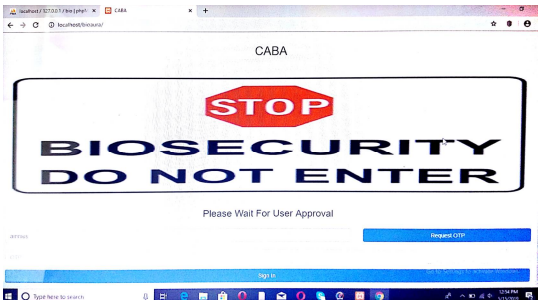
1) Enrollment phase: In the enrollment phase, the authentication system is given a training dataset. The system builds the model using a supervised learning approach, i.e., a machine learning approach in which the model is built based on labeled training data points. Generally, the amount of information needed to build a model varies from one application to another. We evaluated the number of training data points needed to investigate how much information should be sent to the authentication system to build a reliable and accurate model. Each data point in the training set is nine dimensional and consists of the average values of successive measurements of a Biostream over a one-minute timeframe. The value of each dimension is represented using half precision floating-point format that requires two bytes of storage. In order to maintain reliability, CABA should train a new model based on fresh biomedical data obtained at certain intervals.

2) User authentication phase: In this phase, the system makes decisions using the already-trained model. In a continuous authentication scenario, the system should verify the user's identity at certain intervals. The frequency of authentication depends on several factors, such as the required level of security and the amount of information required for one authentication. Therefore, unlike most previously-proposed continuous authentication systems, e.g., keyboard/mouse-based systems, that require the user to wait while they collect authentication information, CABA obtains the required information almost instantaneously because the information has already been gathered and stored on the system. In a single verification attempt:

SVM: The basic concept in an SVM is to find a hyperplane that separates the n-dimensional data into two classes. However, since the data points in the dataset are not usually linearly separable, SVMs introduce the concept of kernel trick that projects the points into a higher-dimensional space, where they are linearly separable. When no prior knowledge about the dataset is available, SVMs usually demonstrate promising results and generalize well.

VII. RESULTS

In this project, we are using three parameters to login a webpage. The parameters we concerned are temperature, pulse rate and the distance between the eyelashes. It is mainly for the office purposes. Firstly, the database of these parameters are stored in to a system using the software python. Whenever a person comes to unlock the webpage, the sensors senses the person's biostreams and it compares the person's biostreams with the stored data. And also a OTP will be sent to the user's smartphone. If the person is not the user then he can't login to the webpage. If he is the user then he will get an OTP and approved for login.



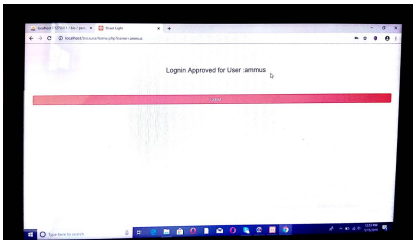
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 6, June 2019



VIII. CONCLUSION

In this project, we proposed CABA, a novel user-transparent system for continuous authentication based on information that is already gathered by sensors for security and therapeutic purposes. We described a prototype implementation of CABA and comprehensively investigated its accuracy and scalability.
We also described how CABA can be used to support user identification. We compared CABA to previously-proposed continuous authentication systems (biometrics- and behaviometrics-based), and highlighted its advantages. We discussed several attacks against the proposed authentication system along with their countermeasures. Finally, we briefly described an privacy concerns surrounding the use of biomedical signals, how CABA can also be used for one-time authentication, and impact of temporal conditions on authentication.

REFERENCES

[1]T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, “Continuous verifi-cation using multimodal biometrics,” IEEE Trans. Pattern Analysis andMachine Intelligence, vol. 29, no. 4, pp. 687–700, 2007.
[2] R. Gravina, P. Alinia, H. Ghasemzadeh, and G. Fortino, “Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges,” Information Fusion, vol. 35, pp. 68–80, 2017.
[3] K. Niinuma and A. K. Jain, “Continuous user authentication using temporal information,” in Proc. SPIE Defense, Security, and Sensing, 2010, p. 76670L.
[4] I. Deutschmann, P. Nordstrom, and L. Nilsson, “Continuous authentication using behavioral biometrics,” IEEE IT Professional, vol. 15, no. 4, pp. 12–15, 2013.