ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization *Vol.5, Special Issue 2, April 2017*

An International Conference on Recent Trends in IT Innovations - Tec'afe 2017

Organized by

Dept. of Computer Science, Garden City University, Bangalore-560049, India

Outsourced Security Guard Service based on IoT

M.Swarnamugi, Dr.R.Chinnaiyan

Assistant Professor, Department of MCA, Jyoti Nivas College Autonomous, Bangalore, India

Professor , Department of Computer Applications, New Horizon College of Engineering, Bangalore, India

ABSTRACT: The future of internet – IoT (Internet of Things) is to enable things (objects) to communicate with each other in an unimaginable fashion. IoT has already gained attention among researchers, scientist, engineers, software developers, academicians and much more professionals over the years for its effectiveness and increased use in many applications. In this sense, this paper presents a simple model to outsourced guard services in the form of an IoT based system that verifies the identity of guards using ECG biometric across the cloud. This paper uses a transform based algorithm called wavelet transform for verification of ECG signal. The ECG signal is preprocessed to remove the noise as to improve the accuracy of feature extraction. This paper focus on extracting the amplitude and slope features of P, QRS Complex and T wave. The similarity of the signals are calculated by using correlation coefficient. The system respond by sending an alert about loss of identity to the substation if there happens a mismatch in the authenticity of the guards**.**

KEYWORDS*:* Electrcardiogram, Wavelet Transform, ECG Sensor,Correlation coefficient, Security Guard Service, ARDUINO UNO micrcontroller.

I. INTRODUCTION

Many corporates, hospitals, financial sectors, educational institutions, and other private and public organizations nowadays focus on their core business activities and outsource other business related supporting tasks that fall outside of their expertise area. On such out fall business related supporting task is security service of their premises. A security guard service or protective agent is a private person or a group of persons who are paid to protect an organization's assets from a variety of hazards that includes tampering of premises rule, misuse of the property, unsafe work behavior, criminal activity etc., The security guards will be given rights to utilize preventive measures to safeguard or protect the organization. There exist two types of security guard service. A company or organization can opt to hire their own staff for protecting the non-business security related task called as in-house security guard service. Another is, an organization outsourcing security to a third party company that provides security to the organization round the clock [15].

There exist several disadvantages for an organization to hire its own staff as security guards directly because of factors such as:

i. For a full time employee, the organization has to spend additional cost such as employee tax, vacation benefits, overtime, holiday pay, medical expenses, annual raises, relief for days off etc.,

ii. There will be a huge amount spend for recruiting, background checks, training, uniforms, equipment and sustainment

iii. Outsource security companies have an inventory of security equipment and systems that can be provided to the security guards. The renewal of this equipment or cost to extend period of time will be paid and taken care by the outsourcing security companies itself and thereby these overheads can be avoided if an organization outsource the security guard service.

iv. An organization that outsource security service parlays a portion of the company's liability and protection to a third party; thereby reducing their insurance premiers and potential claims. If not, the insurance cost saving for shifting a portion of their liability to a third party can offset the cost of out-source security.

Outsourcing security guard services to a third party companies has many advantages and their only mission is: security; and all company efforts and expenses go towards security operations.

For an outsourced guard service, an organization only need to pay the yearly amount or monthly amount as signed in the contract. It need not to look after or maintain the entire database of the guard force. All data about the guard force and their details are maintained and managed by the third party security company. The security company's guards have already been background checked, trained, uniformed and equipped. The management team of the security company often checks the correctness of the data submitted by guards or cops and can consult with their customers to provide the most cost effective security force to meet the customer requirement.

The outsourced guards who are working in organization's premises reports both to the customer (to the organization where they are presently doing the duty) and to their own security company by posting orders, actions, logs. These are scrutinized by both the customer and security company thereby, resulting in a good service. Though there exist so many background check up's for guards, what if the original guard assigned to a certain organization is replaced by a fraudulent guard or agent without the knowledge of security company and without the knowledge of the organization? This kind of fraudulent activity occur not only in the cinematic scenes but also in the real time. Therefore, the identity of outsourced guards working in the organization premises need to be authenticated and trusted. This paper aims to address this issue by using ECG as a biometric, and the whole model is proposed using IoT technique.

The organization of the paper is as follows: Section II describes the background study. The proposed system is explained in section III of the paper. The implementation is explained in section IV.

II. BACKGROUND STUDY

IoT Communication models

The concept of IoT allows physical objects or things around us to interact with each other in an intelligent way with the aid of key elements like Radio-Frequency Identification (RFID) tags, processors, sensors, actuators, WAN, W-LAN etc., with minimal human intervention .IoT supports four communication models described by the Internet Architecture Board: Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing [1]. This paper uses Device-to-cloud model for the implementation of the system. Karthikeyan B et al. [2] illustrated a model to develop an attendance maintenance system for schools, colleges and other organizations. The model is designed to detect any form of intrusion in restricted areas and report it immediately. This system is implemented using a PIR sensor, a RFID reader and a camera. Raspberry pi B+ is used to control the communication between the used peripherals. Nadar Prince et al. [3] proposed an IoT model applied to the basic attendance system in a class room. They designed a portable device used by the student to feed his/her attendance during each lecture. The student verification is done using R-305 Finger Print module. They used ARDUINO to provide data sequence and esp8266 to get access to the internet. Mahesh Sutar et al. [4] proposed Smart Attendance System using RFID tags and readers. Daniel Palma et al. [5] presented a way how classroom control is accessed through Near Field Communication (NFC) and the information is shared via radio frequency. They developed a tool and a device to manage classrooms in real time. To do this, a transmitter/receiver access control for each classroom was created, data are uploaded to the cloud and a Web application to view the data was built. For implementation they used hardware such as ARDUINO UNO and NFC module for Arduino and communication shield from cooking-hacks and Radio Frequency module (433 MHZ).NFC, RF, Arduino, Xively, Google Maps and Zapier technologies are combined in this paper to show the power of the Internet of Things for managing and sharing data.

Biometric Human Identification based on ECG

The electrocardiogram (ECG) is a tool usedto measure irregularities present in the functioning of theheart as it beats. The most important characteristic of the ECG include the information lying in the P, Q, R, S, and T waves corresponding to atrial and ventricular de- polarization or repolarization [6]. Different studies in the literature have proved ECG as a possible biometric toolto measure the authenticity of an individual. Israel et al. [7] illustrated that ECG of an individual human has a unique pattern. They implemented ECG processing for checking the quality and proposed a quantifiable approach for the classification of heartbeats. Hugo Placido et al. [8] provided an evaluation of the stability of ECG signals collected at the fingers. Biel et al. [9] conducted the ECG biometric experiment on a group of 20 individuals where 30 features are extracted from each heartbeat. In order to reduce the amount of information high correlation features are discarded and only 12 features are selected for classification. They used a multivariate analysis based method for classification. Shen et al. [10] conducted the biometric experiment for identity verification using appearance and time domain features of the heartbeat. In their approach most of the features are extracted from QRS complex that are stable with change in the heat rates. They used a decision-based neural network approaches to quantify the identity verification. Singh and Gupta [11] proposed a new approach on ECG to aid in human identification.

Signal processing methods are used to describe ECG wave fiducials from each heartbeat. The proposed approach results are found optimum and stable.

III. PROPOSED SYSTEM

The idea behind the system is to verify the identity of guard protecting the organization premises. The identity of a person can be verified by means of various biometric features such as finger prints, retina, face, hand geometry, voice, writing and typing dynamics, etc. This paper aims to verify biometric identification based on electrocardiogram (ECG). ECG captures the electrical current that are generated by the heart as it beats. And, it is one important distinctive human universal characteristics because, ECG waveforms depend on the anatomic features of the human heart and body [12]. Its authentication capabilities for group of individuals has been shown uniqueness in the literature, ECG can be easily captured using suitable devices, and it is not easily deceived as it depends on individuals anatomic features and heart beats. This motivated to use ECG for the verification and to authenticate the individuals.

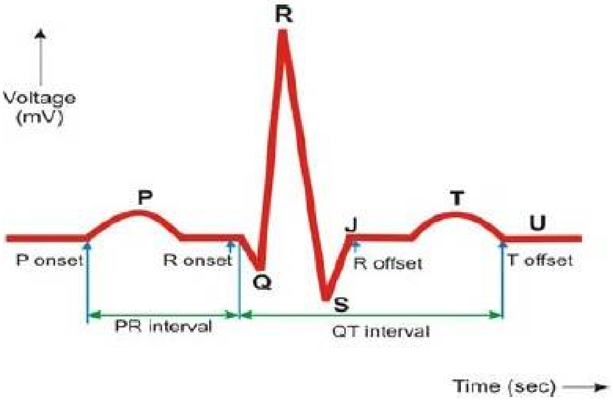

Fig. 1. An ECG Waveform with ECG intervals

ECG Biometric has several advantages than fingerprint, iris or other biometrics.

1) The dynamic parameter such as P wave, QRS complex, T waves are extracted so it allows continuous monitoring.
2) Imposible to clone ECG as it depend on personal uniqueness
3) ECG does not depend on external circumstance. Whereas other biometrics depend on external features.
4) In terms of Compactness and convenience, a small sensor device is needed to capture the signal. Nowadays ECG sensor even comes in a form of small wrist band.

The proposed system involves two important functionalities. Enrolment and Verification. Enrolment is a process of preprocessing and extracting important features of ECG signal to use it as a biometric sample. The extracted features are stored in a cloud with a unique id to the ECG signal using a service called Pushing Box API [13]. Whenever the authenticity need to be checked, the query data (ECG captured at the organization premises) is verified with this stored sample data. The second functionality of the system is verification process. To verify the authenticity of guards, the unique ID assigned during the enrolment process and the captured ECG is compared with the already stored sample data in the cloud. If there happens a mismatch in the ECG data for a unique ID, it is said to be fraudulent access and the alert is send to smart phone of substation manager. Each organization outsourcing security guard service has a substation manager (person/organization staff responsible for maintenance of guard service at the organization) is a SPOC to the security company. Once the alert is received, the substation manager takes the necessary action.

A. Methodology

The proposed system uses a transform based algorithm called wavelet transform for verification of ECG signals. In order to extract information from the ECG signal, the raw ECG signal should be processed. Processing of raw ECG signal happens as two stages: Preprocessing – it remove noises from the ECG signal, Feature extraction – to select relevant information from the ECG signal.

A.1. Preprocessing of the ECG signal

Preprocessing is a process of removing noisy signal in the ECG. All noisy signal that corrupt the ECG should be removed for the feature extraction to be accurate. Noise in ECG signal includes, base line drift caused by low frequency components and frequency interferences caused by high frequency components. Other noises include electrode noise (electrodes attached physically to human body), polarization noise, muscle noise, and motor artifacts. Baseline drift is one important noise in the ECG signal that need to be removed. The technique proposed in [15] is adopted in this paper with the help of median filters to eliminate the baseline drift noise. The ECG signal is processed with median filter of 200-ms to remove QRS and P waves. The ECG signal is then processed with median filter of 600-ms to remove T waves. The resulting signal is said to be the filtered signal. Subtracting the filtered signal with original signal yield a new signal with baseline drift eliminated. The other noises stated are removed using discrete wavelet transform. It first decomposes the ECG signal into several bands and then modifies each wavelet coefficient by applying a threshold function, and construct a noiseless ECG signal.

A.2. Feature Extraction

The features selected is based on the technique proposed by [16]. One important feature extraction in ECG signal is detection of QRS Complex. The detection of QRS complex is based on discrete wavelet transform. The QRS complex produces two modulus maxima with opposite signs, with a zero crossing between them. Therefore thresholds are applied to the wavelet transform of the ECG signal. The other two waves that present in ECG signal is P wave and T wave. The P and T waves consist of modulus maxima pair with opposite signs. The P wave correspond the onset and offset with modulus maxima pair. The search for P wave happens prior to the QRS complex. The zero crossing between the modulus pair refer to the peak of the wave. The T wave found at the zero crossing between the two modulus maxima refer to the peak of the T wave.

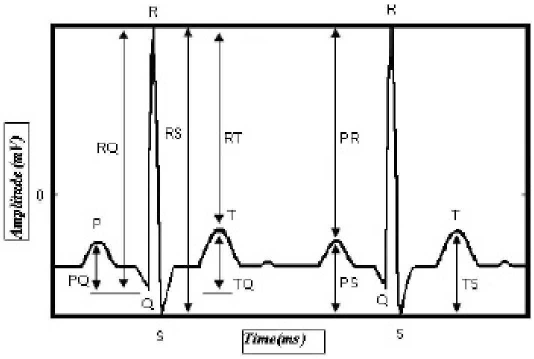

Fig. 2. ECG Feature Extraction

The ECG signals are not same and vary from person to person. The changes are reflected in P wave and PR wave. Amplitude of this waves refers to electrical activity of the heart. Here, the amplitude features such as PQ, RQ, TQ, RT, PS, RP, TS, RS, RT, QS are captured. The slope features such as RS, ST, and QR are also captured for ECG signal verification.

A.3. Verification

The approach of achieving verification uses wavelet coefficient. It is a type of correlation and dependence which is used to measure the statistical relationship between ECG signals. This paper uses this wavelet coefficient to find the similarity of any two ECG signal. The two signals are ECG stored in the cloud and ECG captured from security guard from the organization premises. And it is given as,

$$r_{xy} = \frac{\sum_{n=1}^{N}\left(x_n - \bar{x}\right)\left(y_n - \bar{y}\right)}{\sqrt{\sum_{n=1}^{N}\left(x_n - \bar{x}\right)^2 \sum_{n=1}^{N}\left(y_n - \bar{y}\right)^2}}$$

r_{xy} is the correlation coefficient (similarity) between the obtained ECG from the organization premises and the ECG stored in the cloud. x_n denotes the number of sample stored in the cloud and N is the length, and each sample contains a P wave, QRS complex and T wave. During the verification process, the y_n (the captured ECG signal) is compared against all the amplitude features and the slope features extracted. It provides value 1, -1, where 1 means a match between the two signals and -1 for mismatch of ECG signal.

Figure 3 depicts the entire flow of the system. During the enrolment process the ECG signal captured is first preprocessed to remove the noises for better feature extraction accuracy. The ECG amplitude and slope features such as PQ, RQ, TQ, RT, PS, RP, TS, RS, RT, QS, RS, ST, and QR are extracted and stored in the cloud. On Verification, the captured signal is preprocessed to remove noise and features are extracted. The wavelet transform algorithm verify the similarity against all the amplitude features and the slope features extracted. If there happens a mismatch in the ECG signal captured and ECG stored, it is said to be fraudulent access and the alert is send to smart phone of substation manager.

IV. IMPLEMENTATION

Figure 4. Depicts the implementation of the system proposed. The overall objective is to build an IOT based system that automates the authenticity of security guard. As the initial step, this paper works on ECG sensor module. The verification algorithm to find the similarity of ECG signal is represented here as ECG sensor module. This sensor module is responsible of capturing the ECG signal, preprocessing it and extracting the amplitude features of P, QRS complex and T waves. This sensor module is connected to ARDUINO UNO board. The ARDUINO UNO is based on microcontroller ATmega328. During enrollment, The ECG signal is digitized by 10 bit Analog digital converter of the ATmega328 in Arduino Uno Board. This digitized ECG signal is send to cloud using Wi-Fi module esp8266-01.Esp8266-01 is connected with ARDUINO UNO with the serial port 3.3V. The system uses AT commands to communicate with esp8266 and the cloud.

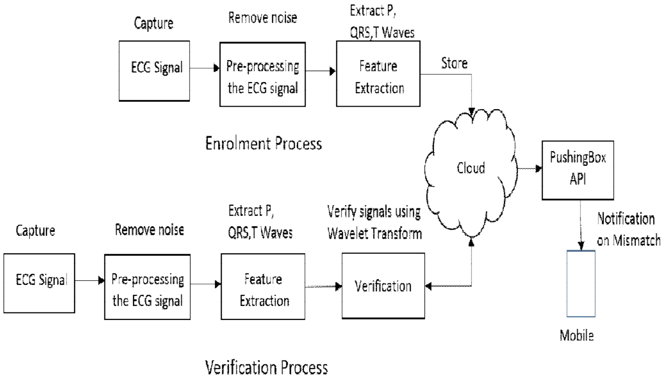

Fig.3. ECG Sensor Block Diagram

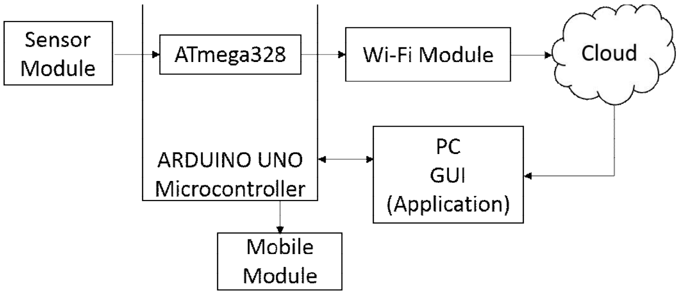

Fig. 4. Block diagram of Implementation system

V. CONCLUSION

An IoT based system is proposed in this paper to verify the authenticity of security guards working in the customer premises. Electrocardiogram as a human identification metric is used in this paper. The identity of the guard is authenticated by the similarity between ECG signal captured in the organization premises and comparing it with the already stored sample ECG signal in the cloud database. If any discrepancy occurred, an alert message is sent to the SPOC of the organization to take necessary action. The advantage of the system is, since ECG is used as a biometric tool, spoofing of data is difficult as it depends on individuals anatomic features and heart beats.

REFERENCES

[1] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", Journal of Future Generation Computer Systems, Volume 29 Issue 7, September, 2013.

[2] Karthikeyan B, Astha Puri, Rohan Mathur, Anurag Mishra, "Internet of Things (IOT) based Attendance and Intrusion Detection System", International Journal of Innovative Research in Computer and Communication Engineering", Vol.4 , Issue 3, March 2016.

[3] Nadar Prince, Abhishek Sengupta, Ms.Keerthi Unni, "Implementation of IoT Based Attendance System on a Dedicated Web-Server", International Journal of Scientific & Engineering Research, Volume 7, Issue 6, June -2016.

[4] Mahesh Sutar, Mahesh Patil , Sachin Waghmare, "International Journal of Advanced Research in Computer Engineering & Technology", Volume 5 , Issue 4, April 2016.

[5] Daniel Palma, Juan Enrique Agudo , Héctor Sánchez and Miguel Macías Macías, "An Internet of Things Example: Classrooms Access Control over Near Field Communication", Sensors 2014.

[6] Yogendra Narain Singh , S. K. Singh, "Evaluation of Electrocardiogram for Biometric Authentication", Journal of Information Security, 39-48, vol 3, 2012.

[7] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold and B. K. Wiederhold, "ECG to Identify Individuals," Pattern Recognition , Vol. 38, No. 1, 2005, pp. 133-142.

[8] Hugo Pl´acido da Silva, Andr´e Lourenco, Ana Fred, Anil K. Jain, "Finger ECG Signal for User Authentication: Usability and Performance", FCT, 2009.

[9] L. Biel, O. Pettersson, L. Philipson and P. Wide, "ECG Analysis: New Approach in Human Identification," IEEE Transaction on Instrumentation and Measurement , Vol. 50, No. 3, 2001, pp. 808-812.

[10] T. W. Shen, W. J. Tompkins and Y. H. Hu, "One-Lead ECG for identity Verification," Proceedings of the Second Joint EMBS/BMES Conference , Houston, 23-26 October 2002, pp. 62-63.

[11] Y. N. Singh and P. Gupta, "Biometric Method for Human Identification Using Electrocardiogram," Proceedings of the 3rd IAPR/IEEE International Conference on Biometrics, ICB 2009, LNCS, Springer-Verlag, Berlin, Vol. 5558, 2009, pp. 1270-1279.

[12] Tatiana S. Lugovaya, "Biometric Human Identification based on ECG", [Master's thesis] Faculty of Computing Technologies and Informatics, Electrotechnical University "LETI", Saint-Petersburg, Russian Federation; June 2005.

[13] Piyush Devikar, Ajit Krishnamoorthy, Aditya Bhanage,Mohit S Singh Chauhan, "IoT Based Biometric Attendance System", International Journal of Advanced Research in Computer and Communication Engineering", Vol. 5, Special Issue 2, October 2016.

[14] S. A. Benade, U.L.Bombale, " Finger Touch Based ECG Monitoring", International Journal of Research in Engineering and technology".Vol. 5, Issue 7, july 2016.

[15] Lenny Holden, "In House vs Outsourced Security", Securitas, Thailand, 2010.

[16] P. de Chazal, C. Heneghan, E. Sheridan, R.Reilly, P. Nolan, M. O'Malley, "Automated Processing of the Single-Lead Electrocardiogram for the Detection of Obstructive Sleep Apnoea", IEEE Trans. Biomed. Eng., 50(6): 686-689, 2003.

[17] P. SASIKALA, Dr. R.S.D. WAHIDABANU, "Identification of Individuals using Electrocardiogram", International Journal of Computer Science and Network Security, VOL.10 No.12, December 2010.