A Secure Cloud-Assisted Wban Health Care System Using Biometric Keys And Qr Pattern Analyze

T.Santhi Vandanna , S.Venkateshwarlu

Abstract: In recent years the use of wireless sensor networks (WSN) inpatient monitoring is emerging steadily due to the inventions made in telecom industries. Today's Internet of Things extends the potential of healthcare monitoring for a wide range of applications such as cardiac measures, sugar level monitors etc.due to its anywhere and anytime network connectivity. To accommodate this growing density in network technology wireless body area networks is emerged as a unique model to regulate this patient monitoring process. As most sensor and its data transmission are wireless in nature, are among major areas of concern. Due to open access and wireless data transmission security and privacy concerns restrict to utilize the optimal benefits of the WBAN system. In addition to this, data exchange between very small sensor nodes and server database over frequently changing environment reliability, resource management, and QoS issues are arising. In this paper, we propose and evaluate an area-efficient security scheme for the WBAN system with a QR pattern-based hybrid cloud authentication framework that supports a wide range of biosignal measures in WBAN communications. In this paper, we explore various integration issues in healthcare monitoring systems and analyze in detail the limitations and all possible countermeasures.

Index Terms: Cryptography, Security, WSN, WBAN, Bio signal Processing,, QR codes, EEG/ECG and Cloud Computing .

1. INTRODUCTION

With an increasing aged peoples rate around the world, which are more fragile to health related problems demands technologically more advancement and very comprehensive healthcare system to ensure instant medical care from any part of geographical location. In this healthcare field, WBAN has been widely preferred which can offer some potentially useful solutions to remote patient monitoring system (Logan et al., (2007), Suh, Myung-kyung, et al., (2011)). Over a period of time many methods has been proposed to improve the health care system still it is in an early development stage due to its integration of small sensor devices with more advanced wireless communications technologies. In WBAN patient's health condition is monitored by sensor devices which is deployed in their body and transmit to medical personals to monitor the patient's conditions. It requires all sensor monitored information need to be effectively transmitted using appropriate wireless technology, data storage with Cloud server and data accessibly to appropriate medical personals. However interconnecting WBAN and Cloud requires some promising security measures to tolerate malicious attacks (Wang et al., (2009)). Moreover path loss may occur during data transmission when sensor information transferred is through frequently changing wireless environment to cloud server data base. This path loss occurs in both sensors to data gathering unit and wireless transmission to cloud (Zhang et al., (2007)). This will degrade the system performance with the inclusion of security and privacy measure in WBAN system. In most cases data encryption is a reasonable countermeasure to protect the sensor data, while some randomized authentication models are incorporated to validate the sensor data and accessibility at server side (Khan et al., (2012)). Here for providing robust cryptographic algorithms to ensure security of the WBAN system is often contradicting the basic system requirement of any typical WSN since all sensors need to run for several days or even years, without any manual interpretations.

The primary objective of this paper is to ensure the reliable communication for most sensitive bio information, cloud storage mechanism for WBAN technology and finally security and privacy of patient and medical personals. This paper includes complete processing steps involves in real time health care system. Here the limitations of WBAN systems over heterogeneous bio information monitoring also disclosed. This paper is organized as follows: section 2 reviews various WBAN health care systems and its distinguished feature metrics. Section 3 details the proposed security and privacy aspects against passive attacks. Section 4 provides an experimental results and parametric measures noted down during data exchanges. Finally section 5 concludes with future extension to improve WBAN performance measures.

2. RELATED WORKS

Several research works investigate the various issues in WBAN health care system such as network, scalability, QoS, data storage, security and privacy etc. The cloud-based secure healthcare system constitutes of several hierarchical processes which includes patient monitoring systems, cloud computing and key management and security. Al Ameen et al., (2012) analyze the cause and effects of privacy and security in WBAN health care applications. In (Javaid, Nadeem, et al., (2013) analyzed the influence of various path losses in WBAN system performance and its robustness to communication. Ali et al., (2013) developed cluster-based hybrid cryptographic measure to secure both intra-WBAN

- [1]Research Scholar,[2]Professor
- [1]KLEF Deemed to be University, Vaddeswaram, Guntur (Dt), A.P, INDIA
- Corresponding e-mail address:[1] chary60@gmail.com, [2] somu23@kluniversity

and inter-WBAN data transmissions. WBAN System proposed in [Rathee, Dheeraj, et al., (2014)] provides some comprehensive solutions to several issues using cognitive spectrum sensing based data communication with appropriate routing methodologies. Tewari et al., (2016) invented resource efficient and secure remote e-healthcare monitoring systems in WBAN using machine learning techniques. Here Antigen and antibody of every individual is used as a unique module to resist malicious attacks from external network. Khan, Farrukh Aslam, et al. (2017) developed optimized Markov model-based abnormality detection from ECG sensor details. Here the attributes extracted from the input ECG are used to generate feature set and based on probability of this feature set accumulation and associate changes abnormality detection mechanism is carried out. In this work initially we focuses on the security of WBAN communication using unique cipher conversion followed by privacy measure for cloud-based patients' medical data storage and accessibility. Saif et al., (2018) proposed Ebola infected patient monitoring using Radio Frequency Identification Device (RFID) sensor technology with cloud medical data storage. Here the close proximity interactions (CPIs) among different individuals are monitor to ensure the state of the outbreak. Bhardwaj et al., (2018) proposed hybrid autonomic resource provisioning method to regulate the cloud computing and queuing model. Here based on service level agreements (SLAs) given to patients the sensory data volume is adjusted according to the application's type. Sareen et al., (2018) used Advanced Encryption Standard (AES) to provide confidentiality, authenticity and security for cloud computing m-health application. And also the impact end-to-end propagation delay during data encryption over maximum permissible delay for medical application is experimentally analyzed.

3. QR PATERN BASED AUTHENTICATION AND ENCRYPTION APPROACHES

In this work, an integrated and fully automated authentication measures to provide security and privacy for cloud based data gathering and appropriate assessments by medical persons in health care monitoring system. It is carried out as three phases: 1) biometric-key generation based cipher conversion 2) QR pattern generation based authentication and 2) a selective pattern analyzes to validate and regulate the medical personal server assessment mechanism using a shared key. Figure 1 describes the secured WBAN health care system.

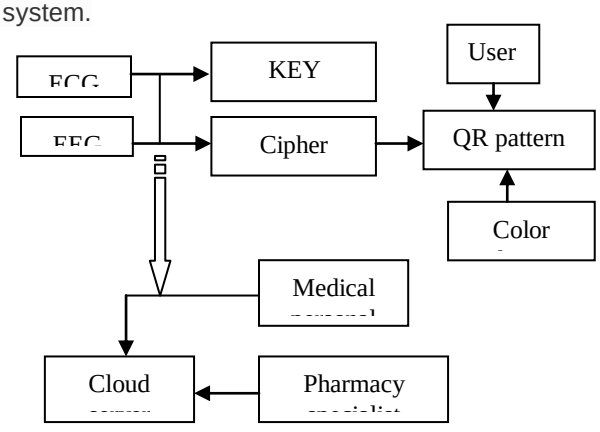
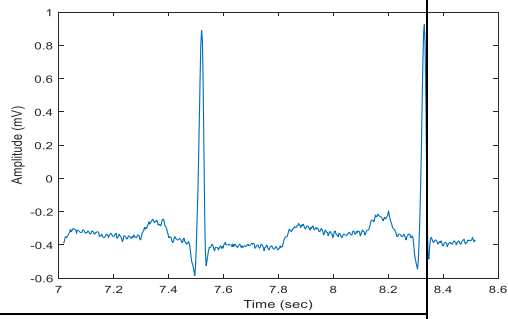
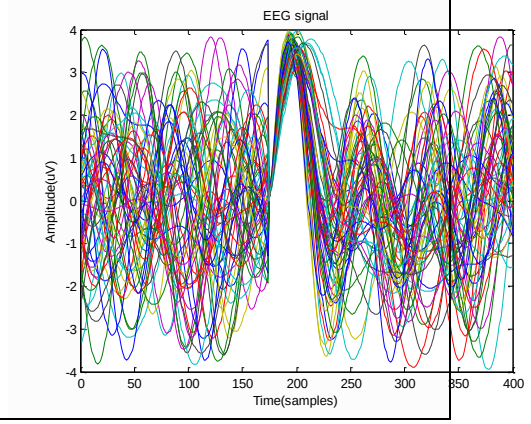


Figure 1: *Highly secured WBAN health care system*

3.1 Selective Encryption using Biometric Information

In this framework, keys are extracted from ECG measures as discussed in [x] to encrypt the features extracted from all three bio signal that also guarantee the acquisition of quality signals. It can provide better transformation compared to global key based ciphers since unique different keys are extracted from different heart beats. Here the level of transformation is depends on both the randomization of key sequence and the number of primitive blocks used in lightweight encryption model.

Table 1: *Input bio signal for WBAN health care system*

Bio signal type	Signal measures
ECG signal	
EEG signal	

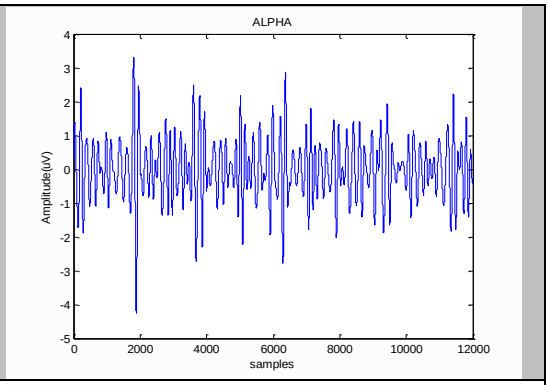
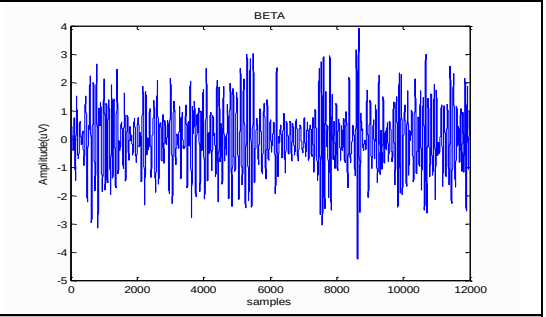
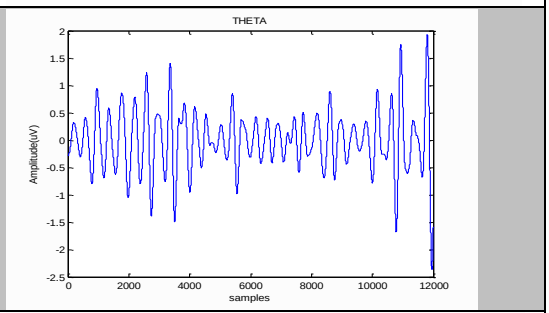
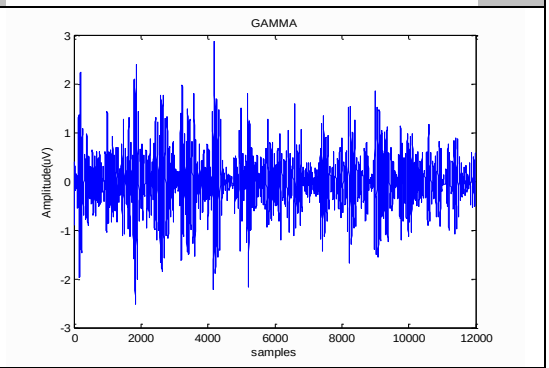
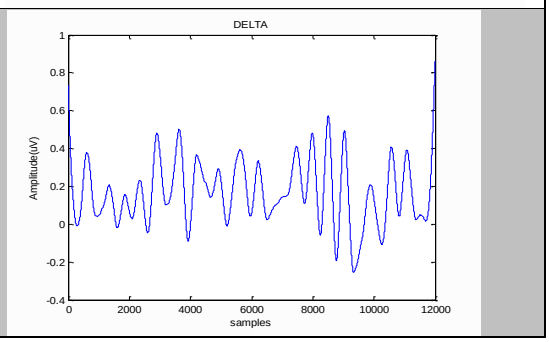
3.2 Wavelet pre-processed EEG signal

Here both ECG and EEG input signals are pre-processed as given in Eqn. (1) using wavelet transforms and redundant details are isolated as shown in table 1. This process helps to preserved R peaks of each ECG signal intervals to generate random binary sequence with succeeded concatenation and to classify the EEG signals into five different signal type according to its statistical frequency characteristics as shown in table 2.

$$W_s s(b) = \int_{+\infty}^{-\infty} f(t)\psi(\frac{t-b}{s})dt \quad (1)$$

Table 2: *Wavelet pre-processed EEG signal measure*

Signal type	Plot

Alpha signal	
Beta signal	
Theta signal	
Gamma signal	
Delta signal	

3.3 Cloud for data storage

In general WBAN system is directly related to human health, so sensor collected information should be made used to provide instant healthcare system, for that all these information should be access by concern medical personnel and physicians. Here data accessibility is provided through cloud server. The cloud based healthcare WBAN should mitigate the limitation of instant data accessibility, remote storage, and all other sensor relevant real time computational capabilities. In this open access system patient life will get into endangered if cloud server data is modified or malicious nodes send wrong details to cloud. To overcome this problem cloud based WBAN health care system should secure the patients' health information's.

Table 3: *color variant QR pattern for authentication*

Signal measures	QR pattern
ECG	
EEG	

Here the real time patient data is accesses by different individual according their key shared as unique QR patterns as shown in table 3. The range of accessibility is differs according their health condition needs of different medical personals like doctor, physician and nutritional analyst etc. at the remote location.

3.5 PERFORMANCE EVALUATION

In this experiment, we choose three different types of bio signals such as EEG, ECG and pulse signals for health care patient monitoring system to validate the pattern analyzes based authentication at the server side. In this case, based on statistical characteristics of bio signals parameters are extracted without using any pre-processing methodologies. The remote monitoring of the signal measures are done from the data stored and viewed on the Thingspeak IoT based Cloud Environment as shown in Fig.3. These validation results showed the superiority and authentication performance of our proposed pattern matching approach.

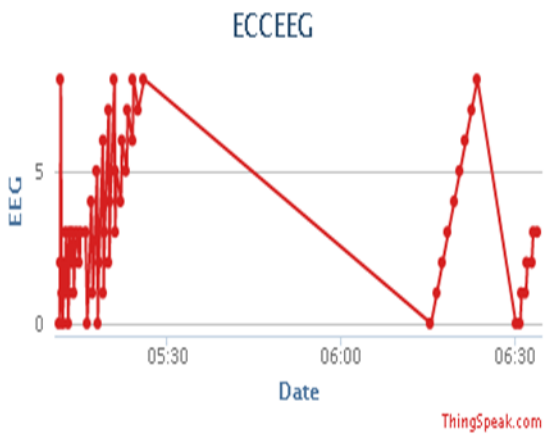


Figure 3. *WBAN reading on ThingSpeak IOT Cloud*

4 CONCLUSION

In this paper, we investigate the QR pattern analyzes based security framework that can protect the patient heath details which is stored in cloud server with least possible computational overheads by utilizing biometric information driven cryptographic measures. To authenticate and validate the sensor information's from each user, distinct patterns were generated for each sensor details with improved accuracy. The proposed framework extends the potential benefits of WBAN for integrating heterogeneous sensor details and provides optimal security and privacy in health care applications.

REFERENCES

[1]. Logan, Alexander G., et al. "Mobile phone–based remote patient monitoring system for management of hypertension in diabetic patients." American journal of hypertension 20.9 (2007): 942-948.

[2]. Suh, Myung-kyung, et al. "A remote patient monitoring system for congestive heart failure." Journal of medical systems 35.5 (2011): 1165-1179.

[3]. Wang, Song, and Jong-Tae Park. "Modeling and analysis of multi-type failures in wireless body area networks with semi-Markov model." IEEE Communications Letters 14.1 (2009): 6-8.

[4]. Zhang, Yue Ping, and Qiang Li. "Performance of UWB impulse radio with planar monopoles over on-human-body propagation channel for wireless body area networks." IEEE Transactions on Antennas and Propagation 55.10 (2007): 2907-2914.

[5]. Khan, Jamil Yusuf, et al. "Wireless body area network (WBAN) design techniques and performance evaluation." Journal of medical systems 36.3 (2012): 1441-1457.

[6]. Wang, Honggang, et al. "An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN)." 2011 IEEE international conference on communications (ICC). IEEE, 2011.

[7]. Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak. "Security and privacy issues in wireless sensor networks for healthcare applications." Journal of medical systems 36.1 (2012): 93-101.

[8]. Javaid, Nadeem, et al. "Ubiquitous healthcare in wireless body area networks-a survey." arXiv preprint arXiv:1303.2062 (2013).

[9]. Ali, Aftab, and Farrukh Aslam Khan. "Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications." EURASIP Journal on Wireless Communications and Networking 2013.1 (2013): 216.

[10]. Rathee, Dheeraj, et al. "Recent trends in Wireless Body Area Network (WBAN) research and cognition based adaptive WBAN architecture for healthcare." Health and Technology 4.3 (2014): 239-244.

[11]. Tewari, Anurag, and Prabhat Verma. "Security and privacy in E-healthcare monitoring with WBAN: A critical review." International Journal of Computer Applications 136.11 (2016).

[12]. Khan, Farrukh Aslam, et al. "A continuous change detection mechanism to identify anomalies in ECG signals for WBAN-based healthcare environments." IEEE Access 5 (2017): 13531-13544.

[13]. Saif, Sohail, Rajni Gupta, and Suparna Biswas. "Implementation of Cloud-Assisted Secure Data Transmission in WBAN for Healthcare Monitoring." Advanced Computational and Communication Paradigms. Springer, Singapore, 2018. 665-674.

[14]. Bhardwaj, Tushar, and Subhash Chander Sharma. "Cloud-WBAN: an experimental framework for cloud-enabled wireless body area network with efficient virtual resource utilization." Sustainable Computing: Informatics and Systems 20 (2018): 14-33.

[15]. Sareen, Sanjay, Sandeep K. Sood, and Sunil Kumar Gupta. "IoT-based cloud framework to control Ebola virus outbreak." Journal of Ambient Intelligence and Humanized Computing 9.3 (2018): 459-476.