Wireless sensor-based authentication of biometrics system for patient health care records

K Muthulakshmi[1] and T. Jayasankar[2]

[1]Professor/ ECE
Sri Krishna College of Technology
Coimbatore
kavi.neha@gmail.com

[2]Assistant Professor (Sr.Gr)
Department of ECE
University College of Engineering
BIT Campus, Anna University
Tiruchirappalli.
jayasankar27681@gmail.com

Abstract

The use of mobile phones in healthcare monitoring and delivery is growing rapidly. For their advanced computing functions, expanded preferences, and varied capabilities, they are sometimes compared to pocket computers. Mobile healthcare (m-health) based applications are made more practical and inventive by their sophisticated sensors and extensive software applications. Both patients and doctors have praised the systems' ease of use, portability, and efficacy in many contexts. In order to improve healthcare delivery, m-health technology makes use of cutting-edge ideas and methods from a variety of disciplines, including electrical engineering, computer science, biomedical engineering, and medicine. In this work, we focus on two crucial facets of modern healthcare sensor applications based on mobile phones. In telemedicine, the innovative and revolutionary, which has significantly limited and distributed communication components. As a visually appealing component of the telemedicine architecture, mHealth is crucial to protecting the privacy and safety of patients by including a variety of sensing technologies in the form of several in-built sensors. To protect patients' privacy when utilising mHealth, this research will focus on enhancing sensor-based defence and attack mechanisms. This study's objective was to develop a taxonomy, and it did so using a multi-level approach. Biometric identification technology plays an important part in protecting patients' personal information and medical records within the healthcare system. The primary objective of this research was to create a Hospital Management System (HMS) that uses fingerprint biometrics for user authentication. Using the Unified Modeling Language (UML) for design and Visual Basic.Net for development, Gellos HMS's primary features were created. The client programme connects to an Access database that stores patient information. To keep everything safe and secure, a combination of pin and biometrics was employed for authentication. Finally, the proposed RSS-based Integrated Secure Authentication (ISA) algorithm is used to accessed the classification accuracy of the model respectively.

Keywords: patient health care records, Integrated Secure Authentication, Wireless sensor, authentication.

DOI Number: 10.14704/nq.2022.20.11.NQ66099 **NeuroQuantology 2022; 20(11): 1039-1049**

1. Introduction

We use of Wireless communications has increased significantly intoday's world. Wireless Communication has a huge impact on all lives thanever before. As a result, a wireless network, a network in which sensors arelinked via wireless communication, has been created. Within WirelessNetwork, Wireless Sensor Network (WSN) is the most rapidly developingtechnology used for

eISSN 1303-5150

monitoring and recording conditions at various locations. n a WSN, a group of sensorscommunicate with each other via radio waves to monitor the physical andenvironmental conditions [1]. They differ from other networks by working in areal-time environment. WSN is used in military, sports and industrialapplications. As per the World Health Organization, chronic diseases, obesity,cardiovascular diseases and diabetes affect most of the world's population,while an aging population is another dominant problem. As a result, having acost-effective health monitoring system is important, particularly in countrieswith conventionally trained healthcare professionals and infrastructure [2].Although studies have shown that early diagnosis can reduce overall curecosts and improve quality of life, traditional healthcare systems fail to identifyand diagnose diseases early. Furthermore, diseases can be averted if thesigns and syndromes are identified early on. Furthermore, traditional systemsprimarily concentrated on medical applications, with little attention paid to non-medical applications.To overcome these challenges, we must concentrate on transformingexisting reactive healthcare systems into specialised healthcare systems thatprovide pervasive monitoring and are fairly priced. HealthCare's havetransferred from hospital to patient assertive services. Wireless Body AreaNetworks (WBANs) have been successful in providing ubiquitous healthmonitoring due to wearable or implantable sensor nodes [3], which usuallymonitor bio-signals. WBANs can transform people's integration of health andcommunication technology as society grows more health-conscious. As aresult, WBANs are ready to expand the desires of traditional healthcaresystems. In WBANs, technological advancements, proposed solutions, andmarketed goods nevertheless confront numerous challenges in theirimplementation. Rising healthcare expenses have pushed new technologicalenhancements to existing healthcare systems. Sensors, wearable systems,ow-power electronic devices, and wireless communication advancementshave laid the groundwork [4].

There are many applications of WBAN. It is used in the healthcare field,particularly for continuous monitoring of physiological data in patients with avariety of disorders, such as diabetics, asthmatics, and heart attacks.Healthcare is specifically meant for elderly persons and patients who sufferfrom chronic disease patients and need medical support at any time. Theother application of WBANs is the monitoring of a sportsman's body. Sensorson a patient give an alert to the hospital for detection and assessment of anychanges in the vital signs [5]. Sensors placed on a person to measure the sugarlevel is also capable of injecting insulin as soon as the sugar level decreases.BANs are likely to make their first appearance in the healthcare sector,particularly for constant monitoring and logging important indicators of patientswith chronic conditions including diabetes, asthma, and heart attacks [6]. Bymonitoring changes in their vital signs, a patient with a BAN can contact thehospital even before they experience a heart attack.Insulin could be auto-injected by a pump into a diabetic patient with aBAN as soon as their insulin level lowers. A BAN can be used to learn about adisease's underlying health status transitions and dynamics. Sports [7], military,and security are some of the other applications of this technology. Extendingthe knowledge to additional domains could also help communication byallowing for unified information flows between people or between peopleand machines.The data collected by the Biosensors can be shared with the nodes thatare connected to them. The energy and memory of these biosensors arelimited.

eISSN 1303-5150

WBAN is essential due to the emerging demands of medicalequipment. Although the potential applications are on the increase, then thesecurity requirements remain unresolved [8-10]. The main issue with WBANreception is ensuring the wireless channel's security and privacy.

Figure 1. Name-and palm-based biometric procedure

2. This user model is a one-of-a-kind, extremely abstract representation of the images that cannot be converted back to the original photos by any means. Core security is ensured by the immediate and permanent removal of the seven images captured during enrollment after the user model is created. The Element system only needs a single picture of a person's palm to determine who they are, which brings us to step two: identification. At this stage, a captured image's one-dimensional vector is compared to the user model; if there is a strong correlation, a match is reported. The Element system then shows the user the taken image (Figure 1) once the image has been processed.

3. Literature review

. In this survey, many authors have tried to exploit the characteristicsof BSN, their applications and architecture, usage of cloud in BSN solutions,security, and mining algorithms related to healthcare. This thesis tries tooutline some of the highlights of the relevant work in this area. A collectionof tools and a variety of algorithms were designed to protect the data such assymmetric, asymmetric and hybrid cryptographic approaches to provide the patient's data security.Wireless sensor networks are the subject of extensive study for potential use in medical settings. The most difficult problems involve BSN architecture, safe data collecting and storage, and healthcare data administration. Because of advances in diagnostics, a mountain of data is being produced. Increases in the volume of sensitive data created by medical sensor networks present numerous difficulties, including issues of scalability, availability, and security. Different security concerns, including those related to privacy, authentication, and performance of algorithms, have been the subject of extensive research.. Hence this intensive survey has helped to design a betterarchitecture for data collection and storage with energy efficiency and asecure authentication algorithm to access the stored data also an intelligentdata management system.

J. Lee et al. [11] fabricated a patch. Long-term HRV assessmentcan be done using the patch's filtering, Analog to digital converter, anddetection of 'R' peaks in ECG signals. 'R' peak detection using the fabricateddevice is measured and calibrated under various conditions of the patients likemental stress, patients were tested and the walking speed of a 5 km/hr patientis tested. The results obtained are sensitivity and very less error. To verify thedevice, the standard MIT-BIH database ECG samples are used as an input

eISSN 1303-5150

tothe device. The algorithm developed is based on the automatic gain control(AGC) and indigenous threshold of the maximum amplitude.

For remote body territory systems, Liu et al. [12] suggested anenergy-efficient and small-area ECG signal data acquisition and signalassessment application sensor node. With high frequency noise removed,these sensor nodes can precisely capture and distinguish the QRS waves ofan ECG waveform. The system made use of CMOS (Complementary MetalOxide Semiconductor) technology, with an area of 0.18m. It has also followedtwo chips, one for analogue front-end ICs and the other for ApplicationParticular Integrated Circuits (ASICs) for specific digital applications. Theanalogue IC consumes 79.6 Watts of power and 4.252 square millimetre,while the digital ASIC utilises9 m at 32KHz with 1.2 square millimetre. ThisECG sensor hub is ideal for continuous supervising of a patient'scardiovascular status and is ideal

Chakraborty, [13]detailed Discrete Wavelet Transform (DWT) to represent P -QRS-T wave. Anoise-suppressed signal is subjected to the pan and Tompkins algorithm fordetecting QRS complex waves after being de-noised using the MIT-BIHcardiac arrhythmia database's ECG signal values. For one complete cardiaccycle, the 200 samples of QRS wave are detected then the 100 samples onthe right and 99 samples in the left.one being in the middle is the reference tocalculate the heartbeat. The 110,094 beats are detected using the standardECG database. The DWT is used to filter out the noise using FIR filters andthe Meyer Wavelet Transform (MWT). The 3-dimensionality reductionmethods are used to minimise the dimensions of DWT coefficients, lineardiscrimination assessment (LDA). PCA works on a direct dimensionalitydecrease system that looks for projection of the information into the directionsof more inconsistency. The comparison of ECG beats through MIT-BIH cardiac arrhythmia database for different researchers is tabulated and its accuracy is checked; this paper shows the performance results of accuracy,specificity and sensitivity 99.28%, 99.83% and 97.97% respectively.

Mirania, [14] proposed to minimize the computational cost inthe ECG signal processing by using the multirate signal processing ascompared with the conventional digital filtering with the MATLAB simulationtool multirate signal processing is used to separate the slow periodic signals inthe heart arrhythmia in the real time environment. Down sampling multiratestructure is designed to reduce the aliasing and the length of the filter.in an improved bio-signal (ECG) cryptography approach (Mathivanan,Balaji Ganesh, and Venkatesan 2019; T. Dimitriou and Krontiris, n.d.; Gadeaet al. 2019). To construct appropriate binary pair series that are transformedas corresponding ciphertext data, the bio-signal encryption procedure treatsECG samples as integers. To provide even more security, the resultingciphertexts are then converted into QR codes through a QR codegenerator/reader. For all the binary pair that are utilised for signal decryption,the encryption approach generates a binary key. On average, the PSNR wasabove 42 dB, but the PRD was less than 3.43 percent. It is furtherdemonstrated that employing only seven QR codes, the suggested techniquecan encrypt a maximum of 226 kb of diagnostic data.

Priority considerations to mental health careprovision and broad application to mHealth were identified as the two main areas of high-priority mHealth technology development considerations in a study of mHealth technologies published in [15]. The National Center for Telehealth and Technology, the United States Army Medical Research and Material Command, and the

eISSN 1303-5150

Telemedicine were all included in this analysis as well.

Yvette [16]absorbed on the integration of BAN deviceand Android smart phone Apps for ubiquitous healthcare monitoring system.Increased efficiency, accuracy of medical treatment are theadvantages of ubiquitous healthcare which is a promising technology. Itprovides better services to both the patient and medical staff, easy to diagnosehealth conditions, monitoring the health without visiting the hospital with thehelp of information and communication technologies and by not consideringlocation and time. The raw data collected from wearable device is sent tothe physician in charge for the particular patient and also it is encoded toAndroid apps and it will procedure and monitored in real-time. Then the healthstatus is presented to the patient, and he reacts accordingly. If the health statusis serious, the emergency call feature is also available in the system.

4. Problem Statement

These drawbacks motivated us to come up with an efficientcryptographic algorithm to secure the medical data. In this research a protocolis attempted to resolve the security and privacy issues. It establishes abiometric based security solution for protecting wireless transmission withinWBAN. In any encryption scheme, the message is encrypted with a secret keyfor providing security. An encryption scheme is included in this protocol byextracting biometric feature as a secret key for communication within WBAN.The secret key for security is derived from the physiological value measuredby the body sensors. The physiological signals measured by the body sensorsinclude ECG, EMG, blood pressure and oxygen saturation. The physiologicalvalue chosen for such a security solution must be distinctive. That is to say,1) The measured value should be different for any two individuals and thesame within an individual's2) The value ought to vary with respect to time and must show a high degreeof randomness.

5. HE PROPOSED ARCHITECTURE

Today any kind of communication is done via Internet. It is playing avital role in day-to-day life. Cloud is an emerging technology mainly used forstoring, sharing and accessing the information of various applications. Theinformation stored in the cloud may be either sensitive or non-sensitive. Securityis an essential parameter for the network-based applications, especially whenhandling with the sensitive data like patient's personal health information.Body sensor networks are mainly used in health care monitoring,and the collected data from the sensors are stored in the cloud for globalaccess.. Even thoughthere are techniques to evaluate the security, one needs an efficient and cost-effective technique to handle the sensitive information.

eISSN 1303-5150

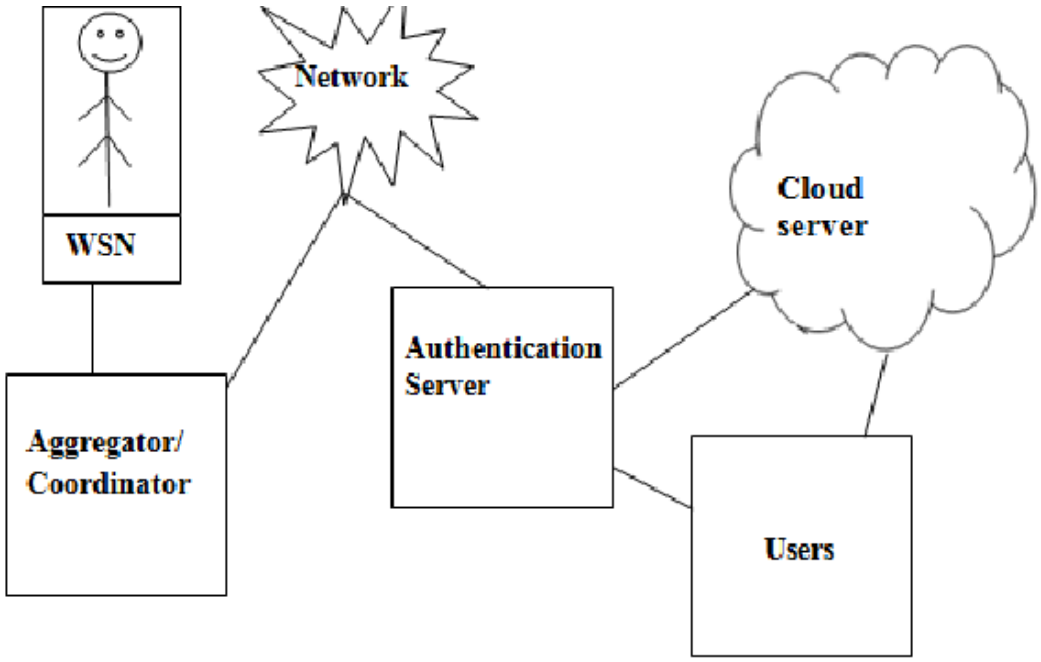

Figure 2: Cloud-based BSN Architecture

The suggested system comprises two stages: the first is the collection phase, and the second is the retrieval phase. The proposed RSS-based Integrated Secure Authentication (ISA) technique is utilised in both to ensure the data are kept and accessed safely. Different studies are conducted to address the sensitive and private issues.

Data Confidentiality)

Maintaining data secrecy requires taking measures to prevent unauthorised or accidental disclosure, as well as safeguarding data while transmitted across networks. It's crucial that we address this problem head-on so that vital patient data can be shared with nearby or external networks. Data confidentiality of patient and its private or personal data can be obtained through a communication channel using a shared secret key and security methods.

Data Authenticity)

Authentication has significant meaning in fields outside of medicine as well. Active nodes in a communication chain have verified their identification. Coordinator and participating nodes need confirmation during transmission that data is going to a trusted destination and not an intruder who may use it for malicious purposes.

6. INTEGRATED SECURE AUTHENTICATION

Spatial information a physical attribute associated with each node that is difficult to manipulate and not based on cryptography, is proposed here for use in Integrated Secure Authentication (ISA) in cloud-based e-health care applications. Like the Authentication server, the Tri Mode Algorithm is introduced to ensure the safety of data storage and fully authenticated data sharing. SetUP, CheckUP, and LockUP are the stages at which the algorithm can be implemented. Both analytical and simulated results show that the suggested strategy is superior to the current method in terms of security, efficiency, and simplicity.

Data Collection Phase

All the body sensor nodes need to be secured in a way such thatprivacy of medical data is assured, and medical personnel can unconditionallytrust the data these nodes generate. The security and trust of a sensor devicesis important, otherwise the wrong decisions about the medicine will affect thelife of the patient. So the best authentication method is needed for avoidinghe spoofing attacks and data modification. In data collection

eISSN 1303-5150

phase,authentication of the sensor nodes is verified by the coordinator node whichcontains the details about sensor node's RSS values and identifier value(MAC address).The ISA algorithm uses the combination of MAC address andRSS value for the verification. All the sensors are present inthe patient body and the RSS value collected from the node also not changedunder the assumption of static location and transmitting power. So spoofingcan be easily identified. Even the MAC address is spoofed the RSS value willnot be matched or spoofed

Training and classification on sensor data.

- Initially train the sensor data vector on normal case and low case.
- Then, classify the query patient information using classification process.
- The classification result and high pressure case is trained.
- Finally, classify the query pressure vector using SVM training.The above training and classification process is done for the pulserate and respiratory rate.

7. MPLEMENTATION STEPS

The prediction model isimplemented by the following steps.

A. Creating patient database.
B. New patient registration.
C. Sensor data generation.
D. User Query report.
E. Training process.
F. Query testing vector.
G. Testing Process with knowledge.

New patient registration

Every new patient should need to register their details to thedatabase and he/ she should submit the details with Patient Name, PatientID(provided), age, Gender , Date of admission and the Patient address and itis updated in the database**.**

C. Sensor data generation

After registering the patient details, sensor data are generated fromvarious sensor types and stored in the sensor data table. The sensor data tablecontains the patient id, date and time of generation, sensor type (pressure,pulse, respiratory) and its value. Sensor data is collected from the patientevery second. The sensor data is often generated for every new entry or any
registration of new patient.

8. Experiments And Performance Analysis

The Matlab programming language is used to realise this project. MATLAB stands for "Matrix Laboratory," and it's a fourth-generation programming language that supports multiple numerical computing paradigms. MathWorks' MATLAB is a programming environment that facilitates operations on matrices, the application of algorithms, the creation of user interfaces, the graphing of functions and data, and the interfacing with programmes written in other languages including C, C++, Java, and Python. Experimental comparisons of classification algorithms are made using metrics of performance that reflect how well they perform in terms of classification accuracy. One of the most important areas of application for which precision is essential is medical mining. The sensor dataset has been classified in this study.

Accuracy:

Accuracy in classifying data is measured as the percentage of observations that fit a predetermined template.

eISSN 1303-5150

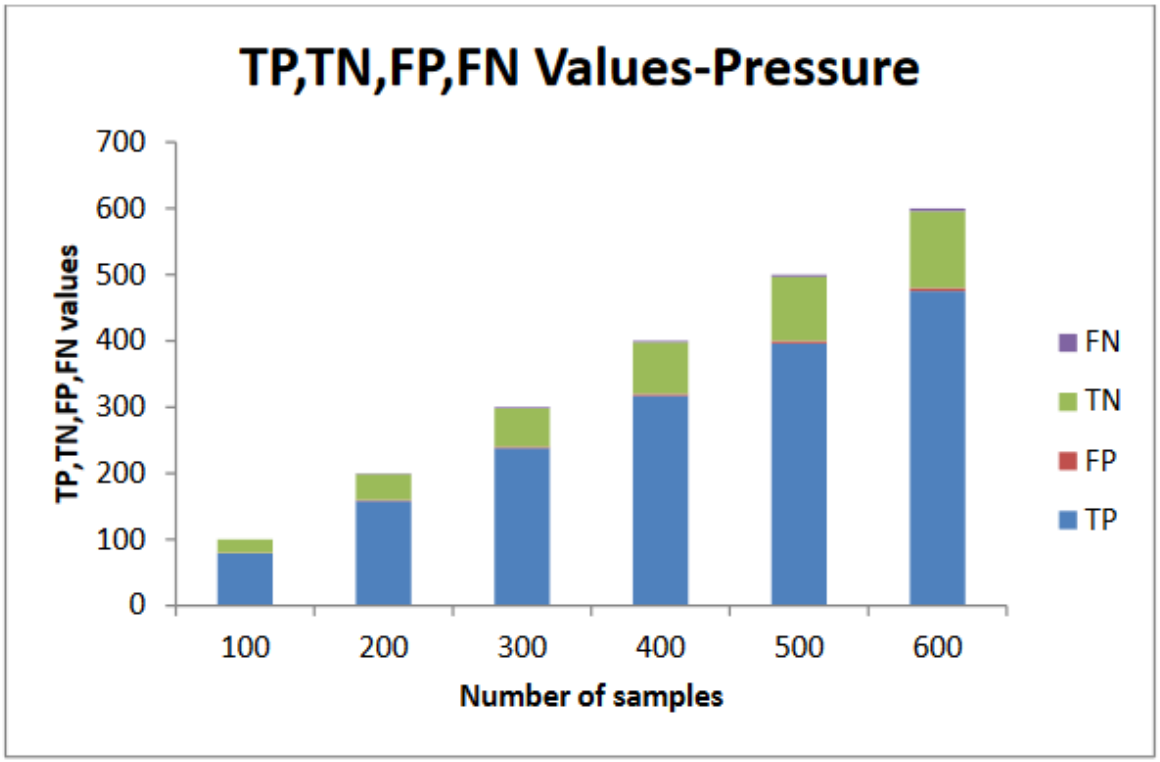

Figure 3: TP, TN, FP, FN values for Pressure data set

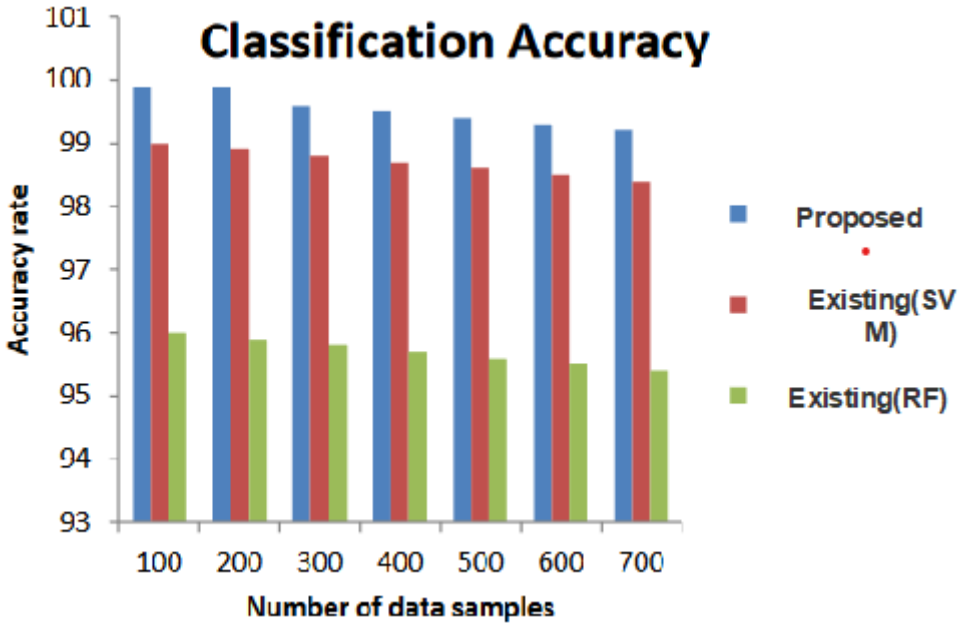

Figure 4: Classification Accuracy

eISSN 1303-5150

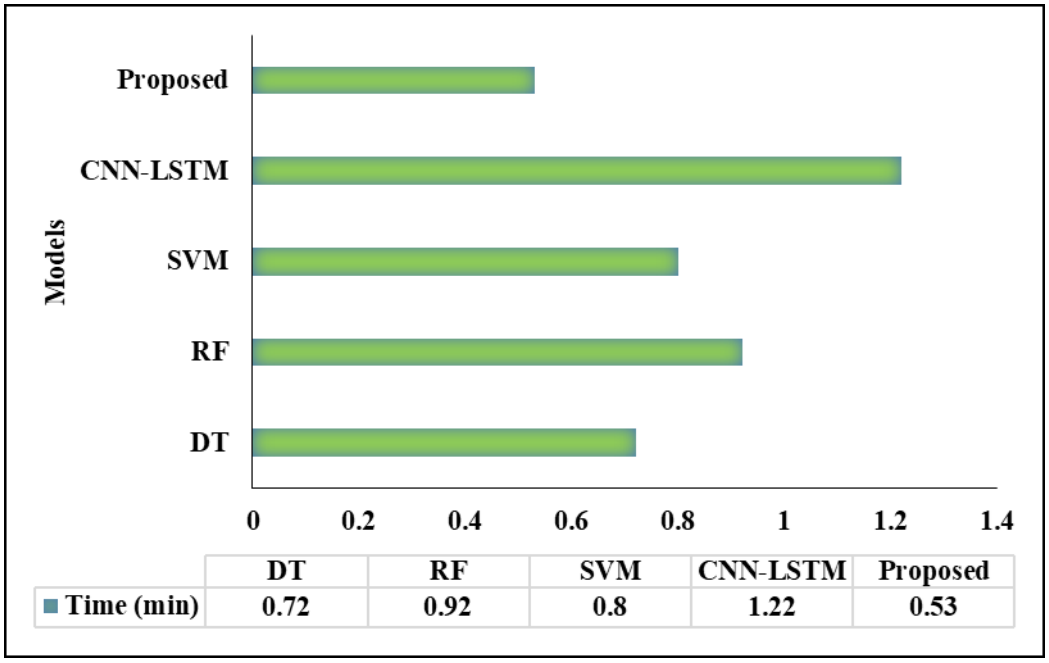

figure 5: represent that the time Comparison.

In the figure 5 represent that the time Comparison. In this comparisons analysis there are different methods are used as DT, RF, SVM, CNN-LSTM and the Proposed model. In this comparisons analysis the proposed take the lowest time period than other compared methods

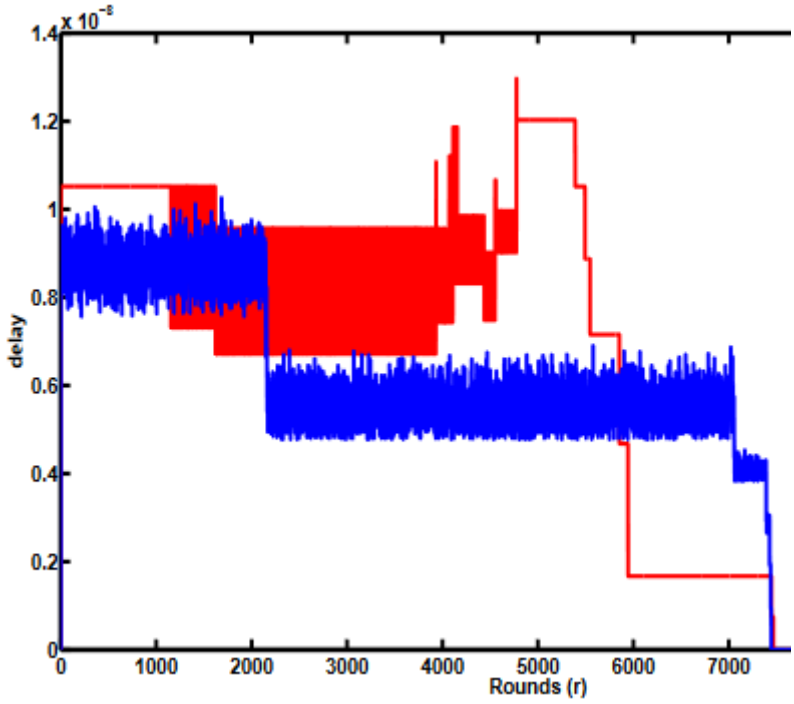

Figure 6: Network Path Loss Delay

As seen in Figure 6, signal attenuation, in decibels, is represented by route loss (dB). Additive White Gaussian Noise (AWGN) [171] also reduces signal strength. The difference between the signal's sent and received strengths is called "path loss," while antenna gain is optional. Because the wave front's surface area has grown, path loss has resulted. The power emitted by a transmitting antenna is lost if any impediment stands between the source and the receiver. In WBSN, the broadcast signal is affected by factors such as the human body, hands, and clothing.

eISSN 1303-5150

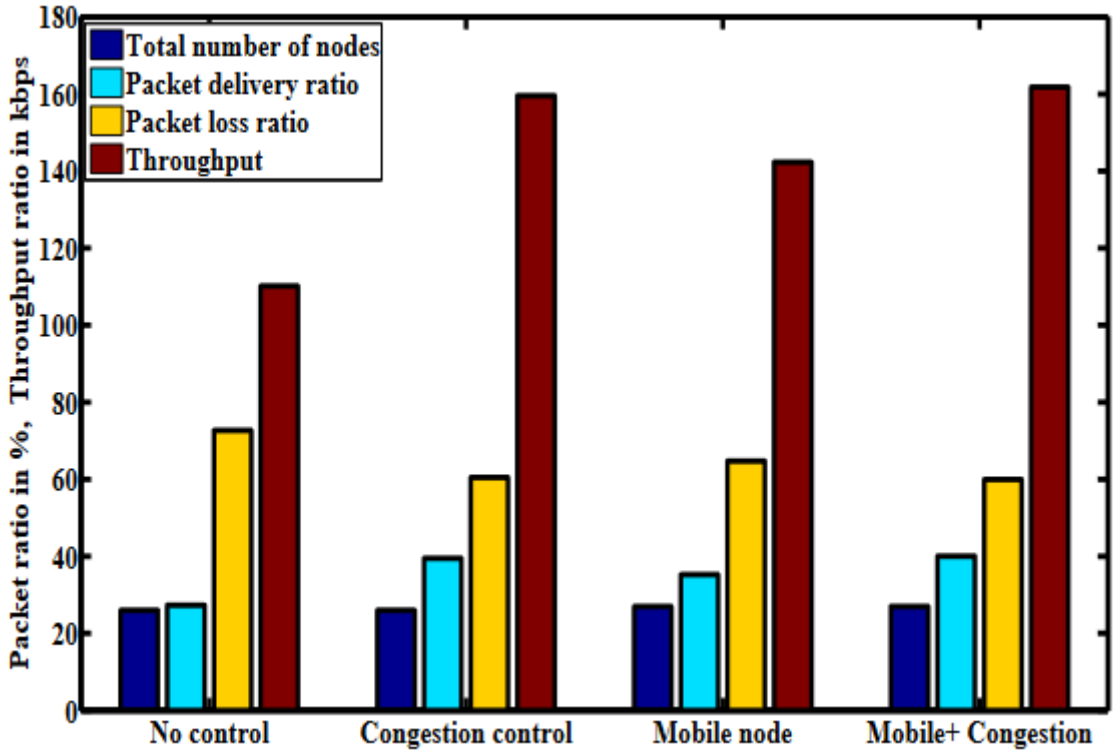

Figure 7: PDR, PLR, Throughput for 4 Distinct Test Cases

Figure 6 provides more detail for these four scenarios. In congestion-controlled circumstances, the PDR is at its highest. Better PDR is achieved in scenarios with movable nodes compared to those without them. When PLR rises, PDR falls, as depicted by the worldwide scenario. When used in tandem, the congestion control mechanism and the mobile node increase the network's throughput in the considered circumstances..

9. Summary of the Work

The benefit of this system lies in the reduction of the expenses neededfor monitoring the patients in hospitals, since this can be done by staying athome. The provision of security and privacy for patient data is a problem in theWBAN system's acceptability. The confidentiality and integrity of theinformation communicated between the sensors should be protected.The information gathered by the biosensors is sent to a cloud storage service, where the classification of the data is checked classification algorithm, the patient's condition is determined, and either medication is prescribed or a wireless alert message is sent to the doctor if the situation is critical.We have purposed more efficient for acquiring security also the proposed RSS-based Integrated Secure Authentication (ISA) algorithm is used to accessed the classification accuracy of the model respectively.Because of the lack of opportunities for replay eavesdropping and other attacks and threats that undermine system security when using algorithms with small keys, biometric frameworks are more secure. In the future, key generation methods could be implemented on nodes of WBANs, and researchers could look into an efficient implementation of authorization, non-repudiation, and integrity to enable secured communication in WBANs.Further investigation would include the reduction of the time of IPI extraction,implementation of the encoding method for generation random BSs, and alsodifferent extraction methods or extraction of features from othercardiovascular signals

eISSN 1303-5150

Reference

[1] Jhaveri H. and D. Sanghavi (2014). Biometric security system and itsapplications in healthcare. International Journal of Technical Research andApplications.

[2] 32) Raja Krishnamoorthy, T.Jayasankar, S.Shanthi,M.Kavitha,C.Bharatiraja, "Design and implementation of power efficient image compressor for WSN systems," Materials Today: Proceedings, vol.45, part 2, 2021,pp.1934-1938,ISSN: 2214-7853

[3] Cheng, X. R., M. X. Li. (2013). The authentication of the grid monitoringsystem for wireless sensor networks, PrzElektrotechniczn.

[4] Darrell S.(2013). Biometrics – Implementing into the healthcare industryincreases the security for the doctors, nurses, and patients", thesis for mastersdegree information assurance.

[5] 12) Dr.K.Muthumayil, Dr.M.Buvana and Dr.T.Jayasankar "Optimization Technique For Enhance the Energy and Network Lifetime of WSN", International Journal of Modern Agriculture, Volume 10, No.2, 2021, pp.1657-1664

[6] ManimekalaiS.(2014). Study on Biometric for Single Sign on Health CareSecurity. International Journal of Computer Science and Mobile Computing,Vol.3 Issue.6, June, pg. 79-87.

[7] . Diaz-palacios, J. R., V. J. Romo-Aledo and A. H. Chinaei (2013). BiometricAccess Control for e-Health Records in Pre-hospital Care. EDBT/ICDT,March 18-22, Genoa, Italy.

[8] 26) Raja Krishnamoorthy, D.Venugopal, M.Sujatha, Sudhakar Sengan, C.Bharatiraja, T.Jayasankar "Hardware design of real-valued NSCT transform for biomedical video compression" Materials Today: Proceedings, vol.45, part 2, 2021, pp.2139-2144, ISSN: 2292-2197

[9] Esam, O. A., S. M. Ngwira and T. Zuva (2014). Biometric authenticationsystem to protect sensitive medical data. Bimodal Biometrics for Health CareInfrastructure Security. Proceedings of the International Multi Conference ofEngineers and Computer Scientists Vol I, IMECS, March 12 - 14,2014, Hong Kong

[10] He, C.S. Bao and Y. Li (2013). A Novel Tri-Factor Mutual Authenticationwith Biometrics for Wireless Body Sensor Networks In HealthcareApplications. International Journal on Smart Sensing and Intelligent SystemsVol. 6, No. 3, June. PP. 910-931.

[11] Le DT, Uram JN, Wang H, Bartlett BR, Kemberling H, Eyring AD, Skora AD, Luber BS, Azad NS, Laheru D, Biedrzycki B. PD-1 blockade in tumors with mismatch-repair deficiency. New England Journal of Medicine. 2015 Jun 25;372(26):2509-20.

[12] Gong J, Liu Y, Chen W. Land suitability evaluation for development using a matter-element model: A case study in Zengcheng, Guangzhou, China. Land Use Policy. 2012 Apr 1;29(2):464-72.

[13] Zhou, W., 2012. Targeting G-quadruplex DNA in promoters of cardiac function-related genes.

[14] Mirania, S.K., Mehra, R. and Pal, G.P., 2015, October. Reducing computational cost of ECG signal using multirate signal processing. In 2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI) (pp. 51-56). IEEE.

[15] Hussain, M. et al., The landscape of research on smartphone med-ical apps: Coherent taxonomy, motivations, open challenges and recommendations. Comput. Methods Prog. Biomed. 122(3):393–408, 2015.

[16] Yvette E Gelogo&Haeng-Kon Kim 2015, 'Integration of Wearable Monitoring Device and Android Smartphone Apps for u-Healthcare Monitoring System', International Journal of Software Engineering & its Applications, vol. 9, no. 4, pp. 195-202