ISSN: 0974-5823 Vol. 6 No. 3 October-December, 2021

International Journal of Mechanical Engineering

FINGERPRINT ACCESS CONTROL FORE-HEALTH RECORDSINHOSPITALS

B. Nivedetha
Faculty, EEE, PSG College of Technology, Coimbatore.

V.Deekshitha
UG Student, EEE, PSG College of Technology, Coimbatore.

M. Harini
UG Student, EEE, PSG College of Technology, Coimbatore.

K.Shalini
UG Student, EEE, PSG College of Technology, Coimbatore.

ABSTRACT

In most of the hospitals, patients medicalrecordsare maintained in traditional methods as large paper files and documents.Technologicaladvancementsareevolvingrapidlyandimprovingthequalityoflifesubstantially.OneoftheadvancementsisElectronicMedicalRecords [6].AnElectronic Health Record is the systematizedcollectionofa patientshealthinformationwhichiselectronicallystorediнadigitalformat.E-HealthRecordscanimprove the kinship between the patientsanddoctors.Identifyingapersonusing thebiometriccharacteristicisanecessary method to increase the security.Though there aremanybiometricfeatures available for authentication,fingerprintisused because it is morepracticalone to capture.Theuseofbiometricsforidentificationhasamajorroleinsustaining the privacy and security [8] of the healthcaresystem.Efficiencyandsecuredaccessofthepatients healthrecordisrequiredtoprescribemedicine.Thepaper proposes to develop a health recordmanagementsystemwithfingerprintbiometricsandloginwithpasswordsforauthentication.Boththefront endand backend is done using MATLAB. ToconnectthedatabasewithMATLAB,PostgreSQLisused.Theproposedworkincludes retrieval of patient's data fromthehealth records of the hospital database whenthe fingerprint is matched and the creation of aloginportal forauthentication.

Keywords:
Fingerprintrecognition,electronichealthrecord,MATLAB

1. INTRODUCTION

On a daily basis, millions of patients visitdoctorsinhospitalsandotherhealthcareclinics [9]. Each of these visits increases the new medical record or modify theexisting record.Forstoringandretrievingof records, a user authentication technology isrequired.Patientsshouldhavethe assurance that the privacy of their recordswill be well kept safe. And for that purpose,theE-HealthRecord(EHR)managementsystemiscreatedwhichis accessedwithbiometricstoprovidesecurity forpatientsand healthcare professionals.

This system isproposedtoreducethelargepaperworkinhospitalsandtoaddressthedeficitofhealthcare staff. Both physicians and patientshave to trust and rely on the data which may be complete,accurate,and secure.The use of technology for enhancing healthcareserviceshasreceivedsignificantoutcomes in recent years. Due to digitization of healthrecords, quality of patientcarewill increase along with large efficiency.Asmoreandmorehospitalsandhealthcare systems migrate to computerizedelectronichealthrecords,morehealthinformat

ionexchangesarebuilttocoordinatecare across networks and with effective datamanagement to ensure it is kept free fromcorruption,modification,orunauthorizedaccess.

Biometricsplaysamajorroleinthissystemasitisthei dentificationofanindividualbasedonfeature they have.Biometricrecognition is necessary asidentityof an individual cannotbedistributedorlost and itcreate a really powerfultoolin identitymanagement. The issue of security is often a concernwhen it comes to the confidentiality of medicalinformation.Herethefingerprintsofthepatientsareu sedtoprovideaccesstousetheirmedicalrecords.It isapatternrecognition system that recognizes a personby his or herfingerprint.Passwordsandpinauthenticationareusedtose curethecomputersystemsfromunauthorizedaccesssinceinc ompleteormisunderstoodhealthcarerecordscanleadtowron gmedications andcomplexities.

2. LITERATUREREVIEW

Therearevariousmethodstoaccesselectronic health records in hospitals. Identificationcardsorsmartcardscanbegivenasproposedby Hinkamp[3],whichstores the information regarding the patient.The information can be retrieved by a servernetworkanddisplayedonascreen.Thismethodprovide sagoodsolutionforreal-timeaccess to emergencies while thedifficulty in using this approach is that thepatient should always carry the identificationcard or smart card while vising the hospital.Thismakestheapproachunfeasibleforthe healthsystem.

Microsoft Health Vault and former GoogleHealth[2]providespacetostoremedicalinformation for any registereduser. Thesewebservicesareeffectiveinstoringinformation.Itdepe ndsonthepatientscredentials, such as username and password.But this approach will become unsuitable ifthepatientforgetssuchcredentialsorisunabletoprovidesuc hinformationinagivensituation.

Theotherapproachesrequiresmartphonesasdescri bedbyGardneretal.[4]. Thepatientwhoentersthehospitalcarriesthehealthrecordsin hissmartphone.Thepatientcan access the records by providing the rightcombinationofpasswordsor biometrics.Anothermethodisusingcontact-lessfingerprintsensorsandfacerecognitionsystems[1]. This method uses a secure, touch-lessdata acquirement from the distancetoreducetheriskof impersonation or fraud. This method alsoreducestheriskofuserscontractinginfections. Butthereissignificantexpenseinvolvedinthe implementationofthesesensors.

3. PROPOSEDWORK

Thissectiondealswiththemodelofoursystemandth eprocessofextractionandthinningoffingerprints.Theotherd etailsandarchitecture of the system will be explainedinthesubsequent sections.Our main objective is to provide paperlessconsultationandcheck-upswithhighefficiency and privacy preserved access tothe medical health records of patients.Wematched the fingerprint in order to providepermission to retrieve the patient's records,which ensures no record mix up takes place.We aimed to provide a centralized databaseaccessthatcanbeusedbyanyhospitals,pharmacies, scanningcentersandtestlaboratories. The system design of EHRis intheFigure1.

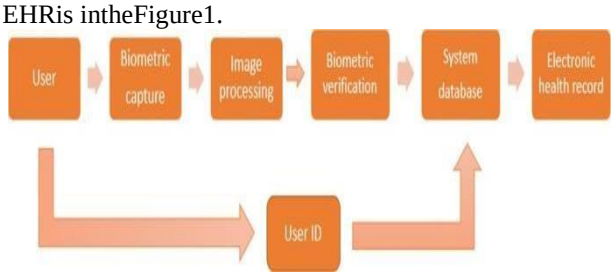

Fig1:System designof EHR

3.1 Userapproachingthesystem

The user is the patient who has come to visitthe hospital in order to treat the ailments ormay be for a normal check-up. He or Sheneed not bring any files or test reports ormedicalprescriptionsofthepreviousvisitsasalltheinforma tionrightfromthediagnosistotreatmenttomedicinesprescrib edwillbestoredintherecords.Thisprovidesthepatientsa hassle-freeenvironment.

3.2 Biometriccapture

Firstthebiometricsampleoftheindividualisloadedi nthedatabase.Whenthepatientwantstoaccessthehealthreco rd,thefingerprintisgivenasinputimage.Fingerprints are obtained by the replication of a fingertipepidermis,whenafinger gets contact withthesmoothsurface.Afterthistheunique features are then extracted from thebiometricsampletocreatetheusersbiometrictemplate [7].

3.3 Imageprocessing

The fingerprintimageof the individualisconverted into a template. The system remembersthetheminutiaeinformationlike itslocation,direction, and users demographicdata as a template in the enrollmentdatabase.

3.4 Biometricverification

The newly formed template is compared withthestored templateand matching is found based on themaximummatchofminutiapoints.Thebiometricverificat ionisdonebythematchingofminutiapointsextractedfromthe inputfingerprintwiththeminutiapointsofalreadystoredfing erprint.

3.5 Storagedatabase

The fingerprints are stored in a folder and itslocation is stored by a name in the database.InordertoaccesstheE-HealthRecords,ifthefingerprintsdonotmatchafterfingerprintverification,wehavecreatedalogindialoguebox where the user has to provide his or heruserIDandpassword.Thegivendetailsshouldmatchwitht hedetailsinthedatabase.Only then the records can be viewed. Weadopted this approach in order to maintainconfidentialityofdataandtoavoiddatathefts.Theda tabaseinexcelformatisshowninfigure2.

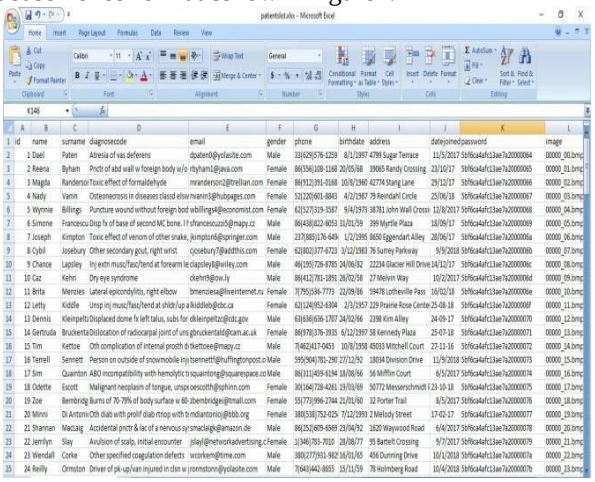

Fig2: Database inexcelformat

3.6 Electronichealthrecords (EHR)

The E-Health Records are the digital recordsof the clinical data up to date of the patientalong with the medical history. It containsName,Diagnoses,E-Mail,Gender,Phonenumber, Date of Birth, Address, Date joinedand Password. Every time the patient visitsthe hospital, the entire information will beupdated. This makes the work of the patientaswellas functioningof hospitals easy.

4. IMPLEMENTATION

Asstatedinsection3.2ourtechniqueinvolvesfinger printextraction,fingerprintmatching and data retrieval which has beenimplementedusingMatlab [5]and PostgreSQL.Fingerprints are peculiar patterns made ofridgesandfurrows, which can be seen on all fingers. All people have unique fingerprint and they cannot be same even for identical twins.The fingerprints identificationis used in almost all areaslike background checking, security access, during disaster determination, and criminal offenses. The two important featuresoffingerprint are its uniqueness and existence. In addition, each person's fingerprints remainunchangedintheir entire lifespan. The new skin cells formed gets blendedwith the existingfurrow pattern and friction ridge.

4.1 Ridgepatterns

Friction ridges are classified into three types as shown in figure 3. Loops, whorls, and arches are with incomparable variations, depending on the shape and relationship of the ridges.

Fig 3: Loop, Whorl & Arch of afingerprint

4.2 Thinningoftheimage

During thinning process, width of the ridges are reduced to one pixel which helps in extracting minutiaepointsfrombinaryimages.Thepixelwisecomputati onoffingerprintimageisshowninfigure4.

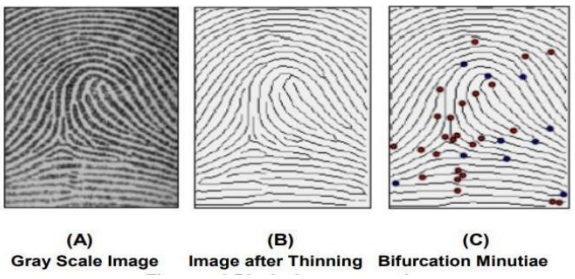

Fig 4:Pixel wise computation

Fingerprintthinningisthetechniqueofreducingthet hicknessofeveryridgepatterntoasinglepixelwidth.Afterextr actingtheminutiaefromtheimproved,binarizedandthinnedi magepost processing is carried out on this image to remove falseminutiae.Theinputfingerprintimageandthinnedfinger print images we obtained are shown infigures5 and 6respectively.

Fig5: InputFingerprint Image

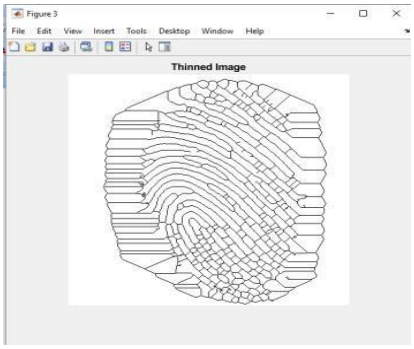

Fig6:Outputimageafter Thinning

4.3 Minutiaeextraction

This is the most popular and widely usedtechnique, being the basis of the fingerprintcomparison. Minutiae are extracted from both fingers and are stored as sets of pointsinthe2Dplane.Then matchingis done among the templateandinputminutiaeto identify maximum quantity of minutiae pairings. TheMinutiaecomparisonisbased onloop, whorl or arch forinitialcomparisonsandfurtheranalysis.

An investigatorofacrimescenefirstgatherfingerprints from the crime sceneand compare the printsside byside with the known fingerprint databaseto identify a match.Generally,fingerprintof good quality willcontain40–100 minutiae points. The figure 7 showsthefingerprintimageafterminutiaeextraction.

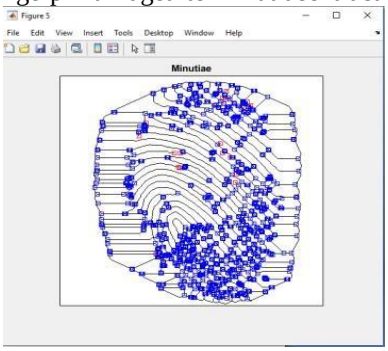

Fig 7: Output image after MinutiaeExtraction

4.4 Ridge end finding & bifurcation

In poor qualityfingerprintimages it is very difficult to extract the minutiae points.However,localorientation, frequency,ridgeshape, andtextureinformation of each fingerprint areextracted which may not show high distinctiveness.Theapproachesbelongingtothisfamilycom parefingerprintsintermoffeaturesextractedfromtheridgepa ttern.Minutiae,fromasimpleperspective,indicatewhereasig nificantchangeinthefingerprintoccurs.Thesechangesaresh owninFigure8.The dark lines in the imagerepresentridgesandlightlinesrepresentvalleys, Arrow A shows a region where oneridgesplitsintotworidgescalledaBifurcationandArrow BshowswhereaRidgeends.

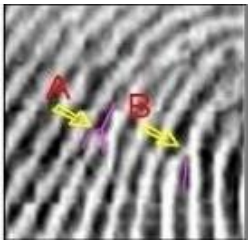

Fig 8: Example of Fingerprint changes

The two most prominent localridgecharacteristicsareRidgeEndingandRidgeBifurca tion.Atridgeendinga ridgeendssuddenly andridgebifurcationmeansthepointwherearidgedivergeint obranchridges.Collectively,thesefeaturesarecalledminutia e.Afterlocatingthesefeaturesinthefingerprint,theminutiaex tractionsoftwaredeterminesasignificantdirectionofthechan geusingArrowBasanexample,thesignificantdirectionstarts attheendoftheridgeandmovesdownward.Thesetofminutiae areshown figure9.

Fig9:Extracted minutiae&axes

The resultant minutae, in their simplest form are the collection of all reasonable bifurcations and ridge endings, their location and their significant direction. Figure 10 shows the ridge end findings in fingerprint image.

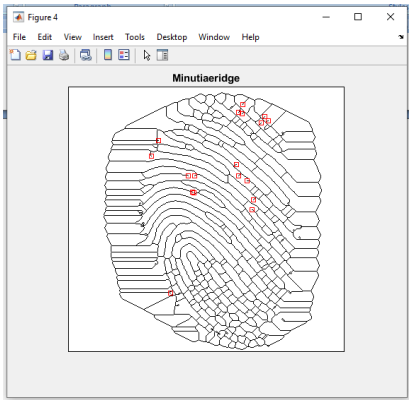

Fig 10:Output image after finding ridgeend

4.5 Dataretrieval

Data retrieval is the process of identifyingand extracting the required information fromthehospitaldatabasesystem.PostgreSQLnative interface database connection is usedto import product data from a database tableintoMATLABusingaPostgreSQLdatabase.Then, a

simple dataanalysis is performed.Thenextstepafterfingerprintmatchingistheretrievalof therecords.

Firstly, a database is created in PostgreSQLusing queries where the dataset is linked tothe database created in order to display thehealth record of a person once fingerprint ismatched. The dataset includes the patient'sname, Diagnoses, E-Mail, Address and othercommoninformation. SincefingerprintmatchingisdoneinMATLABthedatabasecreatedisconnectedwiththeMATLAB.Thefigure11showstheglimpseofdatabaseconnectedusingPostgreSQL.

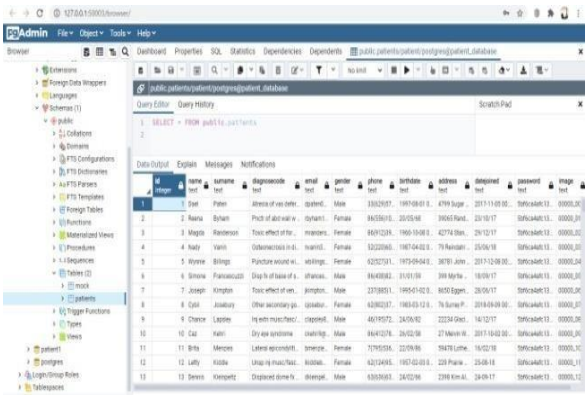

Fig 11: Database in PostgreSQl

The hospitals maintain the health record ofthe patient confidentially, so we downloadeda dataset consisting of patient's health recordfrom Kaggle. This dataset is connected withthe created database. The fingerprints of thepatientsarealsolinkedtothedatabase.Whentheinputfingerprintismatchedwiththefingerprint of patient present in the databasethen the health records associated with thepatients are retrieved from the database andare displayedinthe commandwindow ofMATLAB.Iftheinputfingerprintdoesn'tmatchwiththefingerprintpresentinthedatabasethenapop-upwindowappearsaskingforuserIDandpassword.EmailID ofeverypatientisconsideredastheuserIDanda unique password is given to every patient.Thegivendetailsshouldmatchwiththedetailsintheda tabase.Thenthepatients'datacanbeviewed.

5. RESULTS

5.1 Fingerprint Matches

The output obtained when input fingerprintimage matches with the fingerprint imageinthedatabaseisshownin figure5.1.

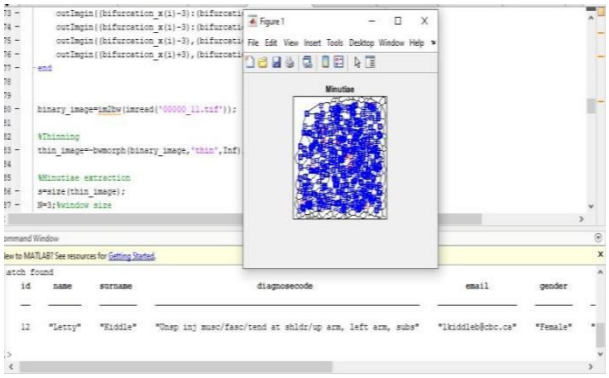

Fig 5.1 Patient's Data Obtained whenFingerprintMatches

5.2 Fingerprint Mismatch

The output image of the login portal whenthe input fingerprint image does not matchwiththefingerprintimageinthedatabaseisshownin figure5.2.

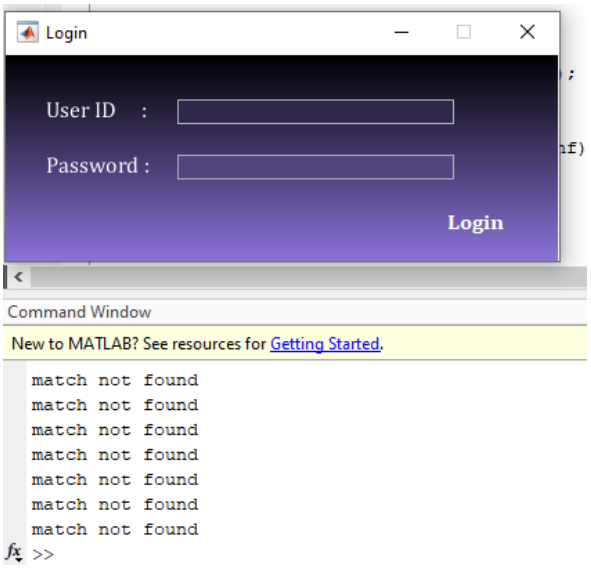

Figure5.2InputFingerprintdoesnotMatchwithFingerprint ImageinDatabase

5.3 Successful Login

TheoutputobtainedwhenthegivenUserIDandpasswordmatchwiththeUserIDandpasswordindatabasealongwiththepatient's data in the command window isshownin figure5.3.

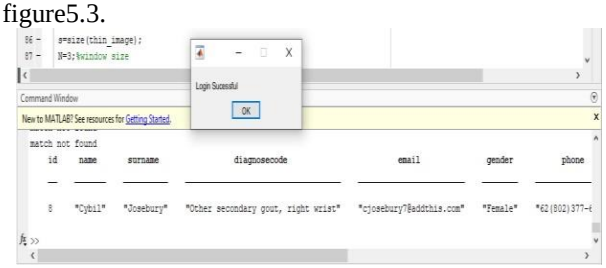

Figure 5.3 Patient's Data Obtained whenLoginis Successful

5.4 Unsuccessful Login

The outputobtained when givenUserIDandpasswordoesnotmatchwiththeUserID and password in database is showninfigure5.4.

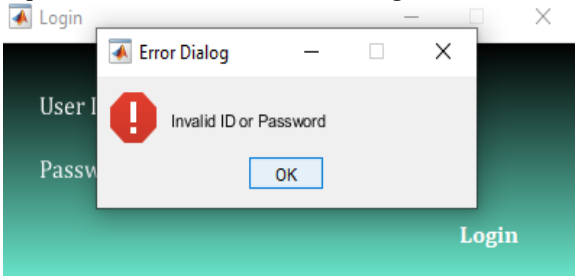

Figure 5.4 Error Dialogue Box OpenedwhenUserIDorPasswordisincorrect

6. CONCLUSION AND FUTUREWORK

Fingerprint matching plays a major part inachieving the result of this paper. For that,firstlyMATLAB2021aapplicationisinstalled.Eitherth efingerprintcapturefrom the scanner or the readily availablefingerprintimagesofthepatientsarestoredin a folder. Health records of the patientsthat consist of name, ID, address, diagnosecode, birth date, email ID, phone numberand password in excel format is connectedtotheMATLAB2021ausingPostgreSQL.

Whenaninputfingerprintisgiventheminutiaepoint sinthefingerprintareextracted and are compared with the otherfingerprints stored. This can be done byminutiae thinning and extraction algorithminMATLAB2021a.Oncomparisontheresult is obtained, whether it is matched ornot.Oncematchedthedetailsoftheparticularpatientisdispl ayed.Healthdetailscanalsobefetchedusinguser IDandpassw ordincaseofunavailabilityoffingerprintsoranydiscrepancie swhilematchingthefingerprints.

Theprocesscanbeextendedtoacentralizedloginap proach.Inthisapproachthehealthrecordsofany personcanbeaccessedinanyhospitalalloverthestateorcity with his or her fingerprint or login ID.Thedatabasecanbelinkedtothescancenters, x-ray centers and pharmacies. Thescan images and prescriptions can also beuploadedalongwiththeirotherrecords.Thisenablesthatth epatientsneednotcarrythepaperreportseverywhere.

Authentication is a second step verificationprocess that is used for security process. Itis also compatible with most of the fields.In arts, archaeology and anthropology, thecommon problem is to ensure that a givenartifactwasproducedbysomeoneorsomewhereorahist oricalperiod.Incomputerscience,verificationofuseridentity is often required to allow access toprivateinformationorapplications.Theways in which a person can be verified fallintothreecategories,basedonwhatareknown as authenticity factors: somethingthe user knows and something the user has.Eachauthenticity itemincludesalistofitems used to verify or verify a person'sidentity prior to granting access, approvingatransactionrequest,signingadocumentorotherpr oduct,authorizingothers,andestablishing a series of authority. This canbe done in future in order to avoid someotherperson to loginillegally.

7. REFERENCES

[1] Biometrics, http://www.biometricupdate.com/

[2] Microsoft Health Vaulthttp://www.healthvault.com/Personal/index.html

[3] Hinkamp T. System providing medicalpersonnel with immediate critical dataforemergencytreatments.PatentApplicationPublicatio n11/510,317,2007.

[4] Akinyele,J.,PaganoM.,Green,M.,Lehmann,C.,Peters on,Z.,andRubin,A.2009."Securingelectronicmedicalrecor ds on smart phone". SPIMACS '09Proceedings of the 1st ACM workshopon Security and privacy in medical andhome-caresystems, November 9- 13, 2009.

[5] A.P.Sricastava,ShashankAwasthi,AwanishKumarK aushik,ShubhamShukla,"Fingerprintrecognitionsystemus ingMATLAB",InternationalConferenceonAutomation,C omputationalandTechnologyManagement,AmityUniversi ty,2019.

[6] AmbroseA.Azeta,Da-OmieteA.Iboroma,VictorI.Azeta,Emmanuel.O. Igbekele , Deborah O. Fatinikun ,EbukaEkpunobi,"ImplementingaMedicalRecordSystem withBiometricsAuthenticationinE-Health",inIEEEAfricon2017Proceedings.

[7] B. Nivedetha, Ila. Vennila, "FFBKS: Fuzzy Fingerprint Biometric Key Based Security Schema for Wireless Sensor Networks",Computer Communications,Volume 150,Pages 94-102, 2020.

[8] DarrellShawl,"Biometrics–ImplementingintotheHealthcareIndustryIncreasestheSecu rityfortheDoctors,NursesandPatients",DavenportUniversi ty,November10,2013.

[9] José R. Díaz-Palacios, Víctor J. Romo-Aledo,AmirH.Chinaei,"BiometricAccessControl for e-Health Records inPre-hospitalCare",UniversityofPuertoRicoat Mayagüez.