UNIVERSITETI I TIRANËS

FAKULTETI I EKONOMISË

DEPARTAMENTI STATISTIKË DHE INFORMATIKË E ZBATUAR

TEMË DIPLOME

Siguria e Rrjetave Wireless Body Area (WBAN)

Diplomë e ciklit të parë të studimeve

"BACHELOR"

PUNOI:
Erinda KAPLLANI

PEDAGOGU UDHËHEQËS:
Msc.Romina MUKA

Tiranë, Shtator 2018

Falenderime dhe Mirënjohje

Në përfundim të këtij rrugëtimi shumë të vecantë, nuk do të mund të lija pa falenderuar njerëz që kanë qenë bashkëudhëtar dhe përkrahës të punës sime.

Shpreh mirënjohjen dhe respektin tim për Zysh Romina Muka, udhëheqësja ime në këtë temë, e cila u tregua në çdo moment e palodhur për të më ndihmuar në realizimin me sukses të këtij punimi. Të falenderoj Zysh Romina që me profesionalizmin dhe përkushtimin tuaj arritët të më motivonit përgjatë kësaj periudhe për të dhënë më të mirën nga vetja, si dhe për çdo vërejtje, sugjerim apo opinion tuajin që padyshim ka ndikuar në përmirësimin e punës sime.

Një falenderim i madh shkon për mikeshat e mia, njëkohësisht edhe koleget e mia në të ardhmen, për çdo kontribut sado të vogël, duke më këshilluar dhe orientuar, por mbi të gjitha ju falenderoj për mbështetjen e pakushtëzuar që më keni dhënë jo vetëm në këtë punim, por në çdo ditë të këtij 3-vjecari që kemi kaluar së bashku.

Së fundmi, dua të shpreh mirënjohjen time të thellë për familjen time, e cila në çdo hap timin ka investuar mundin dhe besimin tek unë. Mirëkuptimi, mbështetja që më keni dhënë dhe mbi të gjitha dashuria juaj ndaj meje më ka bërë të kuptoj që ju jeni padyshim shtysa ime më e madhe. Ju falenderoj nga zemra, jeni padyshim burim force!

ABSTRAKT

Rrjeti Wireless Area Body (WBAN) ka fituar popullaritet si një teknologji e re për e-Health, dhe konsiderohet si një nga degët kyçe të hulumtimit në fushën e shkencave kompjuterike dhe aplikacioneve të kujdesit shëndetësor. WBAN mbledh të dhënat e pacientëve, monitoron parametrat e tyre fiziologjik, duke përdorur sensorë të vegjël dhe i komunikon këto të dhëna duke përdorur teknika të komunikimit *wireless*. WBAN po luan padyshim, një rol shumë të madh në përmirësimin e cilësisë së kujdesit shëndetësor.

Megjithatë, për shkak të natyrës së ndjeshme dhe konkuruese të sistemeve e-Heath, hulumtimet aktuale kanë treguar se projektuesit duhet të marrin në konsideratë sigurinë dhe mbrojtjen e privatësisë së të dhënave të mbledhura nga një WBAN për të mbrojtur pacientët nga shfrytëzime të ndryshme ose sulme të dëmshme.

Ndaj në këtë punim shkencor, fillimisht i është kushtuar një vëmendje e madhe karakteristikave të përgjithshme të WBANs, arkitekturës së komunikimit WBAN, problemeve që shfaqin nivelet e ndryshme në një WBAN, si dhe rolit të padiskutueshëm që kanë aplikacionet dhe teknologjitë e WBAN në përmirësimin e cilësisë së jetës shëndetësore të pacientëve. Një çështje shumë e rëndësishme është edhe shqyrtimi deri në detaje i sigurisë dhe privatësisë së të dhënave dhe profilit të pacientit, duke vënë theksin tek kërcënimet dhe mekanizmat mbrojtës të sigurisë dhe privatësisë. Së fundmi, janë identifikuar specifikisht projekte ekzistuese të WBAN dhe sfidat me të cilat përballet dita-ditës kjo teknologji relativisht e re, por mjaft premtuese. Ndaj, në punim është bërë një parashikim i vogël se cila do të jetë e ardhmja e WBAN (From WBAN to BBN), duke renditur karakteristikat e kësaj teknologjie, aplikacionet dhe trendet të cilat do i duhet të sfidojë.

Fjalë kyçe: *Wireless Body Area Network, siguri, privatësia e të dhënave, kërcënime, aplikacione, teknologji, arkitekturë komunikimi, e-Health, mekanizma mbrojtës, sfida, trende.*

LISTA E FIGURAVE

LISTA E SHKURTIMEVE

WBAN	Wireless Body Area Network
PS	Personal Server
AP	Access Points (Pika Aksesi)
PDA	Personal Digital Assistant
BP	Blood Pressure
EKG	Elektrokardiografi
EMG	Elektromamografi
EEG	Electroencephalogram
GRPRS	General Packet Radio Services
QoS	Quality of Services
DoS	Denial of Services
BLE	Bluetooth Low Energy
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network
BNC	Body Node Coordinator
BSN	Body Sensor Network
PTK	Pairwise Temporal Key
GTK	Group Temporal Key
BBN	Body-to-Body Network

PËRMBAJTJA

Kapitulli 1 - Përmbledhje e studimit

1.1. Hyrje

Në një shoqëri dixhitale, shërbimi shëndetësor elektronik është një nga shërbimet që do të kontribuojë në përmirësimin e cilësisë së jetës së qytetarëve. Kohët e fundit, zhvillimi i shpejtë i komunikimit *wireless* dhe sensorët mjekësor inteligjent, të cilat mund të vendosen në trupin e njeriut, kanë bërë që rrjetat Wireless Body Area (WBANs) të jenë një metodë premtuese në revolucionarizimin e praktikave të kujdesit shëndetësor.

Rrjeti Wireless Area Body (WBAN) lidh nyjet e pavarura (p.sh. sensorë dhe aktuatorë) që ndodhen në rroba, në trup ose nën lëkurën e një personi. Rrjeti zakonisht zgjerohet mbi të gjithë trupin e njeriut dhe nyjet janë të lidhura nëpërmjet një kanali komunikimi *wireless*. Sipas implementimit, këto nyje janë kryesisht të vendosura në një topologji yll. Një WBAN ofron shumë aplikacione të reja premtuese në fushën e monitorimit *remote* të shëndetit , mjekësisë, multimedias, sportit, të cilat përfitojnë nga liria e lëvizjes që një WBAN ofron. Në fushën e mjekësisë, për shembull, një pacient mund të pajiset me një WBAN të përbërë nga sensorë që matin vazhdimisht funksione specifike biologjike, të tilla si temperatura, presioni i gjakut, shkalla e zemrës, elektrokardiogrami (EKG), frymëmarrja etj. Avantazhi është se pacienti nuk është i detyruar të qëndrojë në shtrat, por mund të lëvizë lirshëm nëpër dhomë dhe madje të largohet nga spitali për një kohë të caktuar. Kjo përmirëson cilësinë e jetës për pacientin dhe redukton kostot e spitalit. Përveç kësaj, të dhënat e mbledhura gjatë një periudhe më të gjatë dhe në mjedisin natyror të pacientit, ofrojnë informata më të dobishme, duke lejuar një diagnozë më të saktë dhe ndonjëherë edhe më të shpejtë.

Ne ndeshemi me shumë sfida të reja kur përpiqemi të zhvillojmë një aplikacion shëndetësor WBAN, të tilla si: transmetimi i të dhënave të besueshme, shpërndarja e duhur e të dhënave në kohën e duhur, menaxhimi i fuqisë, llogaritja e nyjeve, *middleware* dhe zbulimi i shpejtë i ngjarjeve. Për më tepër, privatësia e pacientit është e prekshme nëse siguria nuk merret në konsideratë kur implementojmë teknologji të reja në aplikacionet e kujdesit shëndetësor. Veçanërisht duhet të garantohet që të dhënat që lidhen me pacientin të aksesohen vetëm nga përdoruesit e autorizuar, përndryshe, privatësia mund të rrezikohet. Sidoqoftë, meqenëse të dhënat private ruhen në mënyrë distributive në WBANs, ato mund të zbulohen lehtë për shkak të një kompromisi fizik të një nyjeje. Rrjedhimisht, për të siguruar fshehtësinë e pacientëve, nevojitet qasje kriptografike dhe të dhëna të enkriptuara.

1.2. Objektivat e studimit

Objektivat e këtij punimi renditen si më poshtë:

1. Studimi i karakteristikave të Wireless Body Area Network (WBAN) në pajisjet e mjekësisë në fushën e sistemeve të informacionit
2. Arkitektura e komunikimit dhe problemet që mund të shfaqen në nivele të ndryshme në një WBAN
3. Roli që kanë pajisjet e përdorura në WBAN dhe ndikimi që kanë në përmirësimin e cilësisë së jetës së pacientëve aplikacionet dhe teknologjitë e zhvilluara nga WBAN
4. Identifikimi i kërkesave të privatësisë dhe sigurisë duke marrë parasysh kërcënimet ndaj të dhënave shëndetësore të pacientit dhe profilit të tij
5. Përcaktimi i analizës së riskut dhe sigurisë në sistemet WBAN, duke i konkretizuar ato me raste studimore specifike
6. Listimi dhe shpjegimi i secilit prej mekanizmave që përdoren për sigurinë dhe privatësinë e WBAN
7. Identifikimi i sfidave me të cilat duhet të përballen WBANs dhe çfarë premton e ardhmja për to
8. Shembuj konkrektë të projekteve ekzistuese që lidhen me WBAN

Kapitulli 2 - Karakteristikat e WBAN për qëllime mjekësore

WBANs për aplikacionet e kujdesit shëndetësor kryesisht përdoren në monitorimin e pacientëve. Në këtë lloj rrjeti, sensorët shpërndahen në trupin e njeriut duke matur parametra të ndryshëm fiziologjik. Nyjet e sensorëve rreth trupit me *wireless capabilities* janë të një rëndësie të veçantë për këtë lloj WBAN, pasi ato sigurojnë një mënyrë të rehatshme dhe miqësore për të monitoruar gjendjen shëndetësore të pacientit gjatë periudhave të gjata kohore, duke shmangur përdorimin e kabllove të lidhura me pacientin. Në përgjithësi, përbërja e indit të trupit të njeriut ka sasi të ndryshme të ujit. Për shkak të kësaj, përhapja e sinjaleve elektromagnetike nëpër trupin e njeriut ndryshon vazhdimisht dhe i nënshtrohet absorbimit dhe reflektimeve brenda trupit.

Në përgjithësi, janë disa karakteristika të rëndësishme që i japin kuptim përkufizimit që shpesh ndeshim për WBANs, të tilla si:

- **Human Centric Interactions (Aktivizimi):** WBANs janë të lidhura direkt me pjesë të ndryshme të trupit të njeriut për të mbledhur të dhëna, si një koleksion me

informacione sensitive. Trupi njerëzor është shumë i ndjeshëm, si dhe reaktiv për këta sensorë. Pra, këta sensorë duhet të jenë të padëmshëm dhe lehtësisht të pranueshëm për trupin e njeriut.

- **Shkallëzueshmëria:** WBANs përmbajnë më së shumti 10-15 sensorë të bashkëngjitur rreth trupit të përdoruesit. Gama e sensorëve të përdorur këtu në WBANs arrin kryesisht nga 30 deri në 50 metra.
- **Lëvizshmëria:** Është tipari më i rëndësishëm i cili i ka bërë WBAN jashtëzakonisht popullor. Pacientët arrijnë të ndjekin rutinën e përditshme dhe njëkohësisht janë nën mbikëqyrjen e mjekëve.
- **Besueshmëria:** Të dhënat që grumbullohen ndonëse janë të shumta në numër, janë të besueshme dhe shërbejnë në arritjen e rezultateve finale të qëndrueshme.
- **Vendosja:** Këto rrjeta përbëhen nga shumë sensorë të lidhur direkt në pikat e daljes dhe në porta. Sensorët lokalizohen në mënyrë që të formojnë një rrjet me dendësi të madhe.
- **Ndërrimi i baterisë:** Ndërrimi i baterisë mund të jetë kryhet lehtësisht brenda pajisjeve të ndjeshmërisë të përdorura në WBANs. Është e rëndësishme që vazhdimisht të tregohet një kujdes shtesë për ato sensorë që janë implantuar në trupin e pacientit.
- **Pranimi në trupin e njeriut:** Sensorët janë pajisje, të cilat janë të lidhura drejtpërdrejt me trupin e njeriut, kështu që këto normalisht janë të padëmshme në funksionimin e tyre për trupin e njeriut.
- **Topologjia e Rrjetit:** Në WBAN, përgjithësisht përdoren në mënyrë efektive, topologjtë: yll, rrjetë, hibrid ose klaster.

2.1. Arkitektura e komunikimit

Arkitektura e komunikimit e WBAN mund të ndahet në tre nivele të ndryshme si më poshtë:

- **Tier-1:** Komunikimi Intra-WBAN
- **Tier-2:** Komunikimi Inter-WBAN
- **Tier-3:** Komunikimi Beyond-WBAN

Figura 1 ilustron këto nivele të komunikimit në një sistem eficent të bazuar në komponentë për WBAN. Në *figurën 1*, pajisjet janë të shpërndara në të gjithë trupin në një rrjet të centralizuar,

ku vendndodhja e saktë e një pajisje është specifik e aplikacionit. Megjithatë, ndërsa trupi mund të jetë në lëvizje (p.sh. duke vrapuar, duke ecur) vendndodhja ideale e nyjeve të sensorëve është jo gjithmonë e njëjta, prandaj, WBANs nuk konsiderohen si statike.

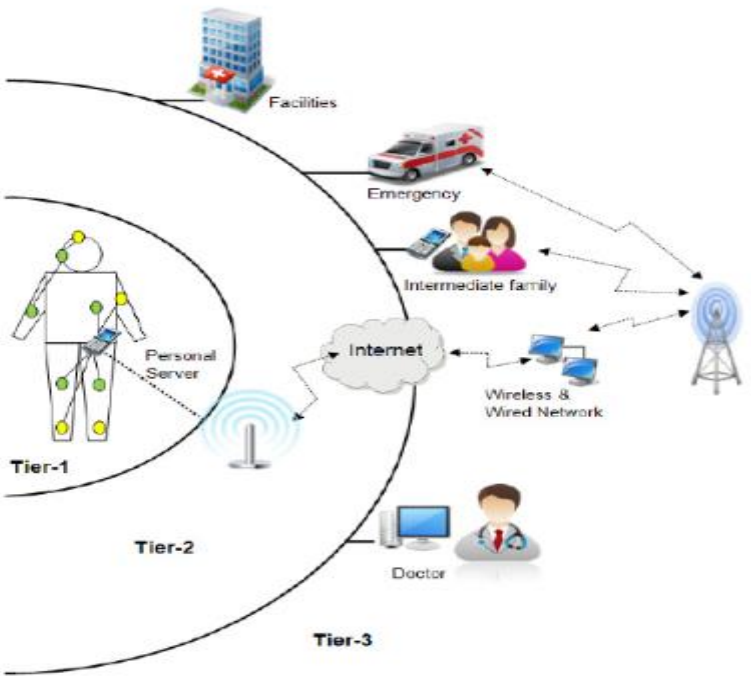

Figura 1. *Arkitektura e komunikimit në një WBAN*

Tier-1: *Komunikimi Intra-WBAN* - Niveli 1 përshkruan ndërveprimin e rrjetit të nyjeve dhe transmetimi i tyre përkatës shkon (~ 2 metra) rreth trupit të njeriut. Fig. 1 ilustron komunikimin e WBAN brenda në një WBAN dhe midis WBAN dhe niveleve të shumta të saj. Në Tier-1, sensorët përdoren për të përcjellë sinjale të trupit në një Personal Server (PS), që ndodhet në Tier-1. Të dhënat fiziologjike të përpunuara transmetohen më pas në një pikë aksesi në Tier-2. **Tier-2:** *Komunikimi Inter-WBAN* - Ky komunikim nivelesh është midis PS dhe një ose më shumë pikave të aksesit (APs). APs mund të konsiderohen si pjesë e infrastrukturës, ose të vendosen strategjikisht në një mjedis dinamik për të trajtuar situatat emergjente. Synimi i komunikimit në nivelin e 2-të ka për qëllim ndërlidhjen e WBAN-it me rrjete të ndryshme, të cilat mund të aksesohen lehtësisht në jetën e përditshme, siç janë rrjetet celulare dhe Interneti.

Paradigmat e komunikimit *Inter-WBAN* janë të ndara në dy nënkategori si më poshtë: **Arkitektura e bazuar në infrastrukturë** – Kjo arkitekturë përdoret në shumicën e aplikacioneve të WBAN sepse lehtëson vendosjen dinamike në një hapësirë të kufizuar sic është një spital, si dhe mundëson një menaxhim të centralizuar dhe kontrollon sigurinë. Pika e aksesit (AP) mund të veprojë si një server i bazës së të dhënave i lidhur me aplikacionin.

Arkitektura ad-hoc - Në këtë arkitekturë, pika aksesi (AP) të shumta transmetojnë informacion brenda qendrave mjekësore. AP-të në këtë arkitekturë formojnë një strukturë rrjeti që mundëson vendosje fleksibile dhe të shpejtë, duke lejuar që rrjeti të zgjerohet lehtësisht, të sigurojë mbulim më të madh të radios për shkak të *multihop dissemination* dhe të mbështes mobilitetin e pacientit. Mbulimi i këtij konfigurimi është shumë më i madh në krahasim me arkitekturën e bazuar në infrastrukturë, dhe për këtë lehtëson lëvizjen rreth zonave me distanca më të largëta. Në fakt, kjo ndërlidhje zgjeron zonën e mbulimit të WBANs nga 2 - 100 metra, e cila është e përshtatshme për të dyja strukturat si ato afatshkurtra edhe ato afatgjata.

Tier-3: *Beyond-WBAN Communication* - Dizajni i këtij nivel komunikimi përdoret kryesisht në zonat metropolitane. Një portë, sic është një PDA mund të përdoret për të bërë lidhjen midis Tier-2 dhe këtij niveli. Megjithatë, dizajni i Tier-3 për komunikim është specifik e aplikacionit. Në thelb, në një mjedis mjekësor, një bazë të dhënash është një nga komponentët më të rëndësishëm të nivelit të 3-të pasi përfshin profilin e përdoruesit dhe historinë e tij mjekësore. Kështu, mjekët ose pacientët mund të njoftohen për gjendjen e emergjencës përmes Internetit ose përmes një mesazhi (SMS). Përveç kësaj, Tier-3 lejon rikthimin e të gjithë informacionit të nevojshëm të një pacienti, të cilat mund të përdoren për trajtimin mjekësor të tyre. Megjithatë, në varësi të aplikacionit, PS në Tier-1 mund të përdorë GPRS / 3G / 4G në vend të komunikimit me një AP.

Hapat e algoritmit:

Hapi 1: Regjistrimi i pacientit → *Hapi 2:* Identifikimi → *Hapi 3*: Vendosja e të dhënave normale në bazën e të dhënave për krahasim → *Hapi 4:* Çdo 2 sekonda mblidhen të dhëna nga pacienti dhe ruhen → *Hapi 5:* Kontrollohen të dhënat e mbledhura me të dhënat normale → *Hapi 6:* Nëse ka ndonjë ndryshim në të dhënat e pacientit, atëherë gjendet numri i mjekut të pacientit → *Hapi 7:* Dërgohet mesazhi mjekut të pacientit.

2.2. Problemet në nivele të ndryshme të WBAN

Dizajni i brendshëm i WBAN ka një arkitekturë me shtresa. Një studim i hollësishëm i shtresave ndihmon në reduktimin e elementeve bazë të: zbatimit, testimit, dizenjimit të *debugging* dhe rrit menaxhimin e rrjetit. Çdo shtresë e një sistemi WBAN përballet me problemet e mëposhtme:

- **Probleme të shtresës fizike (Physical Layer Issues)**

Problemet e ndryshme që lidhen me shtresën fizike të WBAN janë si më poshtë:

1. *Ndërveprimi:* Të dhënat duhet të lëvizin nga një pajisje në një tjetër në një WBAN. Problemi i ndërveprueshmërisë lind për shkak të integrimit të shumë *sensing devices* që operojnë në një frekuencë të ndryshme.
2. *Kontrolli i temperaturës:* Në një WBAN ka pajisje të vogla që kanë transmetues, që konsumojnë shumë më pak energji dhe tolerojnë nxehtësinë ose rrezatimin e trupit të njeriut. Ngritja në temperaturë mund të ndikojë në indet njerëzore, si dhe në pajisje. Pra, një WBAN duhet të projektohet duke mbajtur parasysh të gjitha konsideratat për ngrohje.
3. *Ndryshimi i topologjisë:* Në WBAN së bashku me lëvizjen e trupit, ka një ndryshim në topologji. Kjo shkakton disa lidhje dhe ndërprerje. Kështu që problemet që lindin për shkak të ndryshimit në topologji duhet të trajtohen.
4. *Ndryshimi i nevojës për bandwidth:* Kërkesa e *bandwidth* në një WBAN ndryshon në varësi të aplikacionit. Çdo aplikacion kërkon një *bandwidth* të ndryshëm, për shembull, ka nevojë për shkallë të ulët të të dhënave në rastet e aplikacioneve për monitorimin e shëndetit.
5. *Ndërhyrja:* Ndërhyrja nxitet nga temperatura, indet e brendshme të trupit, pajisjet përreth, WBAN-et e jashtme dhe rrezatimi i nxehtësisë. Ndërhyrje të tilla duhet të reduktohen dhe WBAN-i duhet të jetë në gjendje të bashkëjetojë me rrjetet e tjera.
6. *Pranimi i gabimit:* Në një WBAN ekziston nevoja për të mbajtur komunikimin dhe lidhjen pa ndërprerje, e cila ndikohet nga faktorë të tillë si: topologjia, mjedisi dhe fuqia transmetuese.
7. *Sinjalizim konstant:* Ekziston një nevojë për sinjalizim të vazhdueshëm në disa nga aplikacionet WBAN pasi ato kapin të dhëna të cilat janë të vazhdueshme dhe në kohë reale. Pra, duhet të miratohen procedura të duhura për të kryer detyra konstante të sinjalizimit.
8. *Siguria:* Shtresa fizike vuan nga kërcënime të ndryshme që përfshijnë: *Eavesdropping*, *Tampering* dhe *Jamming*. Duhet të zbatohen masat për zbulimin dhe parandalimin e sulmit.
9. *Cilësia e Shërbimit (QoS)*: Një WBAN kërkon që të dhënat të dorëzohen në kohë reale. Pra, ekziston nevoja për të rritur standardet si dhe kapacitetin e mediumit të transmetimit të të dhënave në mënyrë që QoS të rritet.

- **Probleme të shtresës MAC (MAC Layer Issues)**

  Problemet e ndryshme që lidhen me shtresën MAC të WBAN janë si më poshtë:

  1. *Caktimi dinamik i kanalit:* Caktimi inteligjent i *bandwidth*-it ose ndarja dinamike e kanaleve duhet të sigurohet për të shmangur xhiron e ulët, vonesën e lartë, humbjen e lartë, që ndodhin për shkak të ndërhyrjes.
  2. *Control packets overhead:* Zvogëlojnë sasinë e transmetimit të rrjetit pasi nuk japin të dhëna dhe gjithashtu konsumojnë shumë energji. Pra, duhet të ketë mënyra për të mbajtur paketat e kontrollit sa më të ulta të jetë e mundur gjatë komunikimit.
  3. *Protocol overhead:* I referohet informacionit që dërgohet së bashku me të dhënat që drejtohen nga burimi në destinacion. Disa fusha në *header* si identifikimi i lidhjes (burimi, destinacioni dhe adresa e portit), informacioni specifik i protokollit (lloji i paketës, lloji i sensorit, numri i sekuencës) dhe informacioni specifik i mesazhit (prioritet, *checksum*, gjatësia e mesazhit dhe afati kohor) merren me disa aplikacione dhe përdorin *bandwidth-in* në dispozicion të rrjetit duke shkaktuar probleme.
  4. *Sinkronizimi:* Sinkronizimi përfaqëson pranimin e vazhdueshëm të paketave të komunikimit nën formimin e energjisë dhe xhiros. Për dërgimin e të dhënave në kohë reale, sinkronizimi duhet përmirësuar.

Kapitulli 3 - Pajiset e përdorura në WBAN

Ekzistojnë pajisje të ndryshme në arkitekturën WBAN. Më poshtë renditen 3 prej tyre. **1. Nyjet sensor:** Këto formojnë bazën e secilit WBAN. Në këtë fazë themelore, ka shumë sensorë për të realizuar monitorimin e parametrave fiziologjik, dmth. BP, ECG, Pulse Rate, EEG, etj. Këto nyje sensorë punojnë në trupin e njeriut, marrin sinjalin dhe ja dërgojnë njësisë së përpunimit. Sensorët mund të jenë ose mono ose multifunksionale. Nyjet mund të jenë *Implant node*, *Body surface nodes*, dhe *External node*.

2. Stacioni bazë: Kjo është njësia e përpunimit lokal, e cila përcjell të dhënat, përpunon dhe analizon ato duke dhënë rezultate / feedback tek pacientët. Organizatat e ndryshme kërkimore dhe kompanitë e kanë krijuar këtë stacion bazë, në mënyrë që pacienti të mund ta marrë transmetuesin në shtëpinë e tij dhe nuk është i detyruar të qëndrojë në spital.

3. Server Qendror: Në këtë njësi, ruhen bazat e të dhënave, të cilat dërgohen më pas tek një specialist për konsulencë ose udhëzime të duhura mjekësore.

3.1. Aplikacionet e WBAN

Rrjetat Wireless Body Area (WBANs) mbështesin një numër të shumtë aplikacionesh të reja dhe interesante. Këto aplikacione përfshijnë disa fusha të tilla si: kujdesi shëndetësor, mbikqyrja e jetesës së të moshuarve, situatat emergjente dhe lojërat interaktive. Siç u përmend më parë, shumë hulumtues i klasifikojnë aplikacionet e WBAN si aplikacione mjekësore dhe jo mjekësore.

1. Telemjekësia dhe monitorimi në distancë i pacientëve

Shpenzimet në rritje të kujdesit shëndetësor dhe plakja e popullsisë botërore kontribuojnë në zhvillimin gjithnjë e më shumë të telemjekësisë për ofrimin e shërbimeve shëndetësore. Telemjekësia mundëson shpërndarjen edhe në distanca të largëta të kujdesit të pacientit, duke përdorur sistemet e integruara të informacionit shëndetësor dhe teknologjitë e telekomunikacionit, si dhe lejon që shkencëtarët, mjekët dhe profesionistët e shumtë mjekësorë në mbarë botën të arrijnë t'u shërbejnë më shumë pacientëve. Në fakt, falë sinjaleve që sigurojnë sensorët e trupit, informacioni i mbledhur mund të përpunohet në mënyrë efektive për të marrë vlerësime të besueshme dhe të sakta fiziologjike dhe për të mundësuar komunikimin me mjekun në një kohë reale për diagnozën mjekësore dhe recetën. Një sistem i tillë "*i zgjuar*" i kujdesit shëndetësor mund të ofrojë aplikacione për procedurën diagnostike, mirëmbajtjen e gjendjes kronike dhe shërimin e mbikëqyrur nga një procedurë kirurgjikale që pacienti mund të ketë bërë. Aplikacionet e monitorimit të pacientit, në përgjithësi kontrollojnë sinjale vitale, dhe sigurojnë reagime në kohë reale. Në një situatë të tillë, pacientët mbahen nën monitorimin e mjekut, pa kufizuar aktivitetet e tyre normale dhe pa i dëmtuar ata me kosto të larta. Monitorimi i aktivitetit të përditshëm kontrollon aktivitetin e përditshëm të pacientëve, të cilët mund të jenë prekur nga disa sëmundje specifike, ndërkohë që monitorimi në spital fokusohet në rastet kur pacientët janë të detyruar të qëndrojnë në spital për një kujdes më të mirë dhe për vëzhgime që mund të merren gjatë një kohe të konsiderueshme. Mbikëqyrja e shërimit pas operacionit merret me pacientët në periudhën e tyre të shërimit pas një operacioni. Një WBAN mund të sigurojë matje të vazhdueshme të parametrave fiziologjik, të lejojë zbulimin më të mirë të dështimeve të organeve dhe të reagojë sa më shpejtë ndaj situatave emergjente. Një sistem i tillë i monitorimit në distanca të largëta, do të jetë më i sigurt, më i përshtatshëm dhe më i lirë. Sëmundjet kardiovaskulare, diabeti, zbulimi i kancerit, Parkinson, astma, Alzheimer dhe retina artificiale janë disa shembuj të aplikacioneve specifike të monitorimit të pacientëve.

2. Biofeedback

Vetë monitorimi në distanca të largëta i trupit të njeriut është tani i mundur, duke përdorur WBANs për të aksesuar të dhënat e mbledhura nga sensorët. Sensorët futen ose vendosen në trupin e njeriut për të monitoruar disa sjellje ose patologji dhe për të ndihmuar pacientët të mirëmbajnë shëndetin e tyre përmes fenomeneve të biofeedback si: analiza e temperaturës, zbulimi i presionit të gjakut, elektrokardiografia (EKG), elektromiografia (EMG). Në këtë kontekst, biofeedback i referohet matjes së aktivitetit fiziologjik plus parametrave të tjerë të mundshëm dhe merr të dhëna nga përdoruesit duke bërë të mundur kontrollin dhe modifikimin e aktivitetit fiziologjik, me qëllimin e përmirësimit të shëndetit dhe performancës së tij.

Ditët e sotme është rritur ndjeshëm numri i aplikacioneve të cilat shyrtojnë dhe monitorojnë parametrat fiziologjikë të pacientëve. Më poshtë, janë listuar disa prej tyre.

- **HipGuard System**

  Sistemi HipGuard është zhvilluar për pacientët, të cilët janë duke u shëruar nga kirurgjia në fundshpinë. Ky sistem monitoron pozicionimin dhe rrotullimin e këmbës së pacientit me sensorë *wireless* fiks. Sinjalet e alarmit mund të dërgohen tek njësia e dorës së pacientit nëse pozicionet e këmbës ose rrotullimet nuk janë ato të duhurat, dhe kështu sistemi HipGuard mund të ofrojë informacion të dobishëm në kohë reale për procesin e rehabilitimit të pacientit.
- **MobiHealth**

  MobiHealth është një projekt që përdor teknologjinë e komunikimit *wireless* të GPRS / UMTS për transferimin e të dhënave, bazuar në një iniciativë evropiane për të krijuar një platformë gjenerike për kujdesin shëndetësor në shtëpi, duke përdorur sensorë të bazuara në WBAN dhe teknologji të telefonisë celulare. MobiHealth synon të sigurojë monitorim të vazhdueshëm për pacientët jashtë mjedisit spitalor. Objektivat e MobiHealth, janë përmirësimi i cilësisë së jetës së pacientëve, duke mundësuar shërbime të reja me vlerë të shtuar në fushat e parandalimit të sëmundjeve, diagnozave të sëmundjeve, asistencës së largët, monitorimit të gjendjes fizike dhe madje edhe në hulumtimet klinike. Prandaj, një pacient që kërkon monitorim për periudha të shkurtra ose të gjata kohore nuk duhet të qëndrojë në spital për monitorim. Me MobiHealth WBAN pacienti mund të jetë i lirë të ndjekë aktivitetet e jetës së përditshme.

Figura 2. *Sistemi MobiHealth, duke monitoruar një pacient jashtë ambjentit të spitalit*

- **CodeBlue**

  CodeBlue, i zhvilluar në Universitetin e Harvardit, është një projekt hulumtimi mjekësor i bazuar në rrjetet e sensorëve. Ky projekt përfshin kujdesin para-spitalor dhe kujdesin emergjent në spital, reagimin ndaj katastrofave dhe rehabilitimin e pacientëve. Hulumtimet nga ky projekt kanë potencial për kujdesin, vendimet në kohë reale dhe vëzhgimet afatgjata të pacientëve. Sistemi integron sensorë të shenjave vitale, kompjutera dore dhe etiketa për përcjelljen e vendndodhjes. Ai gjithashtu ofron shërbime për krijimin dhe transferimin e kredencialeve, ndjekjen e vendndodhjes, si dhe për filtrimin në rrjet dhe bashkimin e të dhënave të prodhuara nga sensorët. CodeBlue është projektuar për t'u shkallëzuar në një gamë të gjerë të dendësive të rrjetit dhe vepron në një sërë pajisjesh *wireless*, që nga sistemet e kufizuara deri tek sistemet më të fuqishme të PDA-së dhe PC-ve.

- **UbiMon**

  Projekti i financuar nga DTI, UbiMon, ka për qëllim të ofrojë një sistem monitorimi të vazhdueshëm për pacientin me qëllim kapjen e situatave të papritura . Janë zhvilluar një numër biosensorësh si : *3-lead ECG, 2-lead ECG strip,* dhe *SpO2*. Për më tepër, një *compact flash WBAN card* është zhvilluar për PDA-të, ku sinjalet e sensorëve mund të mblidhen, shfaqen dhe analizohen nga PDA.

- **LifeShirt**

  LifeShirt është një "*veshje e mençur*", e rehatshme dhe tërësisht joinvazive që grumbullon të dhëna gjatë rutinës së përditshme të pacientit, duke dhënë një pamje më të plotë të gjendjes shëndetësore të një pacienti. Kjo i mundëson profesionistëve dhe studiuesve të kujdesit shëndetësor që të monitorojnë me saktësi më shumë se 30 funksione vitale jetësorë. LifeShirt mbledh të dhënat e pacientit duke përdorur sensorë

të integruar duke përfshirë brezat e frymëmarrjes (të cilat matin funksionin pulmonar) dhe EKG (që regjistrojnë aktivitetin elektrik të zemrës). Gjithashtu gjurmon dhe regjistron qëndrimin dhe aktivitetin fizik.

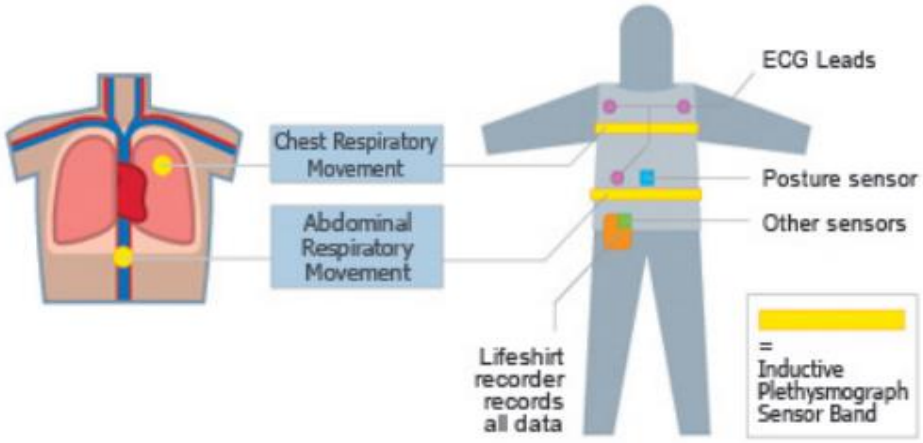

Figura 3. *Smart LifeShirt*

- **eWatch**

  EWatch është një platformë kompjuterike me ndjeshmëri të lartë, që mund të vendoset si orë dore dhe dërgon njoftime në lidhje me parametrat fiziologjikë të pacientit. Një sistem eWatch mund të ndiejë nëse përdoruesi ndihet keq dhe pastaj të pyesë për të konfirmuar nëse është një emergjencë. Nëse përdoruesi nuk përgjigjet, atëherë eWatch mund të përdorë aftësitë e tij të rrjetit për të thirrur për ndihmë. Ewatch gjithashtu mund të njoftojë një pacient kur ai duhet të marr ilaçe të caktuara.

- **Vital Sign Monitoring System**

  Pacientët në një rast fatkeq mund të përfitojnë shumë nga teknologjitë që vazhdimisht monitorojnë statusin e tyre jetësor dhe ndjekin vendndodhjet e tyre derisa ata të shkojnë në spital. Autorët kanë dizajnuar dhe zhvilluar një sistem monitorimi pacientësh në kohë reale që integron sensorë të shenjave vitale, sensorë vendodhje, rrjete *ad-hoc*, shënime elektronike të pacientëve dhe teknologji të web portalit për të lejuar monitorimin e largët të statusit të pacientit.

- **Artificial Retina**

  WBANs gjithashtu mund të ndihmojnë njerëzit e verbër. Pacientët pa shikim ose me shikim të kufizuar mund të shohin në një nivel të arsyeshëm duke përdorur *retina prosthesis chips* të vendosura brenda syrit të njeriut.

3.2. Teknologjitë e WBAN

WBAN mund të përfshijë teknologji të ndryshme në nivele të ndryshme. Në këtë seksion, do të paraqesim një studim gjithëpërfshirës të teknologjive kryesore të propozuara për WBAN.

1. Bluetooth

Teknologjia Bluetooth është projektuar si një standard i komunikimit me valë të shkurtër, me qëllim ruajtjen e niveleve të larta të sigurisë. Në sajë të kësaj teknologjie, çdo pajisje mund të komunikojë njëkohësisht me shtatë pajisje të tjera. Karakteristika kryesore tërheqëse e saj është se lejon një gamë të gjerë të pajisjeve të aktivizuara me Bluetooth për t'u lidhur dhe për të komunikuar me njëra-tjetrën pothuajse kudo në botë. Pajisjet Bluetooth veprojnë në 2,4 GHz ISM band (grupi industrial, shkencor dhe mjekësor), duke shfrytëzuar shkallën maksimale të të dhënave 3 Mbps.

2. Bluetooth Low Energy

Një opsion i nxjerrë nga standardi Bluetooth është Bluetooth Low Energy (BLE), i cili u prezantua si një zgjedhje më e përshtatshme për aplikacionet WBANs, ku konsumimi më i vogël i energjisë është i mundur duke përdorur funksionimin e ciklit të ulët të detyrës. Bluetooth LE ishte projektuar për të lidhur me valë pajisjet e vogla në terminalet e lëvizshme. Këto pajisje janë shpesh shumë të vogla për të mbajtur konsumin e energjisë, si dhe koston e lidhur me një radio Bluetooth standarde, por janë zgjedhje ideale për aplikacionet e monitorimit të shëndetit. Teknologjia Bluetooth Low Energy pritet të ofrojë një shkallë të dhënash deri në 1 Mbps.

3. Zigbee dhe 802.15.4

ZigBee është një nga teknologjitë *wireless* që përdoret gjerësisht. ZigBee është në shënjestër për aplikacionet që kërkojnë një radio-frekuencë të ulët të të dhënave, jetëgjatësi të baterisë dhe rrjetëzim të sigurt, në sajë të mbështetjes 128-bit të sigurisë për të kryer autentikimin dhe garantimin e integritetit dhe privatësisë së mesazheve. Teknologjia ZigBee ndahet në dy pjesë. Së pari, aleanca ZigBee përcakton shtresat e aplikacionet, duke përcaktuar rrjetin, sigurinë dhe shtresat e softuerit të aplikimit. Së dyti, standardi IEEE 802.15.4 përcakton shtresat e kontrollit të qasjes fizike dhe të mesme, ku qasja në kanalin *wireless* është nëpërmjet përdorimit të mekanizmave CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance). Pajisjet *wireless* me bazë ZigBee funksionojnë në frekuencën 868 MHz, 915 MHz dhe 2.4 GHz.

Kështu, një disavantazh i rëndësishëm i Zigbee për aplikacionet WBAN është ndërhyrja në transmetimin e rrjetit të zonës lokale (WLAN), veçanërisht në 2.4 GHz ku funksionojnë sisteme të shumta *wireless*. Një disavantazh tjetër i Zigbee ka të bëjë me shkallën e ulët të të dhënave (250 Kbps), gjë që e bën të papërshtatshme për aplikacione WBAN në shkallë të gjerë dhe reale.

4. IEEE 802.11

IEEE 802.11 është një grup standardesh për rrjetin lokal *wireless* (WLAN). Bazuar në standardet IEEE 802.11, Wi-Fi lejon përdoruesit të shfletojnë internetin me shpejtësi *broadband*, kur lidhen me një pikë hyrje (AP) ose në mënyrë *ad hoc*. Ai është i përshtatshëm për transferta të mëdha të të dhënave, duke siguruar lidhjen *wireless* me shpejtësi të lartë, si dhe duke lejuar videokonferencat, thirrjet zanore dhe *video streaming*. Një avantazh i rëndësishëm është se të gjitha smartphonët, tabletat dhe laptopët kanë Wi-Fi të integruar. Megjithatë, konsumi i lartë i energjisë është një pengesë e rëndësishme.

3.3. Teknologjitë përballë Aplikacioneve

Aplikacionet mjekësore të WBAN premtojnë përmirësimin e cilësisë së jetës së njerëzve dhe përmbushjen e shumë kërkesave të njerëzve të moshuar duke i bërë ata të jetojnë në mënyrë të sigurtë, të shëndetshme dhe të pavarur. Meqenëse mediumi *wireless* siguron një mënyrë shumë të përshtatshme për transmetimin e informacionit, teknologjitë celulare përfshihen në komunikimin midis sensorëve, si dhe midis stacionit bazë dhe sensorëve. Megjithëse *IEEE 802.15.6* është përcaktuar për t'i shërbyer aplikacioneve të ndryshme mjekësore dhe jo mjekësore, standardet më të njohura dhe të përdorura zakonisht janë IEEE 802.15.1 (Bluetooth) dhe IEEE 802.15.4 (gjerësisht duke iu referuar ZigBee) në disa aplikacione. Në fakt, konsideratat e tjera duhet të merren parasysh, siç është shkalla e të dhënave, ndërhyrja që gjenerohet nga bashkëjetesa e teknologjive të ndryshme që punojnë në të njëjtin vend, etj.

Në këtë seksion, diskutohen kërkesat e secilës kategori të aplikacioneve mjekësore që lidhen me teknologjinë celulare. Kërkesat specifike të WBAN janë kryesisht:

1) Besueshmëria: Të dhënat e dërguara nga sensorë të WBAN-it kanë të bëjnë me informacionin për të cilin është e nevojshme besueshmëria e lartë.

2) Latency: Disa aplikacione mjekësore që trajtojnë të dhënat urgjente nuk mund të tolerojnë një kohë të gjatë përgjigjeje. Kështu, kërkohet transmetimi në kohë reale me garancinë e performancës.

3) Siguria: Sisteme të tilla trajtojnë të dhëna personale dhe kritike, ndaj edhe siguria dhe privatësia e këtyre të dhënave po bëhen gjithnjë e më shumë çështje të rëndësishme.

4) Konsumi i energjisë: Zëvendësimi i baterisë në WBAN mund të bëhet shumë lehtësisht.Këto kërkesa mund të ndryshojnë duke marrë parasysh karakteristikat e çdo aplikacioni WBAN. Në fakt, aplikacionet për rehabilitim synojnë të kapin lëvizjet dhe qëndrimet e pacientëve për monitorimin e aktiviteteve të tij gjatë terapisë së rehabilitimit. Aplikacionet klinike të mundshme përfshijnë rehabilitimin kognitiv siç janë: trajtimet e dëmtimit të trurit, si dhe rehabilitimin motorik siç janë: rehabilitimi pas operacionit, rehabilitimi pas aksidentit ose rehabilitimi pas sëmundjes. Sistemi duhet të tregojë saktësi të lartë në grumbullimin e të dhënave dhe përpunimin e të dhënave në mënyrë që të nxjerrë informacione të sakta mjekësore. Ai gjithashtu duhet të mbështesë komunikimet në kohë reale me vonesat e garantuara për të dhënë reagime në kohë reale tek pacienti gjatë seancave të rehabilitimit.

Meqenëse përfshihet shëndeti i pacientëve, sistemi duhet të garantojë dhënien e alarmeve, siç janë rënia e të moshuarve gjatë ushtrimit. *Biofeedback* gjithashtu u ofron përdoruesve aftësinë për të monitoruar vazhdimisht parametrat e shëndetit të tilla si: temperatura e trupit, shkalla e rrahjeve të zemrës, presioni i gjakut arterial, në një mënyrë efikase. Monitorimi i parametrave njerëzor biomjekësor është kritik për të siguruar jetën dhe sjelljen normale të njeriut. Kështu, kapja e këtyre parametrave duhet të jetë sa më e saktë dhe e besueshme që të jetë e mundur. Madje, kur aplikacioni ushqen këtë informacion biologjik përsëri tek përdoruesi, teknologjia *wireless* duhet të marrë parasysh karakteristikat e brendshme të një mediumi të tillë, siç janë ndërhyrjet. Një aplikacion i tillë duhet të marrë një vëmendje të veçantë në kufizimet e energjisë të nyjeve të sensorit. Në fakt, kufizimet e madhësisë së sensorëve kufizojnë kapacitetin e baterisë dhe nëse një sensor ndalon punën, humbet një parametër shëndetësor.

Përveç kësaj, këto aplikacione fiziologjike kërkojnë dizejnimin e zgjidhjeve për të adresuar sfidat e reja në efikasitetin, koston dhe ndërfaqen e përdoruesit. Për një aplikim të tillë, është e domosdoshme transformimi i të dhënave të sensorëve të papërpunuar në të dhëna kuptimplotë për pacientët dhe personelin mjekësor. Shumë zgjidhje të ofruara mbështeten në pajisjet mobile të aktivizuara me Bluetooth, të tilla si Smartphone. Qasje të tjera përdorin një pajisje *handheld* (të tilla si një personal digital assistant (PDA)) për të komunikuar, duke lejuar lëvizjen e

pacientit. Sistemi i integruar i propozuar është i përqendruar në një arkitekturë *wireless* ndërmjet komunikimit *wireless* dhe atij me Bluetooth. Bluetooth është përdorur për lidhjen me rreze të shkurtër midis sensorëve *wearable* dhe një PDA, për reagime të pacientëve. Të dhënat e grumbulluara të pacientëve do të menaxhohen nga një bazë mikro në një PDA dhe transferohen në një server të largët nëpërmjet WLAN, për trajtim të mëtejshëm nga stafi mjekësor nëse kërkohet.

Kapitulli 4 - Siguria dhe kërkesat e privatësisë në WBAN

Është thelbësore për të kuptuar çështjet e sigurisë dhe privatësisë në WBANs, pasi ato janë dy komponentë thelbësor për sigurinë e sistemit të aplikacioneve të monitorimit të kujdesit shëndetësor. Në këtë seksion diskutohet: (1) cilat do të jenë kërkesat e sigurisë në WBAN para se të zbatohen mekanizmat e përshtatshëm të sigurisë; dhe (2) kërkesat e privatësisë së të dhënave të shëndetit elektronik (e-health).

- **Kërkesa për Konfidencialitetin e të Dhënave** është të mbrojë zbulimin e të dhënave të shëndetit elektronik. Nyjet sensor, të cilat dërgojnë të dhëna të ndjeshme në WBANs, mund të kompromentohen shumë lehtë për shkak të natyrës së tyre. Kompromisi mund të çojë në zbulimin e të dhënave, nëse të gjithë të dhënat janë të koduara dhe të ruajtura në një nyje, së bashku me çelësin e enkriptimit. Thirrja e komunikimit mund të dëmtojë seriozisht pacientët, sepse sulmuesi mund të përdorë të dhënat e tyre për qëllime kriminale. Enkriptimi i të dhënave me një çelës sekret fiton konfidencialitetin e të dhënave, dhe ky çelës duhet të shpërndahet në një kanal të sigurt komunikimi ndërmjet nyjeve të sensorit dhe serverave lokalë.
- **Kërkesa për Integritetin e të Dhënave** është të mbrojë modifikimin e të dhënave të lidhura me pacientin kur komunikohen mbi një WBAN të rrezikuar. Të dhënat e ndryshuara të WBANs mund të çojnë në pasoja të rrezikshme, veçanërisht në ngjarjet me rrezik jetën e pacientit. Mekanizmat e përshtatshëm të integritetit të të dhënave në nyjen dhe në serverin lokal vërtetojnë se një sulmues nuk modifikon të dhënat e marra. Kjo mund të arrihet duke përdorur protokollet e vërtetimit të të dhënave.
- **Kërkesa për Disponueshmërinë e të Dhënave** garanton që mjekët gjithmonë mund të marrin të dhëna të lidhura me pacientin në kohën kur i kërkojnë ato. Disponueshmëria e një WBAN mund të jetë një objektiv për një sulmues. Sulmuesi mund të kapë ose çaktivizojë një nyje sensori, duke rezultuar në humbjen e disponueshmërisë së të dhënave.

Rrjedhimisht, është e nevojshme të ruhet operimi i nyjeve të sensorit në aplikacionet e kujdesit shëndetësor dhe të zhvendoset operacioni në një nyje tjetër në rast të humbjes së disponueshmërisë së të dhënave.

- **Kërkesa për Freskinë e të Dhënave** është thelbësore për të siguruar konfidencialitetin dhe integritetin e të dhënave. Kundërshtari mund të ngatërrojë BNC-në duke marrë të dhëna gjatë transmetimit dhe ri-dërgojë ato më vonë. Freskia e të dhënave garanton rifutjen e të dhënave. E thënë më thjesht, kontrollon vendosjen e kornizave të të dhënave. *Weak freshness* dhe *strong freshness* janë dy llojet e freskisë së të dhënave.
- **Kërkesa për Autentifikimin e të Dhënave** është një kërkesë tjetër shumë e rëndësishme për sigurinë e WBAN në aplikacionet e kujdesit shëndetësor. Është thelbësore për secilën nyje sensori dhe server lokal që të provojë se të dhënat u dërguan nga një nyje e besuar dhe jo nga një sulmues, që mashtroi nyjen ose serverin lokal për të pranuar të dhëna të rreme. Dërguesi i të dhënave të shëndetit elektronik duhet të vërtetohet, si dhe nuk duhet të lejohet injektimi i të dhënave jashtë WBAN. Përdorimi i teknikave simetrike mund të arrijë autentifikimin e të dhënave në një WBAN.
- **Kërkesa e Menaxhimit të sigurt** kërkohet në serverin lokal, pasi ai siguron skemat kryesore të shpërndarjes në nyjet e sensorit në mënyrë që të lejojë operacionet e enkriptimit dhe dekriptimit. Shumë përdorues në një aplikacion shëndetësor të WBAN si: mjekët, infermierët, mjekët, kompanitë e sigurimeve, farmacistët dhe punonjësit socialë kanë qasje në të dhënat e pacientit. Pra, rekomandohet të implementohet një mekanizëm i kontrollit të qasjes bazuar në rolet në aplikacionet shëndetësore në kohë reale, që mund të kontrollojnë qasjen në të dhënat fiziologjike të pacientit dhe të garantojnë privatësinë e tij. Kërkesa për lejen e pacientit është e nevojshme kur një ofrues i kujdesit shëndetësor shpërndan të dhënat e tij shëndetësore tek një autoritet tjetër shëndetësor, siç është hulumtuesi mjekësor, kompania e sigurimeve etj.

Përveç kërkesave themelore të sigurisë si konfidencialiteti, mbrojtja e integritetit dhe autentifikimi duhet të plotësohen disa qëllime të tjera. Këtu përfshihen:

- **Efikasiteti:** Një aspekt i rëndësishëm i dizajnit të WBAN është efikasiteti i energjisë për shkak të aftësive të kufizuara të sensorëve. Kërkesat e vazhdueshme të monitorimit të një WBAN mund të pengohen nga zbrazja e shpeshtë e energjisë edhe pse sensorët janë të rikarikueshëm. Kështu që WBAN duhet të ketë komunikim të sigurtë për energji.

- **Përdorshmëria:** Zgjidhjet e sigurisë për WBAN duhet të jenë të përdorshme. Përcaktohen zgjidhjet e përdorshme të sigurisë, të cilat aktivizohen në punë në mënyrë *plug-n-play* me procedura minimale të inicializimit.

Standardi **IEEE 802.15.6** ka propozuar një paradigmë të sigurisë për WBANs, që përcakton tre nivele të sigurisë si më poshtë:

a) **Niveli 0** - *Komunikimi i pasiguruar* - Ky është niveli më i ulët i sigurisë, në të cilin të dhënat transmetohen në korniza të pasigurta dhe nuk ofrojnë asnjë matje për validimin e integritetit, mbrojtjen e autenticitetit, mbrojtjen e privatësisë dhe të konfidencialitetit.

b) **Niveli 1**- *Autentifikimi por jo Enkriptimi* - Në këtë nivel të sigurisë, të dhënat transmetohen në korniza të autentifikuara, por jo të koduara. Ai përbëhet nga masa për validim të integritetit, autenticitetit dhe mbrojtjes. Megjithatë, ajo siguron mbrojtje ose konfidencialitet të privatësisë.

c) **Niveli 2**- *Autentifikimi dhe Enkriptimi* - Ky është niveli më i lartë i sigurisë, në të cilin mesazhet transmetohen në korniza të autentifikuara dhe të koduara, prandaj, sigurohen masa për validimin e integritetit, autenticitetin dhe mbrojtjen e privatësisë. Ai mbulon çështjet që lidhen me nivelin 0 dhe nivelin 1. Gjatë proçesit të asocimit, zgjidhet niveli i kërkuar i sigurisë. Në komunikim *unicast*, aktivizohet një çelës i paravendosur (MK) ose një çelës i ri. Në hapin tjetër, gjenerohet një Pairwise Temporal Key (PTK) që përdoret vetëm një herë në seancë. Në komunikimin *multicast*, gjenerohet një Group Temporal Key (GTK) që ndahet me grupin përkatës.

Të gjitha nyjet dhe koordinatorët në një WBAN duhet të kalojnë nëpër faza të caktuara në shtresën MAC përpara shkëmbimit të të dhënave. Në këtë mënyrë, kornizat kërkohen ose lejohen të shkëmbejnë midis një shpërndarësi dhe një nyjeje.

Pikat kryesore në të cilat duhet të zbatohet siguria brenda WBAN janë:

1. Në sensorë të lidhur rreth trupit të pacientit.

2. Në serverët personalë (ku mbahen informatat e grumbulluara dhe dërgohen jashtë për një përpunim të mëtejshëm).

3. Në kanalet e komunikimit dhe hyrje / dalje të ndryshme ose porta.

4. Në internet (për të lidhur komunitetin mjekësor jashtë WBAN).

5. Tek pajisjet që përdoren nga ndihmësit mjekësorë.

Ka disa arsye se pse kërkesat e sigurisë duhet të përmbushen në mënyrë rigoroze. Disa prej tyre janë si më poshtë:

I. *Jetët e përdoruesve të moshuar* mund të rrezikohen nëse ndonjë sulmues merr dhe keqpërdor informacionin e tyre të tanishëm shëndetësor.

II. *Gruaja shtatzënë* mund të dëshirojë të fshehë statusin e saj të tanishëm, por dikush e dëmton atë dhe e bën atë publike, duke kërcënuar jo vetëm statusin e saj në shoqëri, por duke vënë në rrezik jetën e saj dhe të fëmijës.

III. *Individë që janë përgjegjës për sigurimet shoqërore* mund të modifikojnë politikën e tyre për përdoruesit duke marrë statusin aktual të pacientit.

IV. *Informacioni i gabuar* mund të futet me dashje përmes një kanali të pasigurtë. Në bazë të këtij informacioni të modifikuar, trajtimi mund të ofrohet në mënyrë të papërshtatshme mjekësore. Pra, jeta e pacientit, si dhe reputacioni dhe vullneti i mirë i spitalit dhe i mjekut mund të shkatërrohen.

V. *Zhvillimi i projektit sipas WBAN* do të ndikojë negativisht midis klientëve / përdoruesve të synuar. Besimi i pakët mbi teknologjinë mund të demotivojë dhe parandalojë kërkuesit për përparim të mëtejshëm.

Pra, sistemet vëzhguese të kujdesit shëndetësor të saktë, të besueshëm, të sigurt dhe të besueshëm kërkohen shumë që të zhvillohen duke përdorur WBAN.

4.1.Kërcënimet e sigurisë dhe privatësisë në WBAN

WBANs sigurisht që përmirësojnë cilësinë e kujdesit për pacientët, por pajisjet mjekësore ndjejnë të dhënat sensitive të pacientit dhe përdorin komunikimin *wireless* për ta transmetuar atë. Prandaj, duhet të garantohet siguria dhe privatësia për parametrat fiziologjik të pacientit nga çdo kërcënim i sigurisë. Bazuar në kërkesat e sigurisë, në vijim do të shqyrtohen kërcënimet e sigurisë që do të ishin të dëmshme për aplikacionet shëndetësore të WBAN.

- **Sulmet e fshehtësisë dhe autentifikimit:** Në këtë kategori përfshihen kërcënime të tilla si: përgjimi dhe monitorimi i parametrave vitalë të pacientëve, *spoofing* e paketave dhe sulmet e përsëritjes së paketave. Vëzhgimi (*eavesdropping*) është kërcënimi më i zakonshëm ndaj sistemeve të e-Health. Duke fshehur të dhënat e ndjeshme të pacientit, një sulmues mund të ndjekë lehtësisht aktivitetin e përdoruesve nga kanali i komunikimit. Duke u bazuar në të dhënat e pacientit, ai / ajo mund të analizojë aktivitetet e pacientëve.

Një rast i sulmeve të autentifikimit në WBANs është falsifikimi i alarmeve mbi të dhënat e pacientit. Në një aplikacion të kujdesit shëndetësor WBAN, një kundërshtar mund të mashtrojë lehtësisht një nyje sensori derisa të dhënat e lidhura me pacientin transmetohen në serverin lokal. Në këtë sulm, një nyje e paligjshme e sensorëve vepron si e vërtetë në rrjet. Kjo mund të çojë në alarme të pavërteta të sistemit, për shembull një ekip emergjence mund të fillojë një operacion të panevojshëm shpëtimi. Kështu, sulmet ndaj autentifikimit rrezikojnë aplikacionet shëndetësore të WBANs. Teknikat kriptografike standarde dhe Message Authentication Code (MAC) mund të mbrojnë autenticitetin dhe fshehtësinë e kanaleve të komunikimit.

- **Sulmet e Integritetit të Shërbimit:** Në këtë lloj sulmi, përfshihet kërcënimi ndaj informacionit, kur ai është në tranzit. Në aplikacionet shëndetësore të WBAN-it, pajisjet e sensorëve kapin të dhënat e lidhura me pacientin dhe e dërgojnë në serverin lokal ose në serverin spitalor. Ndërsa të dhënat janë në transit, mund të sulmohen. Kjo mund të shkaktojë një alarm të rremë ose mund të fshehë gjendjen e vërtetë të një pacienti, duke çuar në një ngjarje fatkeqësie. Ndryshimi i mesazhit kërcënon integritetin e nyjeve sensor të WBAN. Sulmet e integritetit të shërbimit nuk ndodhin vetëm gjatë transmetimit, por edhe gjatë kohës së ruajtjes. WBANs mund të mbrohen nga këto sulme nëse zbatohen teknikat e Kodit të Autentifikimit të Mesazhit.
- **Sulmet ndaj Disponueshmërisë së Rrjetit:** Sulmet mbi disponueshmërinë e rrjetit janë referuar gjithashtu si sulme Denial of Service (DoS). Sulmet DoS përpiqen të bëjnë të disponueshme për përdoruesit e saj burimet e rrjetit dhe të ndikojnë në kapacitetin dhe performancën e rrjetit. Kërcënimi DoS mund të jetë edhe më i dëmshëm në aplikacionet shëndetësore të WBAN, pasi është e domosdoshme që rrjeti të jetë gjithmonë në monitorimin e shëndetit të pacientit. Meqenëse WBAN janë një lloj i rrjeteve të sensorëve *wireless* (WSN), shumica e sulmeve të tyre DOS janë trashëguar nga WSN, por për shkak të karakteristikave unike të WBAN ekzistojnë disa dallime midis sulmeve të DOS që mund të ndodhin në WBAN krahasuar me ato në WSN.

4.2. Analiza e riskut në sistemet WBAN

Masat dhe rregulloret e sigurisë janë krijuar për të mbrojtur më tej të gjitha identitetet dhe informacionet. Rregulloret kanë qenë të vendosura mirë për WBAN, pasi WBAN ka qenë një teknologji popullore për më shumë se dy dekada. Në lidhje me WBAN, FDA e SHBA-së (*US Food and Drug Administration*) ka pjesën e saj në procesin e rregullimit, por FCC (*Federal Communications Commission*) dhe HIPAA (*Health Insurance Portability and Accountability*

Act) luajtën rolin më të madh në rregullimin e WBAN dhe se si ajo duhet të sigurojë ruajtjen, transmetimin dhe përpunimin e të dhënave. Çdo mospërputhje e rregullave të tilla mund të çojë në humbje financiare dhe reputacion, madje edhe të shkojë në çështje gjyqësore civile.

- **Rregulloret e FCC**

  Në përmbledhjen e raportit të vitit 2014, FCC ka pohuar se "FCC fillimisht do të miratojë një politikë të tipit *"permit but ask"* që shoqërohet zakonisht me teknologji të re, ku pajisjet kërkohen të testohen dhe të miratohen direkt nga laboratori i testimit FCC, i cili mund të zbatohet në pajisjet e sistemeve WBAN. Përveç miratimit të FCC, pajisjet WBAN gjithashtu do të duhet të marrin miratimin e FDA përpara se të vendosen të përdoren në spitale "(*Buckiewicz, 2015*). Këto rregulla kryesisht merren me aspektet teknike të teknologjisë WBAN, siç janë certifikimi i pajisjes, transmetimi i sinjalit dhe ndërhyrjet. Nga ana tjetër, sigurimi i disponueshmërisë dhe kontrolli i qasjes së përdoruesve përfshihen në fushën e sigurisë kibernetike.

- **Rregulloret e HIPAA**

  Në sektorin e kujdesit shëndetësor, një nga kriteret më të rëndësishme rregullatore është HIPAA, e cila u prezantua në vitin 1996. HIPAA ka vendosur kritere dhe rregulla për mënyrën se si duhet të trajtohen informacionet e kujdesit shëndetësor në mënyrë të tillë që të sigurohet disponueshmëria, integriteti dhe konfidencialiteti. Subjektet e mbuluara duhet të marrin parasysh mbrojtje kritike për të mbrojtur informacionin e kujdesit shëndetësor të çdo personi, duke siguruar gjithashtu që askush të mos zbulojë ose keqpërdor informacionin e shëndetit të njerëzve. Gjithashtu, të njëjtat subjekte duhet të trajnojnë punonjësit për të mbrojtur informacionin, duke kufizuar racionalisht zbulimin dhe përdorimin deri në një nevojë minimale për përmbushjen e qëllimeve të synuara (*Komisioni Federal i Komunikimeve, 2013*). Përveç kësaj, kërkohet që të krijohen masa mbrojtëse për të mbrojtur informacionin shëndetësor dhe për të siguruar që informacioni i kujdesit shëndetësor të mos zbulohet në mënyrë të pahijshme. Dështimi për të ndjekur rregulloret e HIPAA, për të mbrojtur informacionin e pacientit, mund të çojë në një ndëshkim financiar prej 11,000 dollarë, për shkelje.

4.3. Analiza e sigurisë së WBAN

Në këtë seksion, do të përshkruhen tre skenare gjenerike të punës së kujdesit shëndetësor për të ilustruar rreziqet potenciale të sigurisë që lidhen me sistemet WBAN.

1) **Rasti studimor nr.1**

Le të supozojmë se është një paciente e quajtur Luna, e cila ka një sëmundje të zemrës, kërcënuese për jetën. Aktualisht ajo është jashtë SHBA-së dhe vë re një ndryshim në ritmin kardiak, i cili zakonisht tregon një rrezik për pacientin me një sëmundje të tillë. Këtu vihet re sesa thelbësorë dhe i nevojshëm është WBAN-i, pasi ai do të mundësojë komunikimin midis pacientit dhe ofruesit të kujdesit shëndetësor nëpërmjet një aplikacioni shëndetësor. Në këtë rast studimor, njësia e parë e përgjigjes do të identifikojë tagun e Luna-s për të marrë të dhënat e saj mjekësore dhe informacionin ekzistues në bazën mjekësore. Në hapin e rradhës, shenjat e saj jetësore do të bëhen të disponueshme për t'u aksesuar nga profesionistët e kujdesit shëndetësor, të cilat mund të përmirësojnë trajtimin. Me këtë informacion të ruajtur në sistem, informacioni do të jetë i arritshëm për këdo që të intervenojë dhe do të ketë mundësi të ndihmojë. Zakonisht, lihet gjithmonë një praktikant në krye të monitorimit të të gjitha njoftimeve alarmuese për WBAN. Stafi tani është në gjendje të ngarkojë një raport nga WBAN-i i Lunës tek pajisja personale që po transmeton sinjalin. Konfigurimet pastaj bëhen në rrjetin e saj, me qëllim që të konfigurohet se kush do të jetë në gjendje të ketë qasje në WBAN-in e saj. Një përshtatje tjetër do të zhvillohet dhe do të lejojë disa të tjerë të jenë në gjendje të veprojnë në pajisjen e saj dhe të kenë qasje në të gjitha informacionet e saj mjekësore.

Njerëzit që kanë akses përfshijnë: praktikantët, infermierët, departamentin e IT-së dhe stafin tjetër mjekësor brenda spitalit. Edhe vetë Luna mund të ndryshojë politikën e saj të qasjes dhe të menaxhojë se kush fiton akses në informacionet e saj sensitive. Për shembull, vetëm një mjek mund të jetë në gjendje të shohë historinë e abuzimit me drogën, ndërkohë që një infermiere mund të mos ketë qasje në këtë informacion të ndjeshëm. Ajo që ruhet aktualisht si e dhëna mjekësore varet nga nyjet dhe kapaciteti i tyre i ruajtjes. Të dhënat origjinale dhe përditësimi mund të transferohen në një rrjet *wireless* në spital, megjithatë, të dhënat nuk do të ngarkohen derisa të sigurohet një lidhje e sigurt. WBAN-i i Lunës dhe serveri lokal *wireless* do të lejojnë akses në të

dhëna të përditësuara për t'u qasur me shpejtësi, duke i dhënë asaj ndihmën e duhur. Problemi kryesor është se si të garantohet që informacioni i ruajtur në nyje të mos askesohet ose modifikohet nga një përdorues i paautorizuar. Një kundërshtar mund të përfitojë nga dobësitë e ndryshme në sistem për të kompromet uar një nyje më pak të siguruar dhe pastaj mund të manipulojë informacionin brenda sistemit WBAN. Kjo mund të çojë që informacioni i vërtetë të jetë i paarritshëm për personelin mjekësor. Prandaj, të gjitha këto informacione, si dhe të dhënat e saj mjekësore, duhet të jenë të gjitha të koduara për ruajtje dhe është e rëndësishme që ky rrjet të jetë sa më i sigurt.

2) Rast studimor nr.2

Aktiviteti dhe lëvizshmëria e një pacienti duhet të monitorohet dhe rezultatet duhet të vlerësohen dhe të arrihen në kohë, veçanërisht në ato raste kur veprimet e pacientëve mund të çojnë në rrezikun e pacientit. Një shembull është komunikimi midis pacientit dhe ofruesit të kujdesit shëndetësor përmes një akselerometër të veshur me 3 aksa dhe të dhënat analizohen *offline*, pasi nuk kërkohet asnjë veprim i menjëhershëm. Në këtë rast, është e dëshirueshme që të merret një grup i plotë me të dhëna, që kanë të bëjnë me gjatësinë e përgjithshme të sesionit të monitorimit. Nëse të dhënat humbasin ose korruptohen dhe pacienti vuan nga një krizë, ofruesi nuk mund të reagojë. Pa mbrojtjen e përshtatshme, sulme apo ndërhyrje të tilla mund të çojnë në rrezikun e humbjes së jetës dhe të degradimit të shëndetit për pacientët, dhe nga ana tjetër mund të rezultojë me humbje financiare dhe çështje gjyqësore civile për ofruesit e shërbimeve.

Kapitulli 5 – Mekanizmat e sigurisë dhe privatësisë në WBAN

5.1. Mekanizmat e sigurisë

Ekzistojnë shumë mekanizma të sigurisë të rekomanduara për *Wireless Sensor Networks* (WSN), megjithatë disa prej tyre mund të zbatohen në një WBAN që ka një numër të ulët të fuqisë. Për shembull, *IEEE 802.15.4* është një standard i dizajnuar për *Wireless Personal Area Networks* me shkallë të ulët të të dhënave, kështu që ne mund ta quajmë atë një standard të ulët të energjisë. Shtresat e kontrollit që standardi *IEEE 802.15.4* përcakton janë aksesi i medias dhe i shtresave fizike, dhe përqendrohet në shpejtësinë e ulët dhe komunikimin me kosto të minimizuar midis pajisjeve. Ky është një standard shumë i rëndësishëm për WBANs, pasi

mbështet aplikacionet me shkallë të ulët të të dhënave dhe konsumit të kostos së energjisë. Për këtë arsye është zbatuar nga shumë hulumtues dhe dizajnerë për të zhvilluar mekanizma të sigurisë dhe protokolle për WBAN. Formatet e sigurisë të *IEEE 802.15.4* klasifikohen në: *null*, vetëm enkriptim (AES-CTR), vetëm autentifikim (AES-CBC-MAC) dhe enkriptim dhe autentifikim së bashku (AES-CCM).

- **AES-CTR**

  Në AES-CTR, mbrojtja e konfidencialitetit jepet duke përdorur Advance Encryption Standard (AES) *block cipher*. Në këtë mekanizëm, teksti i thjeshtë (*plaintext*) është ndarë në blloqe 16 bitshe, b1, b2, ..., bn, dhe teksti i shifruar (*ciphertext*) llogaritet në anën e dërguesit: **ci = bi XOR Ek (xi)**, ku ci është *ciphertext*, bi është blloku i të dhënave, dhe Ek (xi) është enriptimi i të kundërit të xi. *Figura 4* tregon procesin e enkriptimit dhe dekriptimit të CTR.

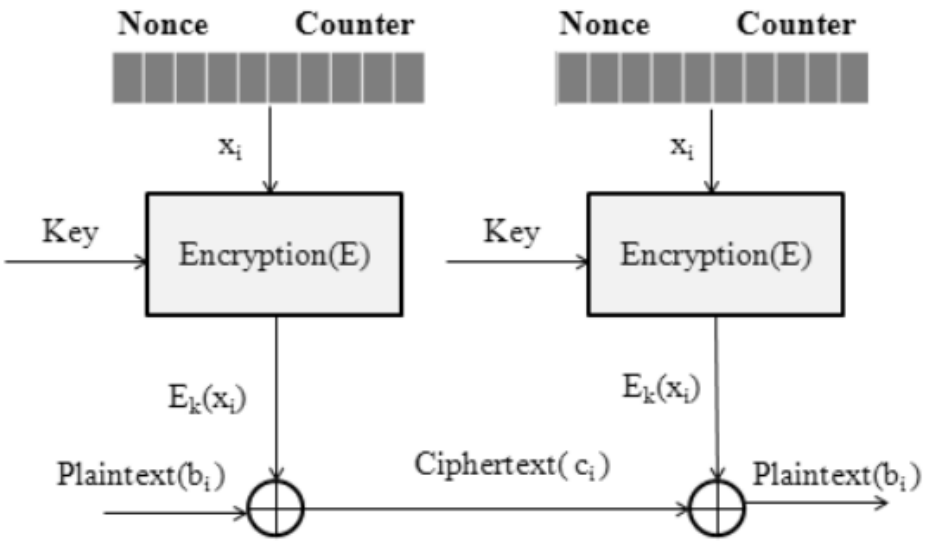

Figura 4. *Procesi i enkriptimit dhe dekriptimit të CTR*

- **AES-CBC-MAC**

  Një mbrojtje e sigurt dhe integriteti i mesazhit kërkohen gjithmonë në një WBAN. Mekanizmi i Cipher-Block Chaining Message Authentication Code (CBC-MAC) tregon se një mesazh n-blloqesh B = b1, b2, ..., bn do të vërtetohet midis dy palëve të përfshira që ndajnë një çelës sekret, K, për bllokun e shifruar, E. Nyjet sensor mund të

llogaritin një MAC me 32, 64 ose 128 bit. Vetëm pjesët që kanë çelësin simetrik mund të llogarisin MAC. Në këtë mënyrë, teksti i thjeshtë është XORed me tekstin e mëparshëm të koduar derisa të arrihet MAC përfundimtare. Në këtë moment teksti i shifruar gjenerohet nga **ci = Ek (bi XOR ci-1)** dhe teksti i thjeshtë mund të gjenerohet nga **bi = Dk (ci) XOR ci-1.** Dërguesi e krahason tekstin e thjeshtë me MAC-un e llogaritur. Marrësi i vendosur në *Tier 2* vërteton mesazhin duke llogaritur MAC-un e vet dhe e krahason atë me MAC-un e marrjes së nyjeve të sensorit. Diagrami i një operacioni CBC-MAC është paraqitur në figurën 5.

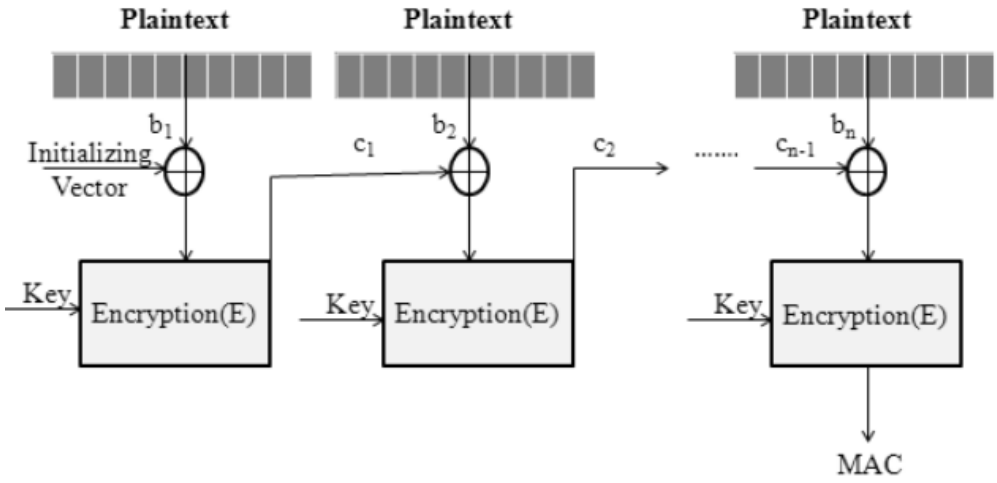

Figura 5. *Operacioni i CBC-MAC*

- **AES-CCM**

Kontrolli me mekanizmin e sigurisë CBC-MAC (CCM) është një kombinim i mënyrave të CTR dhe CBC që adreson një siguri të nivelit të lartë, duke përfshirë edhe enkriptimin dhe integritetin e të dhënave. Nyjet sensor fillimisht aplikojnë mbrojtjen e integritetit në *header* dhe ngarkesën e të dhënave të kornizave MAC duke përdorur mënyrën AES-CBC-MAC dhe pastaj kodojnë kornizat duke përdorur mënyrën AES-CTR. Ajo mund të përdoret për të komunikuar informata të ndjeshme, për shembull për të përditësuar programet në defibrillatorët kardiakë dhe në stimuluesit kardiakë.

5.2. Mekanizmi i privatësisë së të dhënave në WBAN

Zbatimi i këtij mekanizmi përbëhet nga pesë faza: (1) gjenerimi i çelësave të fshehtë të nyjeve; (2) përditësimi i çelësit sekret të nyjes; (3) fragmentimi i të dhënave; (4) klasifikimi dhe transmetimi i të dhënave; dhe (5) dekriptimi dhe verifikimi i integritetit të nyjes. Proçesi specifik është si vijon:

- **Gjenerimi i çelësave të fshehtë të nyjeve**

  Në të gjithë procesin e transmetimit të të dhënave të nyjeve, supozohet se të gjitha të dhënat e grumbulluara nga nyjet janë të sigurta. Për të siguruar transmetimin e sigurt të të dhënave private të përdoruesve, ky dokument përdor kriptografinë simetrike në nyjen e marrjes së të dhënave dhe kriptografinë asimetrike në qendrën e përpunimit të të dhënave të largëta. Në të njëjtën kohë, një çelës publik për çdo nyje duhet të ri-instalohet. Për shkak se të dhënat e grumbulluara nga secili nyje për marrjen e të dhënave në kohë të ndryshme janë dinamike, me qëllim që të shmangen rreziqet e sigurisë të shkaktuara nga veçoritë e çelësit simetrik, dizajni në këtë dokument merr çelësin e gjeneruar në mënyrë dinamike për të siguruar shumëllojshmërinë e çelësave të fshehtë.

- **Përditësimi i çelësit sekret të nyjes**

  Në program, çelësi i fshehtë ndryshon në mënyrë dinamike me përditësimin e të dhënave të grumbulluara. Në WBAN çdo nyje ka dy gjendje: nyja aktive dhe nyja *"e fjetur"*. Kur nyja mbledh të dhëna të reja, do të gjykohet nëse përmbajtja është e njëjtë me gjendjen e mëparshme. Nëse jo, do të përpunohen si të dhëna të rastësishme për të gjeneruar një çelës privat të ri. Procesi i përditësimit specifik është treguar në figurën 6:

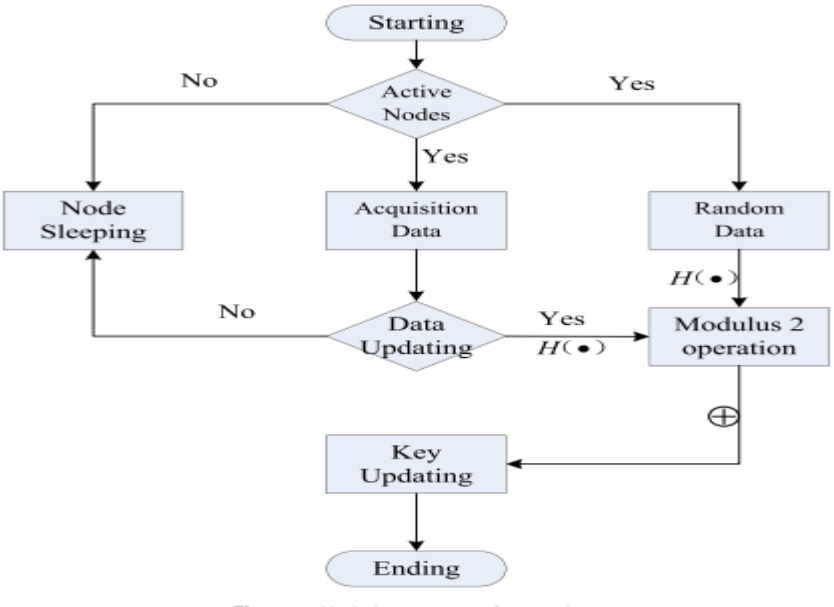

Figura 6. *Procesi i përditësimit të celësit sekret*

- **Faza e fragmentit të të dhënave**

  Kur të krijohet çelësi i fshehtë i çdo nyje marrjeje të dhënash, me qëllim që të mbrohen nyjet nga sulmuesit dhe integriteti i të dhënave nga injektimi i të dhënave nga sulmuesi, dokumenti propozon një teknikë për përpunimin e të dhënave të grumbulluara nga çdo nyje. Dhe kjo teknikë është kombinimi i segmentimit dhe riorganizimit. Ideja themelore është se çdo nyje e marrjes së të dhënave i ndan të dhënat e saj private në mënyrë të rastësishme në J pjesë, ku një nga copëzat J mbahet në vetë nyjen, ndërsa J-1 pjesët e mbetura janë të enkriptuara me nyjen e çelësave privatë dhe dërgohen në J-1 nyjet pasardhëse.

- **Faza e klasifikimit dhe transmetimit të të dhënave**

  Nyjet e sensorëve dërgojnë të dhënat e mbledhura në një telefon celular ose PDA, dhe pastaj telefoni celular ose PDA, duke punuar si pikë hyrjeje në një rrjet të jashtëm, përpunon të dhënat e marra. Pastaj, telefoni celular do ta enkriptojë rezultatin me çelësin publik K_p dhe do ta dërgojë atë në qendrën e përpunimit, domethënë, të riklasifikojë të dhënat e enkriptuara dhe ta rivendosë atë në të dhënat origjinale në secilin nyje, dhe më vonë ta dërgojë në qendrën e përpunimit *remote* direkt pas ri-enkriptimit të tij.

- **Dekriptimi dhe verifikimi i integritetit të nyjes**

Parimi i dekriptimit: dekriptimi i të dhënave kryhet në qendrën e përpunimit *remote* të terminalit *remote*. Dekriptohen blloqet e të dhënave në mënyrë të përsëritur përmes mekanizmit të kodimit asimetrik. Së fundmi, përfitohet një çelës privat për secilën nyje.

Kapitulli 6 - Sfidat me të cilat përballet WBAN dhe e ardhmja premtuese e saj

6.1 Sfidat e një sistemi WBAN

Për të zbatuar sistemin WBAN në botën e telemjekësisë, ne duhet të heqim disa gabime duke shfrytëzuar përparimet e fundit teknologjike. Pajisjet mjekësore që përdoren për krijimin e një rrjeti quhen nyjet e trupit (BNs). Këto BN janë të ndryshme nga njëra tjetra dhe kryejnë funksione të dallueshme, ku çdo funksion kërkon fuqi të ndryshme për të kryer një detyrë specifike në lidhje me ekzaminimin, trajtimin dhe monitorimin e shëndetit të pacientit. Prandaj lind nevoja për cilësi të ndryshme të shërbimit nga secila BN. Për më tepër, numri i nyjeve dhe madhësia e tyre duhet të kufizohen, pasi nyjet e trupit njerëzor përballen me kufizime hapësinore. Prandaj, për shkak të hapësirave të kufizuara hapësinore, funksioni i kryer nga çdo nyje duhet të jetë ekskluziv dhe efektiv. Për të kryer funksionet në mënyrë efektive dhe për të siguruar fuqinë e dëshiruar tek nyjet e trupit ne kemi nevojë për një bateri të aftë për të prodhuar energji të përshtatshme. Meqenëse madhësia dhe pesha e nyjeve të trupit janë drejtpërdrejt proporcionale me kapacitetin e energjisë të baterisë, çdo efekt për të rritur kapacitetin e energjisë të baterisë do të rritë gjithashtu madhësinë dhe peshën e nyjes së trupit që e bën të parehatshme për trupin e njeriut. Ekziston një sfidë për ta bërë BN-në sa më të vogël që të jetë e mundur, në mënyrë që trupi i njeriut ta mbajë atë lehtësisht. Për më tepër, kapaciteti i kufizuar i baterisë gjithashtu vë një kufizim në hapësirën e jetës së nyjeve të trupit. Një nyje me bateri mund të kryejë funksionalitetin e saj për aq kohë sa bateria është e ngarkuar në nivel të pranueshëm. Por, meqë ngarkesa e baterisë bie nga niveli i saj i mjaftueshëm, shkalla e performancës së nyjes së trupit gjithashtu zbret. Më në fund, bateria është drenazhuar dhe nyja bëhet përgjithmonë inaktive. Për të rinisur funksionimin e duhur të nyjeve të trupit, ekziston nevoja për të zëvendësuar baterinë sa më shpejt që të jetë e mundur, gjë që mund të mos jetë praktike gjatë gjithë kohës, pasi ajo mund të rrezikojë pacientin. Ky problem bëhet më akut kur nyja futet brenda trupit, pasi kjo do të kërkojë që pacienti t'i nënshtrohet një procedure kirurgjikale. Është ilustruar se nyjet e sensorit të trupit punojnë në bateri dhe kjo është e

nevojshme për të rimbushur baterinë në intervale të fundme për të rifilluar ose për të vazhduar operimin e sensorit të trupit. Zëvendësimi i baterisë duke ndaluar funksionimin e sensorëve, në rastin e pacientëve nuk këshillohet dhe duhet të shmanget sepse mund të çojë në komplikacione të rënda që mund të çojnë në vdekje. Rritja e kapacitetit të baterisë mund të zgjasë kohën e jetës së sensorit, por kapaciteti i baterisë mund të rritet deri në një kufi pasi varet në mënyrë rigoroze nga madhësia dhe pesha e baterisë dhe gjithashtu nga sensorët që përdoren.

Besueshmëria për aplikacionet e kujdesit shëndetësor të WBAN është shumë e rëndësishme dhe duhet të plotësohet përballë këtyre katër sfidave të veçanta për WBAN-et.

- **Efikasiteti ekstrem i energjisë:** Për të ofruar nivelet e rehatisë dhe mosdiskriminimit të kërkuar për adoptim të gjerë, nyjet sensor WBAN duhet të jenë të vogla dhe të kenë bateri që zgjasin për ditë dhe vite me rradhë, pavarësisht nga aplikacioni. Kërkesa e madhësisë natyrisht kufizon madhësinë e baterive që do të fuqizojnë nyjet, kështu që nyjet WBAN duhet të jenë jashtëzakonisht të kursyera në përdorimin e tyre të energjisë.
- **Karakteristikat unike të kanalit të valëve:** Sjellja e kanalit të valëve rreth trupit të njeriut paraqet një grup sfidash për një komunikim të besueshëm. Ndryshe nga rrjetet e tjera më të gjata ku distanca midis transmetuesit dhe marrësit dominon zbutjen e sinjalit, fuqia e një sinjali WBAN është më së shumti e prekur nga vendndodhja fizike dhe orientimi i nyjave në raport me njëra-tjetrën.
- **Menaxhimi i ndërhyrjeve:** Nyjet në një WBAN mund të koordinohen nga qendra, duke lejuar kështu një numër të madh pajisjesh të bashkëjetojnë në një rrjet të vetëm pa i ndërhyrë njëri-tjetrit. Gjërat bëhen më të ndërlikuara kur njerëzit e shumtë që mbajnë WBANs vijnë në varg të njëri-tjetrit. Në këtë rast koordinimi mund të bëhet i pamundur. Vështirësia vjen nga veprimet e njerëzve, të cilat janë të paparashikueshme nga pikëpamja e një rrjeti dhe mund të rezultojnë në rrjete që lëvizin brenda dhe jashtë fushës së njëri-tjetrit. Në një situatë të tillë nuk ka mënyrë të natyrshme të zgjedhjes së një koordinatori të rrjetit. Si pasojë, çdo skemë e zbutjes së ndërhyrjeve do të duhet të përshtatet më shpejt se shkalla me të cilën ndryshon topologjia e rrjetit nëse është e suksesshme në minimizimin e ndërhyrjes.
- **Kërkesat e aplikimit:** WBAN-et gjithashtu duhet të mbështesin një gamë të gjerë të normave të xhiros (1 kb / s deri 10 Mb / s) për të akomoduar video, duke ofruar ende besueshmëri të lartë në shumë aplikacione mjekësore.

6.2. Projekte ekzistuese të WBAN

Në vitet e fundit janë shfaqur shumë punime në literaturë rreth WBANs. Përpjekjet janë të përqendruara kryesisht në propozimin e zgjidhjeve për çështjet e WBANs. Para prezantimit të standardit *IEEE 802.15.6* nga grupi i punës *IEEE 802.15*, struktura e WBANs, protokollet dhe mekanizmat e shtresës fizike dhe nënshtresës së MAC të WBANs kanë qenë një nga shqetësimet më të rëndësishme që tërhoqën vëmendjen e shumë kërkuesve. Ekzistojnë aktualisht disa grupe kërkimore në të gjithë botën, të cilat fokusohen në hartimin dhe zbatimin e një WBAN. Hulumtuesit kanë përdorur teknologji të ndryshme *wireless* në projektet e tyre, si: IEEE 802 family of WPANs, WLANs, Bluetooth dhe Zigbee.

Për shkak të disavantazheve të mëdha të WPAN dhe WLAN, sistemi i *IEEE 802.15.4 / Zigbee* ka qenë qasja më e favorizuar në projektet ekzistuese para se të futet standardi *IEEE 802.15.6.* Një nga projektet propozon një system, që mund të kryejë monitorim në kohë reale të kushteve komplekse në të dhënat e transmetimit, nga sensorë të ndryshëm të trupit brenda një WBAN-i. Sistemi mundëson zhvillimin e aplikacioneve mjekësore personale duke përdorur pajisje personale elektronike të kombinuara së bashku me sensorë në një WBAN.

Stevan Marinkoviç dhe Emanuel Popoviçi zhvilluan dhe testuan një Nano power Wake up Radio të dedikuar kryesisht për WBANs, por mund të përdoret gjithashtu në lloje të tjera të rrjeteve me valë të ulët. Radioja u testua për konsumin e energjisë dhe qëndrueshmërinë ndaj ndërhyrjeve të komunikimit nga një pajisje celulare e gjetur zakonisht rreth personit që mbante një WBAN.

Janani.K, V.R. , SarmaDhulipala dhe R.M.Chandrasekaran zhvilluan një *framework* të bazuar në WSN për monitorimin e shëndetit të njeriut. Në këtë punim, *framework-u* i propozuar jep një kuptim të qartë se si WSN përdoret për monitorimin e largët të shëndetit të pacientit. Dokumenti kryesisht fokusohet në kuptueshmërinë e monitorimit të largët të pacientit të kryer në spital, parametrat vitalë të rrjetit që duhet të merren parasysh, shkallëzimin dhe konsumin e energjisë.

Jae-Hoon Choi dhe Heung-Gyoon Ryu propozuan një skemë të re QAPM (Quadrature-Amplitude-Position Modulation) për përmirësimin e efikasitetit të energjisë. Ata analizuan PSSK ekzistuese dhe skemën e re QAPM. Skema e PSSK dhe QAPM janë metodë zgjerimi për rritjen e efikasitetit të energjisë. Dhe rezultatet e simulimit, tregojnë se performanca BER e QAPM dhe PSSK është më e mirë se QAM dhe PSK në kanalin AWGN.

Në projektin e Monitorimit të EKG, u hartua dhe zhvillua një sistem monitorimi i gjithanshëm i mbikëqyrjes shëndetësore duke përdorur EKG, Photoplethysmogratphy (PPG), Temperaturën e trupit dhe Accelerometer etj. Në këtë sistem, WBAN, Zigbee, përdoret për të komunikuar midis pajisjeve të sinjalit të lëvizshëm fiziologjik dhe sistemit të lëvizshëm personal. Sistemi i vëzhgueshëm i monitorimit të kujdesit shëndetësor, që mund të përdoret mundëson transmetimin e të dhënave fiziologjike në rrjetin e sensorëve *wireless* për rrjetin mobile.

6.3 Nga WBAN në BBN

Njerëzit që përdorin pajisje të *"zgjuara"* kanë një potencial të madh për të zgjeruar infrastrukturën ekzistuese të Internet of Things (IoT), duke zbatuar aplikacione të vërteta të kujdesit shëndetësor (U-health), duke siguruar lidhjen e pacientëve kudo dhe në çdo kohë. Përmes përcjelljes së të dhënave të ndjeshme nga personi në person deri në arritjen e një shërbimi mjekësor, U-health bëhet më i besueshëm me teknologjinë e Body-to-Body Networks që pritet të zëvendësojnë WBANs në të ardhmen. Motivuar nga nevoja në rritje për zgjidhje të largëta dhe të përmirësuara të kujdesit shëndetësor, WBAN-të ende formojnë një fushë hulumtimi në rritje, të nxitur nga zhvillimi i standardit *IEEE 802.15.6*. Për më tepër, zhvillimi i WBAN-ve të vetme që operojnë në një BBN në shkallë të gjerë bashkëpunuese, është subjekt i një sërë sfidash të projektimit.

1) **Koncepti BBN:** Një Body-to-Body Network (BBN) përbëhet nga disa WBANs, dhe secili komunikon me të afërmin e tij. Pajisja koordinatore luan rolin e një porte që ndan të dhënat e komunikimit me WBAN-et e tjerë. Rrjeti Body-to-Body është teorikisht një rrjetë që përdor njerëzit për të transmetuar të dhëna brenda një zone të kufizuar gjeografike. Duke përdorur pajisje të tilla si *Smartphones* ose *Smartwatches*, një sinjal dergohet nga WBAN tek përdoruesi më i afërt BBN, i cili transmetohet tek përdoruesi tjetër BBN më i afërt dhe kështu me radhë derisa të arrijë destinacionin. Figura 7 ilustron një shembull të rrjetit BBN që përdoret për monitorimin e U-Health të një grupi çiklistësh.

Figura 7. *Body-to-Body Network që përdoret për monitorimin e U-Health të një grupi çiklistësh.*

2) **Standardet:** Ashtu si WBANs , edhe një BBN përdor standardet e komunikimit të tilla si *IEEE 802.15.6*, i cili është një standard *wireless* pa fuqi dhe me rreze të shkurtër të përdorur për pajisjet që veprojnë brenda ose rreth trupit të njeriut. Ky standard mbështet normat e të dhënave deri në 10 Mbps, ndërkohë që përputhet me udhëzimet e rrepta të mosndërhyrjes. Pastaj, *IEEE 802.15.4* (ZigBee), i cili merret me interkonektimin e pajtueshëm të pajisjeve të komunikimit duke përdorur shpejtësinë e të dhënave të ulëta, jetëgjatësi të ulët të energjisë, por shumë të gjatë të baterisë dhe transmetime të radiofrekuencës me rreze të shkurtër (RF) . Sidoqoftë, është e mundur të përdoren standarde të tjera në BBNs, si 802.11 (WiFi) ose 4G.
3) **Sfidat:** Sfidat kryesore për BBN janë: efiçienca e energjisë, kur koordinatorët do të luajnë rolin e kokës së grupit dhe do të përcjellin vlerën ose shenjat vitale në rastin e një aplikacioni mjekësor në WBAN të tjerë brenda një grupi. Pastaj routing e të dhënave të mbledhura përmes WBANs fqinje deri në destinacion, me konsiderata QoS dhe aftësinë për të mbështetur lëvizshmërinë WBANs, është një çështje e dytë. Megjithatë, të dhënat e krijuara dhe të transmetuara në një BBN duhet të kenë akses të sigurt dhe të kufizuar. Gjithsesi, njerëzit mund të shohin BBN-të si një burim kërcënimi për të dhënat e tyre dhe jetën private, ndaj dhe pranimi i tyre është çelësi i suksesit të BBN-ve. Grupet e të dhënave vitale të pacientit mund të jenë të fragmentuara midis disa nyjeve, por nëse nyja nuk përmban të gjithë informacionin e njohur, niveli i kujdesit të pacientit mund të mos jetë aq i mirë.
4) **Aplikacionet:** Rrjetet Body-to-Body mund të përfaqësojnë zgjidhje të reja që sigurojnë përfitime reale sociale, të tilla si kujdesi shëndetësor i largët, monitorimi i saktë i atletëve, ekipet e shpëtimit në një zonë fatkeqësish ose grupe ushtarësh në një fushë beteje etj. Megjithatë, BBN mund të zbatohet në të dy aplikacionet mjekësore dhe jo mjekësore. Sidomos, edhe pse BBN-të përfaqësojnë trendin e ri për sistemet e ardhshme të kujdesit shëndetësor në të ardhmen, në të vërtetë monitorimi i largët i pacientëve që mbajnë sensorë truporë dhe transmetimi i të dhënave fiziologjike të njëri-tjetrit deri në qendrën mjekësore, mund të zvogëlojë në masë të madhe tendencën aktuale të buxheteve shëndetësore dhe të bëjë vizionin e qeverisë për kujdesin e domosdoshëm shëndetësor për pacientët e largët një realitet.

KONKLUZIONE

Një Wireless Body Area Network (WBAN) vlerësohet të jetë një teknologji shumë e vlefshme, me potencial për të ofruar një gamë të gjerë përfitimesh për pacientët, një monitorim të vazhdueshëm të shëndetit dhe dhënien e një reagimi në kohë reale për pacientin ose personelin mjekësor. Siguria është një tipar thelbësor për zbatimin e WBANs. Zbatimi i WBANs duhet të përmbushë kërkesat rigoroze të sigurisë dhe privatësisë. Megjithatë, hartimi i rezultateve të praktikave të sigurisë është një proces i ndërlikuar për shkak të kufizimeve dhe karakteristikave të mjedisit të WBAN.

Një mekanizëm i duhur i sigurisë për WBANs duhet të marrë në konsideratë cenueshmërinë e WBANs ndaj faktorëve të ndryshëm dhe të zbatojë një metodë efikase dhe të fuqishme të rikuperimit të gabimeve. Kur zhvillojmë një zgjidhje sigurie për WBANs, duhet të kemi parasysh se përputhet me çdo anë të WSN-së, siç janë privatësia e të dhënave, integriteti, freskia e të dhënave, autentifikimi i identitetit dhe disponueshmëria që e bëjnë WBANs të jenë të sigurta. Nëse është e nevojshme të rekomandohet një përshtatje e re e politikave në kujdesin shëndetësor, një hap i ardhshëm është zhvillimi i mekanizmit të kontrollit të qasjes më i mirë, më fleksibël, më i sigurt dhe kriptografik.

REFERENCA

- Syed Furqan Qadri, Salman Afsar Awan, Muhammad Amjad, Masood Anwar, Suneel Shehzad. (2012). Applications, Challenges, Security of Wireless Body Area Networks (WBANs) and Functionality of IEEE 802.15.4/Zigbee. https://pdfs.semanticscholar.org/2999/1d3c1b78e15aaa58e19b9df5556d5bef6990.pdf
- Shikha Pathania , Naveen Bilandi. (2014). Security issues in Wireless Body Area Network. https://pdfs.semanticscholar.org/b04a/94c36dcf2d5a0b6cb3b3eb72867c0f744c6a.pdf
- Muhammad Sheraz Arshad Malik, Muhammad Ahmed, Tahir Abdullah, Naila Kousar, Mehak Nigar Shumaila. (2018). Wireless Body Area Network Security and Privacy Issue in E-Healthcare. http://thesai.org/Downloads/Volume9No4/Paper_33Wireless_Body_Area_Network_Security.pdf
- Ilkyu Ha. (2015) . Technologies and Research Trends in Wireless Body Area Networks for Healthcare: A Systematic Literature Review. http://journals.sagepub.com/doi/pdf/10.1155/2015/573538
- Mohammad Ghamari , Balazs Janko, R. Simon Sherratt, William Harwin , Robert Piechockic .(2016). A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environments. http://www.mdpi.com/1424-8220/16/6/831/htm
- Deshpande Niranjan , Vadane Pandurang, Sangle Sagar, Prof. Dighe M.S. (2016). A IOT-based Modern Healthcare System Using Body Sensor Network (BSN). http://www.ijircce.com/upload/2016/november/129_paper%20publish_proMOD.pdf
- Bogdan Antonescu, Stefano Basagni. (2015). Wireless Body Area Networks: Challenges, Trends and Emerging Technologies. http://www.ece.neu.edu/fac-ece/basagni/papers/AntonescuB13.pdf
- Pervez Khan, Md.Asdaque Hussain, Kyung Sup Kwak. (2009). Medical Applications of Wireless Body Area Networks. https://pdfs.semanticscholar.org/910f/599baed6b62d596ad901220153b4f003eba0.pdf
- Ragesh G, Dr.Baskaran. (2012). An Overview of Applications, Standards and Challenges in Futuristic Wireless Body Area Networks.