Spring 6-2021

TË METAT DHE PËRPARSITË E TEKNOLOGJISË ZIGBEE NË SMART HOME

Jetmir Shillova

Programi për Shkenca Kompjuterike dhe Inxhinierisë

TË METAT DHE PËRPARSITË E TEKNOLOGJISË ZIGBEE NË SMART HOME

Punim Diplome Bachelor

Studenti: Jetmir Shillova

Qershor / 2021
Prishtinë

Programi për Shkenca Kompjuterike dhe Inxhinierisë

Punim Diplome
Viti akademik 2013/2014

Jetmir Shillova

Të metat dhe përparsitë e teknologjisë ZigBee në Smart Home

Mentori: prof.Dr.sc Besnik Qehaja

Qershor / 2021

Ky punim është përpiluar dhe dorëzuar në përmbushjen e kërkesave të pjesshme për Shkallën Bachelor

ABSTRAKT

Teknologjia dhe hapat e saj gjigande, dita ditës sa vijnë e bëhen nevojë për shoqërinë moderne. Sa rritet gjithëperfshirja e automatizimit, aq me shumë po rriten kërkesat për zhvillim të mëtutjeshëm të saj, veçori e cila po shtyen depërtimin e digjitalizimit në çdo cep, e madje edhe brenda shtëpive tona. Të gjitha këto benificione dalin nga avancimi i aplikacioneve softuerike të cilat zhvillohen nëpërmjet teknologjive më të reja. Teknologjitë e reja po e bëjnë më të lehtë madje edhe jetesën brenda shtëpive tona. Ashtu siç janë avancuar telefonët, të njejtën ritëm po fillojnë t'a marin edhe shtëpitë, që po na drejtojnë drejt termit Smart-Home, term i cili sot duket mjaft i familjarizuar. Hapat e parë filluan nga Smart-Phone, e që sot kemi arritur deri në Smart-Home. Prandaj, përmes punimit tim shkencor do të trajtoj idenë dhe rrugëtimin e digjitalizimit deri në implementimin e saj brenda shtëpive. Korniza kryesore që qëndron pas këtij procesi është "Të metat dhe përpasitë e teknologjisë Zigbee në Smart-Home". Në punim tregohet se si mund të realizohet ky proces në mënyrë të sigurtë përmes kornizës së lartë përmendur. Analizimi i hapave të teknologjisë, krahasimi i zhvillimit dhe përdorimit të mjeteve jo digjitale me mjetet automatikodigjitale, përparsitë dhe të metat, e çdo aspekt tjetër i cili po përdoret ditëve të sotshme. Poashtu edhe ato veçori që ndoshta janë jo edhe aq të sigurta dhe praktike për të qenë pjesë e shtëpive tona, të gjitha këto do të analizohen, dokumentohen dhe rezultohen, duke perdorur literaturen, hulumtimin, dhe analizën e shtëpive automatike.

Fjalë kyçe: Automatizim, Smart-Home, ZigBee

FALEMNDERIM

Çdo rrugëtim ka një destinacion dhe unë arrita në këtë destinacion. Falë perkushtimit dhe punës së palodhshme unë arrita synimet e mija, arrita që ëndërrat të mos i lë vetëm ëndërra. Jam mirënjohës pafund për familjen time të ngushtë, bashkëshorten Donjeten dhe djalin Roin, të cilët janë motivi im për të vazhduar tutje.

Falemnderim i veçantë shkon për universitetin UBT, për pedagogët e shkëlqyer, me të cilët kam patur kënaqësinë të bashkëpunoj dhe të strukturoj në mënyrën më të mirë së pari karakterin tim, e pastaj vizionet dhe mundësitë e arta për një të ardhme sa më të mirë.

I jam mirenjohës tej mase mentorit tim, prof. Dr.ass. Besnik Qehaja, për mbështetjen dhe ndihmën e palodhshme që ma ofroi gjatë gjithë studimeve të mija. Profesori Qehaja është shembulli më i mirë se si ta duash profesionin dhe si t'i ndihmosh të tjerët ta duan atë që e bëjnë.

PËRMBAJTJA

LISTA E FIGURAVE

FJALORI I TERMEVE

PID – Proportional Integral Derivates

O-QPSK - Offset Quadrature Phase Shift Keying

DSSS – Direct Sequence Spread Spectrum

CSMA-CA - Carrier Sense Multiple Access / Collision Avoidance

CRCs – Center for Reasearch on Computation and Society

FCS – Frame Check Sequence

IEEE – The Institute of Electrical and Electronics Engineers

IoT – Internet of Things

Cisco IBSG – CISCO Internet Business Solution Group

IOS – Iphone Operating System

ISM – Information Security Managment

MBPS – Mega Bit per Second

BLE – Bluetooth Low Energy

WRF – The Weather Research and Forecasting

MHz – Mega Herz

HD – High Definiton

6LoWPAN – Internet Protocol version 6 over Low-Power Wireless Personal Area Network

ID - Identification

TCP/ IP – Transmission Control Protocol / Internet Protocol

PHY – Physical Layer

MAC – Media Access Control

NWK – Networking

APS – Advances Production System

ZDO – ZigBee Device Profile

GPS – Global Positioning System

LAN – Local Area Network

AAL – ATM Adoptation Layer Computing

RFID – Radio Frequency Identification

MCU-PT – Microprocessor Controlled Unit

1. HYRJE

Teknologjia ZigBee apo standardi 802.15.4 filloi të përfshihej në shtëpitë e mençura që nga vitet e 90-ta ku edhe filloi zhvillimi i llambave, sistemeve të sigurisë etj. Si për fillim, kontrollimi i këtyre pajisjeve ishte në mënyre manuale.

Shtëpi intelegjente duhet të ketë mundesinë që ato sisteme të mund t'i kontrollojnë pajisjet të cilat kanë role të caktuara në jetën e përditshme, siç e kemi shembullin e llambave, temperaturës, sistemin për mirëmbajtje të kopshtit, sigurimit të shtëpisë, e shumë pajisje të tjera.

Termi "intelegjencë" përmbanë funksionet të cilat ndihmojnë sistemet e shtëpive të automatizohen dhe të zgjedhin se si të kontrollohen. Pra, kompleksiteti është më i lartë se sa vetëm komandimi i tyre përmes sinjaleve "on/off" kjo për arsye të algoritmave si PID. (Yang, 2008) [31]

Specifikat e ZigBee përmbajnë siguri të lartë në shumë variante: përmban O-QPSK and DSSS, CSMA-CA, 16bit CRCs, mesh networking, end-to-end verify data.

ZigBee përmbanë low-data rate për arsye se esenca e Zig-Bee është wirelessi i cili monitoron dhe kontrollon, pra, nuk ka komunikim përmes këtij wirelessi, e aq me pak, bartje të zërave apo videove.

Protokolet e ZigBee i përshtaten mikrokontrollerëve 8 bitësh me 16 dhe 32 bit zgjidhje të mundshme. Gjithashtu, përdor O-QPSK dhe DSSS, një kombinim i cili mundëson një performancë të shkëlqyer në radio sinjalet e ulëta low signal-to-noise. Për tu siguruar se bitët me të dhëna janë korrekte në secilën paketë ZigBee përdorë 16-bit CRC duke e thirrur Frame Checksum(FCS).

Për pjesën e sigurisë, përdoret NIST dhe AES. Këto standarde përdoren për enkriptim dhe dekriptim të paketave.

Duke patur parasyshë se ZigBee përdor IEEE. 802.15.4, mund të definojmë se përdor një bandë prej 2.4GHz, sepse, IEEE ka përbërjen me këto radio standarde. (Gislason, 2008)

2. SHQYRTIMI I LITERATURËS

2.1. Evaluimi i Rrjetave IoT

Avancimi në teknologji çdo herë e më shumë po mundëson një jetesë më të mirë dhe më të lehtë, mirëpo, klasifikimi social mund të vërehet lehtë.
Interneti i gjërave (IoT) është një ekosistem i pajisjeve të lidhura që shkëmbejnë të dhëna përmes një rrjeti me tel ose pa tel. Këto pajisje mund të jenë telefonat e mençur, laptopët, pajisjet elektrike të mençura, pajisje e mençura në zyre ose çdo pajisje tjeter që përmbanë sensorë. Të dhënat e gjeneruara nga këto pajisje ndahen më pas në serverat e vendosur në cloud ose në serverat lokal, ku përpunohen dhe menaxhohen.

Ekosistemi IoT mund të vendoset jo vetëm brenda zonave të vogla si shtëpitë ose zyret tona por edhe mbi zona më të mëdha si komunitetet e mbyllura, kampusi universitar e qytetet. Pajisjet e mençura që lidhen me njëra-tjetrën janë pjesë e kudondodhur e jetës sonë. Si një përdorues individual ose pronar i biznesit që ofron produkte dhe shërbime të lidhura me IoT, mund të kuptohet evolucioni i IoT. Njohja e së kaluarës na aftëson të parashikojmë të ardhmen dhe të përdorim çdo teknologji në avantazhin tonë. IoT përshkruhet si evaluimi i parë i Internetit. Duke filluar nga një market, evaluimi i saj u rrit duke marë përmasat e një idustrie të tërë. Pajisja e parë e lidhur në internet ishte një pajisje e Coca-Cola e programuar nga programerët lokal diku në vitet e 80-ta. (Keith D.Foote , 2016) [1]

Në fillim të shekullit 21, rreth vitit 2000, termi Internet of Things u shfaq në treg përmes mediave duke marë një etiketim në të gjithë botën. Interesimi për teknologjinë IoT po rritej vazhdimisht, me çrast u organizua edhe Konferenca e Parë Ndërkombëtare e Internet of Things e mbajtur në Zvicër më 2008, ku morën pjesë 23 vende dhe diskutuan rreth komunikimeve pa tel me rreze të shkurtëra dhe rrjete të sensorit. Diku mes viteve 2008-2009 lidhja e objekteve në internet u rrit më shumë se lidhja e njerëzve, ku sipas Cisco IBSG prej aty lindi edhe fjala “Internet of things”. Në vitin 2010, rreth 12.5 miliardë pajisje doli të ishin të lidhura në internet dhe numri u rrit në mënyrë dramatike për të arritur 25 miliardë në 2015. Më pas, duke vazhduar më tej, në vitin 2013, IoT është perfshier në sistem duke përdorë teknologji të ndryshme e deri tek embedded systems. (M. A. Ezechina, K. K. Okwara, A. U. Ugboaja, 2015) [2]

Në 2019, Gartner parashikoi që ndërmarrja dhe tregu i IoT do të rritej në 5.8 miliardë në vitin 2020, duke shënuar një rritje prej 21% nga viti 2019. Gjithçka që mund të lidhet (to be connected) do të lidhet, duke formuar kështu një sistem dixhital gjithëpërfshirës ku të gjitha pajisjet komunikojnë me njerëzit dhe njëri-tjetrin. (EGHAM, 2019) [3]

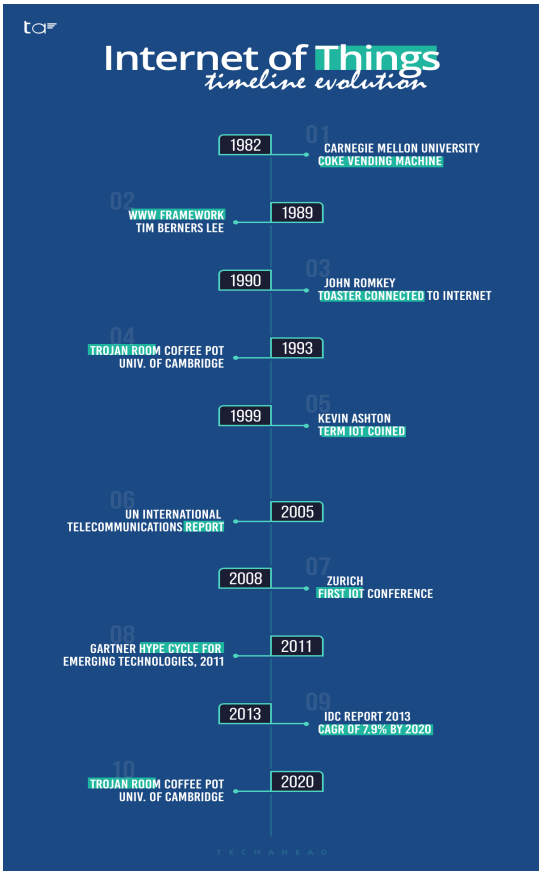

Figura 1. Evaulimi i IoT

Më poshtë janë disa faktorë të rëndësishëm që nxisin këtë zgjerim të shpejtë të IoT:

- Rënia e kostos së senzorëve;
- Rënia e kostos së grumbullimit dhe ruajtjes së të dhënave për shkak të mundësisë Cloud;
- Zgjerimi i gjerë i lidhjes së internetit;
- Rritja e fuqisë informatike;
- Rritja e depërtimit të smartphone dhe tablet.

Trendi i sotëm i internetit përfshinë mobilitetin; individët mund t'i kryejnë gati se të gjitha punët përmes aplikacioneve, rrjetet sociale; kanali i preferuar për komunikim, embedded systems; pajisje të vogla e praktike për ambientet e përditshme të cilat mundësojnë edhe funksionimin e e-health, cloud computing; Zgjidhja më e mirë për ruajtjen e informacioneve. Por, ky trend ka edhe pasojat e saja, ku mund t'i tregojmë përmes disa shpembujve; mundësia e keqpërdorimit te informacionit, shfrytëzuesi mund të kërkoj informata nga ambientet publike, poashtu, shfrytëzuesi mund të përdorë pajisjen pa e pasur fare në pronë.

Fraza "Internet of Things" i'u referohet të gjitha pajisjeve të cilat lidhen në Internet. Investimi në shëndetsi, shtëpi, zyre e kompani, është duke e ngritur cilësinë e jetesës moderne, mirëpo, IoT ka një kosto mjaftë të lartë sidomos kur vihet në pyetje "siguria" dhe "privatësia". Të dhënat e individëve, qoftë pacienti apo klienti, kërkojnë një mbrojte, privatësi e siguri të nivelit të lartë, gjë e cila sot është qështja bazë e diskutimit në IoT. Ndjeshmëria e të dhënave individuale dhe përfshirja pothuajse e domosdoshme e tyra në internet, po e zgjeron edhe më tej rrezikun tek individët, por, në të njëjtën kohë edhe sfidat e zhvilluesve për të sjellë zhvillim të vazhdueshëm të shtresave më të sigurta. Nëse duam t'i japim një definim, "Internet of Thing"- (IoT) përfaqson konceptin se si teknologjia vazhdimisht lidh teknologjitë, në të njëjtën kohë edhe njerëzit mes vete. Mund të gjendet pothuajse gjithandej dhe në të gjitha askeptet, duke filluar nga industritë e deri tek njerëzit. (EGHAM, 2019) [13]

2.2 Teknologjitë dhe implementimi i Rrjetave IoT në industri

Koncepti dhe implementimi i rrjetave në IoT është një sinonim i automatizimit. Synim kryesor është lidhja në mes të pajisjeve komplekse dhe atyre të sofistikuara, në mënyrë që të kontrollohen dhe menaxhohen më lehtë. Ne si përdorues, njëkohësisht, edhe ne si zhvillues është e rëndesishme të kuptojmë se pajisjet IoT përdorin senzorë për gjenerim e të dhënave.

Implementimi i IoT në industi ka për qëllim të reduktoj nderlidhjen njeri-njeri. Siç e kemi cekur edhe më lartë, duke filluar nga smart-phones sot kemi arritur deri tek smart-homes. Nuk është interesante që IoT në prodhim është i dobishëm si për prodhuesit ashtu edhe për klientët e tyre. Industri IoT u mundëson prodhuesve që të shkallëzojnë pajisje të ndryshme të afta për vëzhgim dhe servisim të nivelit të lartë. Kështu, kompanitë mund të kenë një vlerësim të duhur të nevojave të klientëve. Prodhimi si një nga industritë po merr perspektivat e IoT. Shumë impiante tashmë po përdorin sisteme të lidhura kontrolli për procesion dhe mbikëqyrje. Ndërsa konsideratat e sigurisë nuk janë të reja në kontekstin e teknologjisë së informacionit, atributet e shumë implementimeve të IoT paraqesin sfida të reja dhe unike të sigurisë. Zgjidhjet që ofron IoT në industrinë e prodhimit ndihmojnë në organizimin e menaxhimit, monitorimin e përformancave, gjë e cila mundëson jetëgjatësi të harduerëve. Njësoj edhe në industrinë e Agrokulurës e në sektorin e energjisë, zgjidhjet e problemeve që IoT ka pasur rezultate mjaftë pozitive duke mundësuar energjinë solare dhe të erës.

Auto-Makinat, që sot mund të lëvizin edhe pa ndihmën e palës njerzore është një pikë tjetër kyqe e automatizimit në IoT. Me ndihmën e senzorëve, arkitekturen e cloud, senzorëve proximity, dhe disa teknologjive të tjera të cilat përdorin softweret IoT për të qenë të dhënat real-time përgjatë lëvizjes së makinës, matjes së shpejtësisë, sinjaleve, shënjave të ndalimit. (Waher, 2015)

Smart-watch, tjetër teknologji e IoT e cila përdor të dhënat real-time të shfrytëzuesit. Përcjellja e aktiviteteve, monitorimi i të rrahurave të zemrës, numrimi i hapave, të gjitha këto lidhen me smart-phonet tanë përmes IOS dhe Android apps and systems. Përfshirjen e IoT gjithashtu e kemi edhe

në qendrat e shëndetsisë, ku përmes aplikacioneve përfshihet monitorimi në kohë reale i pacientit, nga stafi shëndetsor, përmes lokacioneve të ndryshme. Terapitë pacientët mund t'i marin edhe nga larg, pastaj edhe frigoriferët e vaksinave mundësojnë monitorim nga larg (remote monitoring), shtretër 'smart' të cilat japin të dhëna reale për pacientin. Pra, këto pajisje janë të lidhura me të dhënat IoT.

Smart-Homes, përfshirë automatizim të shtëpive duke mundësuar një jetesë më të lehtë. Sensorët elektik, aplikacionet e ndryshme dhe sistemet elektrike e mekanike mund të përdoren për automatizim dhe ndërlidhje në internet. Sistemet si dritat e mençura mund të kontrollohen përmes telefonave të mençur. I gjithë sistemi i automatizimit të shtëpisë mund të lidhet me platforma të ndryshme, të kontrollohet dhe të menaxhohet nga Al platforma. Të gjitha këto teknologji që përfshihen në IoT po mundësojnë organizim dhe shumë benefite në jetesën moderne. (Alexander S. Gillis, n.d.)[5]

Disa nga përparësitë që IoT na ofron: Teknologjia IoT e bëri jetën e njerëzve më të lehtë dhe më të shpejtë. Ajo ka një rol të madh në kursimin e kohës në situata kritike dhe i bëri njerëzit të mendojnë ndryshe dhe të ndërmarrin veprime korrigjuese në vend që të luajnë me prova dhe gabime. Njerëzit mund të kenë lehtësisht informacion në majë të gishtave të tyre në kohë reale, gjë e cila është mundësuar për shkak të pajisjeve të rrjetit dhe që një person mund të marrë njohuri dhe të punojë për kompaninë e tij nga çdo pjesë e globit, gjë që e bën atë shumë të rehatshëm për të vazhduar punën e tyre edhe nëse ai nuk është i pranishëm fizikisht. (Alexander S. Gillis, n.d.)[5] Komunikimi bëhet i arritshëm për një rrjet të pajisjeve të ndërlidhura që i bën pajisjet e komunikimit më të besueshme dhe zvogëlon joefikasitetin. Proceset i caktohen makinës për komunikim më të mirë gjë që e bëri sistemin të prodhojë rezultate më të mira dhe më të shpejta. Shembulli më i mirë i makinave të këtij sistemi në njësinë e prodhimit.

IoT i ndihmon njerëzit të kryejnë detyrat e tyre të përditshme për të kursyer para dhe kohë. Paketat e transmetimit të të dhënave përmes një rrjeti të vendosur zvogëlojnë kohën dhe paratë. Të dhënat transmetohen dhe merren pa asnjë humbje. Detyra e automatizimit të IoT ndihmon në rritjen e cilësisë së shërbimit automatik dhe zvogëlimin e përpjekjeve njerëzore. (Alexander S. Gillis, n.d.)[5]

Qyteti inteligjent është një tjetër implementim madhor i internetit të gjërave që përdoret për mbikëqyrje inteligjente, shpërndarje uji, transport automatik, monitorim të mjedisit. Njerëzit janë të prirur ndaj ndotjes, furnizimeve të papërshtatshme dhe mungesës së burimeve, dhe fluksi i

parregullt i trafikut zgjidhet me instalimin e sensorëve të trafikut dhe aplikacioni është zhvilluar për të raportuar sistemet komunale. Qytetarët mund të jenë në gjendje të diagnostikojnë keqfunksionimet e thjeshta dhe mund të raportojnë në sistemin elektrik përmes aplikacionit të bordit të energjisë elektrike ose faqeve të internetit, dhe ata gjithashtu mund të gjejnë vende për parkimin e automjeteve lehtësisht përmes sistemit të sensoruar. Një tjetër aplikim i madh internetit është në kujdesin shëndetësor të instaluar për të diagnostikuar dhe kuruar sëmundjen në një fazë të hershme. Shumë algoritme përdoren për përpunimin dhe klasifikimin e imazheve për të zbuluar anomalitë e fetusit para lindjes. (Alexander S. Gillis, n.d.)[5]

Figura 2. Implementimi i rrjetave IoT në industi

2.2.1 Le të shqyrtojmë me gjerë disa nga rastet e përdorimit

Shëndeti dhe Fitneset: Disa nga implementimet më interesante të IoT kanë qenë në gjurmimin e aktivitetit. Tani ekzistojnë mënyra të shumta për të monitoruar të dhënat tuaja për gjendjen fizike, shëndetin dhe madje edhe gjendjen e gjumit. Jo vetëm ajo; gjithashtu mund të ndajmë

dhe rishikojmë në distancë recetat e mjekut në kohë reale. IOT gjithashtu ka zgjidhje të sofistikuara për monitorimin e foshnjës dhe ndihmon në sigurimin e ndihmës për të moshuarit.

Shtëpi: Aplikacionet mobile, termostatet, kontrolli mbi zgjidhjet e ndriçimit tashmë mund të gjenden në raftet e dyqaneve me pakicë. Ekziston gjithashtu një gamë e dukshme e pajisjeve të sigurisë, të cilat përfshijnë tregues të dështimit të sistemit në distancë, ndjekje virtuale etj. Teknologjia po shtrihet gjithashtu në të gjitha pajisjet e tjera të përdorimit në shtëpi.

Biznes: Ka pasur një përmirësim të dukshëm në sofistikimin e monitorimit dhe raporteve përmes zbatimit të teknologjive moderne. Tani është shumë më e lehtë për të menaxhuar shumë vende dhe për të mbajtur një kontroll mjaftë të ngushtë të cilësisë.

Qyteti: Ashtu siç po ndodhë me shtëpitë, edhe qytetet po përfitojnë gjithashtu nga bashkëpunimi dhe implementimi i teknologjisë. Shembujt më të spikatur janë lehtësia e vozitjes (përmes ndjekjes në kohë reale të trafikut dhe senzorëve të parkimit) dhe optimizimi i energjisë elektrike (duke përdorur burimet sipas motit dhe raportimit të mosfunksionimit apo defekteve automatike). Të gjithë qytetet kryesore të botës po mirëpresin zgjidhjet dhe zhvillimet në IOT për automatizime dhe mundësi më të mira.

Makina që mund të kyçen (connected cars): Një tjetër implementim shumë i dobishëm i IOT është prezantimi i makinave qe mund te konektohën. Automjetet mund të mbajnë komunikim të drejtpërdrejtë me ofruesit e shërbimeve si kompanitë e sigurimeve dhe qendrat e riparimit. Kjo ndihmon në gjetje të defekteve dhe riparim te shpejtë dhe të duhur. Gjithashtu, gjurmimi për kompanitë e makinave me qira është më i lehtë për t'u menaxhuar me ndihmën e integrimit të pajisjeve dhe softuerëve.

Mjedisi: Padyshim që kontributi më i rëndësishëm i IoT është në fushën e kujdesit mjedisor, pjesërisht sepse çështjet mjedisore si ngrohja globale janë thelbësore në natyrë dhe gjithashtu nuk kemi pasur evaluim në teknologji mjaftueshme të fortë për ta trajtuar plotësisht këtë çështje. Në një nivel tjetër, IOT lejon njoftime më të shpejta në lidhje me katastrofat natyrore, duke mundësuar kështu një parandalim apo një veprim në kohë reale. Ajo gjithashtu promovon analizë dhe raportim më të mirë. Kur bëhet fjalë për mbështetjen në nivelin e tokës, kjo teknologji e re ndihmon në ndotjen dhe kontrollin e mbeturinave duke përdorur sensorë paralajmërues. IoT mund të luajë një rol jetësor në trajtimin e mbeturinave në një mënyrë të përshtatshme. Me pajisjet që permbajnë sensorë dhe me mjedis të planifikuar të bazuar në IoT, në të gjitha vendet është e mundur menaxhimi i mbeturinave. Duke integruar sistemin, rrjetet

dhe ofruesit e teknologjisë me pajisje të bazuara në IoT mund të zhvillohen qasje inteligjente në koshat e mbeturinave. Koshat smart që mundësojnë ndarjen e duhur të materialeve të mbeturinës dhe me mirëmbajtjen e duhur janë adekuatë për menaxhimin e mbeturinave dhe reciklimin e tyre. Mënyra tradicionale e mbledhjes së mbeturinave në kujdesin shëndetësor mund t'i ekspozojë punëtorët ndaj infeksioneve dhe dëmtimeve toksike. Pajisjet e bazuara në IoT mund të përdoren në transmetimin e të dhënave në lidhje me monitorimin, trajtimin, ripërdorimin, karakterizimin e mbeturinave dhe menaxhimin e tyre në përputhje me rrethanat. Zbatimi i menaxhimit të mbetjeve të bazuara në IoT gjithashtu kërkojnë një analizë të thellë duke marrë parasysh perspektivën sociale, mjedisore, ekonomike, kulturore dhe ligjore të çështjes. Zbatimi i një sistemi të fortë të menaxhimit të mbetjeve ndihmon në ndërtimin e një ambienti të lirë nga çdo lloj infeksioni apo pandemie.

Këto janë vetëm disa shembuj ku IoT ka krijuar pronësi. Ndërsa teknologjia rritet, ndikimi i IOT në jetën tonë të përditshme gjithashtu do të rritet dhe këto ditë janë më afër sesa mund ta imagjinojmë, madje mund ta mendojmë edhe se sapo kemi filluar të jemi pjesë e kësaj kohe. (Banafa, 2018)[6]

2.3 Standarted e Rrjetave IoT

IoT dhe implementimi i rrjetes në të mund të themi se është gjithnjë në progres. Mirëpo, evaluimi i shpejtë ka shpërthyer në numër të madh të zgjidhjeve në IoT, sepse, fokusi i kësaj industrie është zhvillimi i pajisjeve apo harduerëve të duhur për zgjidhje të problemeve. Prandaj është edhe fakti se sot, çdo pajisje elekrike që po përdorim këto ditë është më e mençur (smarter), se pajisjet që përdornim vite më parë. (Simone Ciran, 2019)[7]

Për të arritur deri në këtë pikë te avancimit, zhvilluesit krijuan standardet e “Internetit of things”, sic janë:

Figura 3. Teknologjitë e Bluetooth

2.3.1 Bluetooth: e cila është njëra ndër standardet kryesore te IoT. Teknologjia Bluetooth përdorur radio-valët me frekuencë 2.4 GHz ISM, e cila dërgohet në formë të paketave deri në 79 kanale. Ky standard mundëson lidhjen dhe komunikimin e pajisjeve me shfrytëzuesin. Bluetooth mundëson komunikim të sigurtë dhe përfekt kur bëhet fjalë per komunikim short-range apo në gamë më të ngushtë, duke ofruar kosto më të ulët të përdorimit dhe energjisë.

Karakteristikat bazike të Bluetooth janë:

- Përcjellja e zërit dhe të dhënave në distanca të shkurtra;
- Komunikim point-to-point dhe point-to-multipoint;
- Autentifikim dhe kriptim;
- Shpenzime të ultëta të energjisë;
- Qëndrueshmëri në zhurmë dhe në interference.

Bluetooth ka gjendjet apo moodet si: “active” ku nyja dërgon dhe merr të dhënat, sniff – pajisja futet në fjetje periodike, “hold” nyja është në sleep mode, “park” njësoj si në ‘hold’ pajisja është në fjetje.

Bluetooth ka disa verzione kështu duke filluar nga verzioni 1.0 deri në 3.0, verzione të cilat kanë shpejtësi deri në 3Mbps, mirëpo, në ditët e sotme pajisjet që përdorin Bluetooth përfshijnë verzionin 4.0 apo edhe verzionet më të larta siç është verzioni 4.2, të cilat arrijnë një shpejtësi deri në 24 Mbps. (John, 2020)[9]

Më shumë informacion mbi Bluetooth 4.2:

- Standard: Bluetooth 4.2 core specification
- Frequency: 2.4GHz (ISM)
- Range: 50-150m (Smart/BLE)
- Data Rates: 1Mbps (Smart/BLE)

2.3.2 ZigBee: standard tjetër i cili ndihmon që interneti i gjërave të kaloj në një nivel tjetër. Koncepti i rrjetit pa tel dhe me fuqi të ulët u bë standard në vitet 1990 dhe Aleanca Zigbee u formua për të adresuar këtë statut në 2002. Protokolli Zigbee u krijua pas ratifikimit të IEEE 802.15.4 në 2004. Ky u bë standardi IEEE 802.15.4 -2003. Specifikimi 1.0, i njohur gjithashtu si Specifikimi Zigbee 2004, u bë publik në 13 qershor 2005. Zigbee është e ngjashme me teknologjinë Bluetooth për nga efikasiteti në botën e IoT. Ka një kosto të ulët, siguri të lartë, dhe mbështet një gamë më të gjerë të komunikimit deri në 200 metra, për dallim nga Bluetooth e cila përkrahë vetëm deri në 100 metra. Zigbee është padyshim më i përshtatshëm për zgjidhjen e disa problemeve se sa teknologjitë e tjera. Zigbee shfrytëzon me pak fuqi dhe vetëm dergon të dhëna. Kjo do të thotë se është e shkëlqyeshme për butona dhe sensorë. Më më pak efikase kur janë në pyetje pajisjet me bandwith të lartë, si shembull kemi speakers me wifi. Aktualisht, Zigbee dominon në tregun e ndriçimit inteligjent siç janë llambat me ZigBee. (Anon., 2020)[10]

Figura 3.1 Teknologjitë e ZigBee

2.3.3 Z-Wave: është standardi më popullor dhe i përdorur në IoT. E ngjashme me standardet e tjera, gjithashtu edhe ky standard mbeshtët hargjimin më të ulët të energjisë. Është një Wireless

Radio Frequency (WRF) që përdoret në aplikacionet e shtëpive. Operon në 800-900MHz, për dallim nga ZigBee e cila vepron në 2.4GHz. Nëse na nevojiten pajisjet si sensorët, ka më shumë gjasë të përfundojmë duke përdorë teknologjinë Z-Wave, sepse Z-Wave aktualisht janë duke e udhëhequr këtë treg. (Anon., 2020)[11]

Figura 3.2 Teknologjitë e Z-Wave

Një krahasim të shkurtër mes Z-Wave dhe teknologjive të tjera

- Z-Wave dhe ZigBee - Ndryshe nga Z-Wave, ZigBee operon në frekuencën 2.4GHz të përbashkët me WiFi dhe Bluetooth. Mund të kemi më pak probleme me sinjal kur përdorim teknologjinë Zigbee sesa kur jemi të lidhur vetëm me WiFi ose Bluetooth, por, Z-Wave ka frekuencën e vet të dedikuar.
- Z-Wave dhe Wifi - Z-Wave gjithashtu e mposhtë WiFi-në për sa i përket ndërhyrjeve në rrjet. Ashtu si Bluetooth, pajisjet WiFi konkurrojnë me njëra-tjetrën, kështu që forca e sinjalit dhe shpejtësia e rrjetit ngarkohen kur ka shumë pajisje të lidhura. Sidoqoftë, WiFi mund të sjellë më shumë informacion. Teknologjia Z-Wave dërgon dhe merr mjaft të dhëna për pajisjet inteligjente si llamba, detektorët lëvizës dhe pajisjet e tjera të vogla, por pajisjet që dërgojnë shumë informacion kërkojnë kapacitetin më të madh të rrjetit WiFi. Për shembull, një kamerë mbikëqyrjeje me video HD dërgon më shumë të dhëna sesa mund të trajtoj rrjeti Z-Wave ose Bluetooth me fuqi të ulët. Një dallim tjetër është se Zigbee është softuer opensource, ndërsa Z-Wave është softuer në pronë i mbështetur dhe i çertifikuar nga grupi Z-Wave. Ndërsa të dy teknologjitë po kapen njëkohësisht, teknologjia e Z-Wave

mbështetet nga drejtuesit e industrisë të cilët vazhdimisht e përpunojnë atë. Z-Wave ka dalë në treg për më shumë se një dekadë dhe ka pësuar disa azhurnime dhe përmirësime.

- Z-Wave dhe Bluetooth - Përmirësimi më i madh që bën Z-Wave tek Bluetooth është fuqia e sinjalit. Sinjali Bluetooth është i prirur për të bartur sinjale sepse të gjitha pajisjet Bluetooth dërgojnë dhe marrin informacione në të njëjtën brez 2.4GHz. Ata garojnë me njëri-tjetrin për bandwidth. Me Z-Wave, çdo përsëritje e të valës bashkpunonë për ta bërë rrjetin më të fortë. Çdo pajisje në fakt forcon sinjalin. Sa më shumë pajisje të keni, aq më lehtë është të krijoni një rrjet të fortë që është i aftë të anashkalojë pengesat dhe të kalojë nëpër mure, tavane dhe dysheme. (Anon., 2020)[11]

2.3.4 6LoWPAN: qasje e drejtpërdrejtë për zhvillimin e rrjetes packet data wireless ose rrjetit të sensorëve, ka papajtueshmëri midis formatit IPv6 dhe formateve të lejuara nga IEEE 802.15.4. Këto ndryshime kalojnë brenda 6LoWPAN dhe kjo lejon që sistemi të përdoret si një shtresë mbi 802.15.4 bazë. Për të dërguar packet data IPv6 në 6LoWPAN, është e nevojshme një metodë për shndërrimin e data packet në një format që mund të trajtohet nga sistemi low-layers IEEE 802.15.4. 6LoWPAN është standardi ideal për të krijuar rrjeta Mesh dhe për t'u përdorur në pajisje të vogla, bartë paketat IPv6 ose IPv4 në standardin IEEE 802.15.4, që përmbanë autentifikim dhe enkriptim. Në procesin e formësimit të botës IoT, grupi punues IETF IPv6 mbi fuqinë e ulët WPAN (6LoWPAN) [6LoWPAN GP] filloi në 2007 për të punuar në specifikimet për transmetimin e IPv6 përmes rrjeteve IEEE 802.15.4. Grupi i cili punon në standardin 6LoWPAN është përpjekur që të përcaktoj një shtresë efektive adaptimi në IPv6. Çështje të mëtejshme përfshijnë konfigurimin automatik të adresave IPv6, pajtueshmërinë për mbështetjen e transmetimit të link-layrit rrjetet e përbashkëta, zvogëlimin e routimit dhe menaxhimin e shpenzimeve të larta, miratimin e protokolleve për teknikat e kodimit të të dhënave dhe mbështetjen për mekanizmat e sigurisë p.sh. konfidencialiteti dhe integriteti i të dhënave. (Anon., 2019) [11]

2.4 Sfidat dhe siguria e rrjetave IoT

Fusha e teknologjisë Internet of Things (IoT) përfshinë disa zhvillime, sa të ndara ashtu edhe të shumta. Meqenëse vetë përkufizimi është ende nën diskutim të gjerë, është mjaft e vështirë, madje e ndërlikuar, të vendosësh kufinjë në mënyrë që të përcaktohet qartë se cilat teknologji janë

brenda rrezes së IoT. Duke marrë parasyshë që IoT është e ndërtuar nga "objekte të mençura të cilat janë të ndërlidhura", ne mund ta orientojmë interesin tonë më shumë drejt teknologjive të komunikimit, duke zhvilluar mënyrën e krijimit të kësaj lidhje. Për shkak të faktit se IoT është bërë një element jetik në lidhje me të ardhmen e internetit me përdorimin e tij të shtuar, ajo kërkon një nevojë për të adresuar në mënyrë adekuate sigurinë dhe besimin. Studiuesit janë të vetëdijshëm për dobësitë të cilat aktualisht ekzistojnë në shumë pajisje IoT.

Për më tepër, themeli i IoT vendoset në sensorin ekzistues të rrjetit wireless (WSN). Sulmet e ndryshme dhe dobësitë në sistemet e IoT dëshmojnë se ekziston me të vërtetë një nevojë për dizajne dhe zhvillime të gjëra të sigurisë që t'i mbrojë të dhënat dhe sistemet. Sulmuesit shfrytëzojnë dobësitë në pajisjet specifike duke fituar qasje në sistemet e tyre dhe duke bërë pajisjet të pa sigurta dhe të prekshme. Ky hendek i sigurisë më tej motivon zgjidhje gjithëpërfshirëse të sigurisë që përbëhen nga kërkime të cilat janë efikase në kriptografinë e aplikuar për të dhëna dhe siguri të sistemit. Adresimi i këtyre sfidave dhe garantimi i sigurisë në produktet dhe shërbimet e IoT duhet të jenë një përparësi themelore.

Përdoruesit duhet të kenë besim se pajisjet IoT dhe shërbimet e të dhënave përkatëse janë të sigurta, veçanërisht pasi kjo teknologji bëhet më e përhapur dhe e integruar në jetën tonë të përditshme. Pajisjet dhe shërbimet e IoT me siguri të ulët mund të shërbejnë si pika potenciale hyrëse për sulmin kibernetik dhe të ekspozojnë të dhënat e përdoruesve. Studimi i ri tregon se numri në rritje i pajisjeve për shkak të IoT do të shohë që shpenzimet globale për siguri kibernetike tejkalonë 1.8 miliardë dollarë deri në vitin 2020. Hakimi i lartë i profileve mund të ofrojë thirrje me ndërprerje, por realiteti është se siguria mbetet një mendim i jo edhe aq i përpunuar për aryse pajisjeve të vogla. E projektuar për konsum të ulët të energjisë me lidhje apo komenktim të kufizuar, natyra e tyre shpesh e ulët dhe e disponueshme mbetet një pengesë për përfshirjen e kriptimit dhe masave të tjera më të forta të sigurisë. Nuk është për t'u habitur, krijimi i një protokolli të standardizuar të sigurisë për të adresuar fushën IoT. (Gilchrist, 2017)[12]

Një sfidë qendrore është gjetja e një zgjidhjeje që mund të sigurojnë si pajisjet po ashtu edhe rrjetin duke shmangur ndërhyrjet nga jashtë që bëhen pengesë për angazhim. Ekziston nevoja për më shumë shërbime kriptografike që kanë aftësinë të veprojnë në pajisjet IoT. Kjo do t'ia mundësojë përdoruesit të përdorin dhe vendosin në mënyrë të sigurtë IoT sisteme pavarësisht nga ndërfaqet joadekuate të përdoruesit që janë në dispozicion me pothuajse të gjitha pajisjet IoT.

Përveç aspektet e mbrojtjes dhe sigurisë së IoT, fusha shtesë si konfidencialiteti në komunikim, besueshmëria dhe siguria e palëve të komunikimit dhe integriteti i mesazheve, edhe kërkesat shtesë të sigurisë duhet të jenë gjithashtu të inkorporuara. Këto mund të përfshijnë tipare si të qenit në gjendje të parandalojnë nderhyrjen e palëve të ndryshme nga jashtë. Si shembull, në transaksionet e biznesit, pajisjet e mençura duhet të parandalojnë lehtësimin e qasjes nga jashtë në informacione konfidenciale, në pajisje, dhe kështu të parandalohet përdorimi I informacionit me qëllim të keq. (Gilchrist, 2017)[12]

Rreziqet në IoT mund t'i klasifikojmë si:

1. Rreziqet që ekzistojnë në çdo sistem interneti;
2. Rreziqet që janë specifike për pajisjet IoT;
3. Siguria që asnjë dëm nuk është shkaktuar.

Disa nga rastet më të shpeshta të rreziqeve:

Shkallëzimi: Menaxhimi i një numri të madh të nyjeve IoT që kërkojnë zgjidhje të së sigurisë.

Lidhshmëria: Sfidë tjeter e cila mundohet që më mënyre të sigurtë t'ia mundësoj komunikimet IoT pajisjeve të ndryshme të cilat kryejnë procese të ndryshme.

Siguria End-to-End: Po aq të rëndësishme janë edhe masat e sigurisë End-to-End midis pajisjeve IoT dhe hosteve të Internetit.

Authentifikimi dhe Besimi: Aftësitë e identifikimit dhe besimit të duhur të IoT nuk janë akoma në nivelin e duhur. Kjo parandalon krijimin e marrëdhënieve të besimit apo sigurisë në mes të komponentëve të IoT, të cilat janë një parakusht për aplikimet e IoT të cilat kërkojnë lidhje ad-hoc midis komponentëve të IoT.

Menaxhimi i identitetit: Eshtë nevojë qe indentiteti të jetë i sigurtë dhe se makinat e të dhënave të jenë të plotësuara me të dhëna te sakta. Për shembull, sigurimi i ID-ve, fjalëkalimeve është një kusht i zakonshëm.

Në kontekstin e zgjidhjeve IoT të bazuara në IP, shqyrtimi i sigurisë së TCP / IP protokollet janë të rëndësishëm pasi këto protokolle janë krijuar për t'iu përshtatur ideologjisë dhe teknologjisë së

rrjetit IP. Ndërsa një gamë e gjerë e qëllimeve të specializuara kanë zgjidhje për shkëmbimin e çelësave të sigurisë për domenin e Internetit.

2.5 Arkitektura e ZigBee

Zigbee Technology bazohet në IEEE 802.15.4 standardin dhe pajisjet Zigbee veprojnë pa licencë në 2.4 GHz ISM (ISM - Industriale, Shkencore dhe Mjekësore). Synimi i Zigbee janë sensorët pa tela dhe me kosto të ulët, energji të ulët, me bateri, të cilët nuk kanë nevojë të per updatim të shpeshtë të statusit të tij dhe gjithashtu lejon low power mode.

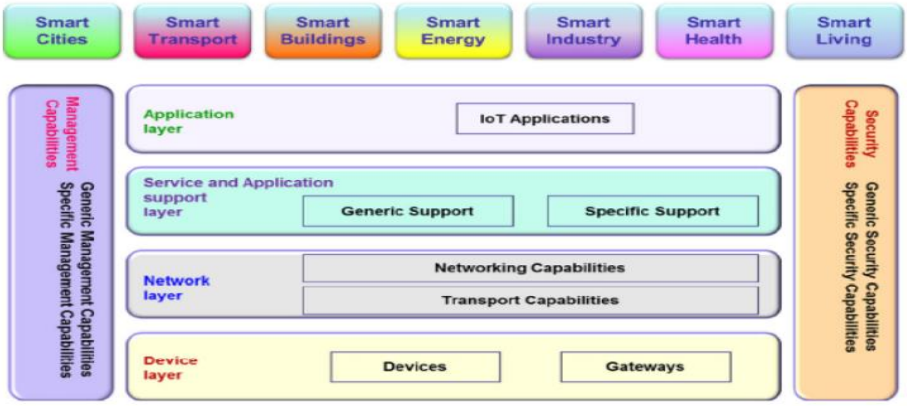

Figura 4. Arkitektura e ZigBee

The PHY (Physical Layer) dhe MAC (Medium Access Layer) janë të definuara nga standardi 802.15.4. Përmbanë edhe NWK (Network Layer) dhe kornizat për Layers të aplikacioneve. Application Support (APS) Layer, ZigBee Device Objects (ZDO) dhe objektet e aplikacioneve janë të gjitha pjese të Application Framework, të cilat janë nën kontrollin e ZigBee Alliance. Physical Layer, Data Link dhe Network Layers janë të pranishëm në ZigBee Stack në formën e PHY, MAC dhe NWK. (Marco Tiloca, 2013)[12]

Katër shtresat e fundit Transport, Session, Presentation dhe Application layers janë të mbuluara në Application Support Sublayer (APS) dhe Zigbee Devices Object (ZDO).

Arkitektura e ZigBee është kombinim i shtresave:

1. Physical Layer (PHY)
2. Application Interface Layer

3. Network Layer
4. Medium Access Control Layer (MAC)
5. Security Layer
6. Application Layer

Shtresa fizike (PHY): Kjo shtresë bën modulimin dhe demodulimin në transmetimin dhe marrjen e sinjaleve. Siç u përmend më herët, dy shtresat PHY dhe MAC përcaktohen nga IEEE 802.15.4. Shtresa PHY është më afër harduerit dhe ajo në mënyrë direkte e kontrollon dhe komunikon me radion Zigbee. Shtresa PHY përkthen data packet në bita për transmetim dhe anasjelltas gjatë marrjes.

Shtresa MAC (MAC Layer): është përgjegjëse për ndërfaqen dhe transmetimin e besueshëm në mes të PHY Layers dhe NËK. MAC Layers është gjithashtu përgjegjëse për sigurimin e PAN ID dhe gjithashtu zbulimin e rrjetit përmes kërkesave të fenerit.

Shtresa e Rrjetit (NWK): Kjo shtresë kujdeset për të gjitha operacionet që lidhen me rrjetin siç janë konfigurimi i rrjetit, lidhja e fundme e pajisjes dhe shkyçja nga rrjeti, rutimi, konfigurimet e pajisjeve e shumë të tjera. NWK vepron si një ndërfaqe në mes të MAC Layer dhe Application Layer. Gjithashtu përgjegjëse për rrjetëzimin me MESH (formimin dhe rutimin e rrjetës) dhe për transmetim të besueshëm të të dhënave nëpër rrjete të ndryshme duke shmangur përplasjen CSMA. Përveç detyrave të mësipërme, NWK Layer ofron siguri në Rrjetet Zigbee që do të thotë se të gjitha të dhënat në NWK Frame janë të enkriptuara.

Shtresa e Aplikacionit: Kjo shtresë është prezente ne nivel të shfrytëzuesit. Në Zigbee Stack është protokolli më i lartë dhe përbëhet nga Application Support (APS) dhe nga nën-shtresat Zigbee Device Object (ZDO). Kjo shtresë mundëson shërbimet e nevojshme të pajisjes Zigbee dhe application objects që të ndërlidhen me shtresat e rrjetit për shërbimet e menaxhimit të të dhënave. Kjo shtresë është përgjegjëse për përputhjen e dy pajisjeve sipas shërbimeve dhe nevojave të tyre. Ai përmban aplikacione të përcaktuara nga prodhuesit. Nën-shtresa APS është përgjegjëse për zbulime. Zigbee Device Object (ZDO) monitoron menaxhimin lokal dhe të rrjetit në distancë. Application Framework përbëhet nga Application Objects që kontrollojnë dhe menaxhojnë shtresat e protokollit në pajisjet Zigbee. Application Framework mund të përmbajë deri në 240 Application Objects.

Security Layer: Arkitektura e sigurisë në ZigBee e plotëson ose e rritë sigurinë e shtresave IEEE 802.15.4.

Eshtë një model i "open trust" bazuar në supozime të caktuara të cilat përshkruhen më poshtë:

- Layers dhe aplikacione të ndryshme po ekzekutohen në një pajisje të vetme prandaj besojini njëra-tjetrës.
- Komunikimi midis Layereve të ndryshëm në të njëjtën pajisje nuk është e enkriptuar.
- Një pajisje nuk do të transmetojë qëllimisht ose pa dashje çelësat në pajisje të tjera nëse nuk janë më të mbrojtura dhe të sigurta.
- Komunikimi në mes të dy pajisjeve është e kriptuar.
- Gjeneratorët e numrave random po punojnë siç pritet nga motori kriptografik
- Hardueri të është rezistent ndaj manipulimit

Parimi i dizajnit arkitektonik të sigurisë ZigBee:

Layeri që organizon një frame është përgjegjëse për sigurinë e saj fillimisht.

Vetëm një pajisje me një çelës aktiv të rrjetit mund të komunikojë me më shumë se një herë në të gjithë rrjetin. Si shtresa APS ashtu edhe shtresa NWK mund të përdorin të njëjtin çelës aktiv të rrjetit për të siguruar frejmët. Përdorimi i ri i çelësave ndihmon në zvogëlimin e hapësirës së ruajtjes. Siguria e mesazhit End to End, pra pajisjet e vetme burim dhe destinacion, mund të deshifrojnë mesazhet e mbrojtura nga një çelës i përbashkët.Një pajisje që formon një rrjet është përgjegjëse për nivelin bazë të sigurisë, politikat e sigurisë dhe vërtetimin e nyjeve në rrjet. Shtresa e aplikacionit mund të ofrojë siguri shtesë të nivelit të aplikimit nëse kërkohet midis dy pajisjeve. (Marco Tiloca, 2013) [12]

2.6 Arkitektura e Smart Home vs Smart City

2.6.1 Smart City

"Smart city quhet teknologjia informative që përdoret për të zgjidhur problemet urbane" – Rudolf Giffinger

Në vitin 2007, në Universitetin e Teknologjisë në Vienë, Rudolf Giffinger e përdori formalisht termin "Smart City". Ky koncept mori jetë pasi lindi nevoja për ngritje të kualitetit në jetën e qytetit. Smart City është duke sjellur mundësi të jashtëzakonshme dhe po ngritë edhe më shumë sfidat në botën e teknologjisë. Pikësynimi i këtij projekti gjigand permbanë zgjidhje të problemeve në aspekt digjital, ku çdo gjë që i nevojitet rrethit shoqërorë të kryhet në menyrë më të lehtë dhe shpejtë. Arkitektura e një smart city duhet të mbështes çdo gjë, duke filluar nga monitorimi e deri tek grumbullimi i të dhënave, e më pastaj, duke kaluar nëpër senzorizime dhe ofrim te shërbimeve të integruara (Eleonora Riva Sanseverino, 2017) [14]

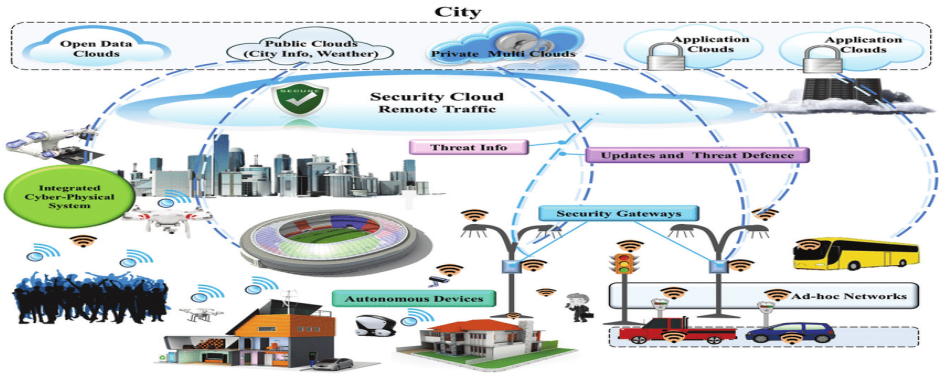

Figura 5. Arkitektura e Smart City

Duke u bazuar në Fig.6. shohim se prej ndriçimit të rrugëve e deri tek integrimi gjithpërfshirës i insitucioneve, automatizimi e teknologjia ka arritur nivelet më të larta të përdorimit, duke e bërë të pashmangshme involvimin e saj edhe brenda shtëpive. Nga city në smart-city, mund të themi se na lejohet që integritetin dhe evaulimin t'i klasifikojmë në verzione. Le të fillojmë nga verzioni i parë: Smart City 1.0, ku ne mënyrë direkte përfshihet IBM e Cisco, për ta vënë në funksion zgjidhjen që ofron ICT. Pastaj fillon vala e dytë, Smart City 2.0, në këtë fazë i jepet qasje

administratorëve të qytetit të jenë përgjegjës për vendimmarrjen që kanë të bëjnë me vendosjen e zgjidhjeve teknologjike. Problemi me këtë fazë është mungesa e pjesëmarrjes së publikut dhe mungesa e besimit ndaj ofruesve të teknologjisë, të cilat më pas emertojnë administratorët e qytetit si vendimmarrës me dije të lartë që rregullojnë mirëqenien e qytetarëve. Gjenerata e tretë Smart City 3.0, një hap tjetër duke perdurur mungesat e fazave të lartëpermendura. Në këtë faze, si organet qeveritare ashtu edhe qytetarët bashkë-krijojnë zgjidhje për çështje që lidhen me rritjen e teknologjisë dhe veprimit të saj në qytete dhe shoqata socio-kulturore. (Rodzi, 2019) [15]

2.6.2 Përbërja e smart city

Trafiku rrugor: Për t'u siguruar se qytetetarët arrijnë nga burimi deri tek destinacioni, në mënyrë sa më të sigurtë, qytetet aktivizojnë zhvillimin dhe implementimin e IOT në problemet që mund të ndodhin në trafik. Përdorimi i senzoreve të ndryshëm, GPS, sinjalet rrugore, të gjitha këto të lidhura më një platformë cloud që mundosojnë zgjidhjen e problemeve që mund të ndodhin në trafik. (Anon., n.d.) [16]

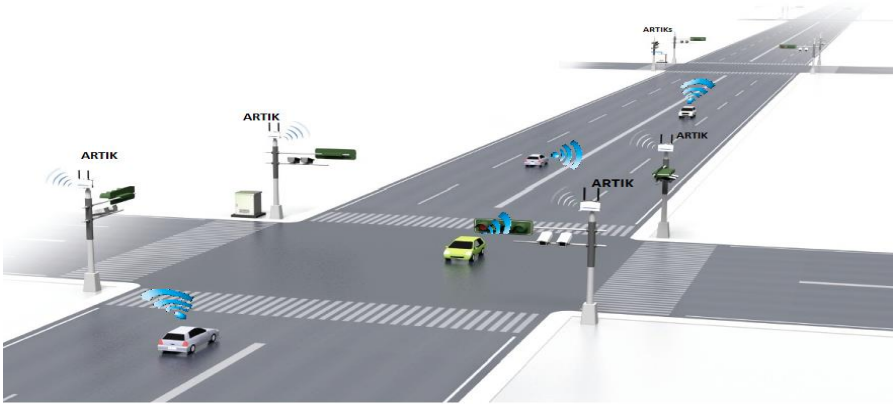

Figura 5.1 Monitori i trafikut rrugor

Parkingjet smart: Duke evituar humbjen e kohës dhe shpenzimin më të ulët të derivative për kërkim të parkingjeve të lira, smart city përmban edhe smart parking, ku përmes GPS dhe aplikacioneve në smarphonet tanë, arrijmë të gjejmë parkingun më të afërt në atë zone ku ne ndodhemi. Nëse asnjë parking nuk është i lirë, atehërë përmes njoftimeve në smartfon, përdoruesi

njoftohet se parkingjet janë të zëna dhe se, nëse ndonjeri lirohet automatikisht niset një njoftim drejt përdoruesit se parkingu me adresë X dhe number X ëdhë liruar.

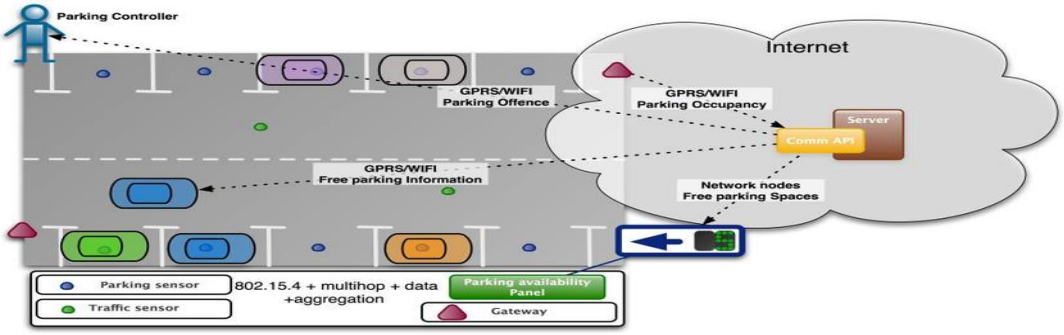

Figura 5.2 Arkitektura e Smart-Parking

Transporti publik: Gjithashtu, siç i përmendem tek parkingjet smart, edhe në trasportin publik përdorim IoT senzorët për të lehtësuar qytetarëve të perdorin trasportet publike. Rrugën të cilën mjeti transportues e bën, kohën dhe vonesat, te gjitha do të jenë të përshkruara në një tebelë smart në cdo stacion dhe brenda mjetit transportues. (Anon., 2014)[17]

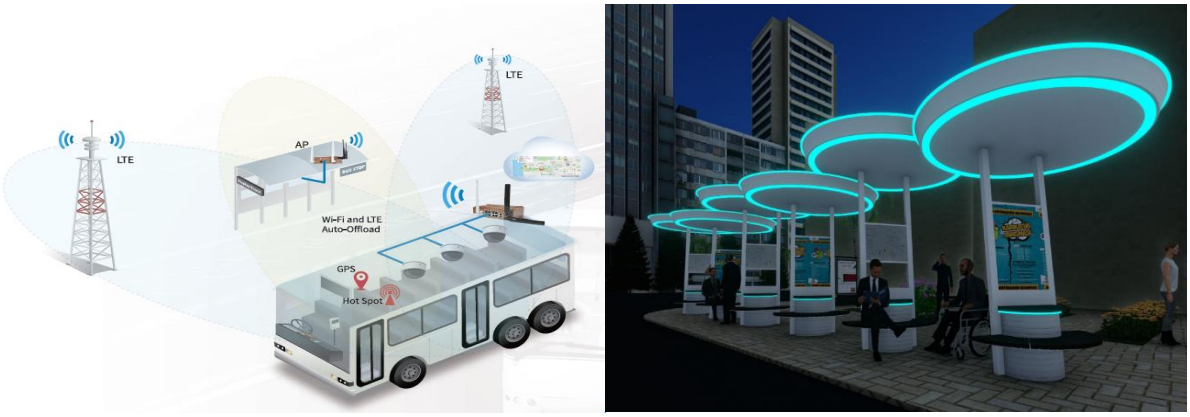

Figura 5.3 Stacionet e autbusëve dhe autobuset smart

Shërbimet publike: IoT mundeson që shfrytëzuesi të bëj monitorimin e gjendjes dhe profilit të tij nga largësia. Nxjerrja e dokumenteve, pagesat, transferimet bankare, qytetari mund t'i kryej nga shtëpia apo nga vendi i punës, pa pasur nevojë per vizitë në insitucionet përkatëse.

Figura 5.4 Sherbimet publike permes teknologjisë

Ndriçimet rrugore: IoT bazuar në smart city kontrollon nga një stacion bazë, dritat e rrugëve. Dritat e rrugëve me senzorë dhe të kyçura në një cloud ndihmon në fikjen dhe ndezjen e tyre në kohë të përshtatshme për ndriqim të rrugëve.

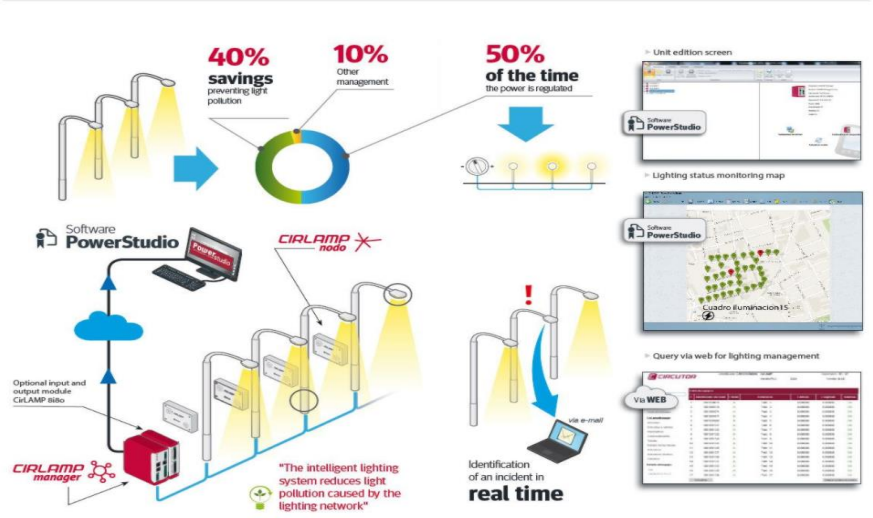

Figura 5.5 Aritektura e ndriçimit rrugor

Siguria publike: IoT i bazuar në smart city ofron pajisjet për monitorimin në kohë reale, analizim dhe pajisje vendim marrëse. Duke kombinuar senzoret dhe involvimin e kamerave arrihet një siguri tek qytetarët, në rast të ndonje krimi apo aksidenti.

Figura 5.6 Monitorimi i qytetit

Sfidat në të cilat Smart City ka kaluar:

Zhvillimi i një qyteti smart kërkon kohë dhe mund e perkushtim të lartë. Eshtë mjaftueshëm delikate krijimi i politikave dhe strategjive për zhvillime në bazë të zonave. Përfshirja e qytetarit është çelësi kryesor për mbeshtetjen e qyteteve 'smart'. Mirëpo, këtë mund ta quajmë një sfidë në vete, ku, edukimi jo i mjaftueshëm i qytetarëve, po ashtu, informim i mangët i qytetarit apo shfrytezuesit në lidhje me teknologjinë është njëra ndër sfidat kryesore që përfshinë automatizimi. Bizneset dhe industritë e shumta nuk e dinë se si funksionon automatizimi, ku nderfaqja në mes të shfrytezuesit dhe makinës është ne nivel të ulët. Pranadaj, rritja e kapaciteteve të administratorëve dhe mentorëve duhet te jetë primare në imlpementim te automatizimit. Sfidë tjetër është besimi i shfrytezuesit në tekologjinë e ofruar, për arsye se të metat janë të parat që vihen në pahë kur bëhet fjalë per diçka të re, njësoj po ndodhë edhe me informim nga mediat në lidhje me rreziqet që teknologjitë në zhvillim e sipër po sjellin në mesin tonë. Rritja e besimit tek shfrytezuesit po luftohet në çdo aspekt për nga ana e zhvilluesve, ku në secilin përditësim dhe gjeneratë vihet re ngritja e sigurisë dhe ulja e rreziqeve të individëve. (Halsey, 2018)[18]

2.6.3 Smart Home

“Ashtu si evaulohemi ne, njesoj duhet të avaulohen edhe shtëpitë tona**”** -Suzanne Turcker

Ajo çfarë e benë një shtëpi smart është përdorimi rrjetave në pajisje, ku monitorimi dhe menaxhimi i tyre bëhet përmes aplikacioneve. Prandaj edhe mund të themi se jetesa në smart home është më e lehtë, më e rehatshme dhe më e sigurtë. Pajisjet me internet përdoren për tu lidhuar me pajisje të ndryshme brenda shtëpive, siç janë: ndriçimi, matësi i temperaturës, kontrolli i dritareve dhe roleteve, sistemet e sigurisë dhe monitorimit, pajisjet brenda kuzhinës, ora, e shumë pajisje të tjera të cilat në mund t’i monitorojmë dhe t’i komandojmë përmes aplikacioneve dhe softuerëve të ndryshem në celularët tanë. Ajo çka e mundoson automatizimin e shtëpive është se, pajisjet të cilat ne duam t’i kontrollojmë dhe t’i monitorojmë nga larg, duhet të lidhen me wireless, ku përmes rrjetës mundësohet kontrollimi nga distanca. Sot, pajisjet të cilat i marim janë në gjendjen self-learning, ku përmes manualëve dhe ndërfaqjeve fizike dhe logjike, i mundëson përdoruesit përdorim sa më të lehtë dhe praktik të pajisjes. (Direct, 2018) [19]

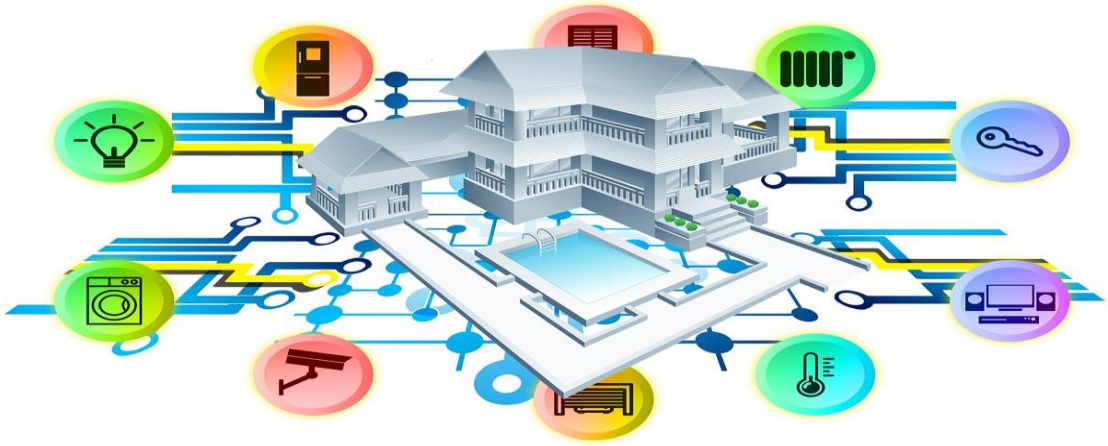

Figura 6. Arkitektura e Smart Home

Smart lighting: Ndër hapat e para që smart home ndërmori në arkitekturen e saj është smart lighting. Kontrollimi i ndriçimit nga distanca, përmes kyçjes në internet, përdorimi i Bluetooth, mundesojnë kontroll përmes aplikacioneve e zërit, përmes të cilave bëhet aktivizimii i dritave, po ashtu mund edhe të bëjmë ndryshimin e ngjyrave të dritave. Aplikacionet kanë dy gjendje në të cilat mund të funksionojnë: automatike dhe manuale. Në gjendjen automatike, përmes orareve të

caktuara, bëhet aktivizimi i llambës pa pasë nevojë për ndërhyje nga shfrytezuesi. Në gjendjen manuale, shfrytezuesi vepron në çdo qast, kur atij i nevojitet ndriçimi. (Jorge Higuera, n.d.)[21]

Figura 6.1. Smart lighting

Smart doors: Hapja dhe mbyllja e dyerve të dhomave, derës kryesore, derës së garazhos, në mënyrë automatike dhe nga çdo distance, ulë në mënyrë drastike rreziqet. Përfshirja e mikrokontrollëreve në pajisje mundëson menaxhimin e tyre edhe nga larg. Në rast se harrojmë dritaret e hapura dhe fillon shiu, atëher përmes aplikacioneve ndërhyjmë nga larg dhe i mbyllim, e njejta ndodhë edhe me dyert, në rast se i harrojmë të hapura dhe nuk gjendemi në shtëpi atëherë pa pasur nevojë të kthehemi e të hargjojme kohë, ne perdorim aplikacionet për mbyllje. Hapja e derës mund te bëhet permes shënjave të gishterinjëve, kartelës, kodit, çelësit, dhe permes aplikacionit në telefoneve të mençur. (Al-Tuma, 2019) [20]

Kamerat e sigurisë: Vezhgimi i shtëpisë sot është më e lehtë se asnjëherë më parë. Pronari i shtëpisë mund të jetë në shtëpi edhe pa qenë aty, ku përmes pamjeve në kohë reale mund të vëzhgohet çdo cep i shtëpisë. Siguria përmes kamerave ulë rreziqet nga keqdashësit dhe parandalon krimet.

Alarmet: Ne rast se ndonjë pajisje merr flakë, alarmet të cilat gjënden brenda shtepisë, përmes senzorëve lëshojnë sinjalet të cilat mund të dëgjohen edhe jashtë shtepisë e deri tek baza e ekipës të cilët kanë bërë instalimin e pajisjeve, gjë e cila mundëson ndërhyrje të shpejtë dhe parandalim të fataliteteve. E njëjta ndodhë edhe me alarmet të cilat janë jashtë shtepisë, në rastë se keqdashësit tentojnë të futen në shtëpi pa leje, apo edhe kafshet të cilat nuk lejohen të hyjnë brenda, permes alarmeve mund të bëjmë ndërhyrje në kohë reale. (Jorge Higuera, n.d.) [21]

2.6.4 Përparsitë e Smart Home:

Smart home kanë aftësinë për ta bërë jetën më të lehtë dhe më të përshtatshme. Pavarësisht nëse jemi në punë ose në pushime, smart home do të na paralajmërojë për atë që po ndodh në shtëpi, përmes sistemit të sigurisë, ku përmes së cilës mund të bëhet ndëryrje e mënjehershme në rast urgjence. Shembull, jo vetëm që një banor do të zgjohej kur të degjoj alarmet e sigurisë, smart home gjithashtu do të zhbllokonte dyert, do të thirrte departamentin e zjarrfikësve dhe do të ndriçonte rrugën për siguri.

Smart homes gjithashtu sigurojnë kursime të energjisë. Meqenëse sistemet si ZigBee vendosin disa pajisje në një nivel të zvogëluar të funksionalitetit, ato mund të kthehen në gjendjen "sleep" dhe të zgjohen kur t'iu jepen komandat. Faturat elektrike bien kur dritat fiken automatikisht nëse një person largohet nga dhoma, po ashtu edhe dhomat mund të nxehen ose të ftohen.

Smart home është mjaftë praktike edhe për personat e moshuar, të cilëve i'u nevojitet një kujdes mjaftë i vecantë. Përmes teknologjive në smart home, mund të njoftohet banori kur është koha për të marrë ilaçe, të lajmëroj spitalin nëse banori rrëzohet apo nuk eshte ne gjendje te mirë. Nëse personi i moshuar do të harronte pak, smart home do të kryente detyra të tilla si ndalja e ujit para se të vërshonte një vaskë ose fikja e furrës nëse kuzhinieri eështë larguar. Ai gjithashtu lejon që fëmijët që mund të jetojnë diku tjetër dhe të marrin pjesë në kujdesin e prindit të tyre të plakur. Sistemet e automatizuara me kontroll të lehtë sigurojne përfitime të ngjashme për personat me aftësi të kufizuara ose me një gamë të kufizuar të lëvizjeve. (Benjamin K. Sovacool, 2020)[22]

2.6.5 Sfidat e Smart Home:

Përveç komoditetit dhe kursit të kostos, Smart home ka edhe disa sfida. Duke filluar nga blerja dhe instalimi i pajisjeve, kosto e tyre është mjaftueshëm e lartë dhe jo çdo familje mund ta arrijë mbulimin e këtyre kostove. Pastaj, sfidë tjetër është rreziku i sigurisë dhe gabimet që vazhdojnë të shqetësojnë prodhuesit dhe përdoruesit e këtyre teknologjive. Hakerët profesionist mund të kenë akses në pajisjet e smart home, ku mund te lidhen me to përmes internetit. Masat për të zbutur rreziqet e sulmeve të tilla bëhet perfshirja e një fjalëkalimi të fortë, duke përdorur kriptimin kur është i valid dhe duke u lidhur vetëm me pajisje të besuara ne rrjete te tjera. (Charlie Wilson, 2017) [23]

2.6.6 Komunikimi i sistemeve në Smart Home:

Komunikimit në shtëpi mund të ndahet në rrjetin e jashtëm, gateway dhe rrjetin e brendshëm.

Rrjeti i jashtëm mund të jetë një rrjet LAN, kabllot televizive, rrjete telefonik, interneti. Intraneti përdoret për të bere lidhjen e pajisjeve te ndryshme shtëpiake.

Gateway i shtëpisë është një pajisje lidhëse e rrjetit që lidh intranetin e shtëpisë dhe ekstranetin, për të siguruar funksionin e pajisjeve ndërlidhëse ne shtëpi. Gjithashtu, gateway mundëson që shtëpia të adoptohet me teknologji të ndryshme të rrjetave. Gateways sigurojnë edhe aftësi tejkalimi nepër nën-rrjeta të ndryshëm per komunikim te pajisjeve me njëra-tjetren brenda atij nën-rrjeti.

- Rrjeti i pajisjeve shtëpiake: Pajisjet shtëpiake frigoriferë, kondicionerë, TV, furra me mikrovalë, lavatriçe, ndricim, etj. përbëjnë rrjete përmes rrjetave me tela ose wireless për të shkëmbyer informacione.
- Siguria: Përfshinë mbrojtjen e zonës përreth, videot dhe pamjet e shtëpise, monitorimin e hyrjes, alarmin e zjarrit dhe te hajduteve, rrjedhjet e gazit, derdhjet e ujit, etj.
- Qasja me shpejtësi të lartë në informacion: Internet, telefonata me video, hyrje në LAN në shtëpi përmes gateëay.
- Shërbimet e Rezidencës: Qendra e Menaxhimit të Komunitetit mund të monitorojë dhe menaxhojë pajisjet dhe mjedisin.

Shtylla kryesore e sistemit të smart home është rrjeti i brendshëm, i cili përfshin dy pjesë: gateway dhe nyja e sensoreve. Smart home gateway lidh çdo node të switchit në rrjetin shtëpiak përmes rrjetit, dhe realizon menaxhimin dhe kontrollin e rrjetit të brendshëm të smart home përmes protokolleve të komunikimit, si dhe shërben si ndërfaqe ndërvepruese e informacionit të rrjetit të brendshem dhe rrjeti te jashtëm. (Charlie Wilson, 2017)[23]

2.7 Rast studimi i implementimit

Sipas Stephen Makonin, Lyn Bartram dhe Fred Popoëich në studimin e tyre të kryer në Universitetin "Simon Fraser" për Smart Homes, duke u bazuar në përvojën e tyre në hartimin e sistemeve të shtëpive, automatizimi i shtëpive dhe avoulimi i teknologjive brenda shtëpive smart, jep një kahje premtuese në projektimin dhe rinovimin e ndërtimeve efikase. Autoret shprehin dhe vlersojnë se; fokusi, dizajnimi, dhe implementimi i teknologjive të avancuara bazohen kryesisht në simulimin e përdorimit të energjisë, automatizimin e sistemeve të ndërtimit për qellim ngritjen e performancës, mirëpo nuk ka të njejten intensitet të mbështetjes efektive në mënyren se si njerëzit i përdorin shtëpitë e tyre. Kompleksiteti i sistemit dhe vështersitë ne automatizim, mund të dekurajojnë investimin për automatizim të shtëpive përmes tekologjive të shumta. Autorët gjithashtu theksojnë se, mbështetja për përdorimin e teknologjisë në shtëpi është e qëndrueshme, dhe se modelet të cilat integrojnë teknologji me të avancuara informuese për perdorim nga banorët, sigurojnë nivele të larta të kontrollit të automatizuar. Optimizimi i energjisë, ndriçimi dhe klimatizimi janë 3 rastet të cilat fokusohen më shumë autorët. Si rezultat i studimit, arrijnë në një rezultat ku; zëvendesimi i pajisjeve me pajisje të tjera të teknologjisë së lartë dhe të avancuar, është mjaftueshëm praktik dhe ekonomik, mirëpo, nevoja që pajisjet të jenë të vetë-menaxhueshme apo "self-driving", është më e theksueshme se sa paisjet të jenë komplet të automatizuara, siç e kemi rastin e dritave. (Stephen Makonin, 2012)[24]

2.8 Rast studimi 1

Nagender Kumar Suryadevara dhe Subhas Chandra Mukhopadhyay, në librin e tyre "Smart Homes design, Implementation and Issues", iu referohen shtëpive smart si AAL (Abmient Assisted Living), duke nxjerrë në pah perspektivën e tyre për një shtëpi të mençur. Vihet re se njëra ndër

pikat kryesore te cilat ata fokusohen janë, kujdesi dhe monitorimi i të moshuarve, ku sipas tyre, personi i moshuar, edhe pse i vetem, mund të jetoj i pavarur në shtepinë e tij. Jetesa në mjedis me asistencë dixhitale, mundëson monitorim dhe ndërmarrjen e masave në kohë, në rast se personat kanë nevoja urgjente. Sipas autorëve, është tej mase e rëndësishme, zhvillimi dhe instalimi i programeve dhe senzorëve për analizim dhe bartje të informacioneve në kohë reale, dhe funksionim efikas i AAL në bazë të kohës, lokacionit dhe nevojës. (Mukhopadhyay, 2015) [25]

2.9 Rast studimi 2

Në librin "Home Automation Made Easy" të punuar nga Dennis C.Breëer, shohim një perspektivë tjetër të automatizimit të shtëpive. Sipas D.B, siguria luan një rol mjaftë të rëndësishëm në shtëpitë tona. Të dukemi sikur se jemi në shtëpi, përderisa ne jemi në pushime apo në takime biznesore jashtë vendit është zgjidhja adekuate për ngritjen e sigurisë në shtëpi. Në këtë pikë, duke krahasuar shtëpinë tradicionale dhe atë automatike, arrijmë edhe në reduktim të energjisë, shembulli i llambës: Kur ne duam te dukemi se jemi në shtëpi gjatë pushimeve, ne lëmë driten hapur gjatë gjithe kohës dhe kshtu arrijmë një shfrytëzim të lartë të energjisë, ndërsa në shtëpitë automatike, përmes smartfonëve mund t'i hapim dhe mbyllim dritat nga larg, kudo që ne gjendemi. (Brewer, 2014)[26]

3. DEFINIMI I PROBLEMIT

Ideja për ngritjen dhe modernizimin e kapaciteteve të shtëpive tradicionale, çdo ditë e më shumë po implementohet. Duke nisur nga aparatet e kafeve e deri tek kontrollimi i pajisjeve nga larg, teknologjia mori çdo gjë përsipër. Mirëpo, gjatë shfletimit të literaturës, hulumtimit dhe analizimit të smart home, arrita të shohë edhe disa anë negative.

Në bazë të hulumtimeve, vërehet se rreziku për bllokim apo daljen e pajisjeve jashtë kontrollës është mjaftë i lartë. Mos-funksionimi i dyerve, sensorëve të zjarrit, bllokimi i dritareve dhe dështimi i pajisjeve tjera mund të perfundojnë me fatalitet. Dështimi i softuerëve mund të jetë rezultat i ndërhyrjeve nga jashtë, mirëpo, në shumicën e rasteve dështimi i pajisjeve vjen si rezultat i mungesës së mirëmbajtjes.

Me anë te stimulimeve do të mundohem t'i shfaqë dy rastet më kritike, dhe të arrijë një rezultat se si ndodhin këto dështime.

Pyetje hulumtuese:

1. A është e mundur arkitektura e Smart Home e propozuar dhe e simuluar t'i përgjigjet problemit?
2. A është efikas implementimi i sensorëve të zjarrit?

4. METODOLOGJIA

Përgjatë punimit të temës së diplomes, u përdoren disa metoda të ndryshme për hulumtim dhe grumbullim të informacioneve. Për grumbullimin e të dhënave është përdorur metoda sasiore, ku përmes librave, publikimeve, revistave e tjera është bërë mbledhja e informacioneve të nevojshme.

Për vizualisim të pajisjeve smart brenda shtëpive, të cilat u implementuan përmes packet tracer tool, është përdorur metoda ekpresimentale, ku u bë programimi, konfigurimi dhe testimi i pajisjeve. Përmes metodës së krahasimit kam arritur të krahasoj 'smart home' dhe 'smart city', në mënyrë që të shihen ndryshimet të cilat përmbajne këto dy pika.

Përmes metodës cilësore është bërë krahasimi i sigurisë së pajisjeve 'smart' me ato tradicionale, metodë e cila mundësori nxjerrjen e rezultateve mjaftë të arsyeshme.

5. REZULTATET

Arrija e rezulateve të këtij punimi bazohet në hulumtim dhe analizë të studimeve të publikuara, e-book, si dhe të faqeve te internetit. Krahasimi i teknologjive në rastet më specifike ka bërë të mundur arritjen e një pikë ku mund t'i ndajmë kategorikisht të metat dhe përparsitë e pajisjeve të cilat shfrytëzuesit mund t'i perdorin.

5.1. Rezultati 1

Në fig. 7 mund ta shohim implementimin e teknologjisë në shtëpi, e cila është realizuar përmes Packet Tracer tool. Kamerat, pajisjet solare, llamba, hapja dhe mbylla e dritareve dhe derës, sensorët spërkatëse të kopshtit, pajisjet në kuzhinë, fluturat, led-at, e sensorët detektues në garazhin e shtëpisë, të gjitha këto pajisje janë konfiguruar përmes Packet Tracer dhe mund të komandohen nga larg, në atë mënyrë që shfrytëzuesi t'a bëj mirëmbajtjen dhe mbikqyrjen e shtëpisë së tij edhe kur nuk është prezent në shtëpi. Mund të themi se arkitektura e Smart Home e propozuar dhe e simuluar mund t'i përgjigjet problemit.

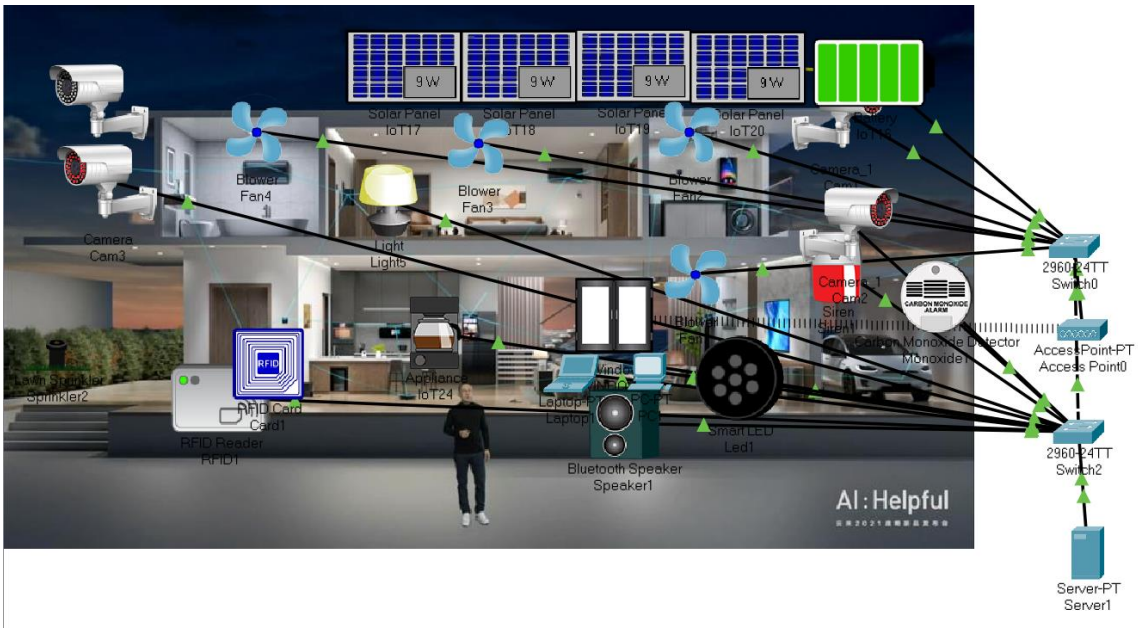

Figura 7. Digjitalizimi i shtëpisë

5.2. Rezultati 2

Sipas një studimi të publikuar në Shkurt të 2021 nga "National Fire Protection Association", arrihet një përfundim se mungesa e alarmeve të zjarrit në shtëpi apo dështimi i tyre ka shkaktuar 40% më shumë vdekje. Pjesë tjetër e dështimit të pajisjes është zbrazja e baterive të cilat shkaktuan 25% dështim të sistemit dhe të cilat përfunduan me fatalitete.

Sipas statistikave të nxjerra nga hulumtimet e bëra përgjatë viteve 2014-2018 në US, arrihet të shihet qartë se përdorimi i alarmeve të zjarrit ulë kategorikisht vdekjet dhe zvogëlon pasojat. Përqindja e vdekjeve për 1000 shtëpi, është 55% më e ulët kur alarmet e shtëpisë janë prezente. Dështimi harduerik i alarmeve pa marrë parasyshë hargjimin e baterive, ka qenë prezente në 48% të rasteve. Ndërsa në 73% të rasteve, sensorët e zjarrit kanë operuar me sukses.

Përmes chart-it do të shfaqë edhe rezultatet për vdekjet gjatë 1000 shtëpive të ndezura në vitet 2014-2018. (Ahrens, 2021)[25]

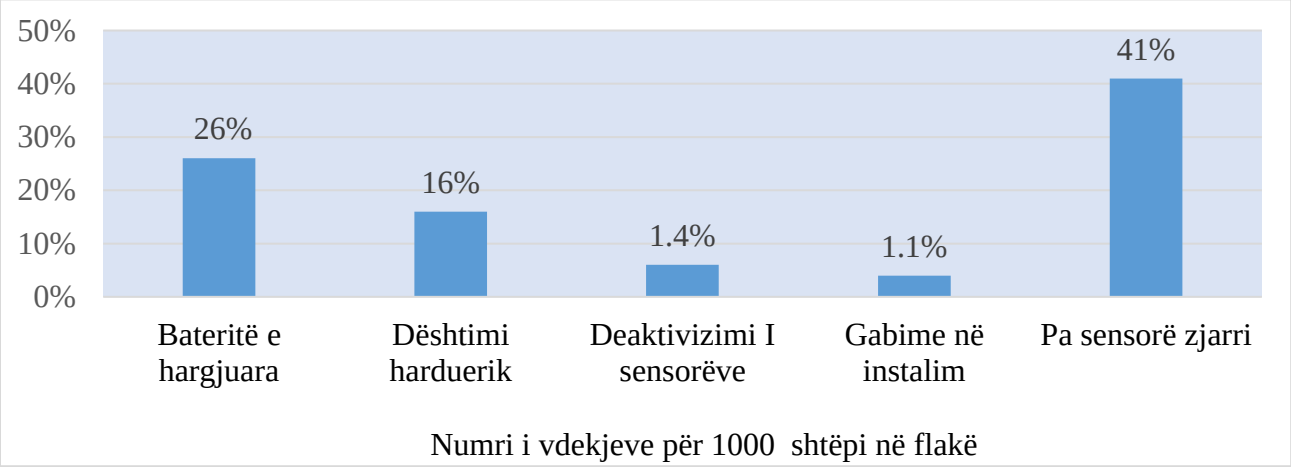

Figura 8. Statistikat e vdekjeve për 1000 shtëpi në flakë

Avantazhet e sensorëve si: monitorimi 24 orësh i shtëpise, detektim dhe ndërhyrja e menjëhershëm e ekipës, alarmim i lehtë dhe i shpejtë, shihet qartë se ulin rreziqet dhe mundësojnë shfrytëzuesit të kenë një jetesë të sigurtë dhe komode.

6.DISKUTIME DHE PËRFUNDIME

Në punimin e temës të nivelit bachelor, unë kam mësuar shumë. Fusha që përzgjodha më jep mjaftueshëm vullnet dhe më ngritë kureshtjen që të vazhdoj edhe më tutje studimet për këtë fushë dhe t'i implementoj në menyrë të vazhdueshme njohuritë e fituara.

Teknologjitë të cilat po funksionojnë përmes ZigBee kanë siguri të lartë. Mundësitë për ndërhyrje nga jashtë janë zvogëluar dukshëm. Gjithashtu, zhvillimi i pajisjeve të reja për shtëpi të mençura, kanë bazë përdorimin e rrjetit ZigBee, të cilat dita ditës po përfshijnë çdo cep të shtëpisë.

Nga ky studim kam arritur të nxjerrë këto rekomandime:

- Automatizimi i shtëpisë për siguri sa më të lartë. Monitorimi dhe kontrollimi nga distanca e pajisjeve të automatizuara që posedojmë në shtëpi, rritë sigurinë dhe komoditetin. Pra, harresa e fikjes së pajisjeve gjatë pushimeve mund të kenë pasoja fatale, ndërsa, monitorimi dhe kontrollimi i tyre edhe nga larg mundëson fikjen dhe uljen e rrezikut.
- Instalimi i sensorëve të zjarrit ulë gjithashtu rreziqet për fatalitete. Reagimi në kohë reale gjatë zjarrit brenda shtëpisë, mund të shmang vdekjet dhe të gjitha dëmet. Funksionimi i tyre bëhet kur temperatura e caktuar rritet dhe tymi shfaqet, atëherë, përmes aktivizimit në mënyrë automatike fillon pajisja të spërkas me lëndën kundër zjarrit.

Pra, me pak fjalë mund të themi se rreziqet nuk mund t'i ndalim asnjëherë, mirëpo, uljen e fatalitetеve të cilat shkaktohen brenda apo jashtë shtëpive tona dhe të cilat shkaktohen nga pakujdesitë tona, mund ta bëjmë përmes implementimit të teknologjive të reja.

Unë pasi përfundova studimin e temave të caktuara, mund të rekomandojë implementim gjithëpërfshirës të teknologjisë brenda shtëpive, pra, automatizimi i shtëpive lehtëson jetën dhe dukshëm ngritë cilësisë e jetesës.

7.REFERENCAT

[1] A brief history of the Internet Of Things by Keith D. Foote on August 16, 2016

[2] The internet of Things: A Scale Approach to Connecting Everything by IJES, 2015

[3] Gartner research from EGHAM, UK, 2019

[4] ZigBee Wireless Networks and Transcievers by Shahin Farahani

[5] Internet of Things Agenda by Alexander S. Gillis

[6] Secure and Smart Internet of Things by Ahmed Banafa, 2018, USA

[7] Internet of Things Protocols and Standards, 2019, UK

[8] Internet of Things Standardization by Jaydip Sen, 2018, UK

[9] What is Bluetooth from Steven John, 2020, https://www.businessinsider.com/what-is-bluetooth

[10] ZigBee Technology Architecture and Its Applications by https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/

[11] What is 6LoWPAN- the basics, 2019 by Electronics Note

[12] IoT Security Issues by Alasdair Gilchrist

[13] IEE 802.15.4 and ZigBee as Enabling Technologies for Low-Power Wireless Systems with Quality-of-Service Constraints by Stefano Tennina, Roberta Daidone, Anis Koubaa

[14] Smart Cities: Case Studies by Eleonora Riva Sanseverino, Ina Macaione and Enrico Anello AG 2017 ITALY

[15] The smart city infrastructure development & monitoring by Mahmound AL-HADER and Ahmad Rodzi, 2009 Dubai

[16] High Speed Digital System Laboratory HS DSL 2017 Traffic monitoring system based on Wifi

[17] Tom Rye and Till Koglin, Research Gate 2014 Parking Management

[18] Smart cities face challenges and opportunities by Noman Akhtar and Kecil Halsey- 2018

[19] Smart Home: Architecture, Technologies and Systems, ICICT 2018, Science Direct

[20] Khalid Asaad Hashim Al-Tuma 2019 Smart Door Lock Based on Bluetooth and IoT

[21] Jorge Higuera, Aleixa Llenas, Josep Carreras, IREC, Spain, Trends in Smart Lighting for the IoT

[22] Smart home technologies in Europe review of concepts, benefits, risks and policies, 2020, Benjamin K. Sovacool, Dylan D. Furszyfer Del Rio

[23] Benefits and risks of smart home technologies, 2017, Charlie Wilson, Tom Hargreaves, Richard Hauxwell-Baldwin

[24] Stephen Makonin, Lyn Bartram and Fred Popoëich 2012 Simon Fraser University, A Smarter Smart Home Case Studies of Ambient Intelligence

[25] Nagender Kumar Suryadevara and Subhas Chandra Mukhopadhyay 2015 Smart Homes, design, implementation and Issues from http://makonin.com/doc/PvC_2013.pdf

[26] Dennis C Brewer 2014 Home Automation Made Easy

[27] National Fire Protection Association USA website from https://www.nfpa.org/Neës-and-Research/Data-research-and-tools/Detection-and-Signaling/Smoke-Alarms-in-US-Home-Fires

[28] A Systematic Survey on Sensor Failure Detection by Nancy E.ElHady and Julien Provost, online book, 2018

[29] Simulation of Intelligent Fire Detection and Alarm System by V.B.Pati, S.P.Joshi

[30] Khalid Asaad Hashim Al-Tuma 2019 Smart Door Lock Based on Bluetooth and IoT

[31] A Zigbee Based Home Automation: System Design and Implementation by Fang Yao and Shuang-Hua Yang, 2008