Winter 1-2021

ACCESS CONTROL FOR THE INTERNET OF THINGS

Yllka Bahtiri

Programi për Shkenca Kompjuterike dhe Inxhinierise

ACCESS CONTROL FOR THE INTERNET OF THINGS

Shkalla Bachelor

Yllka Bahtiri

Janar/2021
Prishtinë

Programi për Shkenca Kompjuterike dhe Inxhinierise

Punim Diplome
Viti akademik 2014-2015

Yllka Bahtiri

ACCESS CONTROL FOR THE INTERNET OF THINGS

Mentori: Phd. Can. Blerton Abazi

Janar/2021

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

ABSTRAKT

Access control for the internet of things controlli i qasjes ne koncept është siguria që minimizon rrezikun për biznes apo organizata të ndryshme të qasjes së paautorizuar në sistemet fizike dhe logjike.

Ndryshe mundemi të themi se është një teknik që rregullon cilët persona çfarë munden te shikojnë dhe çfarë munden të perdorin në një mjedis informatikë.

Interneti i gjerave mundëson shërbime që do ta përmisojnë jetën e përditshme të njerzëve, do të krijojnë biznese të reja dhe do të bëjnë ndërtesa, qytete dhe transportin më te zgjuar. Internet of things ka ardhur për të përshkruar një numer të teknologjive dhe diciplinave kërkimore që mundësojnë internet për të arritu jashtë botës reale të objekteve fizike.

“Things” ka identitet që vepron në hapsira të zgjuara duke përdorur ndërfaqe intelegjente për të lidhur dhe komunikuar brenda sociales, mjedisit rrethues dhe kontekstit të përdoruesve.

Ndërsa po lëvizim nga "Things" në rrjet në Internetin e Gjërat (IoT), lindin kërkesa të reja të sigurisë.

Kontrolli i qasjes ne kete mjedis është një problem i vështir dhe sfidues, një sistem i kontrollit të qasjes duhet të jete i mjaftueshem për të mbuluar kerkesat e aplikacioneve që perhapen përmes IOT.

Nga ana tjetër ky sistem duhet të jetë i lehtë i qas’shëm dhe i zbatueshem.

Në këtë dokument do të shpejgohet mënyra e përdorimit të internet of things në access control, mënyra e përdorimit dhe zbatitmi në aplikacionet që neve na nevoitet.

Do të spjegojme mënyrën si të punojme pa çelësa publikë dhe të krijojm një çelës simetrik të përbashkët të enkriptimit që mund të përdoret për të siguruar komunikimin midis përdoruesve të autorizuar dhe "Things". Kjo formë mundëson privatësine e përdoruesit dhe lehtëson krijimin e aplikacionëve të reja.

MIRËNJOHJE/FALENDERIME

Së pari shprehe faleminderimet e mia familjes time për mbeshtetjen e tyre të pakushtezuar, prej fillimit të kësaj etape të edukimit tim e deri në perfundim të saj. Gjitha sukseset e mija ja dedikoj familjes time për kontributin mirkuptimin dhe dashurin e tyre të pakursyer.

Poashtu, një falenderim i sinqertë shkon edhe për profesorin Phd. Can. Blerton Abazi, që montiroj punën time, për gadishmerin e tij, për këshillat, vrejtjet, udhëzimet me anë të të cilave arrita të finalizoj me sukses këtë punim. Sinqerisht faleminderit!

Gjithashtu nje falenderim shkon edhe per miqtë e mi për përkahjen dhe mbështetjen e tyre gjatë këtyre viteve. Falënderoj edhe koleget e kolegët, me të cilët u njoha gjate këtyre viteve , më të cilët shkëmbyem dituri mbështetje të pakursyer.

Sinqerisht faleminderit!

Yllka Bahtiri
Janar/2019

TABELA E PËRMBAJTJES

LISTA E FIGURAVE

FJALORI I TERMAVE

IoT - Internet of Things
RFID – Radio-frequency identification
WSN- Wireless Sensor Network
OT – Operational Technology
PIN-Personal identification number
LDAP-Access Protocol to Local Directory
SAML- Significant Markup Language
ACL-access control list
DAC-Discretionary Access Control
RBAC-Role-Based Access Control
HBA-History Based Approach
DAC-Discretionary Access Control
IBAC-Access Identity Access Control
OrBAC-Organization Based Approach Control
RAC-Rule Based Approach
NAC-Network Access Control
VPN-private virtual private
RFIDs-radio frequency identification cards
RFID – Radio-frequency identification
WSN- Wireless Sensor Network
OT – Operational Technology

1 HYRJE

Interneti i Gjërave i referohet pajisjeve "të zgjuara", operacionet e të cilëve drejtohen nga kontrollorët e pajisjeve dhe programeve kompjuterike që komunikojnë me njëri-tjetrin dhe me shërbime të bazuara në internet.

Ekosistemi IOt përfshin pajisje fizike (në veçanti, sensorë dhe aktuatorë) dhe aplikacionet softuerike në industrinë industriale, mjekësore, qytetare, dhe cilësime të tjera.

Pajisjet si kyçjet e derës dhe kamerat e vëzhgimit janë përgjegjëse për funksionalitetin e ndjeshëm ndaj privatësisë ose kritikave të sigurisë, kështu që çdo kuadër i IO-së duhet të zbatojë pajisjen për pajisjen dhe kontrolli i aksesit nga app-to-device.

Interneti i gjërave (IoT) ka probleme të veçanta të sigurisë dhe privatësisë. Task Forca e Inxhinierisë së Internetit po dizajnon mekanizma të legalizimit dhe autorizimit për pajisjet më të kufizuara që janë pjesë e Internetit të gjërave.

Në shumë prej aplikacioneve të Internetit të gjërave (IoT), sensorët matin variabla të tilla si shpejtësia, presioni, konsumimi, temperatura ose te rrahurat e zemrës dhe aktuatorët kontrollojnë sistemet fizike, si frenat, valvolat, dritat, qarqet e energjisë ose dispenzuesit automatic te drogës. Ajo që i bën këto skenare interesante nga perspektiva e sigurisë dhe privatësisë, është se ata të gjithë ndikojnë në botën fizike, ndonjëherë duke kontrolluar infrastrukturën kritike dhe nganjëherë duke grumbulluar informata shumë private rreth individëve.

Është e qartë, ekziston një nevojë për sigurinë dhe mbrojtjen e privatësisë në IoT. Sistemet e kontrollit të qasjes kryejnë autentifikimin e identifikimit dhe autorizimin e përdoruesve dhe entiteteve duke vlerësuar kredencialet e kërkuara të identifikimit të cilat mund të përfshijnë fjalëkalime, numra identifikimi personal (PIN), skanime biometrike, tregues sigurie ose faktorë të tjerë autentikimi.

Ekzistojnë dy lloje të kontrollit të qasjes: fizike dhe logjike.

Kontrolli i aksesit fizik kufizon aksesin në kampuset, ndërtesat, dhomat dhe asetet fizike të IT. Kontrolli i qasjes logjike kufizon lidhjet me rrjetet kompjuterike, skedarët e sistemit dhe të dhënat.

Sot, në vend të çelësave, ne kemi kartat e hyrjes ose shënjat e identifikimit për të fituar hyrje në zonat e siguruara. Sistemet e kontrollit të qasjes gjithashtu mund të përdoren për të kufizuar

qasjen në workstations, dhomat e skedarëve që strehojnë të dhëna të ndjeshme, printera, si dhe dyert hyrëse.

Kemi edhe kontrollin e qasjes mobile si dhe atë në baze të intërnetit.

Kontrolli i qasjes mobile presupozon që telefonat mobil, tabletat dhe pajisjet elektronike të përdorshme të funksionojnë si kredencialet e përdoruesve kur hyjnë në zyra apo objekte të tjera të biznesit. Ndërsa gjithnjë e më shumë punëdhënës inkurajojnë sjelljen e Bring your Own Device (BYOD), kontrolli i qasjes së aplikacionit bëhet një mjet i shkëlqyeshëm për të shtuar një shtresë shtesë sigurie për çdo organizatë

Sistemet e kontrollit të qasjes me bazë në internet mund të përfshijnë si rrjetet kabllore ashtu edhe ato pa tel për të menaxhuar lexuesit dhe bravërat. Për më tepër, një teknologji e njohur si PoE (Power over Ethernet) po përdor lidhje që sigurojnë energji dhe të dhëna në një pajisje të lidhur përmes një kablli të njëjës.

Listat klasike të kontrollit të qasjes (ACLs) përcaktojnë një veprim, një subjekt, një objekt, dhe "miratojë ose mohojë" vendimin. Ata nuk janë ekspresive të mjaftueshme për IOT, ku shpesh varen vendimet e kontrollit të qasjes mbi situatën, kontekstin, ose gjendjen e botës.

2 SHQYRTIMI I LITERATURËS

2.1 Çka është Access control for the Internet of Things?

IoT është një koncept i ri i rrjetit të integruar të llojeve të ndryshme të pajisjeve informatike në fushën e teknologjisë së informacionit. Bazohet në rrjetin IP në të cilin çdo makinë individuale e përdorur në fushën e prodhimit, sigurisë, transportit dhe fushave të tjera të jetës sonë në ditë është caktuar një IP unike për të komunikuar me njëri-tjetrin.

Qdo her qe dikush perdor njeren prej mjeteve te kontrollit te qasjes, regjistrohet automatikisht ne sistem, keshtu behet e mundur te mbajme gjurmet e te gjitheve.

Autoret : Benantar**,** Messaoud ne libren e tyre " Access Control Systems Security, Identity Management and Trust Models" . Theksojne se libri shpjegon sistemet e kontrollit te qasjes qe perqendrohen ne sigurine, menaxhimin e identitetit dhe modelet e besimit.

Sistemet e Kontrollit të Qasjes si Siguria, Menaxhimi i Identitetit dhe Modelet e Mirëbesimit ofrojnë një hyrje të plotë në themelet e sigurisë së sistemeve të programimit, duke përfshirë menaxhimin e identitetit, modelet e besimit dhe teorinë e modeleve të kontrollit të qasjes. Libri detajon mekanizmat e kontrollit të qasjes që po dalin me teknologjitë më të fundit të programimit në Internet dhe shqyrton të gjitha modelet e përdorura dhe mënyrën se si ato punojnë, dhe ceket standardi i fundit i kontrollit te qasjes qe bazohet ne role (RBAC).

IoT ka evoluar nga konvergjenca e teknologjive wireless, sistemeve mikro-elektromekanike (MEMS), mikroservices dhe internetit. Konvergjenca ka ndihmuar në shkatërrimin e mureve të silo-ve midis teknologjisë operative (OT) dhe teknologjisë së informacionit (IT), duke lejuar analizimin e të dhënave të gjeneruara nga makina të pastrukturuara për njohuri që do të nxisin përmirësime. Kevin Ashton, bashkëthemelues dhe drejtor ekzekutiv i qendrës Auto-ID në MIT, për herë të parë përmendi internetin e gjërave në një prezantim që i bëri Procter & Gamble në vitin 1999. Ja se si Ashton shpjegon potencialin e Internetit të gjërave:

"Sot kompjuterat - dhe, për rrjedhojë, interneti - janë pothuajse tërësisht të varura nga qeniet njerëzore për informacion. Pothuajse të gjitha rreth 50 petabytes (një petabyte është 1,024 terabytes) të të dhënave në dispozicion në internet u kapën dhe u krijuan fillimisht nga njerëzit

duke shtypur, shtypur një buton rekord, duke marrë një foto dixhitale ose duke skanuar një kod bar.
Problemi është që njerëzit kanë kohë të kufizuar, vëmendje dhe saktësi - të gjitha këto do të thotë se nuk janë shumë të mira në kapjen e të dhënave rreth gjërave në botën reale.

Karakteristikat kryesore të Internet of things janë:

- Ambienti intelegjent
- Struktura fleksibile
- Ndarja sematike
- Complex access technologies
- Event driven

Pse Internet of things?

- Kontrolla dinamike e industris dhe jetës së përditshme
- Përmison raportin e përdorimit të burimeve
- Relacion më i mire ndërmjet njerëzve dhe natyres
- Formon një entitet intelektual nga integrimi i shoqëris njerëzore dhe sistemeve fizike
- Konfigurimi fleksibil dhe P&P
- Universal transport&Internetworking
- Qasshmëria&Përdoshmeria

2.2 Çfarë është Kontrolli i Qasjes si Shërbim?

Sistemi i Kontrollit të Qasjes pengon hyrjen e paautorizuar dhe mundëson menaxhmentin e kompanisë të vendosë kufizime në atë se cilës personel ambientet kanë qasje në varësi të rolit të tyre brenda një kompanie. AcaaS qëndron për Kontrollin e Qasjes si Shërbim. Zbaton teknologjinë Software as a Service (SaaS) dhe, kështu, është bazuar në cloud. Ndërsa të gjitha pajisjet e kontrollit të qasjes mbeten në vend, softueri dhe serverat hiqen nga mjediset e një kompanie dhe ruhen në qendra të fuqishme të të dhënave.
Krahasuar me kontrollin tradicional të qasjes, Kontrolli i Qasjes si Shërbim ka një numër

si fillim AcaaS është dukshëm më e lirë se kontrolli i qasjes së trashëguar.
ne mundemi të menaxhonjme kontrollin e qasjes nga çdo cep i botës për aq kohë sa kemi qasje në internet, themi se eshtë një mjet i pazëvendësueshëm i centralizuar për monitorimin e zyrave të shumta.
Edhe pse ka shqetësime lidhur me sulmet e mundshme të hakerave, AcaaS përdor encryptions sigurt, kështu që ju nuk duhet të shqetësohen për sigurinë.
Kontrolli i qasjes si një shërbim ju mundëson të merrni një siguri gjithëpërfshirëse si shërbim. Ju mund të integroni sistemin e alarmit, mbikëqyrjen video, zbulimin e ndërhyrjeve, etj.
Duke zbatuar kontrollin e Qasjes si shërbim, jo vetëm që rritni sigurinë tuaj dhe minimizoni kostot e ardhshme që lidhen me blerjen e serverëve të nevojshëm për kontrollin e qasjes tradicionale, por gjithashtu thjeshtësoni operacionet tuaja dhe kurseni kohë në aktivitetin e monitorimit të zyrave tuaja të shumta.
Funksionimi i sistemve hyrese pa qelsa perfshijne kyçe që përmbajnë një tastierë të kombinuar, bravë me kontrollin kryesor të fobit dhe brava të mençura që përfitojnë nga protokollet pa tela si Bluetooth, Wi-Fi ose Z-Wave për kontrollin e qasjes dhe menaxhimin e bllokut të largët.

2.2.1 Perdorimi i kontrollit të qasjes

Qëllimi i kontrollit të qasjes është të minimizojë rrezikun e qasjes së paautorizuar në sistemet fizike dhe logjike. Kontrolli i qasjes është një komponent themelor i programeve të pajtueshmërisë së sigurisë që siguron teknologjinë e sigurisë dhe ekzistojnë politikat e kontrollit të qasjes për të mbrojtur informacionin konfidencial, siç janë të dhënat e klientit.
Kontrolli i qasjes është një proces i integruar në mjedisin IT të një organizatë. Mund të përfshijë sisteme të menaxhimit të identitetit dhe qasjes. Këto sisteme sigurojnë softuerin e kontrollit të qasjes, një bazë të të dhënave të përdoruesit dhe mjete të menaxhimit për politikat e kontrollit të qasjes, auditimin dhe zbatimin.
Një listë e kontrollit të qasjes (ACL) është një tabelë që tregon një sistem operativ kompjuterik i cili akseson çdo përdorues në një objekt të veçantë të sistemit, si një skedar skedari ose një skedar individual. Çdo objekt ka një atribut të sigurisë që identifikon listën e kontrollit të qasjes. Lista ka një hyrje për secilin përdorues të sistemit me privilegje të qasjes. Privilegjet më të zakonshme përfshijnë aftësinë për të lexuar një skedar (ose të gjitha skedarët në një direktori),

për të shkruar në skedar ose skedarë dhe për të ekzekutuar skedarin (nëse është skedar i ekzekutueshëm ose program). Microsoft Windows NT / 2000, NetWare e Novell, OpenVMS e Digital dhe sistemet e bazuara në UNIX janë ndër sistemet operative që përdorin listat e kontrollit të qasjes. Lista është implementuar ndryshe nga çdo sistem operativ.

Në Windows NT / 2000, një listë e kontrollit të qasjes (ACL) është e lidhur me çdo sistem objekt. Çdo ACL ka një ose më shumë hyrje të kontrollit të qasjes (ACEs) që përbëhen nga emri i një përdoruesi ose grupi përdoruesish. Përdoruesi mund të jetë gjithashtu një emër roli, të tilla si "programues" ose "kontrollues". Për secilin prej këtyre përdoruesve, grupeve ose roleve, privilegjet e qasjes shprehen në një varg bitesh të quajtur një maskë aksesi.

2.3 Aplikacionet e Internet of Things

- Smart Home: Shtëpia e zgjuar ka të ngjarë aplikacionin më të njohur të IoT për momentin, sepse është ai që është më i volitshëm dhe i gatshëm për konsumatorët.
- Wearables: Oret nuk janë më vetëm për të treguar kohën.
  Apple Watch dhe smartwatches të tjerë në treg i kanë kthyer kyçet e dorës në holistë të smartfonëve duke u mundësuar tekst mesazhe, thirrje telefonike dhe të tjera.
- Smart Cities: IoT ka potencialin për të transformuar qytete të tëra duke zgjidhur problemet reale që qytetarët përballen çdo ditë. Me lidhjet dhe të dhënat e duhura, Interneti i Gjërat mund të zgjidhë çështjet e trafikut dhe të zvogëlojë zhurmën, krimin dhe ndotjen.
- Connected Car: Këto automjete janë të pajisura me qasje në internet dhe mund të ndajnë atë qasje me të tjerët, ashtu si lidhja me një rrjet pa tel në një shtëpi apo zyrë.

3 SIGURIA DHE RENDESIA E ACCESS CONTROL FOR THE INTERNET OF THINGS

3.1 Siguria e IoT

Interneti i Gjërave (IoT) nuk është thjesht një hap përgjatë rrugës për transformimin digjital, ajo është forca shtytëse. Sidoqoftë, për deri sa IoT duket të jetë vetëm një teknologji, në të vërtetë përfshihen teknologji të tjera të mëdha, të tilla si cloud computing, analiza e te dhënave, mobile, sensorë, dhe komunikimet makine-makine. Vlera reale e IoT-se nuk vjen nga të gjitha lidhjet që krijon, por nga të dhënat që gjeneron. Me analize të të dhënave në kohë reale, IoT bëhet një rrjet i drejtpërdrejtë i komunikimit për të nxitur njohuri dhe përmirësime

Kontrolli i qasjes fizike është një çështje e kujt, ku, dhe kur. Një sistem kontrolli i qasjes përcakton se kush lejohet të hyjë ose të dalë, ku atyre u lejohet të dalin ose të hyjnë dhe kur atyre u lejohet të hyjnë ose të dalin. Kontrolli i qasjes në Internetin e Gjërat (IoT) shpesh varet nga një situatë - për shembull, "përdoruesi është në shtëpi" - që mund të gjurmohet vetëm duke përdorur pajisje të shumta. Në kontrast me smartphone kornizat, zbatimi i kufizimeve të situatës në paraqitjen e IOs sfida të reja, sepse kontrolli i qasjes është thelbësisht i decentralizuar. Ajo zhvillohet në kuadër të shumëfishtë të pavarur, lëndë shpesh janë të jashtme ndaj sistemit të zbatimit dhe ndjekjes së situatës kërkon ndërveprim ndër-kornizë dhe leje.

Ekzistimi i kuadrit ekzistues të IP-së ngatërrojnë zbatimin e kontrollit të qasjes

dhe ndjekja e situatës. Risi jonë kryesore është të prezantojmë "oracles e situatës mjedisore" (ESO) si objekte të klasit të parë në ekosistemin e IOt. Një ESO encapsulates zbatimin e asaj se si një situatë është ndjerë, inferred, ose actuated. Kornizat e kontrollit të hyrjes në IOO mund të përdorin ESO-të për të zbatuar kufizimet e situatës, por ESO dhe kornizat mbeten të pavëmendshme për detajet e zbatimit të njëri-tjetrit. Mund të përdoret një ESO e vetme nga korniza të shumëfishta të kontrollit të qasjes përgjatë ekosistemit.

Kjo zvogëlon joefikasitetin, mbështet zbatimin e vazhdueshëm të zakonshëm

politikat dhe-sepse ESO-të përmbajnë një qasje të ndjeshme të pajisjes të drejtat - zvogëlon mbivlerësimin.

ESO-të mund të vendosen në çdo shtresë të stack-ut të iPT-së ku zbatohet kontrolli i qasjes. Ne implementuam ESO prototip për shtresën e burimeve të IoT, bazuar në kornizën IoTivity, dhe për shërbimet e internetit IoT, bazuar në middleware Passport.

Shumë korniza të IO-së ndjekin situatat që janë relevante për politikat e përbashkëta të kontrollit të qasjes. Për shembull, Nest dhe SmartThings gjurmoni vendndodhjen e telefonit të përdoruesit për të konkluduar nëse përdoruesi është në shtëpi.

Konsideroni GetSafe dhe aplikacione të ngjashme mobile që u mundësojnë përdoruesve
shikoni ushqen nga kamerat e sigurisë në shtëpi në smartfonët e tyre. GetSafe mund të punojë me kamerën e shtëpisë Nest Cam, por kërkon leje nga shërbimi Nest për të hyrë në të. Gjithashtu mund të regjistrohet pa përfshirjen e drejtpërdrejtë të përdoruesit, p.sh., kur zbulohet një vjedhje e mundshme. Meqë qëllimi primar i aplikacionit është monitorimi në shtëpi kur përdoruesi është larg, e drejta e saj për të hyrë në kamera duhet të kushtëzohet në situatën "përdoruesi nuk është në shtëpi".

IoT vs kornizat smartphone.

Objektet IoT dhe smartphone kanë shumë të përbashkëta: të dyja kontrollojnë dhe përdorin sensorë të shumëfishta dhe actuators, janë të nxitur nga ngjarjet, kanë modele të ngjashme të qasjes API, dhe të zbulojë të dhëna dhe operacione të ndjeshme për aplikacionet e palëve të treta. Këto ngjashmëritë sipërfaqësore motivojnë arkitekturën e qasjes-kontrollit të IoT
që punojnë në të njëjtën mënyrë si në OSes mobile, me vëzhgues të centralizuar të referencës që mbledhin të gjithë informacionin e duhur dhe të situatës të bëjë vendime të kontrollit të qasjes.

Ndërveprime të reja midis njerëzve, gjërave dhe makinave.

Algoritmet që kontrollojnë makinat po bëhen gjithnjë e më të sofistikuara. Ne tashmë kemi makina vetëlëvizëse dhe robotë të vetë-mësimit. Duke vendosur komunikime makine për makinë dhe duke krijuar algoritme që mundësojnë gjërat dhe makinat për të kontrolluar njëri-tjetrin, ne do të krijojmë një nivel të ri të automatizimit që do të ndryshojë në mënyrë dramatike se si ndërveprojmë, punojmë dhe bashkëpunojmë.

Ne do të shohim shumë ndërveprime të reja mes njerëzve, gjërave dhe makinave që sot duken si fantashkencë. Shumë nga gjërat në jetën tonë të përditshme në shtëpi dhe në punë do të ndërveprojnë me njëri-tjetrin, duke na mundësuar që t'i përdorim ato në mënyra të reja. Në këtë botë të lidhur, qasja në gjëra të tilla si makina do të bëhet më e rëndësishme sesa t'i zotërosh.

Në nivelin e njeri- makinë, ne do të jemi në gjendje të vlerësojmë statusin e makinave, të marrin paralajmërime kur ata kanë nevojë për mirëmbajtje dhe të kontrollojnë rolet e tyre në prodhim në çdo moment të caktuar. IoT gjithashtu do të na mundësojë të kontrollojmë zgjerimet robotike të trupave tanë, të tilla si zëvendësimet për gjymtyrët e humbura ose me aftësi të kufizuara për të përmirësuar forcën dhe aftësitë tona të tjera. Dhe njerëzit dhe makinat do të punojnë së bashku si skuadra, duke komunikuar përmes IoT. Duke përdorur IoT, makinat do të bashkërendojnë dhe komunikojnë me makina të tjera për të krijuar ushtri të mëdha të robotëve të automatizuar të aftë për të vepruar së bashku në mizëri, siç bëjnë milingonat në natyrë. Makinat gjithashtu do të jenë në gjendje të monitorojnë njëri-tjetrin për problemet potenciale dhe të kryejnë riparime pa ndërhyrje njerëzore.

Connect Priority Assests

Shumica e aseteve fikse të një kompanie ende nuk janë interaktive përmes IoT-it. Si rezultat, kompanitë nuk kanë pamje gjithëpërfshirëse për statusin e aseteve dhe vlerën e tyre. Nga digjitalizimi i aseteve më të rëndësishme nëpërmjet IoT, kompanitë mund të rrisin ndjeshëm shfrytëzimin e aseteve dhe jetëgjatësinë duke shtuar shërbime të mirëmbajtjes parashikuese dhe duke matur dhe përmirësuar performancës e tyre dhe përdorimin.

Reinvent Processes

Lidhja në rritje e njerëzve, gjërave dhe makinave do të ndikojë ndjeshëm në modelet e sotme të biznesit, shumica e të cilave janë zhvilluar në epokën analoge. Organizatat do të duhet të transformohen në mënyrë digjitale ose të rrezikojnë përçarje dhe zhdukje.
Përkundër rëndësisë strategjike të IoT-se për shumë biznese, adoptimi mbetet i ulët.

ReimagineWork

Duke krijuar rrjete të makinave dhe pajisjeve në vendet tona fizike dhe virtuale, IoT do të rrisë produktivitetin. Punonjësit mund të reagojnë në kohë reale për kërkesat, ndryshimet dhe mundësitë. Gjërat dhe makinat do të kenë rritje të shfrytëzimit dhe jetëgjatësisë.

Enable Operability and Openness

Potenciali i IoT-it mund të realizohet plotësisht, megjithatë, kur gjërat, pajisjet dhe makinat teknikisht janë në gjendje të ndërveprojnë me njëri-tjetrin jo vetëm brenda kufijve të kompanisë, por brenda një ekosistemi më të madh të biznesit. Të gjitha asetet e digjitalizuara do të kenë nevojë për një nivel të lartë të ndërveprimit në mënyrë që ata të mund të komunikojnë nëpërmjet standardeve moderne të IoT-së dhe të lidhin me sistemet e biznesit të një kompanie.

Por rendesia e vërtetë i IoT-së është në të dhënat që mblidhen nga të gjitha gjërat, pajisjet dhe makinat që janë të lidhura së bashku. Kompanitë do të kenë nevojë për një strategji të të dhënave për IoT, duke përdorur standarde të hapura për shkëmbimin e të dhënave.

Customer Experience

Digitizimi po ndryshon rrënjësisht përvojën e konsumatorit. Duke përdorur IoT si një kthesë kthyese të drejtpërdrejtë përgjatë udhëtimit të klientit, bizneset mund të rrisin çdo eksperiencë blerjeje dhe ndërveprimi për të transformuar konsumatorët pasivë në partnerë interaktivë dhe bashkë-inovatorë. Përfitimi i vërtetë i IoT-së në këtë rast është që të ofrojë një eksperiencë të personalizuar dhe kontekstuale për konsumatorët në këtë moment.

3.1.1 Si përdoret IoT në sistemin e kontrollit të qasjes?

Interneti i gjërave është një shtyllë e sistemit të kontrollit të qasjes moderne të IO-së, i njohur zakonisht si sisteme inteligjente të mbylljes së derës. Në këtë sistem, çdo bllokohet, kontrolluesi i qasjes së bllokimit, lexuesi i kartës dhe pajisjet e tjera të lidhura u caktohet një adresë IP e veçantë, e cila përdoret për komunikim midis pajisjeve.

Në një ndërtesë të vetme, të gjitha ato makina inteligjente normalisht lidhen përmes rrjeteve pa tel në softuerin e menaxhimit të tyre të konsoliduar ose aplikacionin celular. Këto aplikacione mund të konfigurohen për funksionimin automatik dhe manual të kyçjeve dhe kontrollorëve të ndryshëm. Alarmet dhe njoftimet e sigurisë mund të konfigurohen gjithashtu për të marrë në aplikacionet celulare në kohë reale.

Çdo pajisje apo makinë është e konfiguruar për kushtet, kriteret, ndjeshmërinë dhe autoritetin e tij në programin kryesor të kontrollit të menaxhimit, i cili përdoret si kontrollues i gjithë sistemit. Një kontroll i kopjuar i këtij sistemi përdoret si një aplikacion mobil në pajisjet e tua të

lëvizshme gjithashtu; ju mund të merrni statusin e sistemit tuaj të qasjes dhe gjithashtu mund të lëshoni udhëzime nga aplikacioni juaj. Çdo aktivitet me qëllim të keq në sistemin tuaj të qasjes gjeneron një alarm dhe njoftim të hollësishëm në aplikacionin tuaj celular ose kontrolluesin kryesor të softuerit të menaxhimit.

Cilat produkte e perdorin ate?

Interneti i gjërave është përdorur nga mijëra lloje të produkteve në përgjithësi dhe pothuajse të gjitha pjesët e sistemit të sigurisë së internetit të përdorura zakonisht në ndërtesat moderne. Në kontrollin e qasjes, flokët inteligjentë, lexuesit e kartave, tastierat dhe pajisjet e tjera të lidhura përdorin teknologjinë prapa konceptit të internetit të gjërave.

Çdo pajisje e autorizuar mobile gjithashtu përdor adresën unike të saj IP në rrjet për të marrë një qasje në kontrolluesin kryesor për përdorimin e sistemit të mbylljes inteligjente. Serveri kryesor gjithashtu ka një adresë të veçantë IP për të vendosur komunikimin midis komponentëve të ekosistemit të kontrollit të qasjes në IOt tërësisht

3.2 Pse Endpoint Security është i rëndësishëm?

Siguria përfundimtare konsiderohet të jetë një element gjithnjë e më i rëndësishëm për rrjetet e korporatave, pasi një numër në rritje i të punësuarve dhe të huajve të autorizuar (duke përfshirë, konsulentët, klientët, partnerët e biznesit dhe klientët) u jepet aksesi i rrjetit nëpërmjet internetit dhe pajisjeve.

Përparimet teknologjike janë duke nxitur zhvillimin e mbrojtjes fundore. Elementet e sigurisë aktualisht përbëhen nga mbrojtja dhe parandalimi i ndërhyrjeve, si dhe programi i bllokimit të sjelljes që do të ndihmojë në monitorimin e aktiviteteve të pajisjes për mbrojtjen e përfundimeve për aplikime jozyrtare ose qëllime me qëllim të keq.

Ekzistojnë disa programe komplekse të mbrojtjes nga fundi që përqendrohen në legalizimin e pajisjes së përdoruesit. Si përdorues përpiqet të identifikohen, kredencialet verifikohen, pas së cilës pajisja skanon për pajtueshmëri me politikat e korporatave, të cilat mund të përfshijnë një skanim për softuer të palicencuar, softuer antivirus, firewall, rrjet privat privat virtual (VPN), softuer të korporatave të detyrueshme një sistem operativ i miratuar (OS). Pajisjet që nuk i plotësojnë politikat e tilla të korporatës mund t'u jepet akses i kufizuar ose në karantinë. Kjo

quhet kontrolli i qasjes në rrjet (NAC), i cili përdoret për unifikimin e shumë elementeve të sigurisë së rrjetit në fund. Qasja jepet kryesisht sipas profilit të përdoruesit. Për shembull, një punonjës i burimeve njerëzore (HR) mund të jepet vetëm akses i përgjithshëm në një rrjet dhe skedarë të departamentit të HR.

Sistemet më të mira të kontrollit të aksesit të vitit 2018

Kur bëhet fjalë për mbajtjen e sigurt të biznesit tuaj dhe punonjësve, kontrolli i qasjes në objekt është mënyra më efikase për të parandaluar vizitorët e paautorizuar, kufizojnë punonjësit e caktuar nga qasja në zona të ndjeshme dhe menaxhimi i aksesit të punonjësve tuaj.

Në vend se t'i jepni secilit prej punonjësve një sërë çelësish për biznesin tuaj, ju mund të vendosni të lidhni dyert tuaja me një sistem kontrolli të qasjes në derë, duke i lejuar punonjësit tuaj të hyjnë në biznes duke përdorur kredencialet e specializuara, si një kartë kryesore, që ata futin në një lexuesi për të zhbllokuar derën. Ju mund të vendosni nivelin e sigurisë dhe të gjeni ekuilibrin e duhur midis sigurisë dhe komoditetit për ju dhe punonjësit tuaj. Kur një punonjës lë kompaninë tuaj, thjesht çaktivizoni kredencialet e tyre për t'i mohuar atyre akses të mëtejshëm.

Me sigurinë e kontrollit të qasjes në kartë, ti e di se kush hyn në biznesin tënd, kur kanë hyrë dhe çfarë dere kanë përdorur. Duke përdorur ndërfaqen e raportit që vjen me shumicën e sistemeve të kontrollit të qasjes, ju mund të gjurmoni se ku janë punonjësit tuaj. Ju gjithashtu mund t'i ndani dhomat ose zonat tek punonjësit e autorizuar dhe merrni raporte të aktivitetit të dyshimtë, si dikush që përpiqet të hyjë në diku ku nuk i përkasin.

Çmimet për sistemet e kontrollit të qasjes ndryshojnë shumë varësisht nga hardueri specifik që dëshironi, pavarësisht nëse zgjidhni një sistem tradicional ose IP, nëse e keni instaluar sistemin kundrejt vetë duke bërë vetë dhe sa pika aksesi keni. Ju me siguri do të duhet të flisni me një përfaqësues të kompanisë për nevojat tuaja specifike para se të mund të merrni një vlerësim të saktë të asaj se cili do të kushtojë sistemi juaj i kontrollit të qasjes.

4 DEKLARIMI I PROBLEMIT

4.1 Si do të ndikojë IoT në sigurinë dhe privatësinë?

Interneti i gjërave është duke lidhur më shumë pajisje çdo ditë dhe ne jemi drejtuar për një botë që do të ketë 24 miliardë pajisje IoT deri në 2020.

Kjo rritje ka benefitet e veta, dhe eshte nje menyr tjeter e perceptimit individual. Te kesh nje shtepi te zgjuar eshte padyshim diqka e re, dhe ta perdoresh me gjithe ate pako qe vjen me teeshte diqka e paparashikueshme.. Pastaj pajisjet e lidhura shëndetësore u japin njerëzve një vështrim më të thellë dhe më të plotë në shëndetin e tyre ose mungesën e tyre, sesa kurrë më parë.

Por me të gjitha këto përfitime vjen rreziku, pasi rritja e pajisjeve të lidhura i jep hakerëve dhe kriminelëve kibernetikë më shumë pika hyrëse.

4.2 Problemet e Sigurise te IOT

Per shkak se paisjet e IoT jane te lidhurame internet, ato jane te prekshme ndaj sulmeve kibernetike qe edhe munden te demtojne sistemin kompjuterik te konsumatorit , apo ndonje shfrytezuesi te caktuar qe mundemi te kemi. Paisjet e IoT funksionojne ne ate menyre qe krijojne nje vector te perbashket sulmesh per hakerat për të perfituar qasje në rrjete të tërë. Egzistojne disa rreziqe unike të sigurise qe paraqiten nga perdorimi I paisjeve te IoT në shërbime cloud. Ndarja e kontrollit mbi paisjen dhe te dhenat zvogelon aftesin e cilit do ofrues per te kufizuar qasjen dhe sigurin e vazhdueshme ku behet e nvarur nga harmonizimi i praktikave te sigurise dhe të dhënave midis palëve të ndryshme që janë përgjegjes për grumbullimin, transmetimin dhe ruajtejen e tyre. Ne varesi te funksioneve te paisjeve te IoT , siguria kibernetike mundet te kete pasoja te renda , kemi shembull hakimin e ndonje veture ku mundet të qojë deri tek vrasja e atyre personave që ndodhen në veture. Një kategori tjetër e pajisjeve IoT që mund të hakohen me pasoja të tmerrshme janë pajisje personale mjekësore, të tilla si defibrillators, stimuluesve kardiakë, dhe pompat e insulinës; sulmi i ndonjë prej këtyre pajisjeve mund të çojë në lëndime fizike ose vdekje.

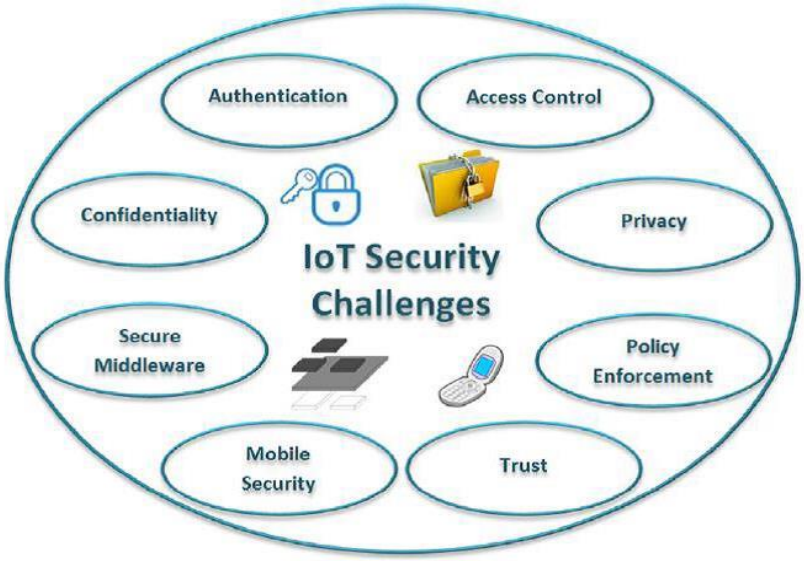

Figura 1:Sfidat e sigurise ne IoT

4.3 Problemet me privatesin e IoT

Mbrojtja e intimitetit të konsumatorit bëhet gjithnjë e më e vështirë pasi që IoT-ja bëhet më e përhapur. Sa më shumë pajisje janë të lidhura me lloje të ndryshme të pajisjeve dhe aq me shume kjo rritje në lidhjen dhe rezultatet e mbledhjes së të dhënave kontrollohen më pak. Të dy kontrolli i të dhënave dhe kontrolli i pajisjeve shumë të lidhura janë në rrezik. Kontrolli mund të humbasë nëse dikush hakon në telephone te mencur ose në kompjuter që vepron si një telekomandë për pajisjet e tjera. Në rastin e kompjuterëve dhe telefonave të mencur, ky hakim mund të bëhet larg dhe shpesh i pazbuluar. Telefonat e mencur, ashtu si kompjutera, mbajnë një sasi të madhe të informacionit personal në lidhje me pronarët e tyre. Ata shpesh lidhen me llogaritë bankare, llogaritë e-mail, dhe në disa raste pajisje shtëpiake. Të dhënat e vjedhura mund të rezultojnë me probleme serioze. Automjetet përmbajnë shumë kompjuterë që kontrollojnë funksionin e tyre. Fillimisht, këta kompjuterë nuk mund të hakoheshin. Me rritjen e lidhjes së IoTs, megjithatë, automjetet tani janë në rrezik për shkak të lidhjes me internetin.

Në një kuptim tjetër, kontrolli mund të humbet pasi gjithnjë e më shumë kompani mbledhin të dhëna për përdoruesit. Këto të dhëna shpesh paraqesin një pamje të detajuar të përdoruesve individualë përmes mbledhjes së aktiviteteve online. Çdo gjë që kërkoni, të gjitha aktivitetet tuaja në internet, po gjurmohen nga kompanitë që përdorin këto të dhëna. Këto kompani shpesh përdorin të dhëna për të përmirësuar përvojën e përdoruesit, por gjithashtu përdorin këto të dhëna

për të shitur produktet e përdoruesve ose për të shitur tek kompanitë e tjera që shesin produktet e përdoruesve.

Konsumatorët do të bëhen gjithnjë e më të vetëdijshëm për implikimet e privatësisë së këtij niveli të lidhjes nëpërmjet ndërveprimit me IotT dhe ekspozimit ndaj politikave që kompanitë ofrojnë për ta.

- To much data: Shuma e madhe e të dhënave që pajisjet IoT mund të gjenerojnë është tronditëse. Një raport i Komisionit Federal të Tregtisë me titull "Interneti i Gjërave: Privatësia dhe Siguria në një botë të lidhur" zbuloi se më pak se 10,000 familje mund të gjenerojnë 150 milionë pika të të dhënave diskrete çdo ditë.
- Profili publik i padëshiruar: Pa dyshim që ju keni rënë dakord kushteve të shërbimit në një moment, por a keni lexuar ndonjëherë një dokument të tërë? Raporti i lartpërmendur FTC gjeti se kompanitë mund të përdorin të dhënat e mbledhura që konsumatorët me dëshirë ofrojnë për të marrë vendime për punësim. të ndodhë edhe për sigurimin e shëndetit ose të jetës në sajë të gjurmuesve të palestër.
- Besimi i konsumatorit: Secili prej këtyre problemeve mund të dëmtojë dëshirën e konsumatorëve për të blerë produkte të lidhura, gjë që do të parandalonte betejën për të përmbushur potencialin e saj të vërtetë.
- Vëzhgimi: Prodhuesit ose hakerat mund të përdorin një pajisje të lidhur për të pushtuar pothuajse shtëpinë e një personi.

4.4 Security risks

Rreziku më i zakonshëm i sigurisë për ndërhyrje nëpërmjet një sistemi të kontrollit të qasjes është thjesht duke ndjekur një përdorues të ligjshëm nëpërmjet një derë, dhe kjo quhet si backgating. Shpesh përdoruesi legjitim do të mbajë derën për ndërhyrës. Ky rrezik mund të minimizohet përmes trajnimit të ndërgjegjësimit të sigurisë të popullatës së përdoruesit, ose me mjete më aktive siç janë turnstiles. Në aplikime shumë të larta të sigurisë ky rrezik minimizohet duke përdorur një port të quajtur, ndonjëherë i quajtur një depo sigurie ose mantra, ku ndërhyrja e operatorit kërkohet me sa duket për të siguruar identifikimin e vlefshëm.

Rreziku i dytë më i zakonshëm është nga levizja e një derë të hapur. Kjo është relativisht e vështirë në dyert e siguruara siç duhet me greva ose forca magnetike me forcë të madhe

mbajtëse. Sistemet e kontrollit të qasjes të zbatuara plotësisht përfshijnë alarmet e detyruara për monitorimin e derës. Këto ndryshojnë në efektivitet, zakonisht duke dështuar nga alarme të larta false, konfigurim të dobët të bazës së të dhënave, ose mungesë të monitorimit aktiv të ndërhyrjeve. Shumica e sistemeve më të reja të kontrollit të qasjes përfshijnë disa lloj alarmi të derës për të informuar administratorët e sistemit për një derë të hapur më shumë se një periudhë kohore të caktuar.

Rreziku i tretë më i zakonshëm i sigurisë është fatkeqësitë natyrore. Për të zbutur rrezikun nga fatkeqësitë natyrore, struktura e ndërtesës, deri në cilësinë e rrjetit dhe pajisjeve kompjuterike është vitale. Nga një perspektivë organizative, lidershipi do të duhet të miratojë dhe zbatojë një plan të të gjitha rreziqeve, ose Plani për Reagimin e Incidenteve. Pikat kryesore të çdo plani incidentesh të përcaktuar nga Sistemi Kombëtar i Menaxhimit të Incidentit duhet të përfshijnë Planifikimin Para-incident, gjatë veprimeve të incidentit, rikuperimit të fatkeqësive dhe pas rishikimit të veprimit. [9]

Ngjashëm me levizjen është duke u rrëzuar përmes mureve të ndara të ndarjes. Në hapësirat e përbashkëta të qiramarrësit, muri i ndarjes është një dobësi. Një cenueshmëri përgjatë vijave të njëjta është thyerja e dritave të jashtme. [Citimi i nevojshëm]

Pajisja e mbylljes së bllokimit është mjaft e thjeshtë dhe më elegante sesa levizja. Një magnet i fortë mund të përdorë bulonat e kontrollit të solenoidit në pajisjet e mbylljes elektrike. Brava të motorëve, më të përhapura në Europë se sa në SHBA, janë gjithashtu të ndjeshëm ndaj këtij sulmi duke përdorur një magnet të formës së donutit. Është gjithashtu e mundur që të manipulohet fuqia e bllokimit ose duke hequr ose shtuar sistemin aktual, edhe pse shumica e sistemeve të kontrollit të hyrjes përfshijnë sisteme rezervë të baterive dhe kyçet janë pothuajse gjithmonë të vendosura në anën e sigurt të derës.

Kartat e qasjes vetë kanë provuar të prekshme ndaj sulmeve të sofistikuara. Hakerët ndërmarrës kanë ndërtuar lexues portativë që kapin numrin e kartelës nga karta afërt e përdoruesit. Haker thjesht ecën nga përdoruesi, lexon kartën dhe pastaj e paraqet numrin tek një lexues që siguron derën. Kjo është e mundur për shkak se numrat e kartelave dërgohen në mënyrë të qartë, pa asnjë encryption. Për të kundërshtuar këtë, duhen përdorur gjithmonë metoda të dyfishta të legalizuara, si një kartë plus një PIN.

Numri i serive unike të kredencialeve të kontrollit të qasjes janë programuar në mënyrë sekuenciale gjatë prodhimit. Njohur si një sulm vijues, nëse një ndërhyrës ka një kredenciale të

përdorur një herë në sistem ata thjesht mund të rriten ose zvogëlojnë numrin serial derisa të gjejnë një kredenciale që aktualisht është e autorizuar në sistem. Rekordimi i kredencialeve me numra serialë të rastësishëm të veçantë rekomandohet për të kundërshtuar këtë kërcënim. [10]
Së fundi, shumica e pajisjeve elektrike të mbylljes ende kanë çelësa mekanike si një dështim. Çelësat çelësa mekanikë janë të ndjeshëm ndaj bumping(perplasje).

4.5 Siguria kompjuterike

Në sigurinë e kompjuterave, kontrolli i përgjithshëm i qasjes përfshin vërtetimin, autorizimin dhe auditimin. Një përkufizim më i ngushtë i kontrollit të qasjes do të mbulonte vetëm miratimin e qasjes, ku sistemi merr një vendim për të dhënë ose refuzuar një kërkesë për qasje nga një subjekt tashmë i vërtetuar, bazuar në atë që subjekti është i autorizuar për të hyrë. Autentifikimi dhe kontrolli i qasjes shpesh kombinohen në një operacion të vetëm, kështu që qasja miratohet në bazë të një autentifikimi të suksesshëm ose në bazë të një token anonim të qasjes. Metodat dhe argumentet e autentifikimit përfshijnë fjalëkalime, skanime biometrike, çelësa fizikë, çelësa elektronikë dhe pajisje, shtigje të fshehura, barriera shoqërore dhe monitorim nga njerëzit dhe sistemet e automatizuara.
Në çdo model të kontrollit të qasjes, subjektet që mund të kryejnë veprime në sistem quhen lëndë, dhe subjektet që përfaqësojnë burimet për të cilat qasja mund të kenë nevojë të kontrollohen quhen objekte (shih gjithashtu Matricën e Kontrollit të Qasjes). Subjektet dhe objektet duhet të konsiderohen si subjekte softuerike, sesa si përdorues të njeriut: çdo përdorues i njeriut mund të ketë efekt në sistemin vetëm nëpërmjet entiteteve software që ata kontrollojnë.
Megjithëse disa sisteme e barazojnë subjektet me ID të përdoruesit, kështu që të gjitha proceset që fillon nga një përdorues me parazgjedhje kanë të njëjtin autoritet, ky nivel i kontrollit nuk është i holluar mirë për të përmbushur parimin e privilegjit më të vogël dhe ndoshta është përgjegjës për mbizotërimin e malware në sisteme të tilla (shih pasigurinë e kompjuterit) [citim i nevojshëm]
Në disa modele, për shembull modelin e aftësive të objektit, çdo njësi softueri potencialisht mund të veprojë si subjekt dhe objekt.
Që nga 2014, modelet e kontrollit të qasjes kanë tendencë të bien në një nga dy klasat: ato të bazuara në aftësitë dhe ato të bazuara në listat e kontrollit të qasjes (ACLs).

• Në një model të bazuar në aftësi, mbajtja e një reference ose aftësie të palodhshme për një objekt siguron qasje në objekt (përafërsisht analoge me atë se si posedimi i çelësit të shtëpisë i jep një qasje në shtëpinë e dikujt); qasja i transmetohet një pale tjetër duke transmetuar një aftësi të tillë mbi një kanal të sigurt. Në një model të bazuar në ACL, qasja e një personi në një objekt varet nga fakti nëse identiteti i tij shfaqet në një listë të lidhur me objektin (përafërsisht analogji me mënyrën se si një mashtrues në një palë private do të kontrollonte një ID për të parë nëse emri shfaqet në Lista e te ftuarve); qasja përcillet duke e redaktuar listën. (Sistemet ACL të ndryshme kanë një sërë konventash të ndryshme lidhur me atë se kush ose çfarë është përgjegjës për redaktimin e listës dhe si është redaktuar.) Të dyja modelet e bazuara në aftësi dhe në bazë të ACL-së kanë mekanizma për të lejuar të drejtat e qasjes për t'u dhënë të gjithë anëtarëve të një grupi subjektesh (shpesh grupi vetë modelohet si subjekt). Sistemet e kontrollit të qasjes sigurojnë shërbimet thelbësore të autorizimit, identifikimit dhe autentifikimit (I & A), miratimin e qasjes dhe llogaridhënien ku:

• autorizimi specifikon se çfarë mund të bëjë një subjekt

• Identifikimi dhe autentifikimi sigurojnë që vetëm subjektet e ligjshme mund të regjistrohen në një sistem

• Aksesimi i qasjes jep akses gjatë operacioneve, nga shoqata e përdoruesve me burimet që u lejohet të kenë qasje, në bazë të politikës së autorizimit

• Përgjegjësia identifikon se çfarë ka bërë një lëndë (ose të gjitha lëndët që lidhen me një përdorues).

4.6 Operacioni i sistemit të kontrollit të hyrjes

Kur një kredencial i prezantohet një lexuesi, lexuesi dërgon informacionin e kredencialit, zakonisht një numër, tek një panel kontrolli, një procesor shumë i besueshëm. Paneli i kontrollit krahason numrin e kredencialeve në një listë të kontrollit të qasjes, jep ose e mohon kërkesën e paraqitur dhe dërgon një regjistër transaksioni në një bazë të dhënash. Kur qasja mohohet bazuar në listën e kontrollit të qasjes, dera mbetet e mbyllur. Nëse ka një ndeshje në mes të kredencialit dhe listës së kontrollit të qasjes, paneli i kontrollit vepron me një staf që e zhbllokon derën. Paneli i kontrollit gjithashtu injoron një sinjal të hapur derë për të parandaluar një alarm. Shpesh lexuesi siguron reagime, të tilla si një LED të ndezur të kuq për një hyrje të refuzuar dhe një LED të gjelbër ndezje për një akses të dhënë.

Kredencialet mund të kalohen përreth, duke e përmbysur kështu listën e kontrollit të qasjes. Për shembull, Alice ka të drejtat e hyrjes në dhomën e serverit, por Bob nuk. Alice ose i jep Bobit kredencialet e saj, ose Bob e merr; ai tani ka qasje në dhomën e serverit. Për ta parandaluar këtë, mund të përdoret autentifikimi me dy faktorë. Në një transaksion dy faktor, kredencialet e paraqitura dhe një faktor i dytë janë të nevojshme për qasje që duhet dhënë; një faktor tjetër mund të jetë një PIN, një kredenciale e dytë, ndërhyrje e operatorit ose një input biometrik.
Ekzistojnë tre lloje (faktorë) të informimit të vërtetimit:

• diçka që përdoruesi e di, p.sh. një fjalëkalim, frazë ose PIN

• diçka që përdoruesi ka, të tilla si karta inteligjente ose një çelës kyç

• diçka që përdoruesi është, të tilla si gjurmët e gishtave, të verifikuara me matje biometrike

Fjalëkalimet janë një mjet i zakonshëm për të verifikuar identitetin e një përdoruesi përpara se qasja t'u jepet sistemeve të informacionit. Përveç kësaj, tashmë njihet një faktor i katërt i legalizimit: dikush që njeh, ku një person tjetër i cili di ju mund të sigurojë një element njerëzor të vërtetimit në situata ku sistemet janë ngritur për të lejuar skenarë të tillë. Për shembull, një përdorues mund të ketë fjalëkalimin e tyre, por harron kartën e tyre të mençur.

Llojet e lexuesve

Lexuesit e kontrollit të qasjes mund të klasifikohen sipas funksioneve që ata janë në gjendje të kryejnë:

• **Lexuesit bazë (jo inteligjentë):** thjesht lexoni numrin e kartelës ose PIN-in dhe përcillni atë në një panel kontrolli. Në rast të identifikimit biometrik, lexuesit e tillë nxjerrin numrin ID të një përdoruesi. Në mënyrë tipike, protokolli Wiegand përdoret për transmetimin e të dhënave në panelin e kontrollit, por opsionet e tjera si RS-232, RS-485 dhe Clock / Data nuk janë të pazakonta. Ky është tipi më popullor i lexuesve të kontrollit të qasjes. Shembuj të lexuesve të tillë janë RF Tiny nga RFLOGICS, ProxPoint by HID, dhe P300 nga Farpointe Data.

• **Lexuesit gjysmë-inteligjentë:** kanë të gjitha hyrjet dhe rezultatet e nevojshme për të kontrolluar hardware-in e derës (bllokohet, kontaktoni derën, butoni i daljes), por mos merrni vendime për qasje. Kur një përdorues paraqet një kartë ose fut një PIN, lexuesi i dërgon informacion kontrolluesit kryesor dhe pret përgjigjen e tij. Nëse lidhja me kontrollorin kryesor është ndërprerë, lexuesit e tillë ndalojnë punën ose funksionojnë në një mënyrë të degraduar. Zakonisht lexuesit gjysmë-inteligjentë janë të lidhur në një panel kontrolli nëpërmjet një autobusi

RS-485. Shembuj të lexuesve të tillë janë InfoProx Lite IPL200 nga CEM Systems, dhe AP-510 nga Apollo.

• **Lexuesit inteligjentë:** kanë të gjitha hyrjet dhe rezultatet e nevojshme për të kontrolluar hardware-in e derës; ata gjithashtu kanë kujtesën dhe fuqinë e përpunimit të nevojshme për të marrë vendime të hyrjes në mënyrë të pavarur. Ashtu si lexuesit gjysmë-inteligjent, ata janë të lidhur me një panel kontrolli nëpërmjet një autobusi RS-485. Paneli i kontrollit dërgon përditësime të konfigurimit, dhe rikthen ngjarje nga lexuesit. Shembuj të lexuesve të tillë mund të jenë InfoProx IPO200 nga CEM Systems dhe AP-500 nga Apollo. Ekziston edhe një gjeneratë e re e lexuesve inteligjentë të referuar si "lexues IP". Sistemet me lexues IP zakonisht nuk kanë panele tradicionale të kontrollit, dhe lexuesit komunikojnë direkt në një kompjuter që vepron si një mikpritës.

4.7 Sistemet e Kontrollit të Qasjes dhe Karakteristikat e Llojeve te Tyre

Sistemet e kontrollit të qasjes janë sistemet elektronike që janë të dizajnuara për të kontrolluar nëpërmjet një rrjeti dhe ata duhet të kenë qasje në një rrjet. Sistemi i Kontrollit të Qasjes njeh autentifikon dhe autorizon hyrjen e një personi për të hyrë në objekt duke dhënë mbrojtje të plotë duke siguruar siguri me sistemin.

Shumë sisteme të kontrollit të qasjes përdorin rrjetin për qëllime komunikimi dhe informacioni komunikohet nëpërmjet këtyre rrjeteve.

Shembull i një sistemi të kontrollit të qasjes: Një derë mund të jetë e hapur me një kartë shpullë, një sistem RFID ose me teknologjinë e sistemit bio metrik.

Çfarë është sistemi i kontrollit të qasjes?

Sistemi i kontrollit të qasjes siguron siguri duke i dhënë kontroll fleksibël se kush lejohet të hyjë në lokalet tuaja. Sistemi i kontrollit të hyrjes është një nga sistemet më të zakonshme të përdorura në kontrollin elektronik të derës duke përdorur një kartë ose një shirit magnetik që mund të arrihet duke rrokullisur përmes një lexuesi në derë. Këto sisteme të kontrollit të qasjes përdoren për qëllime sigurie. Zonat ose organizatat që kërkojnë siguri të lartë përdorin lloje të ndryshme të sistemeve të kontrollit të qasjes, si bio metrikë, RFID, kontrollorët e derës dhe lexuesit e kartelave etj. Çdo pikë aksesi mund të kontrollohet individualisht sipas kërkesës së kompanisë ose organizatave ku është e nevojshme siguria e lartë. Siguria e rrjetit është gjithashtu e rëndësishme, veçanërisht në një kompani që merret me të dhëna të ndjeshme.

Me anë të këtyre sistemeve të kontrollit të qasjes në kartë mundësohet hyrja në hapësirat kufizuese të njerëzve në njërën anë të derës. Në disa raste, sistemet e kontrollit të qasjes fizike janë të integruara me ato elektronike duke kufizuar përdoruesit duke i lejuar ata të shfrytëzojnë burimet e kufizuara në një sistem kompjuterik.

Bio metric Access Control System

Sistemi i kontrollit të aksesit të metrikës është një sistem i kontrollit të frekuentimit me gjurmë gjurmë dhe ndjek dhe regjistron të dhënat e Vizitorëve dhe Punonjësve përmes Software-it të Qasjes. Kjo është përdorur gjerësisht në vende konfidenciale për instalimin e saj të lehtë dhe siguri të lartë.

Bio Metric Access Control System përdor gjurmën e gishtit në vend të sistemit të kartelave për qasje. Sistemi i Kontrollit të Qasjes jo vetëm që lejon hyrjen, por edhe jep të dhëna në lidhje me hyrjen e personave. Programi i Pjesëmarrjes mund të integrohet me ndonjë softuer ekzistues të listës së pagave dhe jep regjistrim automatik të informacionit të gjeneruar nga Sistemi i Pjesëmarrjes dhe kjo kursen kohë dhe burime në regjistrim. Kjo rrit produktivitetin dhe rentabilitetin për çdo organizatë.

Figura 2:Bio metric Access Control System

5 METODOLOGJIA

5.1 Siguria Hyrje

Interneti i gjerave eshte nje sistem komples qe evulon me kohen ne shpejtesi te madhe. Per te kuptuar implikimet, rreziqet dhe per te gjetur nje zgjidhje te sigurte, duhet ti shohim edhe komponentet e tjerë, siq jane big data dhe intelegjenca artificiale.

IoT eshte nje sistem kompleks, ku paisjet jane vetem nje komponent. Qdo komponent mund te jete lidhja me e dobet e sistemit, keshtu qe kemi nevoje per nje qasje holistike ndaj sigurise.

Siguria e IoT eshte pergjegjesi e madhe e shume qeshtjeve, kur e shohim ate si nje sistem, ne mund te numerojme nje numer te madh partish qe munden dhe duhet te kontribojne ne sigurine e IoT:

- Furnizuesit e sensorëve dhe pajisjet
- Zhvilluesit e mesazheve
- Zhvilluesit e aplikacioneve
- Operatorët e platformës së mesme
- Operatorët e shërbimeve të aplikacionit

Jashtë fushës teknike numri i subjekteve është gjithashtu i rëndësishëm:

- Shitësit me pakicë dhe rishites
- End-users: Përdoruesit e shtëpisë dhe të zyrës
- ISP-të dhe ofruesit e shërbimeve
- Kompanitë e sigurimeve
- Politikëbërësit dhe rregullatorët

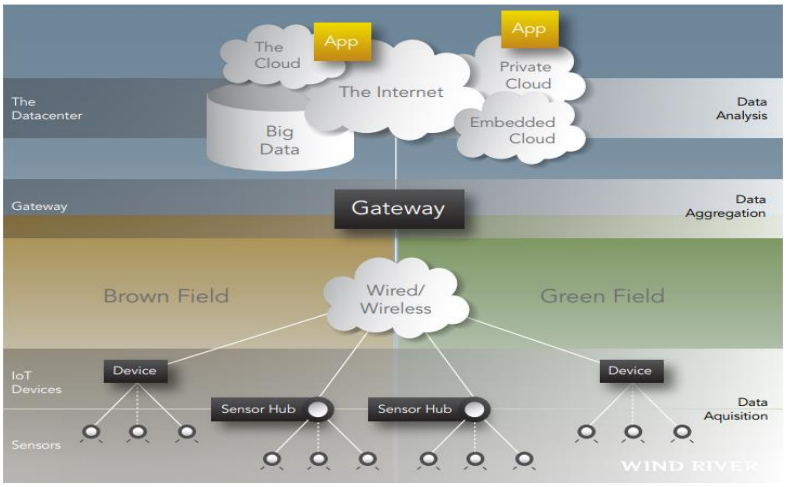

Figura 3:Një topologji e përgjithshme e IoT

5.1.1 Building Security In From The Bottom Up

Aftësia për të lidhur dhe për të menaxhuar në distancë një numër të pallogaritshëm të pajisjeve të automatizuara dhe të rrjetëzuara nëpërmjet internetit është normale e re në botën e digjitalizuar. Nga linja e asamblesë së makinave në sallën e operacionit spitalor në dhomën e banimit, njerëzit po bëhen gjithnjë e më shumë të varur nga Interneti i Gjërat (IoT) për të drejtuar bizneset e tyre dhe për të jetuar jetën e tyre. Tani ka një bollëk të pajisjeve inteligjente në vendin e punës dhe në shtëpi, duke përfshirë:

- TV dhe telefona të zgjuar në dhomat e konferencave;
- sisteme zgjuar alarmi;
- pajisje intuitive HVAC;
- makina te kujdesit shendetesor;
- menaxhimi i shkathët i trafikut dhe parkimi;
- frigoriferë të mençur, makina larëse dhe termostate; dhe
- lodra dhe pajisje robotike.

Përhapja e pajisjeve me IOT-enabled ka transformuar rolin e TI në siguri. Siguria duhet të ndërtohet nga poshtë lart.

A janë rreziqet reale?

Dobia e pajisjeve IoT është po aq e vërtetë sa kërcënimet e sigurisë që ato paraqesin. Çdo ndërhyrje me qëllim të keq ose aksidentale në një reaktor bërthamor, një tren udhëtarësh, ose një stimulues kardiak, përbën një kërcënim për jetën njerëzore. Në mënyrë të ngjashme, çdo operacion i pakufishëm i një vegël të përdorur në biznes mund të nënkuptojë fundin e biznesit.Institucioni mjekësor, i konsumit dhe i ndërmarrjeve IoT përballen të njëjtat sfida të sigurisë. Ndërsa zyrat, fabrikat, shtëpitë dhe automjetet po bëhen më të mençura, hakerët po krijojnë teknika më të rafinuara për të avancuar tregtinë e tyre.

Si mundet ndërmarrjet të trajtojnë kërcënimin e sigurisë së internetit?

Ekzistojnë një numër hapash që ndërmarrjet mund të ndërmarrin për të zbutur rreziqet që lidhen me IOT.Rishikoni bazat. IOt është kryesisht për gjërat fizike. Mundësitë e dëmtimit të dëmshëm tani përfshijnë jo vetëm vjedhjen e të dhënave, sulmimin e faqeve të internetit, ose lëvizjen e parave, por edhe shkatërrimin e infrastrukturës fizike. Johan Sys, drejtues kryesor i Internetit të Gjërat në Verizon, këshillon ndërtimin e sigurisë që nga fillimi.

Siguria e IOs duhet të sjellë oficerët e sigurisë përsëri në bazat: analizën e rrezikut dhe menaxhimin e të gjitha komponentëve të IoT, të tilla si pajisjet, rrjetin, sistemet operative dhe aplikacionet. Rreziqet që lidhen me pajisjet mjekësore të lidhura janë të ndryshme nga ato të bankave të mençura. Organizatat duhet të dinë dhe të ndjekin çdo pajisje të lidhur me rrjetin, të përcaktojnë dobësitë e tyre specifike dhe të planifikojnë kurse të përshtatshme të veprimit në shenjën e parë të problemeve.

Sigurimi i mbështetjes së ciklit të jetës. Edhe lojtarët e mëdhenj mund të përfundojnë me miliona pajisje të pasigurta dhe të paqëndrueshme. Shumica e telefonave, për shembull, kanë një vjetërsi të planifikuar afatshkurtër. Prodhuesit do të përdorin më mirë burimet e tyre për të zhvilluar produkte të reja se sa të ofrojnë përditësime për mallrat me jetë të shkurtër. Prandaj, ndërmarrjet duhet të sigurojnë siguri nga dizajni fillestar në mjedisin operativ. Ata duhet të gjejnë shitës me të cilët ata mund të krijojnë marrëveshje për përditësime jetësore dhe mbështetje të ciklit të jetës. Zbatimi i kontrollit të qasjes dhe vërtetimit të pajisjes. Kontrolli i qasjes është një komponent i rëndësishëm i sigurisë së internetit, sepse ndihmon në parandalimin e përdorimit të paautorizuar të pajisjes dhe rrjetit. Siguron që punonjësit të

kenë qasje vetëm në burimet që kanë nevojë për të bërë punët e tyre. Në mënyrë të ngjashme, vërtetimi i pajisjes kontrollon funksionimin e një pajisjeje manualisht ose automatikisht brenda rrjetit bazuar në një grup të miratuar kredencialesh.

Ngritur një sistem sigurie me shumë shtresa. Risqet e sigurisë së internetit IoT vazhdojnë të jenë më komplekse dhe më të shpeshta. Përpjekjet e dëmshme tani mund të organizohen nga pika të shumta. Zbatimi i sigurisë në shumë shtresa në të gjithë ndërmarrjen mban biznese të sigurta në çdo nivel të mbrojtjes. Ndërmarrja duhet të krijojë një strategji të koordinuar të sigurisë përgjatë grupit të sigurisë së IT, ekipit të sigurisë fizike dhe prodhuesve të pajisjes.

Kur pajisjet e automatizuara funksionojnë në internet, gjithmonë ekziston rreziku që kontrolli të bjerë në duar të gabuara. Kur është fjala për IOT, siguria e ndërtimit nga poshtë lart është e dorës së parë.

5.1.2 End-to-End IoT Security

Çështja e sigurisë së internetit IoT është një punë shumë e madhe, dhe shumë inxhinierë e njohin nevojën për të adresuar çështjet e sigurisë. Partneriteti midis dy kompanive është një përpjekje për ta bërë më të lehtë për projektuesit e internetit të internetit të futin sigurinë në pajisjet dhe rrjetet e tyre IoT, si dhe për të rritur monetizimin e zgjidhjeve IoT.

Për këtë qëllim, zgjidhja bashkëpunuese e sigurisë së IO-së premton të ofrojë një numër të veçorive të sigurisë, duke përfshirë:

- Kontrollet për nisjen e sigurt dhe përditësimin për të ruajtur integritetin e pajisjes
- Siguria për një sërë protokollesh të rrjetëzimit, duke përfshirë celularin dhe LoRa
- Mbështetje për legalizimin e shumëfaktorëve
- Provimi dhe menaxhimi i identitetit për pajisjet IoT
- Çelësi dhe menaxhimi i certifikatave për portat dhe terminalet e IP ut

"Sigurimi i sigurisë dhe besueshmërisë së pajisjeve të lidhura është më e rëndësishme se kurrë," tha CEO i Mocanës Bill Diotte. "Bashkëpunimi me ndonje kompani te forte do të lehtësojë prodhuesit e pajisjeve dhe ofruesit e reve për të siguruar identitetin e pajisjes, të inkorporojë rrënjë të forta të bazuara në hardware dhe të integrojë kontrollet e provuara të softuerëve të sigurisë në internet në aplikacionet e ngulitura në pajisjet IoT dhe infrastrukturën kritike".

Përtej sigurisë, kompanitë shpresojnë të ofrojnë zgjidhje të zhvilluesve të IoT për të fituar para nga mjetet e tyre të internetit. Ndërsa IOt ofron mundësi të reja dhe modele biznesi, zhvilluesit mund të kenë nevojë për ndihmë në lundrimin e opsioneve të ndryshme monetare. "Një nga premtimet më të mëdha të IoT është ndryshimi në mentalitetin për të bërë biznes - një mendim për të lëvizur nga një qasje monetare e bazuar në produkt në një qasje të bazuar në shërbime", shkruan përshkrimi i Gemalto për monetizimin e IO. "Kjo kërkon një kornizë monetizimi që u lejon të gjithë kontribuesve të shfrytëzojnë modelet e reja të biznesit të iPT dhe të kenë agility për të vendosur aplikacione të reja shpejt për të patur një ROI më të shpejtë".

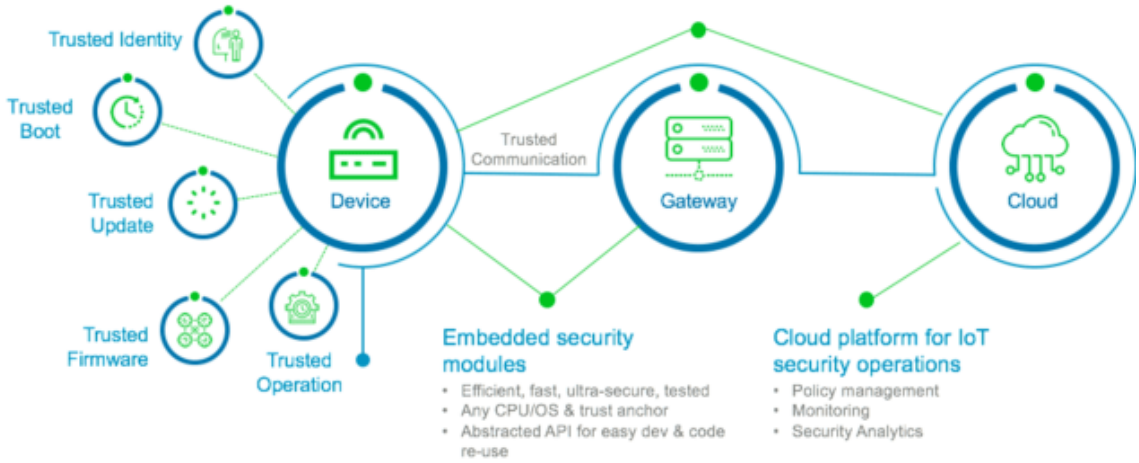

Figura 4:End-to-End IoT Security

5.2 Pritvatësia

Interneti i Gjërave si një arkitekturë globale e informacionit në internet që shfaqet paraqet një rrjet fizik dhe pajisjet virtuale, objekte dhe sensorë të ngulitur në objekte të tjera dhe mjedisi me të specializuar elektronikë, softuer dhe fuqi të përpunimit që ua mundëson këtyre objekteve të mbledhin, përpunojnë, shkëmbejnë lirshëm dhe shpërndarjen e të dhënave.

Shembuj të IOt përfshijnë objekte të zgjuar që ndërveprojnë nëpërmjet sensorëve të përfshirë në shtëpi dhe pajisje shtëpiake (p.sh.termostat dhe kontrollet e ndriçimit, frigoriferë zgjuar, televizorë dhe makina larëse), qytete të zgjuara (p.sh.akses të sigurt për ndërtim, objekte të zgjuara që kontrollojnë bllokimet e trafikut, krimin, ndotjen dhe makinat e lidhura)

dhe veshjet (p.sh. shikon zgjuar dhe wristbands për workouts, monitorimin e lëvizshmërisë, shëndetin e njerëzve kushtet, shëndetin e largët dhe administrimin e ilaçeve).

Objektet e reja të IO do të kontribuojnë me pasurinë e paimagjinueshme në jetën tonë që do të ndikojë në mënyrën se si ndërveprojmë sociale, mjekësore dhe teknologjike. Ndërsa lëvizim në një botë me lidhshmëri më të madhe dhe rrjetëzim të aktivizuara përmes Internetit të Gjërat (IoT), po lëvizim edhe në një epokë të mbledhjes së të dhënave më të mëdha

të lidhura me jetën tonë individuale, lëvizjet, ndërveprimet me botën, të tjerët dhe objektet shqisore, dhe të dhënat e lidhura me sjelljen përmes pajisjeve dhe objekteve të mbikqyrjes. Prandaj, fuqia e informatikës inteligjente e kombinuar me karakteristika të reja teknologjike të rrjetëzimit dhe infrastruktura teknologjike të përmirësuara për të shpërndarjen dhe përpunimin e të dhënave mbajnë premtime të mëdha për të përshtatur, përqëndruar dhe përshtatur ofrimin e shërbimeve për përditshmërinë tone jetesës, mirëqenies, nevojave sociale dhe mjekësore.

Përdoruesit e IoT vlerësojnë privatësinë e të dhënave

Edhe pse përhapja dhe përdorimi i mjeteve dhe teknologjive të medias sociale japin përshtypjen e një bota e privuar nga privatësia, shumica e të intervistuarve tanë (si përdoruesit dhe dizajnerët) mendonin se ata i vlerësonin ato informacion personal dhe donte ta mbante nën kontrollin e tyre. Diskutimet fillestare u përqëndruan në kuptimi i privatësisë dhe dëshmive tregoi qartësi në kuptimin e "privatësisë" si shqetësim për kufizimin ekspozimi i informacionit personal që konsiderohet i ndjeshëm. Shumica e pjesëmarrësve mendonin se kishte një kufi të qartë

duke përshkruar atë që të tjerët duhet të dinë për veten, siç përmblidhet nga një nga komentet e pjesëmarrësit: Privatësia do të thotë se ka gjëra që unë nuk dua që njerëzit të dinë për mua, dhe ka gjëra që unë jam të lumtur që njerëzit të dinë për mua dhe më pëlqen të mendoj se unë i projektoj gjërat që dëshiroj njerëzit di, dhe pastaj mos projekto gjërat që unë nuk dua që njerëzit të dinë (U1)Privacy ka të bëjë me mbajtjen e ... çfarë doni të mbani fshehur ose sekret ... konfidencialitetin. Pra, për mua, privatësia është konfidencialiteti '(U2)

Njerëzit që nuk dinë gjëra për mua se unë nuk dua të zbuloj. Kështu që mund të jetë shëndeti, mund të jetë feja, mund të jetë pozicioni i punës, mund të jenë marrëdhënie të caktuara që kam. Kështu për shembull, në punë, jeta ime e punës dhe jeta ime private janë të ndara dhe më pëlqen kjo. Dhe, do të doja të pohoja se (U7)

Për këtë arsye, përdoruesit e IP-së kishin një kuptim të qartë të privatësisë.

IoT bazohet në numrin e madh të sensorëve pa tela që përfshijnë aksesueshmërinë, disponueshmërinë, saktësinë dhe problemet e konfidencialitetit. Kështu, problemet e sigurisë fillojnë nga faza e mbledhjes së të dhënave dhe vazhdojnë gjatë të dhënave të grumbulluara. Shumica e njerëzve nuk i lexojnë politikat e privatësisë për çdo pajisje që blejnë ose çdo aplikacion që shkarkojnë, dhe, edhe nëse ata u përpoqën ta bënin këtë, shumica do të shkruheshin në gjuhë juridike të pakuptueshme për konsumatorin mesatar. Këto pajisje të njëjta gjithashtu zakonisht vijnë me kushte të pakuptueshme të përdorimit, të cilat përfshijnë klauzola arbitrare të detyrueshme që i detyrojnë ata të heqin dorë nga e drejta e tyre për t'u dëgjuar në gjykatë nëse dëmtohen nga produkti.

Konsumatorët duhet të kërkojnë të dinë se cilat të dhëna mblidhen dhe si përdoret. Industritë duhet të zhvillojnë praktikat më të mira të privatësisë që përputhen me pritjet e klientëve të tyre. Komisioni Federal i Tregtisë duhet të sjellë veprime të zbatimit për praktikat mashtruese ndaj kompanive që nuk i përmbahen politikave të tyre të privatësisë, duke i mbajtur ata përgjegjës ndaj klientëve të tyre. Duhet gjithashtu të shqyrtojë mundësinë e ndalimit të klauzolave të arbitrazhit të detyrueshëm para mosmarrëveshjes, në mënyrë që konsumatorët të kenë shkak të veprimit kur shkelen privatësia e tyre.

Por, para se kjo të ndodhë, konsumatorët duhet të kërkojnë të dinë se cilat të dhëna mblidhen nga pajisjet e tyre në IoT.

5.2.1 IoT Reference Model

Modeli i Referencës përbëhet nga disa nën-modele, të cilat përcaktojnë hapësirën për hapësirën e dizajnit Ikt. Dhe që adresojnë pikëpamjet arkitekturore. Siç u tha më lart, modeli primar dhe kështu kyç është Modeli Domain i IOs, i cili përshkruan të gjitha konceptet që janë relevante në Internetin e Gjërat. Të gjitha modelet e tjera dhe Arkitektura e Referencës IoT janë të bazuara në konceptet e futura në Modelet e IOt-së të Domainit. Ndërsa modele të caktuara, të tilla si Modeli i Komunikimit të IoT dhe Besimi i Trashëgimisë, Siguria dhe Modeli i Privatësisë mund të jenë më pak kritike në disa skenarë të aplikimit, Modeli i IOE i Domosdoshëm është i detyrueshëm për të gjitha përdorimet e ARM-së së Xeotit. Në varësi të aplikimit individual të Modeli Domain i IO, pjesët e mëvonshme në këtë kapitull japin detaje rreth modeleve të tjera.

Tjetra, ne shpjegojmë, cilët nën-modele në Modelin e Referencës së IO-së lidhen dhe lidhen me njëri-tjetrin, dhe si ato formojnë një model referimi të integruar.

Modeli i Referencës së IO-së synon të krijojë një bazë të përbashkët dhe një gjuhë të përbashkët për arkitekturat e IO-së dhe sistemet IoT. Ai përbëhet nga nën-modele të paraqitura në Fig, të cilat i shpjegojmë më poshtë. Shigjetat e verdha tregojnë se si konceptet dhe aspektet e një modeli përdoren si bazë për një tjetër.

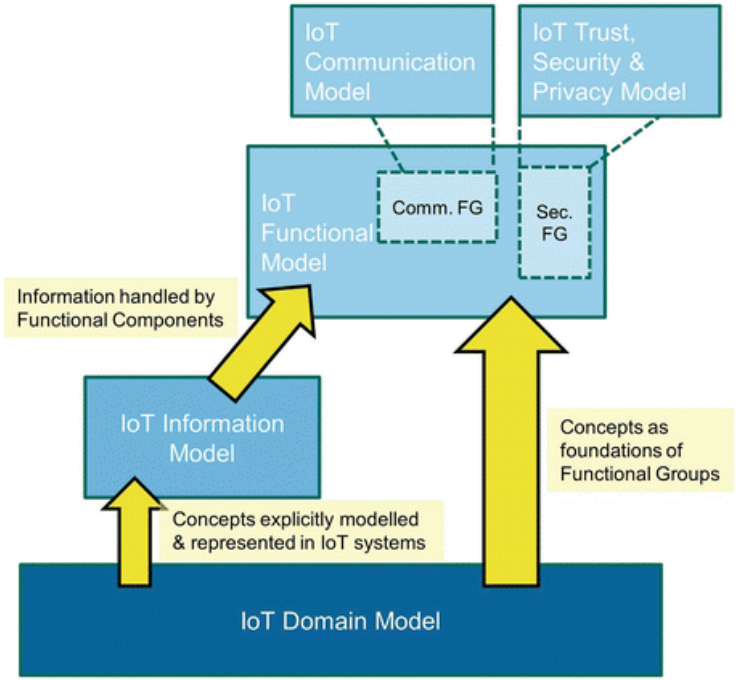

Figura 5:Interaction of all sub-models in the IoT Reference Model

Themelimi i Modelit të Referencës së IOE-së është Modeli Domain i IO, i cili prezanton konceptet kryesore të Internetit të Gjësendeve si Pajisjet, Shërbimet IoT dhe Entitetet Virtuale (VE), dhe gjithashtu prezanton marrëdhëniet midis këtyre koncepteve. Niveli i abstragimit të Modelit të IOt-së të Domainit është zgjedhur në mënyrë të tillë që konceptet e tij të jenë të pavarura nga teknologjitë specifike dhe përdorimi i rasteve. Ideja është që këto koncepte nuk pritet të ndryshojnë shumë gjatë dekadave të ardhshme ose më gjatë.

Bazuar në Modelin e Domainit të IO-së, është zhvilluar Modeli Informativ i XoT. Ai përcakton strukturën (p.sh. marrëdhëniet, atributet) e informacionit lidhur me IOs në një sistem IoT në një nivel konceptual pa diskutuar se si do të përfaqësohej. Informacioni që ka të bëjë me ato koncepte të Modeli të Domainit të IO-së është modeluar, i cili është grumbulluar, ruajtur dhe përpunuar në mënyrë eksplicite në një sistem IoT, p.sh. informacion mbi pajisjet, shërbimet IoT dhe entitetet virtuale.

Modeli Funktikor IOt identifikon grupet e funksionaliteteve, nga të cilat shumica janë të bazuara në konceptet kyçe të Modeli Domain i IO. Një numër i këtyre Grupeve të Funksionimit (FG) ndërtohen mbi njëri-tjetrin, duke ndjekur marrëdhëniet e identifikuara në Modulin Domain IO. Grupet e Funksionalitetit ofrojnë funksionalitete për bashkëveprimin me rastet e këtyre koncepteve ose menaxhimin e informacionit që lidhet me konceptet, p.sh. informacion rreth entiteteve virtuale ose përshkrimet e Shërbimeve të IO-së. Funksionalitetet e FGs që menaxhojnë informacionin përdorin Modelin e Informacionit të IO-së si bazë për strukturimin e informacionit të tyre.

Një funksionalitet kyç në çdo sistem kompjuterik të shpërndarë është komunikimi ndërmjet komponentëve të ndryshëm. Një nga karakteristikat e sistemeve të internetit është shpesh heterogjeniteti i teknologjive të komunikimit të përdorura, të cilat shpesh janë reflektim i drejtpërdrejtë i nevojave komplekse që sistemet e tilla duhet të përmbushin. Modeli i Komunikimit të IoT paraqet koncepte për trajtimin e kompleksitetit të komunikimit në mjedise heterogjene të IOt. Komunikimi gjithashtu përbën një FG në Modelin Funksional të IOt.

Së fundi, Besimi, Siguria dhe Privatësia (TSP) janë të rëndësishme në skenarët tipik të përdorimit të IP-së. Prandaj, funksionalitetet përkatëse dhe ndërvarësitë dhe bashkëveprimet e tyre futen në Modulin e IOs TSP. Ashtu si në rastin e komunikimit, siguria përbën një FG në Modelin Funksional.

6 KONKLUZION

Ky dokument paraqet një analizë të detajuar të sfidave të sigurisë, kërcënimet e privatësisë dhe sfidat e përgjithshme në internetin e gjërave. Ne fillim treguam se qfarë është IoT, përfshirja në sigurine e paisjeve që ne përdorim qdo ditë, si dhe mënyra e e volucionit të saj. Kontrolli qasjes si shërbim është shumë i rëndësishëm të implementohet me gjitha hapat dhe të monitorohet në vazhdimsi, në mënyr që të mos shfaqen probleme në sigurinë e të dhënave tona konfidenciale.

Qëllimi i kontrollit të qasjes është të minimizojë rrezikun e qasjes së paautorizuar në sistemet fizike dhe logjike, pra eshte nje process kontrollimi i qasjes i integruar në mjedisin IT të një organizatë. Kontrolli i qasjes fizike është një çështje e kujt, ku, dhe kur. Një sistem kontrolli i qasjes përcakton se kush lejohet të hyjë ose të dalë, (IoT) shpesh varet nga një situatë - për shembull, "përdoruesi është në shtëpi" - që mund të gjurmohet vetëm duke përdorur pajisje të shumta.

Për shkak se paisjet e IoT janë të lidhura me internet, ato janë të prekshme ndaj sulmëve kibernetike që edhe munden të dëmtojnë sistemin kompjuterikë të konsumatorit , apo ndonje shfrytezuesi të caktuar që mundemi të kemi.

Paisjet e IoT funksionojnë në atë mënyrë që krijojnë një vector të perbashkët sulmesh për hakerat për të përfituar qasje në rrjete të tërë.

Mbrojtja e intimitetit të konsumatorit bëhet gjithnjë e më e vështirë pasi që IoT-ja bëhet më e përhapur. Sa më shumë pajisje janë të lidhura me lloje të ndryshme të pajisjeve dhe aq me shume kjo rritje në lidhjen dhe rezultatet e mbledhjes së të dhënave kontrollohen më pak. Në rastin e kompjuterëve dhe telefonave te mencur, ky hakim mund të bëhet larg dhe shpesh i pazbuluar. Telefonat e mencur, ashtu si kompjutera, mbajnë një sasi të madhe të informacionit personal në lidhje me pronarët e tyre. Ata shpesh lidhen me llogaritë bankare, llogaritë e-mail, dhe në disa raste pajisje shtëpiake. Të dhënat e vjedhura mund të rezultojnë me probleme serioze. Automjetet përmbajnë shumë kompjuterë që kontrollojnë funksionin e tyre. Fillimisht,

këta kompjuterë nuk mund të hakoheshin. Me rritjen e lidhjes së IoTs, megjithatë, automjetet tani janë në rrezik për shkak të lidhjes me internetin.

Në një kuptim tjetër, kontrolli mund të humbet pasi gjithnjë e më shumë kompani mbledhin të dhëna për përdoruesit.

Rreziku më i zakonshëm i sigurisë për ndërhyrje nëpërmjet një sistemi të kontrollit të qasjes është thjesht duke ndjekur një përdorues të ligjshëm nëpërmjet një derë, dhe kjo quhet si backgating. Shpesh përdoruesi legjitim do të mbajë derën për ndërhyrës. Ky rrezik mund të minimizohet përmes trajnimit të ndërgjegjësimit të sigurisë të popullatës së përdoruesit, ose me mjete më aktive siç janë turnstiles.

Ekzistojnë tre lloje (faktorë) të informimit të vërtetimit:

• diçka që përdoruesi e di, p.sh. një fjalëkalim, frazë ose PIN

• diçka që përdoruesi ka, të tilla si karta inteligjente ose një çelës kyç

• diçka që përdoruesi është, të tilla si gjurmët e gishtave, të verifikuara me matje biometrike

Fjalëkalimet janë një mjet i zakonshëm për të verifikuar identitetin e një përdoruesi përpara se qasja t'u jepet sistemeve të informacionit.

Sistemet e Kontrollit të Qasjes si biometric access control system dhe finger print access janë disa metoda që mundemi të perdorim ne sot.

Çështja e sigurisë së internetit IoT është një punë shumë e madhe, dhe shumë inxhinierë e njohin nevojën për të adresuar çështjet e sigurisë. Partneriteti midis dy kompanive është një përpjekje për ta bërë më të lehtë për projektuesit e internetit të internetit të futin sigurinë në pajisjet dhe rrjetet e tyre IoT, si dhe për të rritur monetizimin e zgjidhjeve IoT.

7 DISKUTIME DHE PËRFUNDIME

Në këtë dokument kam treguar për origjinat e IoT dhe se si kjo ka paraqitur një sfidë të madhe për standardizimin dhe një vizion të vetëm të përgjithshëm. Nga ana tjetër, ka shkaktuar sfida për sigurinë dhe privatesin në IoT. Vështirësitë paraqiten në arritjen e konsensusit dhe besimit ndërmjet palëve që kanë vizion dhe interes të ndryshëm.

Ndërkohë që kërcënimet gjithmonë do të ekzistojnë me IOT si ato me përpjekjet e tjera të teknologjisë, është e mundur të rritet siguria e mjediseve të internetit IoT duke përdorur mjete sigurie të tilla si encryption të të dhënave, autentikim të fortë të përdoruesve, kodim elastik dhe API të standardizuara dhe të testuara që reagojnë në një parashikueshmëri mënyrë.

Në fakt, mungesa e mjeteve të sigurisë në pajisjet vetë ose mungesa e azhurnimeve në kohë të sigurisë në pajisjet është ajo që mund të bëjë sigurimin e IOT disi më të vështirë nga llojet e tjera të iniciativave të sigurisë, Marchany thotë. "Siguria fizike ndoshta është më shumë një çështje, pasi këto pajisje zakonisht janë jashtë në vende të hapura ose në vende të largëta dhe çdokush mund të ketë qasje fizike në të," thotë Marchany. "Pasi dikush të ketë qasje fizike në pajisje, shqetësimet e sigurisë rriten në mënyrë dramatike".

Siguria duhet të ndërtohet si bazë e sistemeve IoT, me kontrolle rigoroze të vlefshmërisë, vërtetimit, verifikimit të të dhënave dhe të gjitha të dhënat duhet të kodohen. Në nivelin e aplikimit, organizatat e zhvillimit të softuerit duhet të jenë më të mirë në kodin e shkrimit që është i qëndrueshëm, elastik dhe i besueshëm, me standarde më të mira për zhvillimin e kodeve, trajnime, analiza kërcënimi dhe testim. Ndërsa sistemet ndërveprojnë me njëri-tjetrin, është thelbësore që të ketë një standard interoperabiliteti të dakorduar, i cili është i sigurt dhe i vlefshëm. Pa një strukturë të ngushtë fundore, ne do të krijojmë më shumë kërcënime me çdo pajisje të shtuar në IOT. Pajisjet e lidhura mund të bëhen një pikë hyrjeje në rrjetin tuaj në shtëpi nëse ata janë të hackuar,prandaj duhet vendosur një fjalëkalim të mire.

Pasi hakerët të kenë qasje në rrjet, ata mund të kenë mundësi të hyjnë në pajisje të rëndësishme siç janë laptopët që mbajnë informacione financiare.

Për të përmirësuar sigurinë, sigurohuni që të vendosni një fjalëkalim që nuk mund të plasaritet lehtë nga hakerët - edhe për pajisjet në dukje të ulëta të rrezikut, si kukulla dhe robotët e lodrave. Dhe mos vazhdoni të përdorni një fjalëkalim të parazgjedhur që erdhi me një pajisje.

Është gjithashtu jashtëzakonisht e rëndësishme për përdoruesit e internetit të internetit për të siguruar routerët e tyre, duke vendosur fjalëkalime të forta dhe duke u siguruar që azhurnimet e sigurisë të instalohen menjëherë.

Sistemet e kontrollit të qasjes janë sistemet elektronike që janë të dizajnuara për të kontrolluar nëpërmjet një rrjeti dhe ata duhet të kenë qasje në një rrjet. Sistemi i Kontrollit të Qasjes njeh autentifikon dhe autorizon hyrjen e një personi për të hyrë në objekt duke dhënë mbrojtje të plotë duke siguruar siguri me sistemin.

Shembull i një sistemi të kontrollit të qasjes: Një derë mund të jetë e hapur me një kartë , një sistem RFID ose me teknologjinë e sistemit bio metrik.

Sistemi i kontrollit të qasjes siguron siguri duke i dhënë kontroll fleksibël se kush lejohet të hyjë në lokalet tuaja.

Sistemi i kontrollit të hyrjes është një nga sistemet më të zakonshme të përdorura në kontrollin elektronik të derës duke përdorur një kartë ose një shirit magnetik që mund të arrihet duke rrokullisur përmes një lexuesi në derë. Këto sisteme të kontrollit të qasjes përdoren për qëllime sigurie.

Me anë të këtyre sistemeve të kontrollit të qasjes në kartë mundësohet hyrja në hapësirat kufizuese të njerëzve në njërën anë të derës. Në disa raste, sistemet e kontrollit të qasjes fizike janë të integruara me ato elektronike duke kufizuar përdoruesit duke i lejuar ata të shfrytëzojnë burimet e kufizuara në një sistem kompjuterik.

Bio Metric Access Control System përdor gjurmën e gishtit në vend të sistemit të kartelave për qasje. Sistemi i Kontrollit të Qasjes jo vetëm që lejon hyrjen, por edhe jep të dhëna në lidhje me hyrjen e personave. Programi i Pjesëmarrjes mund të integrohet me ndonjë softuer ekzistues të listës së pagave dhe jep regjistrim automatik të informacionit të gjeneruar nga Sistemi i Pjesëmarrjes dhe kjo kursen kohë dhe burime në regjistrim. Kjo rrit produktivitetin dhe rentabilitetin për çdo organizatë.

Sistemi i kontrollit të qasjes së afërsisë është sistemi më i besueshëm për kontrollin e qasjes. Ajo siguron një mjedis të sigurisë dhe përdoret gjerësisht në zyra, fabrika, bankë etj.

8 REFERENCAT

[1] https://www.getkisi.com/resources/types-of-access-control Common Types of Access Control, Autor: Kisi Security Platform.

[2] https://www.getkisi.com/guides/internet-of-things-iot Internet of Things - How it Works in Access Control, Autor: Internet Engineering Task Force (IETF).

[3]http://www.digitalistmag.com/executive-research/live-business-the-importance-of-the-internet-of-things The Importance of the Internet of Things, Autor: Strategic CIO, Technology Trends.

[4]http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security IoT security (internet of things security), Autor: This content is part of the Essential Guide:Managing information security amid new threats: A guide for CIOs.

[5] https://blog.zooma.se/what-is-internet-of-things-and-why-is-it-important What is Internet of Things and why is it important? Written by Ingrid Wallgren (Apr 28, 2016)

[6] https://epic.org/privacy/internet/iot Internet of Things (IoT), Autor: Electronic Privacy Information Center

[7] https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf Internet of things Privacy & Security in a Connected World, Autor: FTC Sta Report JANUARY 2015

[8] Bruce Sinclair, IOT Inc:How your Company can Use the Internet of Things to Win the Outcome me Economy, 1 edition , McGraw-Hill Education; (May 29,2017)

[9]Maciej Kranz , “Building the Internet of Things” , 1 edition, Wiley; (November 21, 2016)

[10] http://www.tandfonline.com/doi/full/10.1080/23738871.2017.1366536 Security and privacy in the internet of things, Autor: Maple, Carsten

[11]https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html The future of IoT: 10 predictions about the Internet of Things, Autor: By Steve Symanovich, a Symantec employee

[12]https://www.internetsociety.org/blog/2017/06/there-is-no-perimeter-in-iot-security/?gclid=EAIaIQobChMIu9uR6oC_1wIVGl4ZCh1x8QDEEAAYAyAAEgJFgPD_BwE There is No Perimeter in IoT Security, Autor: By Andrei RobachevskySenior Technology Programme Manager

REFERENCIMI I FIGURAVE

Michael Alba posted on July 31, 2017
https://www.google.com/imgres?imgurl=https%3A%2F%2Fres.cloudinary.com%2Fengineering-com%2Fimage%2Fupload%2Fw_640%2Ch_640%2Cc_limit%2Cq_auto%2Cf_auto%2Fimage001_uwzozc.jpg&imgrefurl=https%3A%2F%2Fwww.engineering.com%2FIOT%2FArticleID%2F15354%2FEnd-to-End-IoT-Security.aspx&docid=_qPqA0WWiB3YKM&tbnid=TkKNPPL-6jDasM%3A&vet=10ahUKEwiIpMLFzZjhAhUSY1AKHYNjC84QMwhBKAUwBQ..i&w=640&h=282&bih=625&biw=1366&q=end%20to%20end%20security&ved=0ahUKEwiIpMLFzZjhAhUSY1AKHYNjC84QMwhBKAUwBQ&iact=mrc&uact=8 date accessed 26/12/18

DANNY THAKKAR POSTED ON 2013
https://www.google.com/search?biw=1366&bih=625&tbm=isch&sa=1&ei=LlWWXKfTDMnNwQL9hrXIDA&q=biometrik+access&oq=biometrik+access&gs_l=img.3...25984.33181..33402...0.0..1.146.1809.11j7....2..2....1..gwswizimg.....0..0i67j0i131j0j0i5i30j0i8i30j0i24j0i10i24.UuVaeFhizLE#imgdii=tmdetA5hvAtbuM:&imgrc=NrYrwh5HlnqUSM: date accessed 26/12/18

Clare Hopping, IT Pro 20 Feb, 2018
https://www.google.com/search?biw=1366&bih=625&tbm=isch&sa=1&ei=UVWWXIWwI7XpxgPqoqiYBQ&q=internet+of+things&oq=internet+of+things&gs_l=img.3..0l10.1943.4615..4777...0.0..0.210.1968.8j9j1....2..1....1..gws-wiz-img.....0i67j0i131.uNsApyc_udQ date accessed 26/12/18

Springer, Berlin, Heidelberg 06 September 2013
https://www.google.com/search?hl=en&biw=1366&bih=625&tbm=isch&sa=1&ei=AbN5XJajBpDGwQKw57CACA&q=iot+domain+model&oq=iot+domain+model&gs_l=img.3..0j0i8i30j0i24l2.2259.5444..5857...0.0..0.191.2152.0j16....2..1....1..gwswizimg.....0i131j0i67j0i5i30j0i30.G2fZeeTmS7g#imgrc=Hs6MQtgKDnlF_M date accessed 26/12/18