KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

Gediminas Petkus

DAIKTŲ INTERNETO OBJEKTŲ IDENTIFIKAVIMO METODŲ PROGRAMINIAME LYGMENYJE TYRIMAS

Baigiamasis magistro darbas

Vadovas
Doc. dr. Jevgenijus Toldinas

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

DAIKTŲ INTERNETO OBJEKTŲ IDENTIFIKAVIMO METODŲ PROGRAMINIAME LYGMENYJE TYRIMAS

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) Doc. dr. Jevgenijus Toldinas
(data)

Recenzentas
(parašas) dr. Dangis Rimkus
(data)

Projektą atliko
(parašas) Gediminas Petkus
(data)

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos fakultetas

(Fakultetas)

Gediminas Petkus

(Studento vardas, pavardė)

M4096N21 Informacijos ir informacinių technologijų sauga

(Studijų programos pavadinimas, kodas)

„Daiktų interneto objektų identifikavimo metodų programiniame lygmenyje tyrimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 17 m. 05 22 d.

Kaunas

Patvirtinu, kad mano **Gedimino Petkaus** baigiamasis projektas tema „Daiktų interneto objektų identifikavimo metodų programiniame lygmenyje tyrimas“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

Gediminas Petkus

(vardą ir pavardę įrašyti ranka) *(parašas)*

Petkus, G. „Daiktų interneto objektų identifikavimo metodų programiniame lygmenyje tyrimas“. Magistro baigiamasis projektas / vadovas doc. dr. Jevgenijus Toldinas; Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterinių sistemų inžinerijos katedra.

Kaunas, 2017. 63 p.

SANTRAUKA

Daiktų interneto tematika yra plačiai aprėpiama šiandieniniame pasaulyje. Dauguma žmonių negali įsivaizduoti savo gyvenimo be kokio nors daiktų interneto objekto – ar tai būtų vaikų stebėjimo sistema, įvairios vaizdo kameros, fiksuojančios judėjimą, jutikliai ir sensoriai, pranešantys informaciją apie žmogų arba aplinkoje, kurioje jis yra įvykstančius reiškinius. Iš pirmo požiūrio visa tai skamba ganėtinai gražiai. Daiktų internetas palengvina ar neretais atvejais automatizuoja mūsų kasdienius veiksmus.

Naivu būtų tikėtis, kad ši technologija neša vien teigiamą dalį pasaulyje. Sistemos, kurios palengvina žmonių gyvenimą neretai tampa įrankiu įsilaužėliu rankose, skirtu pakenkti vartotojui. Neretais atvejais pasitaiko situacijų, kuomet įsilaužėliai pasinaudodami savo gebėjimais sugeba sutrikdyti sistemos darbą, pateikti fiktyvią informaciją į serverius, į kuriuos siunčia duomenis koks nors jutiklis arba sensorius pvz., rodmenis apie temperatūra patalpoje. Iš pažiūros paprastam vartotojui tai gali atrodyti kaip neturintis įtakos darbui veiksmas, tačiau vartotojas net nesusimasto apie tai, kad tarkim didžiulis temperatūros duomenų užkėlimas arba sumažinimas gali sutrikdyti sistemos darbą ryšium su tuo, kad būtų siunčiama komanda iš serverio pusės i vedinimo sistemą ir staigus temperatūros šuolis, arba šuolių seka gali visiškai suparalyžiuoti serverio darbą.

Detalizuojant pagrindinę daiktų interneto problemą galima teigti, jog keletas esminiu jų būtų tai, kad objektų turima daug. Objektai turi savo paskirtį, kuria jie buvo sukruti atlikti. Tačiau svarbu yra tai, kad esant tokiai objektų gausai tampa labai sudėtinga juos identifikuoti kaip objektus t.y., kaip užtikrinti faktą, kad duomenys į serverį, kurie yra siunčiami apie paciento širdies darbą atkeliauja iš prie paciento prijungto jutiklio, o ne siunčiami fiktyvus iš įsilaužėlio. Galima įsivaizduoti scenarijų, kuomet siunčiami klaidingi duomenys įsilaužėlio dėka, todėl medicinos personalas gavęs tokius duomenis turėtų imtis atitinkamų veiksmų žmogui padėti, nors ši pagalba jam būtų nereikalinga. Todėl suteikus jam nereikalingą pagalba, būtų iškeliama rizika asmens sveikatai ar net gyvybei.

Tinkamas objektų identifikavimas ir autentifikavimas yra viena iš esminių daiktų interneto tematikos problemų. Tai yra problema, kuria būtina spręsti ryšium su nuolatos daugėjančių objektų kiekių ir jų paklausa iš vartotojų pusės. Suteikiant galimybę tinkamai identifikuoti ir autentifikuoti objektus yra suteikiama galimybė vartotojams savo terpėje užtikrinti, kad objektas, kuris atlieka kasdienius veiksmus pvz., siunčia informacija apie vaiką, kuris miega namuose, kol šeimos narys yra kur nors išėjės ir būti ramiam, kad perduodama informacija yra identifikuota ir autentifikuota t.y., vartotojas yra užtikrintas, kad pvz., transliuojamas vaizdas iš kameros yra būtent tos kameros, o ne klaidinantis įrašas pateiktas įsilaužėlio.

Rašomo magistrinio darbo pagrindinis objektas - Daiktų interneto objektų identifikavimo metodų programiniame lygmenyje tyrimas.

Darbo struktūra:

- Pirmoji darbo dalis aprėpia daiktų interneto objektų identifikavimo metodų programiniame lygmenyje analizę. Nagrinėjami objektų identifikavimo metodai,

kylančios saugos grėsmės bei saugos būdai bei priemonės. Taipogi apžvelgiami ir objektų komunikavimo protokolai, jų saugumo bei pažeidžiamumo faktoriai.

- Antroje darbo dalyje pateiktas koncepcinis daiktų ir paslaugų interneto objektų identifikavimo programiniame lygmenyje metodų tyrimo sistemos modelis. Aprėpiama pateiktos sistemos architektūra, kliento bei serverio pusės komunikacijos schema, tarpinių programų komunikavimo principai, duomenų apsikeitimo mechanizmas, sistemos veikimo principas. Sistemoje vykstantys procesai yra iliustruoti pateikiant grafikus.
- Trečioje darbo dalyje pateikti eksperimento tyrimo rezultatai. Eksperimento metu ištirtas daiktų interneto objektų identifikavimo programiniame lygmenyje metodas. Tyrimo metu išnagrinėta siunčiamų duomenų įtaka laiko sąnaudų prasme taikant minėtą metodą lyginant su atvirų duomenų persiuntimu neatliekant objektų identifikavimo ir autentifikavimo.
- Pabaigoje yra pateikiamos darbo išvados.

Petkus, G. *Research On Methods Of Application Level Iot Objects Identification*: *Master's* thesis supervisor assoc. prof. Jevgenijus Toldinas. The Faculty of Informatics, Kaunas University of Technology.

Research area and field: Internet of Things

Key words: Internet of Things object identification

Kaunas, 2017. 63 p.

SUMMARY

Problems that are faced on the field of internet of things are widely known worldwide. Many people nowadays can't even imagine a life without some sort of a device developed in a field of internet of things. Should it be a video camera that focuses on movement, various sensors and measurement devices that inform about user activity on the field or various nature happening events such as weather changes.

At first glance it all sounds quite charming. Internet of things encourages to ease off a user's life in the world by automating various actions that a user produces on a daily basis. It would be quite naïve to think that technologies nowadays produce only a negative effect on the life quality we as users have. Quite frankly it also becomes a widely used tool for various forensic hackers to forge a system and do what is intended in the first place. There is quite a variety of situations when forensic cybercriminals by using their abilities enable themselves to disable various systems up work. By giving a server fake information from the controlling units for example some kind of a measurement unit corresponds data of current temperature in the room. If fake data would be transmitted for example high and then low periods of temperature increase and decrease the ventilation system would power on producing cold and hot airflow periods that would distract servers workflow and the server would collapse.

In deepening the main cause of failure in the field of internet of things it would be wise to point out that a few of the main reasons why the field is vulnerable is that we have huge number of devices that have its purpose that they were developed in the first place to do. Having a huge scope of internet of things devices that surround us it becomes very difficult to identify and authenticate them thus how to verify the fact that the data that is being transferred at the moment to the server from where they are sent from a measurement device that is hocked up to a patient that monitors a patient's heart beats is valid and not being transmitted by a forensic cybercriminal. It is quite possible to image a scenario like this whether the data that is sent is not valid the personal of this medical institution would have to provide medical assistance to a patient who does not need assistance at all because the data that was given by the server to the medical personal is forged but the medical personal does not know that and by providing unnecessary assistance the medical personal would cause damage to the patient's body or even cause early death.

Thus having the ability to properly identify and authenticate devices in the field of internet of things thematic of solving these kinds of problems. It is a problem that has to be dealt with in addition to increasing number of devices and their growing need based on the users perspective in the world we live today.

Providing the ability to correctly identify and authenticate devices is a crucial part for a user to obtain because the devices that produce various task on a daily basis it's a must to confirm that the data that is transferred between the controller and the server is valid and not forged. Let's say that a user has a baby monitor with a video camera included in it. The device transfers data to a user about a toddler that is sleeping at home while the user is out of home and to be calm that the information that he sees from this device is valid thugs identified and authenticated thus providing positivity for a user that for example the video data that he sees is transmitted from a real camera that he has at home and not forged by a cybercriminal.

The main object of master thesis is - Research on Methods of Application Level Internet of Things Objects Identification

Structure of work

- First part of the work is based on Research on Methods of Application Level IoT Objects Identification Analysis. Various identification methods must be analyzed and the security issues they have vulnerability to and the tools that can be implied to avoid these vulnerabilities.
- Second part provides a conception model of Research on Methods of Application Level Internet of Things Objects Identification. It contains system architecture model, client server based communication schemes and the method of object identification and authentication itself by communication mechanisms based on middleware layer principles, data exchange mechanisms, system usability guidelines. The illustrations are visualized by using graphical pictures developed using unified modeling language.
- Third part provides the results of the investigation theme. By the investigation period there is a deep perception analysis of Research on Methods of Application Level Internet of Things Objects Identification model. Based on the investigation the information gathered provides the data influence on a timespan basis compared to using and not using the intended method of device identification and authentication.
- In the end work conclusions are provided

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

DoS – Paslaugų atsisakymo aptarnauti ataka (*angl. Denial of Service*)

WPA – Wi-fi prieigos apsaugos protokolas (*angl. Wi-Fi Protected Access*)

IPSec – Internetinio protokolo apsauga (*angl. Internet Protocol Security*)

WAP – Bevielis aplikacijų protokolas (*angl. Wireless Application Protocol*)

ROM – Tik skaitomojo tipo atmintis (*angl. Read-only Memory*)

Agentas – Autonominė programinės įrangos dalis, kuri vykdo vartotojo nurodytus veiksmus arba užprogramuotos situacijos sprendimus.

ĮVADAS

Daiktų interneto tematika yra plačiai aprėpiama šiandieniniame pasaulyje. Dauguma žmonių negali įsivaizduoti savo gyvenimo be kokio nors daiktų interneto objekto – ar tai būtų vaikų stebėjimo sistema, įvairios vaizdo kameros, fiksuojančios judėjimą, jutikliai ir sensoriai, pranešantys informaciją apie žmogų arba aplinkoje, kurioje jis yra įvykstančius reiškinius. Iš pirmo požiūrio visa tai skamba ganėtinai gražiai. Daiktų internetas palengvina ar neretais atvejais automatizuoja mūsų kasdienius veiksmus.

Naivu būtų tikėtis, kad ši technologija neša vien teigiamą naudą. Sistemos, kurios palengvina žmonių gyvenimą, neretai tampa įrankiu įsilaužėliu rankose, skirtu pakenkti vartotojui. Neretais atvejais pasitaiko situacijų, kada įsilaužėliai pasinaudodami savo gebėjimais sugeba sutrikdyti sistemos darbą, pateikti fiktyvią informaciją į serverius, į kuriuos siunčia duomenis koks nors jutiklis arba sensorius, pvz., rodmenis apie temperatūra patalpoje. Iš pažiūros paprastam vartotojui tai gali atrodyti kaip neturintis įtakos darbui veiksmas, tačiau vartotojas net nesusimąsto apie tai, kad, tarkim, stiprus temperatūros duomenų padidinimas arba sumažinimas gali sutrikdyti sistemos darbą , nes būtų siunčiama komanda iš serverio pusės įvėdinimo sistemą ir staigus temperatūros šuolis arba šuolių seka galėtų visiškai suparalyžiuoti serverio darbą.

Detalizuojant pagrindinę daiktų interneto problemą galima teigti, jog keletas esminių būtų tai, kad objektų turima daug. Objektai turi savo paskirtį, kuriai jie buvo sukurti atlikti. Tačiau svarbu yra tai, kad esant tokiai objektų gausai tampa labai sudėtinga juos identifikuoti kaip objektus, t. y., kaip užtikrinti faktą, kad duomenys į serverį, kurie yra siunčiami apie paciento širdies darbą, atkeliauja iš prie paciento prijungto jutiklio, o ne įsilaužėlio siunčiami fiktyvūs . Galima įsivaizduoti scenarijų, kada įsilaužėlio siunčiami klaidingi duomenys todėl gavęs tokius duomenis medicinos personalas turėtų imtis atitinkamų veiksmų žmogui padėti, nors ši pagalba jam būtų nereikalinga. Dėl šios priežasties suteikus jam nereikalingą pagalbą, būtų iškeliama rizika asmens sveikatai ar net gyvybei.

Rašomo magistro darbo pagrindinis objektas – daiktų interneto objektų identifikavimo metodų tyrimas programiniu lygmeniu.

Darbo problematika ir aktualumas

Tinkamas objektų identifikavimas ir autentifikavimas yra viena iš esminių daiktų interneto tematikos problemų. Tai yra problema, kurią būtina spręsti dėl nuolatos daugėjančių objektų kiekių ir jų paklausos iš vartotojų. Suteikiant galimybę tinkamai identifikuoti ir autentifikuoti objektus yra suteikiama galimybė vartotojams savo terpėje užtikrinti, kad objektas, kuris atlieka kasdienius veiksmus, pvz., siunčia informaciją apie vaiką, kuris miega namuose, kol šeimos narys yra kur nors išėjęs, leidžia būti ramiam, kad perduodama informacija yra identifikuota ir autentifikuota, t. y. vartotojas yra užtikrintas, kad, pvz., transliuojamas vaizdas iš kameros yra būtent tos kameros, o ne įsilaužėlio pateiktas klaidinantis įrašas.

Darbo tikslas ir uždaviniai

Sukurti daiktų interneto objektų identifikavimo programiniame lygmenyje metodą, kurio paskirtis būtų apimanti pagrindinę daiktų interneto saugos tematiką – objektų identifikavimas ir autentifikavimas.

Tikslui įgyvendinti keliami tikslūs uždaviniai:

- atlikti daiktų interneto objektų identifikavimo programiniame lygmenyje jau esančių metodų bei jų grėsmių analizę;
- suprojektuoti daiktų interneto objektų identifikavimo programiniame lygmenyje sistemos modelį bei identifikavimo bei autentifikavimo mechanizmą;
- pasiremiant sudarytu modeliu realizuoti sistemos prototipą;
- pagal sukurtą prototipą atlikti sistemos greitaveikos priklausomybės nuo siunčiamų duomenų eksperimentinį tyrimą;
- išnagrinėti eksperimentinio tyrimo rezultatus bei pateikti išvadas apie minėtą daiktų interneto objektų identifikavimo programiniame lygmenyje metodo panaudojimą.

Darbo rezultatai ir jų svarba

Pateiktų rezultatų esminiai tikslai yra pademonstruoti sukurto daiktų interneto objektų identifikavimo programiniame lygmenyje metodo veikimo principą bei sudaromas papildomas laiko sąnaudas atitinkamam duomenų kiekiui persiųsti taikant metodą lyginant su duomenų persiuntimu netaikant metodo. Svarbus akcentas yra tas, kad taikant saugos sprendimus yra svarbu užtikrinti kiek įmanoma mažesnes laiko sąnaudos dirbant su sistema. Darbo rezultatų svarba yra pademonstruoti įtaką sistemos darbui taikant metodą.

Darbo struktūra

- Pirmas skyrius aprėpia daiktų interneto objektų identifikavimo metodų programiniame lygmenyje analizę. Nagrinėjami objektų identifikavimo metodai, kylančios saugos grėsmės bei saugos būdai bei priemonės. Taipogi apžvelgiami ir objektų komunikavimo protokolai, jų saugumo bei pažeidžiamumo faktoriai.
- Antrame skyriuje pateiktas koncepcinis daiktų ir paslaugų interneto objektų identifikavimo programiniame lygmenyje metodų tyrimo sistemos modelis. Aprėpiama pateiktos sistemos architektūra, kliento bei serverio pusės komunikacijos schema, agentinių programų komunikavimo principai, duomenų apsikeitimo mechanizmas, sistemos veikimo principas. Sistemoje vykstantys procesai yra iliustruoti pateikiant grafikus.
- Trečiajame darbo skyriuje pateikti eksperimento tyrimo rezultatai. Eksperimento metu ištirtas daiktų interneto objektų identifikavimo programiniame lygmenyje metodas. Tyrimo metu išnagrinėta siunčiamų duomenų įtaka laiko sąnaudų prasme taikant minėtą metodą lyginant su atvirų duomenų persiuntimu neatliekant objektų identifikavimo ir autentifikavimo.

1. DAIKTŲ INTERNETO OBJEKTŲ IDENTIFIKAVIMO METODŲ PROGRAMINIAME LYGMENYJE ANALIZĖ

Kibernetiniai nusikaltėliai yra asmenys, kurie naudoja skaitmeninius objektus siekdami atlikti nusikaltimus kibernetinėje erdvėje. Šiuo metu kibernetinis nusikalstamumas yra taip išplitęs, jog kelia rimtą grėsmę informacijos saugumu. Įsilaužėlių pagrindiniai tikslai yra sukelti materialių nuostolių pasirinktam vartotojui.

Šių piktavalių dėka nukenčia nekalti žmonės, įvairios organizacijos patiria didžiulius finansinius nuostolius. Dauguma kibernetinių įsilaužimų yra paremti duomenų rinkimu, šnipinėjimu, informacijos kitiems asmenims nutekinimu.

Daiktų internetas yra suvokiamas kaip infrastruktūra, kuri teikia visuomenei pažangiausias paslaugas sujungiant įvairius daiktus (tiek fizinius tiek virtualiuosius). Daiktų internetas įgalina realius „daiktus“ panaudoti įvairiomis paslaugomis tuo pat metu užtikrina tai, kad būtų laikomasi tiek saugumo tiek privatumo standartų.

Toliau darbe bus gilinamasi į kibernetinio nusikalstamumo pėdsakų fiksavimo metodus ir jų prevenciją.

1.1. Daiktų interneto belaidžio ryšio protokolų analizė

Šiandieniniame pasaulyje daiktų interneto objektai daugumos vartotojų gyvenime atlieka didžiulę rolę. Patys objektai yra valdomi naudojant įvairius protokolus. Šiame skyriuje bus apžvelgiami darbe nagrinėjamas belaidžio interneto protokolas. Skyriuje bus išnagrinėjamas protokolo veikimo principas, panaudos atvejai ir apžvelgiami įvairūs protokolo saugumo faktoriai.

Pagrindinis aspektas naudojant belaidį interneto ryšį yra tai, kad turi būti užtikrintas saugus informacijos perdavimas [20]. Šiandien vyrauja daug belaidžio ryšio perdavimo saugumo mechanizmų ir visi jie turi tenkinti šias pagrindines funkcijas:

- autentiškumas – turi būti patikrintas tapatumas su stotimis, su kuria vyksta komunikacija;
- konfidencialumas – belaidžiu tinklu perduodama informacija privalo išlikti privati ir neprieinama piktavaliams.
- vientisumas – tinklu perduodami kadrai turi pasiekti tikslą nepažeisti.
- autentifikacija – mechanizmas įvyksta komunikuojant tarp kelių belaidžio ryšio stočių.

1.1.1. WEP protokolo saugos analizė

WEP (angl. *Wired Equivalent Privacy*) protokolas – tai toks protokolas, kuris buvo sukurtas, kad būtų suderinami konfidencialumo, prieigos kontrolės ir duomenų vientisumo kriterijai viename belaidžiame tinkle. Protokolo problema yra tokia, kad jis naudoja RC4 šifravimo algoritmą konfidencialumo sąlygai užtikrinti. RC4 yra srautinis šifras, kurio veikimo principas yra plėsti trumpą begalinį raktą į pseudoatsitiktinį srautinį raktą. Norint išvengti atvejo, kai atsiranda du atsitiktiniai teksto fragmentai su tuo pačiu srauto raktu, naudojamas inicializavimo vektorius (IV), kurio paskirtis yra sustiprinti slaptą raktą ir kiekvienam paketui sukurti skirtingus raktus. Vektorius susideda iš 24 bitų, jis suteikia 64 arba 128 bitų raktą.

Norint užtikrinti MAC kadrų vientisumą WEP panaudoja vientisumo kontrolinių sumų mechanizmą. Mechanizmas įgyvendina 32 bitų ciklinę pertekliaus kontrolę (CRC-32). CRC kontrolinė suma yra apskaičiuojama kiekvienam MAC kadrui atskirai, ši suma yra pridedama kiekvieno kadro pabaigoje. Svarbus akcentas yra toks, kad jeigu CRC, kuri buvo apskaičiuota iš šaltinio pusės ir išsiųsta

su pranešimu yra lygiai tokia pat, kaip gavėjo iš naujo apskaičiuota, toks pranešimas yra traktuojamas kaip galiojantis ir yra perduodamas kanalo lygiui. Tačiau jeigu nutinka taip, kad gauta kontrolinė suma yra skirtinga, tai yra traktuojama kaip vientisumo pažeidimo atvejis ir pranešimas yra pašalinamas.

WEP naudoja dviejų rūšių autentifikavimo metodiką – atvirąją arba bendrojo rakto. Tačiau atvirasis autentifikavimo metodas nėra traktuojamas kaip „autentiškumo procedūra“, nes prieigos taškas priima kiekvieną stotelę neturėdamas tapatybės patvirtinimo. Stotis pasikeičia su prieigos tašku dviem žinutėmis, iš kurių viena nurodo tapatybę, kita prašymą patvirtinti. Prieigos taškas duoda atsakymą patvirtindamas sėkmingą autentifikavimą. Įvykdžius atpažinimo ir susiejimo procedūras WEP gali būti naudojamas duomenims šifruoti, tada klientui reikia turėti atitinkamą, t. y. tik jam skirtą raktą. Bendrojo rakto autentifikavimo atveju norint prisijungti reikia turėti slaptą raktą. Minėtu atveju, autentiškumui įgyvendinti stotis pradeda keturių krypčių keitimąsi pranešimais procedūrą.

1 lentelė. Belaidžio tinklo WEP saugos protokolo parametrai [28]

WEP		
Autentifikavimas	Metodas	Atviras sistemos autentifikavimas Bendrojo rakto autentifikavimas
Rakto šaltinis ir valdymas	Raktas	Šifravimo raktas: 40 bitų bendrasis raktas 24 bitų IV. Pilnas raktas – 64 bitų. 104 bitų bendrasis raktas 24 bitų IV Pilnas raktas – 128 bitų
Konfidencialumas	Duomenų srauto šifravimas Šifro algoritmai srauto duomenims ir raktų dydžiui Užšifruoti kadrai	Nėra RC4 – 64 bitų raktas (WEP-40) RC4 – 128 bitų raktas (WEP-104 MPDU + ICV
Vientisumas	Vientisumo algoritmas Apsaugoti kadrai	32 bitų ICV kartu su CRC-32 MPDU

1.1.2. WPA protokolo saugos analizė

Ankstesniame skyriuje apžvelgėme, kad WEP neužtikrina saugumo. Pagrindiniai trūkumai: RC4 naudoja silpną rakto režimą, kriptografinis raktas ir inicializavimo vektorius yra per trumpi ir negali būti automatiškai ir dažnai atnaujinami, CRC-32 neužtikrina vientisumo ir yra neatsparūs atakoms. Remiantis šiomis priežastimis buvo sukurtas WPA (angl. *WiFi Protected Access*), kuris yra 802.11i standarto dalis.

Siekiant užtikrinti konfidencialumo ir vientisumo kriterijus WPA naudojasi laikinojo rakto vientisumo protokolu (TKIP), kuris saugiai keičia WEP raktą su kiekvienu duomenų paketu. Remiantis tokiu kodavimo būdu yra užtveriamas kelias slaptam pasiklausymui. Deja, lygiai taip pat kaip ir WEP protokolas, WPA protokolas ą užšifravimui ir iššifravimui naudoja RC4 šifrą. Tačiau siekiant užtikrinti didesnį saugumą TKIP padidina inicializavimo vektoriaus lauką iki 48 bitų rakto ilgio. TKIP naudoja sumaišytą raktą, sudarytą iš laikinojo rakto, siuntimo adreso ir sekos skaitiklio TSC. Tokiu atveju yra užtikrinama, kad kiekvienas duomenų paketas siunčiamas su savo unikaliu šifravimo raktu.

Autentifikavimui yra naudojamas 802.1X autentifikavimo protokolo mechanizmas arba iš anksto padalintų raktų metodas. Šis metodas yra skirtas belaidžio ryšio sesijų identifikavimo raktams kurti. Mechanizmas skirtas naudoti mažuose namų arba įmonių tinkluose, kuriuose kritiškas autentifikavimas nėra svarbus. Metodui gyvuoti yra būtini du komponentai – klientas ir autentifikatorius. Prieigos taškas naudodamas PSK yra atsakingas tik už kliento priėmimą į tinklą.

Ilgainiui CRC algoritmą skirtą duomenų vientisumui patikrinti pakeitė MIC algoritmas. CRC algoritmas, kuris buvo naudotas 802.11 protokole yra nesunkiai apeinamas. MIC algoritmas yra žymiai stipresnis. Duomenų teisėtumo procedūros tikrina duomenis nuo žalingų bei atsitiktinių duomenų perdavimo iškraipymų. 802.1X yra saugesnis nei PSK, tačiau būtina turėti RADIUS autentifikavimo serverį.

2 lentelė. Bevielio tinklo WPA saugos protokolo parametrai [28]

WPA		
Autentifikavimas	Metodas	802.1X autentifikacija Bendrojo rakto autentifikacija
Rakto šaltinis ir valdymas	Raktas	TKIP 48 bitų IV laukas naudojamas kaip MPDU TKIP sekos skaitiklis (TSC)
Konfidencialumas	Duomenų srauto šifravimas Šifro algoritmai srauto duomenims ir raktų dydžiui Užšifruoti kadrai	Nėra RC4 kartu su 256 bitų raktu MPDU + MIC + ICV
Vientisumas	Vientisumo algoritmas Apsaugoti kadrai	64 bitai MIC 32 bitai ICV [MIC]: (MSDU) [ICV]: MPDU

1.1.3. WPA2 protokolo saugos analizė

Konfidencialumo ir vientisumo užtikrinimo atveju WPA2 protokolas naudoja skaitiklio režimą su CBC-MAC protokolu. Šifravimui ir duomenų vientisumui CCMP naudoja AES 128 bitų rakto ilgio šifrą.

Vientisumui užtikrinti CCM-MAC operacijos išplečia pradinį MPDU dydį iki 8 – 16 baitų CMP antraštei ir 8 baitų MIC laukui. CCM reikalauja naujo laikinojo rakto kiekvienai sesijai ir unikalios reikšmės kiekvienam kadrui. Šiuo tikslu naudojamas 48 bitų paketas. CCM nenaudoja WEP kontrolinių sumų mechanizmo (ICV). CCM apsaugo papildomus autentiškumo duomenis, kurie sudaryti iš MPDU antraštės ir apima polaukius iš MAC kadro kontrolės, šaltinio adresus ir paskirties laukus, sekos kontrolę, QoS kontrolės lauką, todėl užtikrinama didesnė vientisumo apsauga.

Autentifikavimui naudojamas 802.1X autentifikavimo protokolo mechanizmas arba iš anksto padalintų raktų metodas PSK.

3 lentelė. Belaidžio tinklo WPA2 saugos protokolo parametrai [28]

WPA2		
Autentifikavimas	Metodas	802.1X autentifikavimas (RADIUS serveriu) Bendrojo rakto autentifikavimas
Rakto šaltinis ir valdymas	Raktas	PMK generuoja individualų laikiną raktą PTK, iš kurio gaunami trys raktai: 1-2) 128 bitų, 3) 256 arba 128 bitų.
Konfidencialumas	Duomenų srauto šifravimas Šifro algoritmai srauto duomenims ir raktų dydžiui Užšifruoti kadrai	Laikino rakto šifravimas: 1. RC4 su 128 bitų šifravimo raktu, 2) su AES 128 bitų šifravimo raktu. AES-CCM su 128 bitų laikinu raktu. MDPU +MIC
Vientisumas	Vientisumo algoritmas Apsaugoti kadrai	1) 64 bitai CCM MIC pranešimų srautui 2) A) HMAC-MD su pagrindiniu patvirtinimo raktu, B) HMAC-SHA1 su 128 bitų pagrindiniu patvirtinimo raktu pasisveikinimui. [MIC]: MPDU+ papildomas duomenų autentiškumo tikrinimas, kurį sudaro MPDU antraštė, polaukiai iš MAC kadrų kontrolės, šaltinio ir paskirties adresai, sekos kontrolė, QoS kontrolės laukas [HMAC]: 4 kartų pasisveikinimas

Jeigu yra naudojamas bendrasis raktas PSK, tai norint sukruti individualų pagrindinį raktą PMK, naudojamas slaptažodis. PMK generuoja individualų laikiną raktą PTK, iš kurio gaunami trys raktai:

1) 128 bitų raktas autentifikavimo procedūrai;
2) 128 bitų raktas šifravimui, kuris reikalingas srautinio rakto konfidencialumui per „pasisveikinimo“ (*angl. handshake*) principą su AES;
3) 256 bitai TKIP arba 128 bitai laikinajam raktui AES-CCMP. Naudojama WPA2 konfidencialumui;

Atlikus analizę belaidžio ryšio grėsmių terpėje peršasi išvada, jog pasyvių atakų tokių kaip slaptas pasiklausymas yra ganėtinai sudėtinga išvengti naudojant analizėje minėtus saugos protokolus. Tačiau, pasyvių atakų atžvilgiu jeigu rinktis saugiausia sprendimą tai jis būtų ties WPA2 protokolo sauga.

1.1.4. RFID protokolo saugos analizė

Savybės, kurias turėtų užtikrinti RFID kiekvieno saugumo atveju yra šios:

- privatumas
- vientisumas
- autentiškumas
- pasiekiamumas
- anonimiškumas
- ne susekamumas

Žvelgiant į tai, kad norint įgyvendinti visus paminėtus kriterijus prireiktų naudoti daugybė skirtingų kriptografinių metodų. RFID tai toks protokolas į kurį sudėtinga įdiegti kriptografinius metodus. [22] Tai yra dėl to, kad RFID savyje turi ganėtinai mažus resursus. Šiai problemai išspręsti buvo pradėti kurti pigūs ir saugūs kriptografiniai metodai, kurių paskirtis padidinti komunikacijos saugumo lygmenį tarp RFID žymos ir jos skaitytuvo.

Šiandien egzistuoja daug kriptografinių metodų (neretais atvejais vadinami protokolais), kurie užtikrina RFID sistemos apsaugą nuo jos suklastojimo. [23]

Žemiau pateikiama lentelė su pastaruoju metu naudojamomis RFID saugumo užtikrinimo metodikomis.

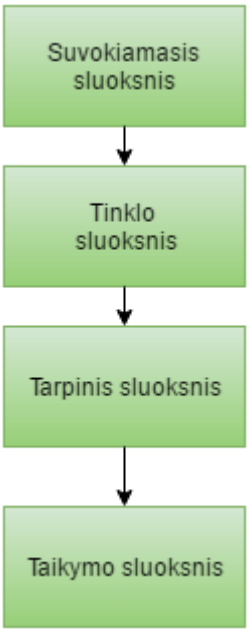
4 lentelė. RFID saugumo metodų palyginimas

Pažeidžiamumai	Metodai					
	RHLK	**HIDV**	**SRAC**	**HBIV**	**LCRP**	**A-SRAC**
Informacijos nutekinimas	-	-	-	-	+	+
Suklastojimo ataka	-	-	-	+	+	+
Pakartojimo ataka	-	+	-	+	+	+
Persiuntimo saugumas	-	-	+	+	-	-
Desinchronizavimas	-	+	-	-	-	-
Vietos privatumas	-	-	-	-	-	-
Abipusė autentifikacija	+	-	+	+	-	-
Atsisakymo tarnauti ataka	-	-	-	-	-	-

Atlikus analizę paaiškėjo, kad stipriausia grėsmė pažeidžiamumo prasme tyko yra informacijos nutekinimas. Įvykdžius šį pažeidimą būtų pvz., nutekinama įvairi informacija. Minėta apsauga turi tik du metodai: LCRP ir A-SRAC.

1.2. Daiktų interneto programinės įrangos sluoksnis

Daiktų interneto pasaulyje vyrauja daugybė objektų. Pagrindinė problema, kaip visus šiuos objektus identifikuoti. Šiandieniniame pasaulyje daugybė objektų yra prijungiama prie daiktų interneto taikant tarpininko (angl. *middleware*) architektūrą. Tai tokia architektūra, kuri įgalina didžiulį kiekį sensorių būti prijungtiems į tinklą suteikiant jiems jungimosi galimybes tiek jutikliams, tiek programinės įrangos sluoksniams. Įvairūs jutikliai, sensoriai gali būti prijungiami naudojant tam tikrą API (angl. *Application Programming Interface*) [29]. Žemiau pateikiamas nagrinėjamos srities struktūros modelis (1 pav.). Struktūra susideda iš keturių sluoksnių – suvokiamasis, tinklo, tarpinis, taikymo sluoksniai.



1 pav. Daiktų interneto sluoksniai

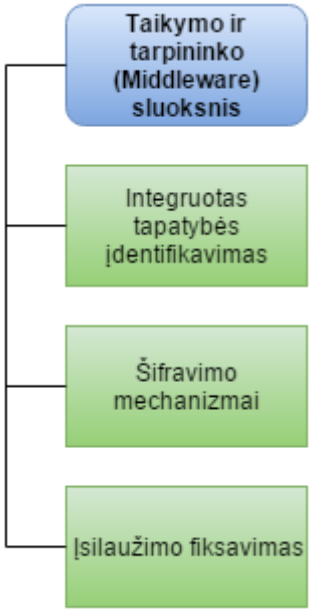
Suvokiamasis sluoksnis susideda iš tokių įvairių jutiklių kaip RFID, brūkšninio kodo skaitytuvai, temperatūros jutikliai, šviesos davikliai. Pagrindinis šio sluoksnio uždavinys yra identifikuoti unikalius objektus ir išsaugoti surinktą informaciją. [29]

Tinklo sluoksnio paskirtis yra persiųsti surinktą informaciją iš suvokiamojo sluoksnio į tam tikrą informacijos apdorojimo sistemą naudojant interneto ryšio prieigą [29].

Sluoksnis susideda iš informacijos apdorojimo sistemų, kurios priima automatizuotus veiksmus, paremtus gautais duomenimis iš aukštesnio lygmens.

Taikymo sluoksnis yra paremtas praktiniais vartotojų ir organizacijų poreikiais, pvz., išmanusis namas, išmanusis televizorius ir t. t.

Žemiau pateiktas daiktų interneto apsaugos modelis (2 pav.). Šis modelis suvienija tarpininko ir aplikacijos sluoksnius sudarydamas integruotą saugos mechanizmą.



2 pav. Tarpinės programos saugos sudedamosios dalys

Yra būtina pereiti autentifikavimo mechanizmą. Šis procesas uždraudžia prieigą bet kokiam kenkėjiškam vartotojui patekti į sistemą. Nors dauguma technologijų, naudojančių šią metodiką, yra debesų ir virtualizacijos technologijos, jos yra savaime paruoštos įvairioms atakoms. Tarkim, debesų technologija gali būti pažeista taikant įsilaužimo metodus (angl. *insider threat*). Virtualizacijos atveju pavojus kyla taikant *DOS* atakas ir duomenų vagystę [29].

Duomenų saugumas yra užtikrinamas taikant įvairius kriptografinius metodus, kurie apsaugoja nuo duomenų vagystės – *Anti-DOS* ugniasienės, įvairios antivirusinės programos.

Tačiau vis dėlto išlieka didžiausia problema. Dabartiniame pasaulyje, kai aplink yra daugybė objektų, kurie yra įjungti į tinklą, susiduriama su problema, kad visus šiuos objektus yra sunku identifikuoti. Todėl įvykus įsilaužimui tampa sudėtinga identifikuoti objekto tapatybę, t. y. ar jutiklis, kuris siunčia informaciją yra tikrai tas jutiklis, kuris ir turi ją siųsti. Piktavalis gali pakeisti įvairių sensorių rodmenis ir priversti sistemą veikti netikslingai, siųsti klaidingus duomenis vartotojui arba sutrikdyti sistemos darbą tam tikram laiko tarpui.

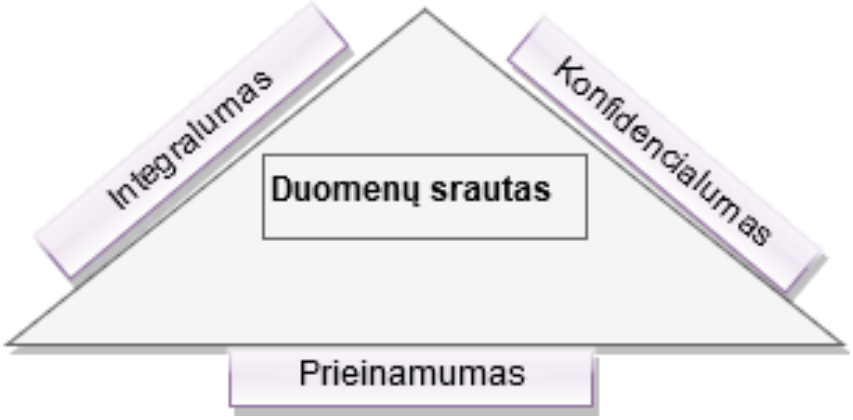
1.3. Tyrimo objektas, sritis ir problema

Daiktų interneto objektų apsuptyje šiandien diena yra daugybė objektų, kuriuos vartotojai naudoja kiekvieną dieną. Tokie objektai kaip vaiko priežiūros stebėjimo kameros, planšetiniai kompiuteriai, automobiliuose esantys kompiuteriai. Tokie objektai yra ganėtinai plačiai naudojami ir šiai dienai turi galimybę komunikuoti tarpusavyje. Šie objektai, kurie patys savaime ankščiau nebuvo traktuojami kaip išmanūs objektai, šiandien dienai galima pastebėti begale objektų, kurie savyje turi daugybę įvairių daviklių, jutiklių ir kitų komponentų savyje.

Suvokiant faktą, kad dauguma svarbių sekcijų šiandien yra pilnos daiktų interneto technologinių subtilybių. Tokių kaip – Debesų technologijos, Virtualizacija, Mobilūs įrenginiai, kompiuterizuoti davikliai ir jutikliai, RFID technologijos, dirbtinis intelektas. Tačiau, su šiomis technologijomis savaime atsiranda ir įvairūs įsilaužimo atvejai kibernetinėje erdvėje dėl įvairių sumetimų vienas iš priežasčių yra galimos saugumo spragos.

1.4. Įsilaužimų aptikimas kibernetinėje erdvėje.

Didžiausias saugumo tikslas daiktų interneto terpėje tai įskiepyti tinkamus identifikavimo ir autentifikavimo mechanizmus bei užtikrinti duomenų srauto konfidencialumą. (3 pav.)



3 pav. Duomenų saugumo užtikrinimo dėsningumo trikampis

Duomenų konfidencialumas – punktas, kuris leidžia vartotojui užtikrintai bei laisvai naudotis savo duomenimis, nebijant, kad jų turinys bus kaip nors paliestas neautorizuotų asmenų. Duomenų konfidencialumas gali būti užtikrinamas taikant įvairius saugumo mechanizmus, todėl būtų išgaunamas duomenų užslėpimas siekiant apsaugoti juos, kad jie būtų pasiekiami tik tiems vartotojams, kuriems yra suteikiama minėta prieiga prie šių duomenų prieiti.

Vyrauja įvairūs mechanizmai, kurie yra skirti duomenų konfidencialumo užtikrinimui. Tokie mechanizmai kaip duomenų šifravimas, kuomet duomenys yra performuojami į kriptografinį tekstą. Tada tampa daug sunkiau vartotojams, neturintiems autorizacijos pasiekti reikiamus duomenis. Analogiškai yra taikomas ir biometrinis autentifikavimas. Kiekvienas vartotojas savyje turi unikalių dalių tokių kaip žmogaus pirštų antspaudai, jų pagalba vartotojas gali būti identifikuotas.

Duomenų integralumas – kuomet yra užmezgama komunikacija, duomenys gali būti paveikti kibernetinių nusikaltėlių. Vyrauja įvairūs faktoriai, kurie nepriklauso nuo žmogiškojo faktoriaus. Tokie atvejai apima serverio darbo sutrikdymą, elektromagnetinio lauko disbalansą. Duomenų integralumas apima duomenų saugą nuo kibernetinių nusikaltėlių arba duomenų perdavimą į kitą terpę.

Duomenų prieinamumas – vienas iš didžiausių daiktų interneto siekių saugume yra padaryti taip, kad duomenys būtų pasiekiami jų savininkams (vartotojams) bet kuriuo metu, kada minėti duomenys tampa reikalingi. Duomenų prieinamumas suteikia užtikrintiną duomenų pasiekimą autorizuotiems vartotojams. Atsižvelgiant į tai, kad dabartiniame pasaulyje dauguma įmonių smarkiai priklauso nuo duomenų prieinamumo čia ir dabar tuomet tampa labai svarbu, užtikrinti, kad darbinėje aplinkoje būtų įdiegtos reikiamos ugniasienės, kurios padėtų kovoti su tokiais įsilaužėliu sukeliamais iššūkiais kaip serviso atsako atmetimo atakos (*angl. DoS*) kuomet minėtas atakos metodas gali nutraukti duomenų prieinamumo galimybę galutiniam vartotojui, siekiančiam pasiekti jam svarbių duomenų paketą.

1.5. Saugumo iššūkiai ir problematika.

Atsižvelgus į tai, kad plačiau liečiant daiktų interneto tematiką iš esmės buvo pasiekta daug pasiekimų mokslinių tyrimų ir bandymų dėka. Tačiau šiai dienai vis dar egzistuoja daugybė iššūkių minėtos technologijos sferoje. Šiame skyriuje apžvelgiamos įvairių architektūrinių sluoksnių pažeidžiamumo kryptis.

1.5.1. Iššūkiai „Suvokiamojo sluoksnio“ lygmenyje

Suvokiamasis sluoksnis susideda iš įvairių jutikliu technologinių gairių tokių kaip pvz., RFID. Pastaruoju metu yra plačiai spekuliuojama apie tai, kokie yra esminiai principai, kuriais remiantis minėtos technologijos atskleidžia savo pažeidžiamumus. Žemiau apžvelgiami pagrindiniai pažeidžiamumo atvejai užfiksuoti pastaruoju metu ir objektyviai apžvelgti mokslinėje literatūroje.

Neautorizuota prieiga naudojant fiktyvias žymas.

Dauguma RFID sistemų pasižymi skurdžiu autentifikavimo mechanizmu tarkim yra RFID sistemų, kurias įsilaužėlis gali netik nuskaityti, bet ir pakeisti RFID kortelėje esančia informaciją arba ja neatstatomai ištrinti.

Žymų klonavimas

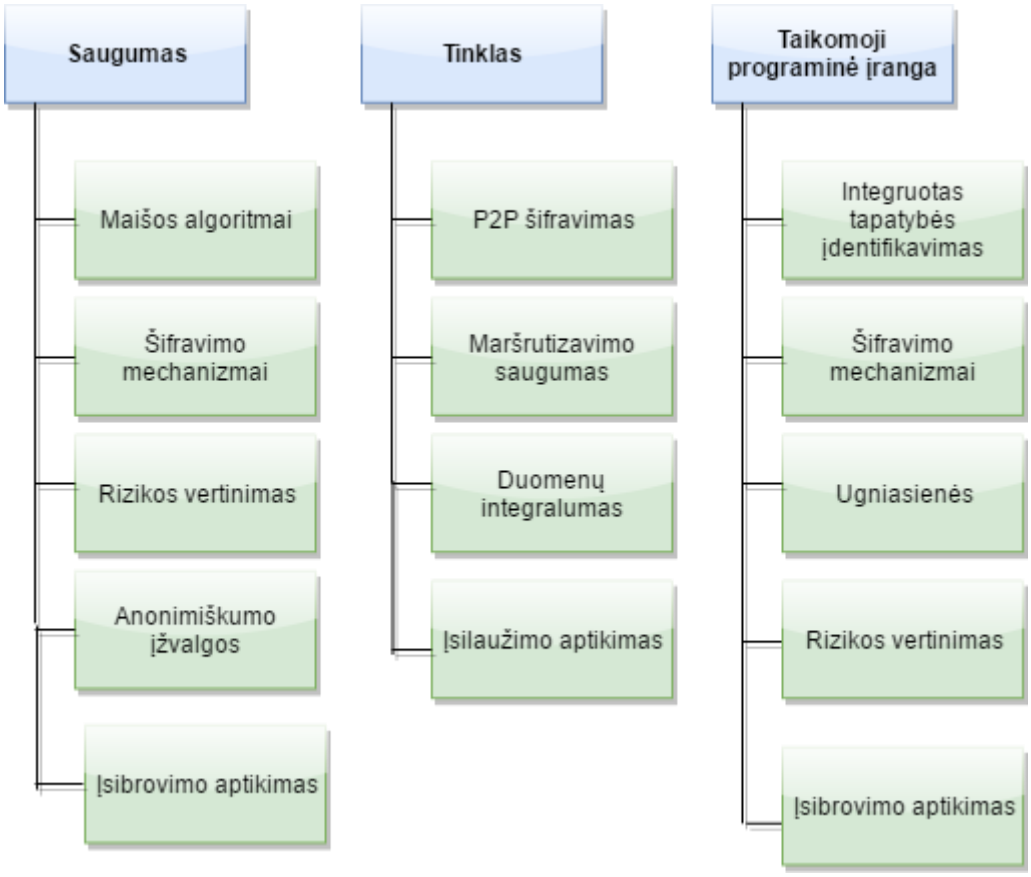
Suvokiant tai, kad žymos yra įdiegiamos ant įvairių objektų, kurie yra aiškiai matomi, ir jų duomenys visgi gali būti nuskaityti, o tuo pat metu ir pakeisti ar ištrinti. Naudojant įsilaužimo technologiją įsilaužėlis gali sukruti minėtos žymos kopiją t.y., ją nuplagijuoti, todėl žymos skaitytuvai neretai nebesugeba atskirti, kur yra tikra, o kur yra fiktyvi žyma. Iš čia išsiskiria problema, kad viena iš pagrindinių daiktų interneto problemų yra objektų identifikavimas.

Duomenų perklausymas

RFID kaip technologija pasižymi gebėjimu belaidžiu principu perduoti duomenų srautą. Iš vienos pusės tai yra pliusas, kad galima perduoti informacija belaidžiu principu tačiau iš to išplaukia problema, kad įsilaužėliai neretai panaudoja tai savo naudai. Tai nutinka todėl, nes žvelgiant iš įsilaužėlio pusės tampa nesudėtinga perskaityti informacija, kuri keliauja tarp RFID žymos ir jos skaitytuvo. Įsilaužėlis tampa įgalintas nuskaityti tokia informaciją kaip vartotojo slaptažodžiai, ar kokia kita asmeninę informaciją, kuri yra patalpinta RFID žymoje.

Atkartojimas

Įsilaužimo mechanizmas naudojamas tuomet, kai įsilaužėlis bando atkartoti skleisdamas fiktyvia informaciją. Tarkim RFID žyma siunčia informacija į siųstuvą. Įsilaužėlis gali pabandyti siųsti savo fiktyvią informaciją į siųstuvą, taikydamas šį metodą jis gali užkirsti sistemą. Jai nustojus tinkamai funkcionuoti iškyla rizika, kad įsilaužėlis gali patekti į pastatą.

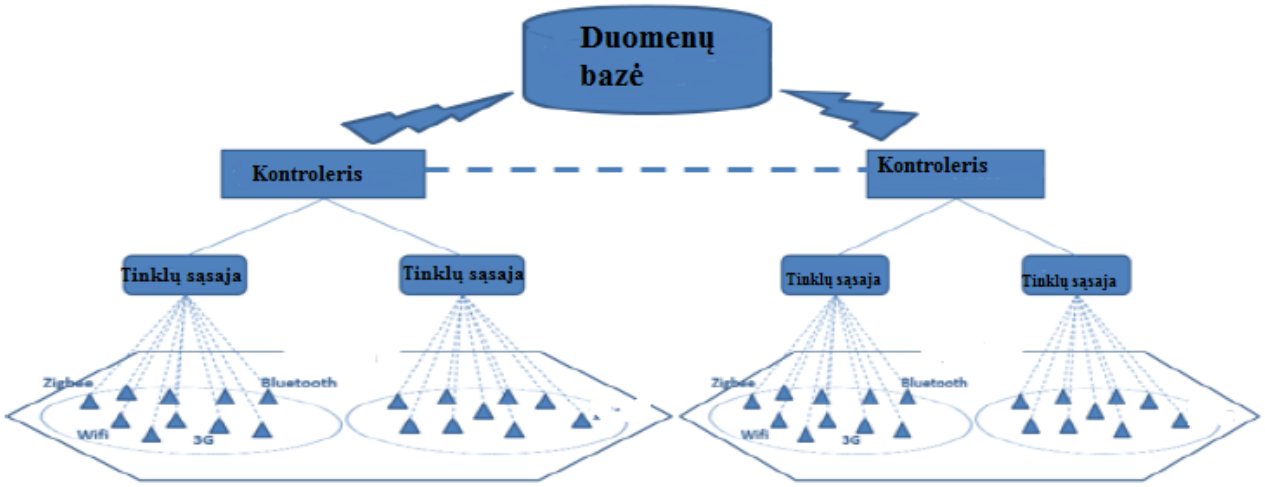


4 pav. Daiktų interneto saugumo architektūra

Daiktų internetas yra svarbus elementas todėl yra skiriamos didžiulės pastangos saugos architektūros plėtrai (4 pav.). Dauguma mokslininkų siekia pateikti patikimą, gerai apibrėžtą saugios architektūros mechanizmą, kuris užtikrintų duomenų saugos konfidencialumą bei privatumą. Svarbiausias akcentas minėtoje architektūroje yra taikomosios programinės įrangos lygis. Mechanizmo esmė susideda iš veiksmų sekos, kas po ko turi būti įvykdyta siekiant pasiekti reikiamo rezultato. Įvykdomas autentifikavimo tapatybės patvirtinimo tarpsnis, tai yra reikalinga tam, kad negalėtų į sistemą prisijungti tam nepriskirtas vartotojas. Svarbu suvokti tai, kad neegzistuoja tokia sistema, kurios nebūtų įmanoma nulaužti. Vadovaujamasi principu, kad jeigu vienas žmogus sukūrė, kitas gali sugebėti tai sugriauti. Nutikus atvejui, kuomet įsilaužėliui pavyko patekti į sistemą yra iškviečiamas įsibrovimo signalas į serverį aptikus įtartina veiklą. Būtina nuolatos vertinti įvairias rizikos grėsmes, ir priimti sprendimus, kaip nuo to galima apsisaugoti ateityje.

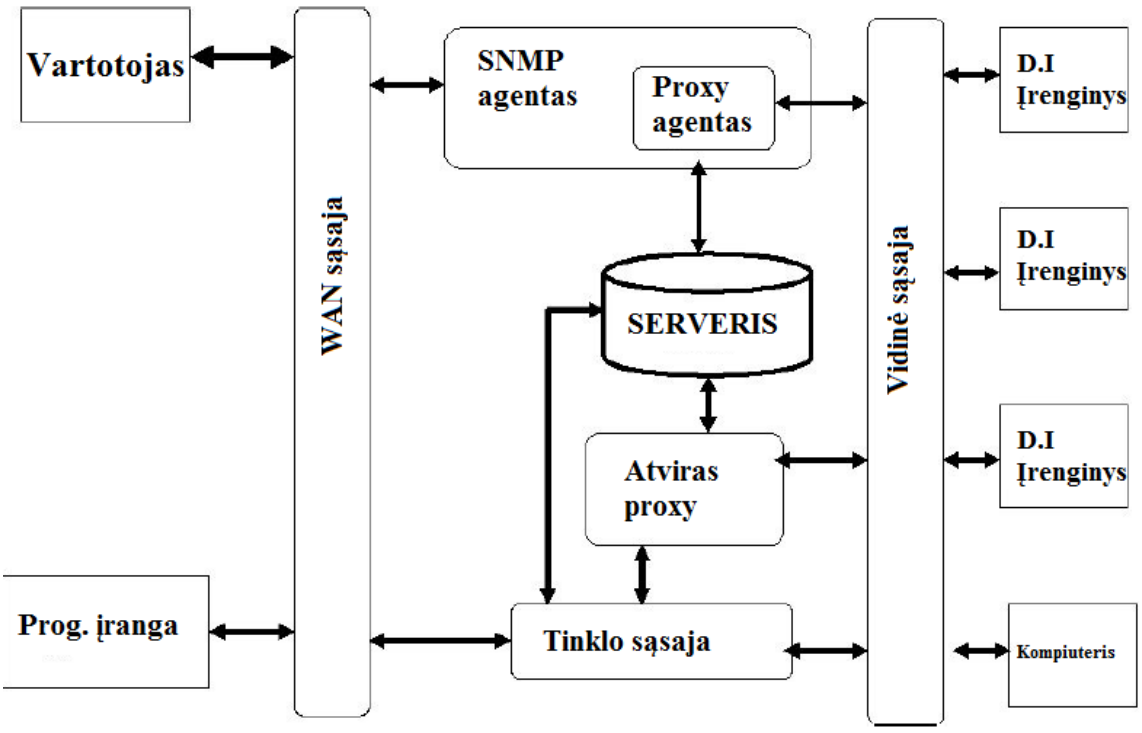
1.6. Daiktų interneto objektų identifikavimo bei autentifikavimo metodai

Objektų identifikavimas yra svarbi problema daiktų interneto sferoje ryšium su sparčiai didėjančia paklausa iš vartojimo pusės todėl sprendimų, kaip identifikuoti objektus yra. Skyriuje pateikiama keletas pagrindinių metodų kaip galima identifikuoti objektus įvairiuose lygmenyse, su kokiomis problemomis yra susiduriama ir kaip jas yra bandoma išspręsti.



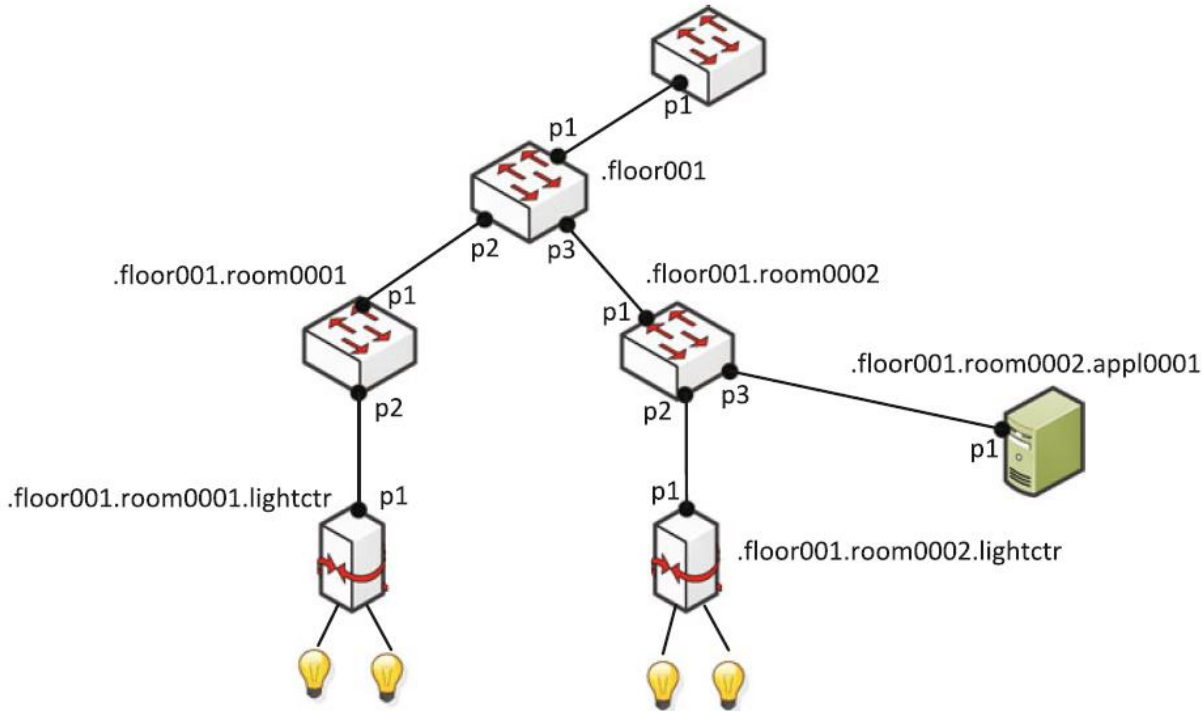
5 pav. Objekto identifikavimas tinklo lygmenyje [30]

Pagal pateiktą paveikslą (5 pav.) atvaizduotas objektų identifikavimo modelis. Minėto modelio veikimo principas susideda iš duomenų bazės, kurioje yra saugoma informacija apie objektus, kontrolerių, kurie siunčia informacija į minėtą duomenų bazę apie objektus, su kuriais jie komunikuoja bei patys daiktų interneto objektai susieti su kontroleriu. Sprendimas taikomas suformuojant identifikatorių iš kontroleriui sugalvoto identifikatoriaus, tai skaičių derinys, prie kurio papildomai yra pridedamas objekto suteiktas IP adresas ir atsitiktinis skaitmuo [30]. Vykdoma tarpusavio komunikacija tarp duomenų bazės serverio ir kontrolerio. Jeigu siunčiamas identifikatorius atitinka tokį, kuris yra įrašytas į duomenų bazę, informacija patvirtinama.



6 pav. Objekto identifikavimas taikant SNMP agentus [29]

Pagal pateiktą objektų identifikavimo modelį taikant SNMP agentines programas (6 pav.) vartotojas pasiekia objektų valdymo bloką tik prisijungęs prie SNMP agentinės programos bloko. Prisijungus per Proxy serverį vartotojas gali priskirti jam norimus objektus suteikdamas identifikatorių, kokio jis pats nori tai gali būti objekto pavadinimas, objekto paskirtis [29]. Vienas iš pastebėtų akcentų tiriant pateiktą identifikavimo modelį yra faktas, kad objekto identifikavimas vykdomas neužtikrinant objektų autentiškumo. Taikant minėtus metodus yra praktiškai neįmanoma užtikrinti, kad daiktų interneto objektas, kuris siunčia informaciją yra būtent tas, o ne fiktyvus įsilaužėlis bandantis sukompromituoti sistemą. Žemiau pateikiamas alternatyvus objektų identifikavimo sprendimas, kuris įgalina netik identifikuoti objektus, bet ir autentifikuoti (7 pav.).



7 pav. Objektų identifikavimas taikant duomenų pasiskirstymą

Taikant pateiktą hierarchinio adresavimo metodą galima sekti objektų fizine vietą, Vietos nustatymui naudojami atskiri tinklo mazgai. Mazgai pagal pateiktą medžio išsišakojimą geba kešuoti siunčiamą informaciją ir ja išsaugoti paskesnėms užklausoms taikant objektų identifikacijos tikrinimą t.y., persiustos informacijos validumą. Kuomet taikomas vieno objekto identifikavimo tarpsnis, toliau sekančius objektus gali apdoroti kiti medyje suformuoti tinklo mazgai. Metode taikoma bendrinė atstumo logika, kad objekto informaciją turi apdoroti pirmiausia ja gavęs, arčiausiai esantis tinklo mazgas, tai yra daroma todėl, kad kiek įmanoma mažiau būtų apkraunamos tinklo mazgų grupės ir komunikavimo mechanizmas vyktų kiek įmanoma greičiau ir sklandžiau. Taipogi mazgai savyje saugo tik tam tikras objekto identifikavimo informacijos dalis tai yra daroma todėl, kad kuomet yra bandoma persiųsti didelius duomenų kadrus tampa nebereikalinga persiųsti visą sukauptą informacija, o galima ja išskaidyti į atitinkamas dalis, kurias gali apdoroti visi tinklo mazgai lygiomis dalimis. Taikant šį būdą yra išvengiama tinklo perkrovos problemų bei duomenys yra pasiekiami per trumpa laiko tarpą.

Pagrindiniai metodo akcentai suteikiantis unikalumo yra šie:

- Taikant pavadinimų suteikimą objektams taikomas hierarchijos principas, yra nurodoma, kur koks objektas yra, koks aukštas, kambarys, ir koks kodas objekto, kuris yra priskiriamas.

- Energijos taupumas objektams. Tai yra pasiekiamas taikant duomenų kešavimo ir duomenų saugojimo mechanizmą.
- Objektų identifikavimas taikant suformuota identifikatoriaus sąrašą iš atskirų komponenčių
    - Adreso ilgis;
    - Galutinis siunčiamas adresas;
    - Siunčiamas pranešimas;
    - Pranešimo galiojimo laikas;
    - Duomenų perkrova;

Taikant minėta metodą objektai, kurie siunčia informaciją yra tinkamai identifikuojami ir gali būti užtikrinamas jų autentiškumas. Taikant duomenų kešavimo bei mazgų eilės pasiskirstymo mechanizmą yra užtikrinamas sistemos ilgalaikis funkcionalumas, apsisaugojama nuo perkrovos atvejų.

1.7. Analizės išvados

Išanalizuotos įvairios daiktų interneto objektų komunikavimo technologijos ir belaidžio ryšio protokolai.

Išanalizuoti protokolų veikimo principai, pažeidžiamumai ir saugumo užtikrinimo atvejai. Taipogi detalizuota daiktų interneto struktūra, buvo aprašyti ir detalizuoti daiktų interneto koncepciją sudarantys sluoksniai.

Nors daiktų interneto objektų identifikavimo ir autentifikavimo problema yra žinoma mokslininkai plačiai dirba ties šia problemine sfera ir jau galima aptikti galimų sprendimų problemai spręsti.

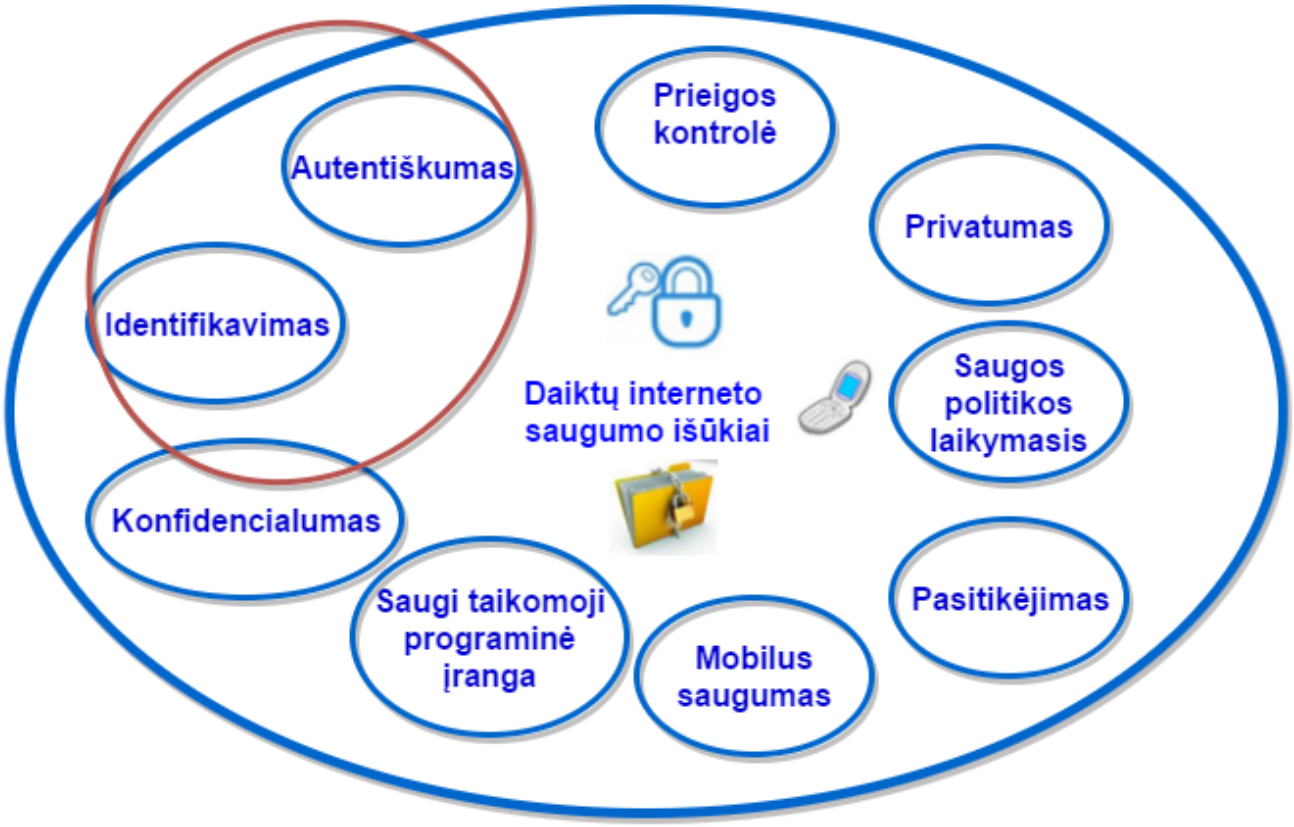
Daiktų interneto objektų identifikavimo sprendimų yra, tačiau nepavyko aptikti sprendimų, kurie užtikrintų autentifikavimą, nors tai yra viena iš esminių daiktų interneto probleminių sričių, kuria yra būtina tinkamai išspręsti, kad užtikrinti sklandų objektų identifikavimo ir autentifikavimo procesą.

2. DAIKTŲ INTERNETO OBJEKTŲ IDENTIFIKAVIMAS PROGRAMINIAME LYGMENYJE

Šiame skyriuje aprašomas siūlomas daiktų interneto objektų identifikavimo programiniame lygmenyje metodo modelis. Pateikiamas siūlomos sistemos koncepcinis modelis, architektūra, serverio ir kliento komunikacijų modeliai ir apibrėžiami metodo saugumo profiliai bei jų sudedamosios dalys.

Bendrame lygmenyje siekiant suvokti kaip korektiškai turėtų veikti minėto metodo modelis būtina įsigilinti į pačia daiktų interneto koncepcija. Daiktų internetas savyje tai yra esybe objektų, kurie daugybe vartotojų supa kiekviena dieną. Daiktų interneto dėka gyvenimas tampa gerokai lengvesnis, tačiau retas atsižvelgia į tai, kad kaip ir beatkuri sistema žvelgiant viso pasaulio mastu, daiktų interneto objektai savyje turi daugybe problemų, kurias yra svarbu tinkamai įvertinti bei įdėti didžiules pastangas, kad jos būtų tinkamai išspręstos. Žemiau esančiame 8 paveiksle yra pateikiamos bendrinės daiktų interneto erdvėje esančios problemos susijusios su saugos tematika.

2.1. Pagrindinės daiktų interneto saugos problemos



8 pav. Pagrindinės daiktų interneto saugos problemos

Problematika galima išdėstyti į keletą bendrų punktu, kuriais remiantis ir kyla dalis problemų su kuriomis tenka susidurti šiai dienai. Visų pirma būtina suvokti, kad esame apsupti daugybės objektų, kurie iš pažiūros duoda didžiulę naudą vartotojui. Tačiau kyla problemos, kuomet yra itin svarbu užtikrinti siunčiamos informacijos autentiškumą. Problema tame, kad kaip tinkamai identifikuoti objektą, kuris pvz., siunčia informacija apie paciento gulinčio ligoninėje rodmenis apie širdies darbą.

Esant įsilaužimo atvejui ir sufalsifikavus tokia informacija gali kilti grėsmė asmens gyvybei. Analogiškai susijusios ir kitos problemos, kad jeigu yra siunčiama informacija, ir jeigu ta informacija, kuri yra siunčiama yra autentifikuota kyla problema, kad informacija yra būtina išlaikyti konfidencialią ir tik tam tikriems autentifikuotiems vartotojams, t.y., svarbu užtikrinti ir prieigos kontrolę prie duomenų. Tai yra tik maža dalis esminių problemų, su kuriomis tenka susidurti šiandien dienai ir į tai yra būtina atsižvelgti.

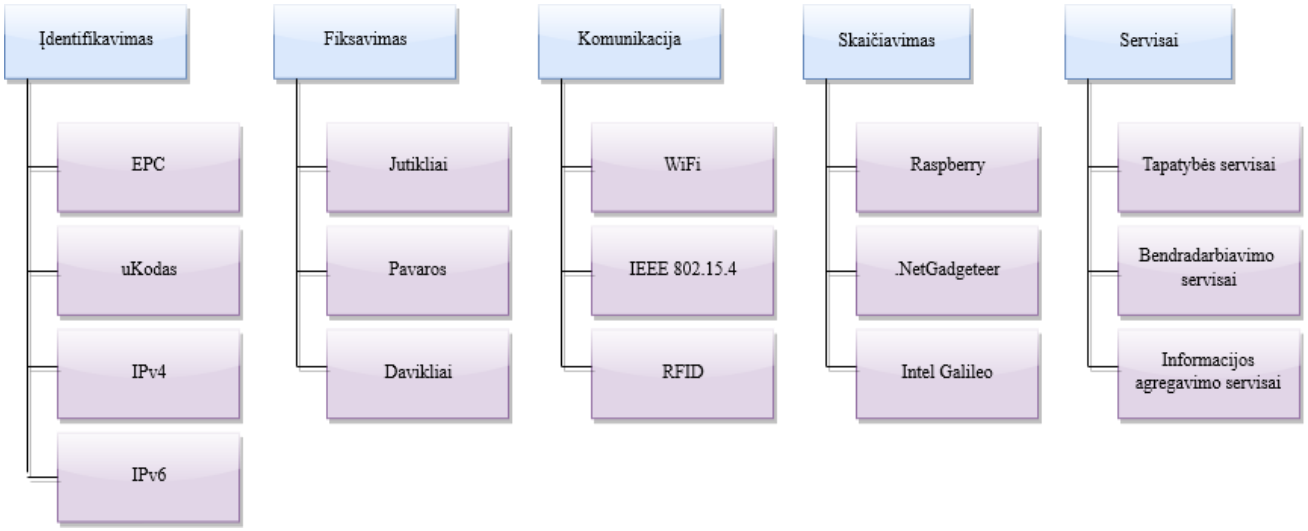
2.2. Daiktų interneto atvirieji iššūkiai

9 pav. Daiktų interneto atvirieji iššūkiai

Projektavimas svarbus etapas bet kokios idėjos realizavimo etape. Daiktų interneto objektų realizacija yra ne išimtis. Neretai prieš įsivaizduojant objektą kaip jis atrodys, jo paskirti bei suderinamumą vartotojo kasdieniu veiksmų atlikimo tarpsnyje tai yra ar sprendimas ras savo vietą vartotojo dienotvarkėje bei buityje yra svarbu numatyti ir pagrindinius platformos projektavimo iššūkius su kuriais tenka susidurti (9 pav.). Laikotarpis, kuriame dabar gyvename pilnas iššūkių, daiktų interneto objektų projektuotojams tenka susidurti su begale problemų, tokių kaip didelės talpos informacijai užtikrinimas, objekto suderinamumas su kitais objektais, duomenų persiuntimo optimizavimu, siekiant užtikrinti sklandų duomenų apsikeitimą tarp objektų, efektyvų energijos panaudojimą ir kainą, kurį būtų prieinama eiliniam vartotojui.

Objektai tarnauja vartotojui, jie padeda organizuoti įvairius darbus, taupo laiko sąnaudas, automatizuoja begale procesų. Tačiau dauguma vartotojų net nesusimasto, kad daiktų interneto objektai, nors ir padeda, tačiau keli iš daiktų interneto platformos atvirųjų iššūkių yra informacijos autentiškumo užtikrinimas ir informacijos saugumo ir privatumo užtikrinimas. daiktų interneto objektų

identifikavimo metodų programiniame lygmenyje tyrimo metodologija apima objektų identifikavimą ir autentifikavimą. Tai yra svarbu ryšium su tuo, kad taikant dabartinius esamus rinkoje sprendimus, kurie komunikuoja kliento – serverio principais yra sudėtinga užtikrinti, kad jeigu objektas turintis paskirtį pagal temperatūros pokyčius palaikyti tolygią patalpos temperatūrą, informacija į serverį siunčiantis objektas yra tikrai tas, kurio paskirtis yra atlikti minėtus veiksmus temperatūros palaikymui, o ne kibernetinis įsilaužėlis siekiantis sukompromituoti tolygų sistemos veikimą.



10 pav. Daiktų interneto objektų sandara

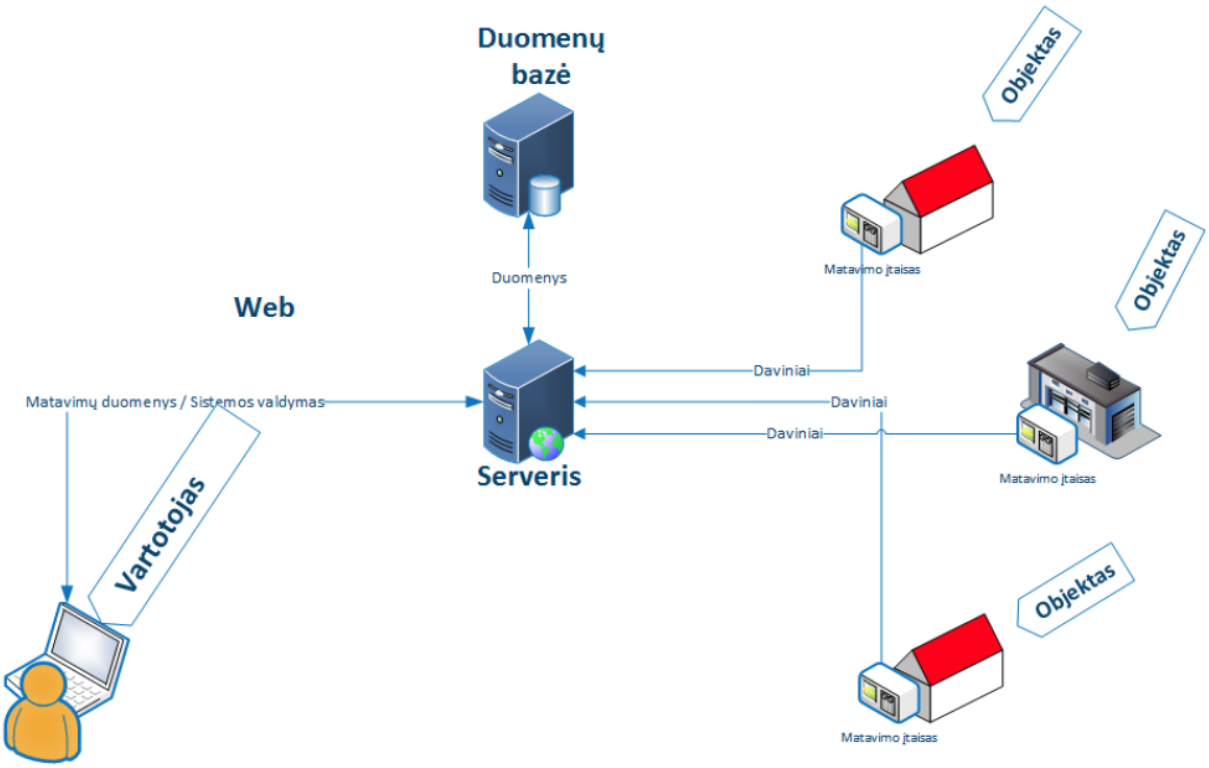
Objektų identifikavimas yra nuolatos mokslininkų ir analitikų plėtojama tema. Kiekvienas objektas turėtų būti identifikuojamas. Objektai gali būti skirstomi į identifikavimo grupes pagal atitinkamus scenarijus. Identifikuojant objektus svarbu užtikrinti jų unikalumą. Vieni objektai turi turėti savo unikalų identifikatorių, tai gali būti priskiriama objektams, kurie atlieka tam tikrą specifinę užduotį. Kitiems objektams galimas grupės identifikavimo principo taikymas pvz., pastate esantys ventiliatoriai. Visiškai nesvarbu, koks jų gamintojas, jų paskirtis yra analogiška, palaikyti tam tikrą temperatūra patalpoje. Objektų identifikavimas gali būti įgyvendintas taikant keletą skirtingų taikymo principų. Vienas iš jų yra taikant fizinį objektų žymėjimo metodą tarkim taikant RFID, QR kodus ar panašaus pobūdžio technologiją. Taikant minėtą būdą objektas bet kuriuo momentu gali būti „nuskaitytas“ ir visa informacija apie ji būtų pateikiama tarkim taikant RFID kortelių skaitytuvus. Skaitytuvas gražintų serveriui objekto identifikatorių, užtikrindamas sklandžia komunikaciją. Objektų identifikatorius galima laikyti duomenų bazėje. Susijusią informaciją, aprašymą, siunčiamus duomenis.

Kitas metodas, kuris ir apima koncepcinį daiktų ir paslaugų interneto objektų identifikavimo programiniame lygmenyje sistemos modelį yra suteikti objektui savitą unikalų identifikatorių, Aprūpinus beviele komunikacija, objektas galėtų nevaržomai komunikuoti su serveriu ir keistis siunčiama informacija.

Viena esminių problemų daiktų interneto rėžiuose yra objektų įvardijimas. Dauguma taikomųjų programų turėtų komunikuoti naudojant unikalius identifikatorius.

2.3. Daiktų interneto objektų identifikavimo programiniame lygmenyje sistemos vizija

Daugybė daiktų interneto objektų yra sujungti į tinklą. Tačiau vyrauja problemos susijusios su daiktų interneto objektais. Svarbiausia dalis yra ta, kad kaip galima pasitikėti objektų, kaip įsitikinti, kad informacija, kuri ateina iš jutiklio pusės yra teisinga ir nepakeista (11 pav.).



11 pav. Daiktų interneto objektų identifikavimo programiniame lygmenyje sistemos vizija

Rezultato galima pasiekti realizuojant objektų identifikavimo agentinę sistemą, kuri susideda iš keturių agentinių sistemų – agentas registratorius, agentas gavėjas, agentas siuntėjas ir agentas identifikatorius (12 pav.). Agento registratorius - paskirtis atlikti daiktų interneto objektų registravimą. Turi būti suprojektuotas objektų registravimo mechanizmas, kuris susideda iš pateiktų agentui skirtų komandų:

- registravimas;
- naikinimas;
- priskyrimas;

Agentų siuntėjo paskirtis yra išsiusti duomenis gavėjo programai supakuotus bei užšifruotus.
Agentų gavėjo paskirtis yra pasiimti užšifruotus duomenis iš agentų siuntėjo
Agento identifikatoriaus užduotis yra iš gavėjo programos gautus supakuotus duomenis išsišifruoti ir identifikuoti objektą. Jeigu objektas teisėtas – praleisti siunčiamus duomenis. Jeigu objektas neteisėtas t.y., neatitinka objektų įidentifikavimo algoritmo tuomet identifikavimo programa

siunčia informacija siuntėjo programai, kuri kreipiasi į registravimo programą ir toks objektas yra pašalinamas arba suspenduojamas iš sistemos.

Agentinės programos tarpusavyje sąveikauja siųsdamos gautą informaciją ir į ją reaguodamos. Veikimo principas paremtas šiais aspektais. Agentas identifikatorius autentifikuoja objektus, kurie bando jungtis į sistemą, jeigu objektas yra netikras t.y., atsiųsta informacija netenkina minėtos objektų autentifikavimo architektūros yra siunčiamas atsakymas agento registratoriaus programai, kurios paskirtis yra uždrausti prieigą minėtam objektui. Agentinės siuntėjo programos užduotis yra supakuoti duomenis pagal minėta metodiką iš kelintinės pusės, tuomet agentas gavėjas privalo priimti duomenis iš siuntėjo, juos išpakuoti ir jeigu minėti duomenys yra teisingi įrašyti į duomenų bazę.

12 pav. Agentinių programų tarpusavio sąveika

Toks programų tarpusavio sąveikos modelis užtikrina, kad objektas, kuris bando užmegzti komunikacijos sesiją ta galės padaryti tik praėjęs agentinių programų patikros ciklą, nuo identifikavimo bei registravimo iki pat duomenų siuntimo agentinių programų sąveikos. Tačiau svarbu yra užtikrinti ne tik tinkamą programų sąveiką identifikuojant objektus, tačiau užtikrinti ir pačia objektų identifikavimo metodiką.

2.4. Daiktų interneto objekto identifikavimo metodas

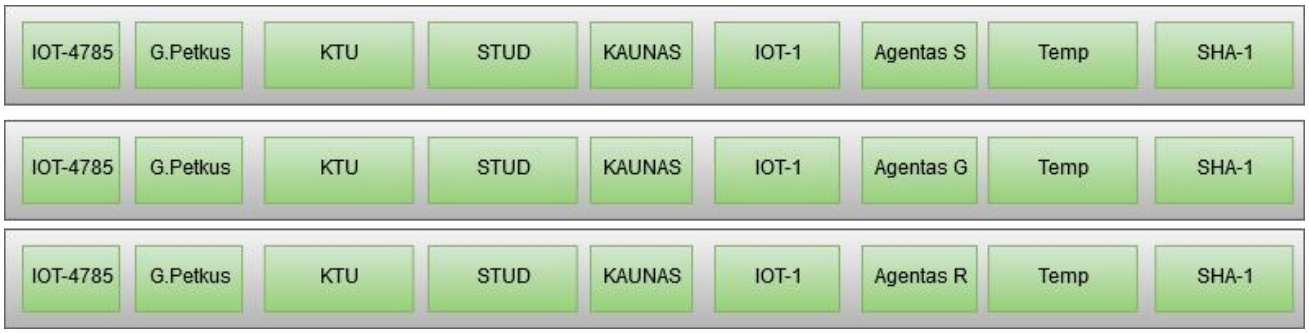
Siūloma objektų identifikavimo metodo komandos struktūra parodyta 13 paveiksle.

13 pav. Siūloma objektų identifikavimo komandos struktūra

Vartotojo kodas – Unikalus identifikatorius suteikiamas administratoriaus
V.Pavardė – Vartotojo vardas bei pavardė
Organizacija – Organizacija kurioje vartotojas naudojasi sistema.
Pareigos – Vartotojo rolė naudojantis sistema
Vieta – Vieta, kur patalpintas kontroleris (kabinetas)
Daiktų interneto objektas – Kontroleris su pvz., temperatūros jutikliu, RFID kortelių skaitytuvu.

Agentas. – Agentinė programa (siuntėjas, gavėjas, registratorius, identifikatorius)
Jutiklis - Jutiklio komunikuojančio su kontroleriu pavadinimas (identifikatorius)
Kontrolinė suma – SHA-1, SHA-256, SHA-512.

Remiantis žemiau pateiktu paveikslėliu yra detalizuotas realus identifikavimo mechanizmo taikymo pavyzdys. Vartotojui yra suteikiamas unikalus identifikatorius šiuo atveju IOT – 4785. Tai yra ta dalis, pagal kuria apsprendžia faktą ar reikia toliau bandyti apdoroti siunčiamą informaciją ar ją atmesti. Tarkim informacija, kuri yra siunčiama neturi minėto identifikatoriaus, tai ji automatiškai bus atmesta ir vartotojas gaus pranešimą apie tai, kad neautorizuotas vartotojas bandė kreiptis į sistemą ir buvo atmestas.
Jeigu identifikatorius yra teisingas ir validus, tuomet sistema renka sekančia informaciją apie siunčiamą duomenų paketa t.y., jį išskaido į minėtas dalis



14 pav. Siūlomos objektų identifikavimo sistemos komandų pavyzdžiai

Vartotojo kodas – Unikalus identifikatorius suteikiamas administratoriaus, šiuo atveju **(IOT – 4785)**
V.Pavardė – Vartotojo vardas bei pavardė **(Gediminas Petkus)**
Organizacija – Organizacija kurioje vartotojas naudojasi sistema. **(KTU)**
Pareigos – Vartotojo rolė naudojantis sistema **(STUD)**
Vieta – Vieta, kur patalpintas kontroleris (kabinetas) **(KAUNAS)**
Daiktų interneto objektas – Kontroleris su pvz., temperatūros jutikliu, RFID kortelių skaitytuvu. **(IOT-1)**.
Agentas. – Agentinė programa (siuntėjas, gavėjas, registratorius, identifikatorius) (Pagal užduoties pasirinkimą:

- agentas siuntėjas
- agentas gavėjas
- agentas registratorius
- agentas identifikatorius

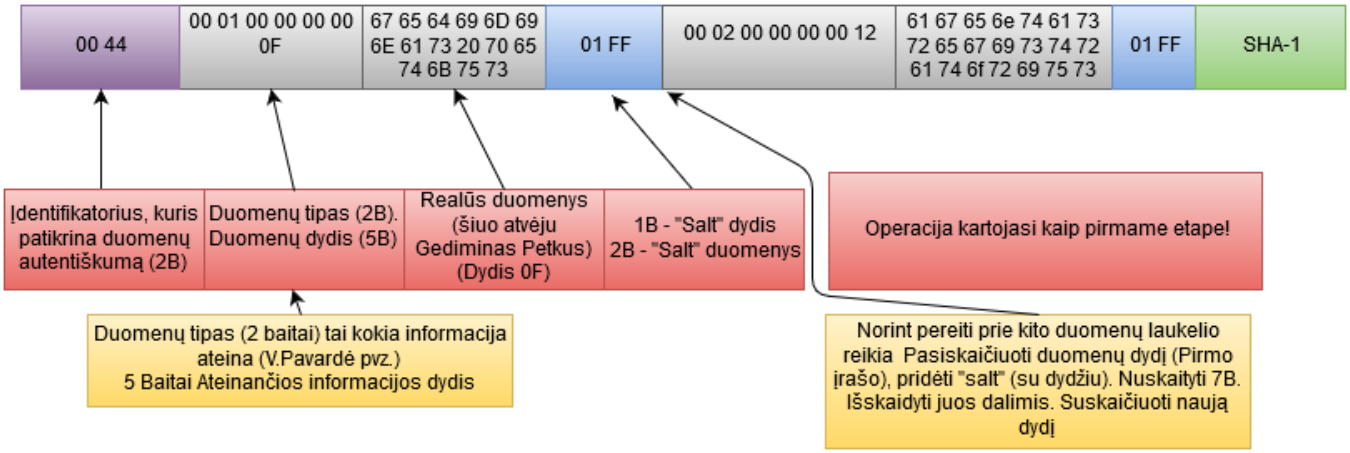
Jutiklis - Jutiklio komunikuojančio su kontroleriu pavadinimas (identifikatorius)
Kontrolinė suma – SHA-1, SHA-256, SHA-512.

Pateikiamas objektų identifikavimo koncepcinis modelis. Objektų identifikavimo modelyje yra siekiama sutalpinti informacijos tiek apie patį vartotoją, kuris naudojasi sistema, tiek apie pačius įrenginius, kurie komunikuoja tarpusavyje iš kliento ir serverio pusės. Kiekvienas įrenginys (kontroleris) turi gauti iš serverio pusės jam unikalų identifikatorių. Tiek pats įrenginys (kontroleris) tiek prie jo prijungti jutikliai yra identifikuojami naudojant jiems priskirtus identifikatorius. Metodo

principas remiasi tuo, kad pranešimo pirmieji baitai yra identifikatoriai, jie apsprendžia ar gauta informacija yra autentiška (15 pav), pvz., ar ji atitinka tolimesnius apspręstus įrenginių identifikavimo rėžius). Jeigu informacija, kuri atkeliavo neatitinka identifikatoriaus reikalavimų (pvz., įsilaužėlis bando siųsti savo fiktyvią informaciją) ji yra atmetama.

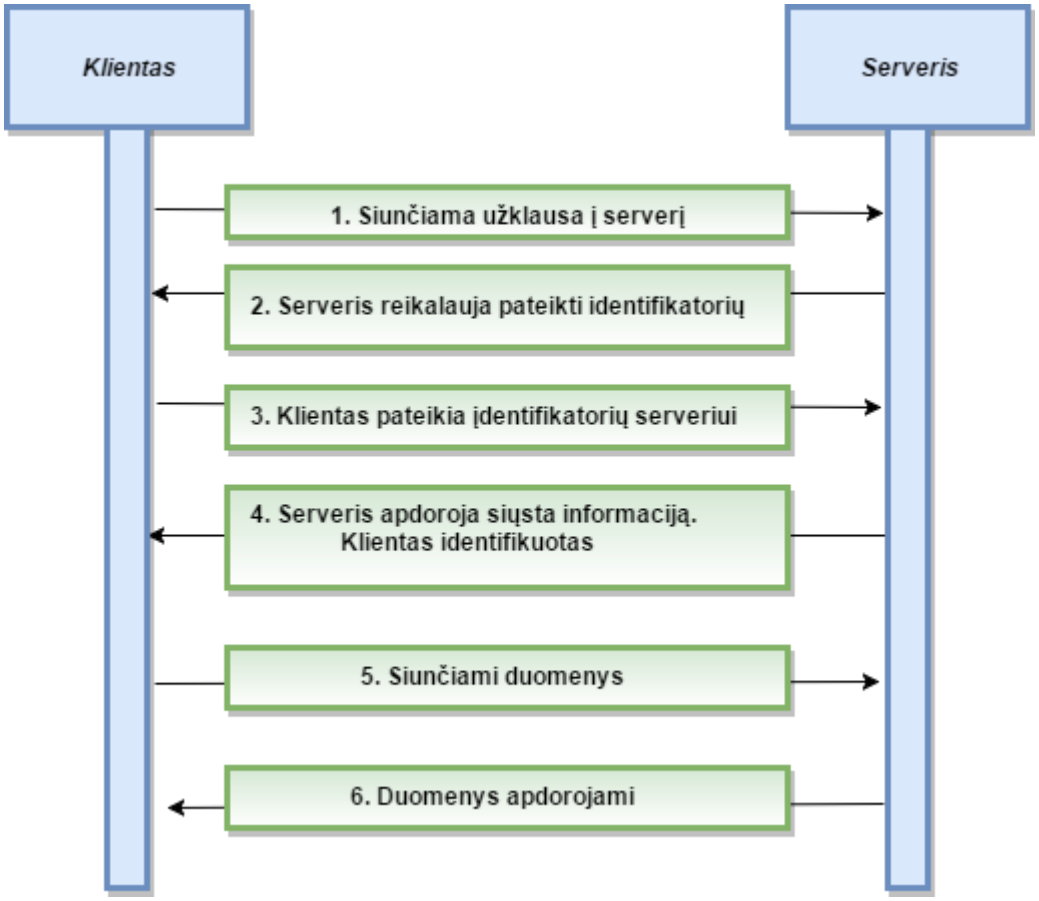
15 pav. Siūlomos objektų identifikavimo sistemos duomenų apsikeitimo formatas

Tenkinus identifikatoriaus reikalavimus informacija išskaidoma į kelis blokus t.y., indeksavimo ir duomenų tipo blokas, šiam blokui yra išskirti 7 baitai iš kurių 2 baitai apsprendžia kokia informacija atkeliauja (tarkim vartotojo V.Pavardė, koks daiktų interneto objektas komunikuoja, arba koks jutiklis ir kokia informaciją siunčia). Likę 5 baitai yra skirti informacijos ilgiui nustatyti. Trečiasis laukelis – duomenų laukelis. Šiame laukelyje talpinami realūs duomenys binariniu formatu. Papildomai naudojama „maiša“ duomenų identifikavimo apsunkinimui dėl to, kad įsilaužėlis negalėtų taip lengvai įsilaužti. 16 paveiksle pateikiamas realus objektų identifikavimo architektūros pavyzdys su realiais duomenimis.



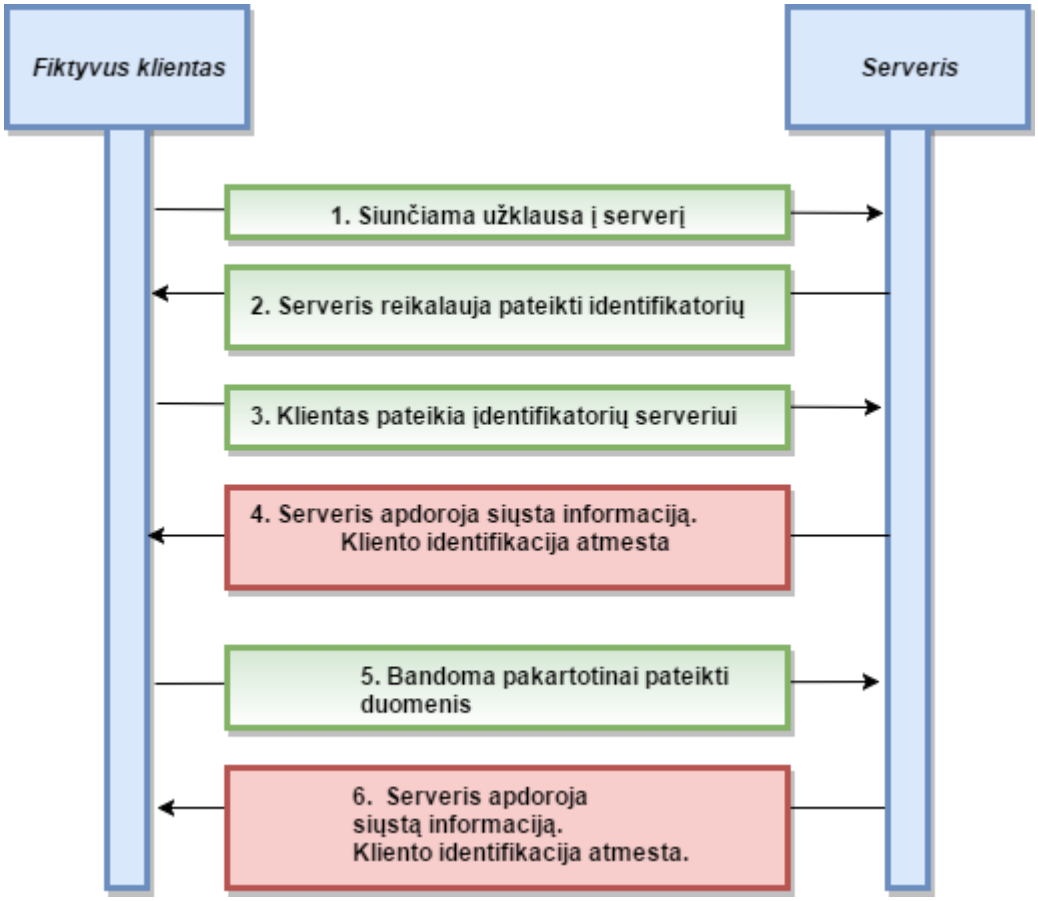
16 pav. Siūlomos objektų identifikavimo sistemos duomenų siuntimo formato pavyzdys

Objektų identifikavimo ir autentifikavimo procese svarbus veiksnys yra komandų vykdymo seka. Siekiant korektiškai identifikuoti objektą visų pirma yra svarbu užtikrinti, kad duomenys, kurie yra siunčiami atitinka duomenų siuntimo pagal pateiktą mechanizmą autentiškumą. 17 paveiksle pateikiamas komandos pranešimų siuntimo mechanizmas, kuomet objektų identifikavimo autentifikavimo procesas yra įvykdomas su objektais, kurie turi prieigą komunikuoti su serveriu.



17 pav. Pranešimų perdavimo mechanizmas

Komunikacijos užmezgimo principas yra paremtas kliento serverio pagrindu. Klientas, tai yra daiktų interneto objektas, kurio paskirtis yra atlikti kokia nors užduotį pvz., siųsti informacija apie kambaryje esančia temperatūrą. Tokiam objektui taikant pateiktą identifikavimo ir autentifikavimo metodą visų pirma reikia užmegzti komunikacijos sesiją su serveriu. Traktuojame, kad objektas, kuris siekia užmegzti sesiją yra identifikuotas sistemoje, t.y., jam yra suteiktas unikalus identifikatorius. Pirmas etapas iš kliento pusės yra siusti užklausą serveriui pateikiant supakuotą informacijos paketą, kuriame yra identifikatorius, kuris buvo suteiktas unikaliai šiam objektui bei komanda, kuri skirta užmegzti sesijai. Serveris gavęs duomenų paketą jį išpakuoja ir jeigu informacija yra teisinga jis gražina atsakymą objektui apie sėkmingai užmegzta sesiją su serveriu. Toliau yra siunčiamos atitinkamos komandos skirtos objekto valdymui. Komunikacija tarp serverio ir kliento užtikrina agentinės programos, kurių paskirtis yra užtikrinti korektišką duomenų srauto perėjimą tarp serverio ir kliento pusės bei savo paskirties užduočių vykdymą.

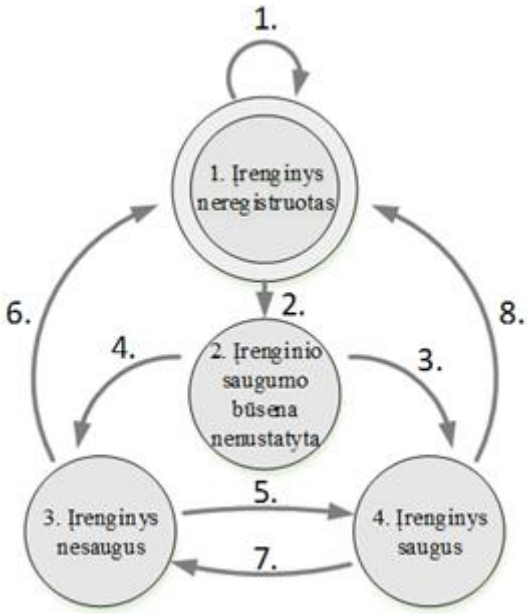


18 pav. Pranešimų perdavimo mechanizmas kai identifikavimas nesėkmingas

Pasitaikius atvejui, kuomet išprovokuojamas klaidingas sesijos užmezgimo pranešimas (18 pav.), tarkim kibernetinis įsilaužėlis bando patekti į sistemą serveris reikalauja pateikti unikalų objektui suteiktą identifikatorių. Tačiau objektui nesugebėjus to padaryti serveris po siųstos informacijos apdorojimo objekto užklausą atmeta.

5 lentelė. Objektų tarpusavio komunikacijos komandos

Komanda	Komandos kodas	Komandos veiksmas
Objekto registravimas	254050870001H04695214	Įregistruoti objektą į sistemą
Objekto išregistravimas	502H046952132	Išregistruoti objektą iš sistemos
Objekto identifikavimas	1043H04655214	Identifikuoti prisijungusį objektą
Objekto autentifikavimo pralaida	2321H04545214	Suteikti prieigą prisijungusiam objektui.
Objekto autentifikavimo atmetimas	873H046952414	Atmesti prieigą prisijungusiam objektui.
Objekto siunčiamos informacijos gavimas	1234H04697214	Priimti objekto siunčiamą informaciją.
Objekto siunčiamos informacijos siuntimas	973H04695914	Persiųsti objekto siunčiamą informaciją.



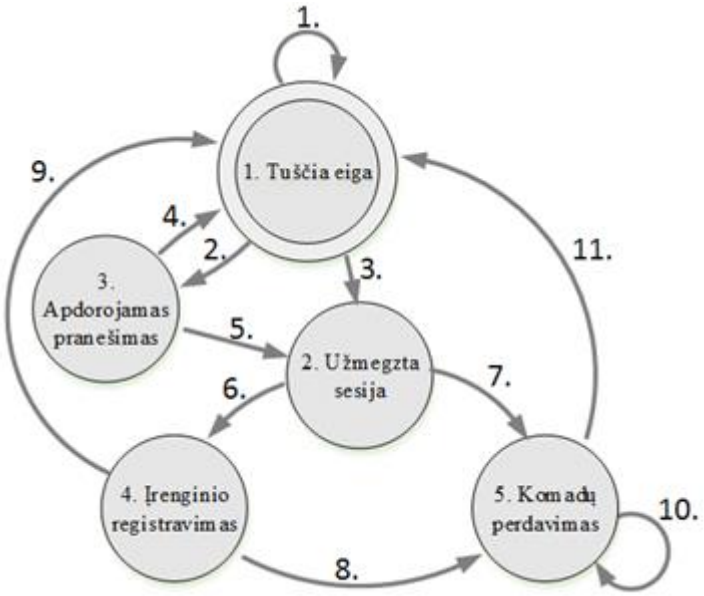
19 pav. Objektų identifikavimo ir autentifikavimo kliento dalies būsenų diagrama

19 paveiksle pateiktoje kliento komunikacijos būsenų diagramoje yra 4 esminės būsenos. Pati pirmoji ir paskutinioji būsenos atitinka įrenginio registracijos nebūvimo faktą. Į šią būsena patenka objektas tada, kai tuo metu jis neegzistuoja sistemoje ir negali komunikuoti su serveriu.

6 lentelė. Objektų identifikavimo ir autentifikavimo kliento dalies būsenų diagrama

Pokyčio Nr.	Dabartinė būsena	Pokytis	Sekanti būsena	Rezultatas
1.	Įrenginys neregistruotas	Įrenginio registracija nesėkminga.	Įrenginys neregistruojamas į sistemą	-
2.		Įrenginio registracija sėkminga	Įrenginys įtrauktas į sistemą	-
3.	Įrenginio saugumo būsena nenustatyta	Įrenginio konfigūracijų patikra. Reikalavimai tinkami	Įrenginys saugus	Dirbti su įrenginiu leidžiama
4.		Įrenginio konfigūracijų patikra. Reikalavimai netinkami	Įrenginys atmetamas, išregistruojamas	Darbas su įrenginiu neleidžiamas, įrenginys pašalinamas
5.	Įrenginio neidentifikuotas (nesaugus)	Įrenginio konfigūracijų patikra.	Įrenginys saugus	Dirbti su įrenginiu leidžiama

		Reikalavimai tinkami		
6.		Įrenginys pašalinamas iš sistemos	Įrenginys neregistruotas sistemoje	Darbo su įrenginiu pabaiga
7.	Įrenginys identifikuotas (saugus)	Įrenginio konfigūracijų patikra. Reikalavimai tinkami	Įrenginys atmetamas	Darbas su įrenginiu neleidžiamas
8.		Įrenginys pašalinamas iš sistemos	Įrenginys atmetamas	Darbo su įrenginiu pabaiga



20 pav. Objektų identifikavimo ir autentifikavimo serverio dalies būsenų diagrama

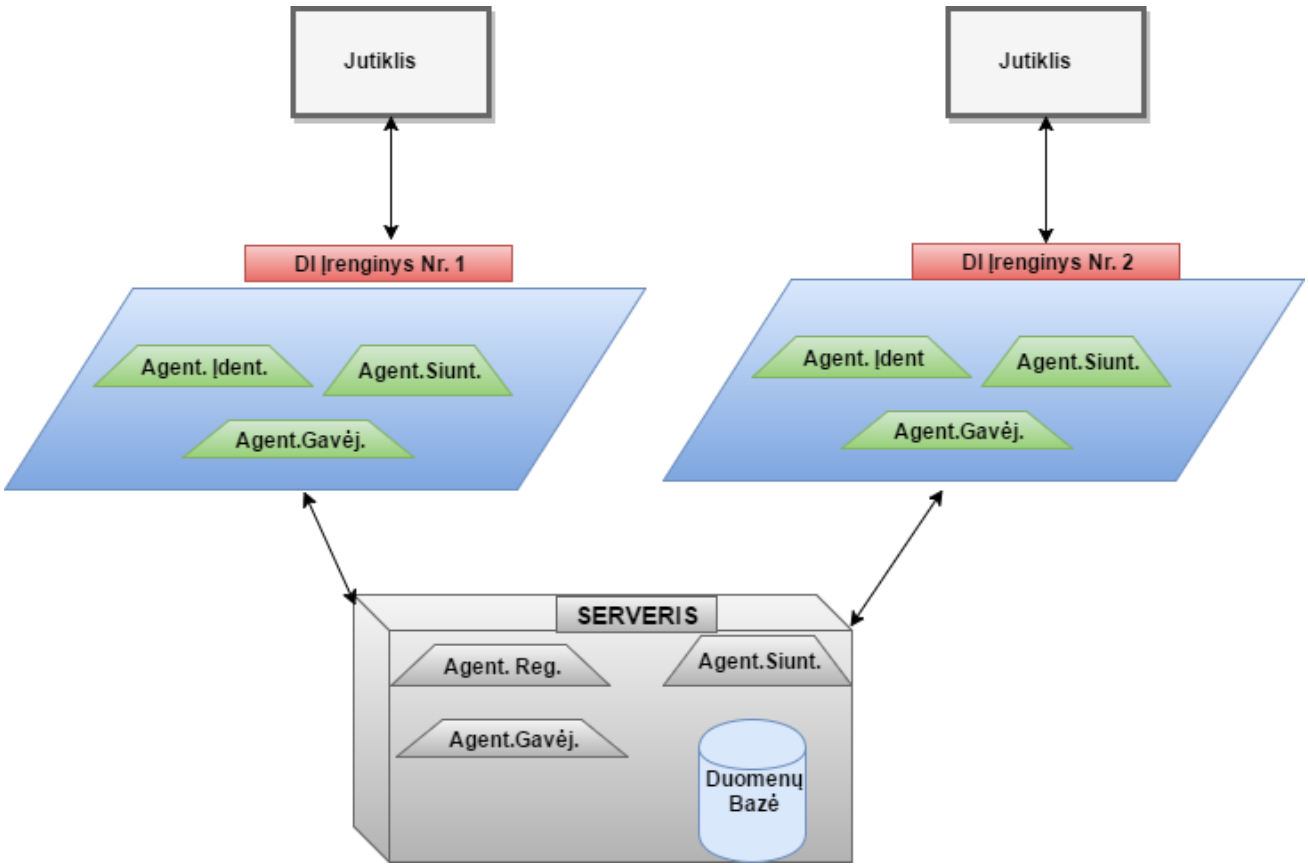
20 paveiksle pateikta objektų identifikavimo ir autentifikavimo serverio dalies būsenų diagrama susideda iš 5 būsenų į kurias serveris gali patekti. Pirmoji ir paskutinė būsena tai tuščia eiga. Į šią būseną serveris gali patekti tada, kai negavo užklausos iš kliento pusės su identifikavimo užklausa.

7 lentelė. Objektų identifikavimo ir autentifikavimo serverio dalies būsenų diagrama

Pokyčio Nr.	Dabartinė būsena	Pokytis	Sekanti būsena	Rezultatas
1.	Tuščia eiga	-	Tuščia eiga	-
2.		Suformuojamas pranešimas iš kliento pusės serveriui	Serveris apdoroja siųsta pranešimą	Pranešimas identifikuojamas
3.		Serveris siunčia atsakymą klientui	Klientas gauna siųstą pranešimą	-
4.		Objektas bando sudaryti sesiją su serveriu	Serveris apdoroja informaciją	Identifikuojamas ir autentifikuojamas įrenginys – sudaryta sesija.
5.	Pranešimų apdorojimas	Sesija sudaryta nesėkmingai	Tuščia eiga	-
6.		Sesija sudaryta sėkmingai	Užmezgama sesija	Identifikuojamas ir autentifikuojamas įrenginys – sudaryta sesija.
7.	Užmegzta komunikacijos sesija	Suformuojama sesija su kliento dalimi	Objekto registracija	Atliekamas objekto registravimas / išregistravimas
8.		Perduodamos agentų valdymo komandos	Komandų perdavimas agentams	Valdomas objektas
9.	Objekto registracija	Perduodamos valdymo komandos agentinėms programoms	Komandų perdavimas	Valdomas objektas
10.		Objekto registracijos pabaiga	Tuščia eiga	-
11.	Komandų perdavimas	Perduodamos sekančios valdymo komandos agentinėms programoms	Komandų perdavimas	Valdomas objektas
12.		Sesijos pabaiga	Tuščia eiga	-

2.5. Programinės ir techninės įrangos projektas

Sudaroma komponentų techninės ir programinės įrangos struktūra (21 pav.).



21 pav. Programinės įrangos komponentų diagrama

Programinė įranga susideda iš dviejų dalių. Pirmoji yra serverio programinė įranga. Sudedamosios dalys:

- **Duomenų bazė** – kuriamos sistemos duomenų bazė;
- **Agentas** – Agentinė programa (siuntėjas, gavėjas, registratorius, identifikatorius) (Pagal užduoties pasirinkimą:
  - agentas siuntėjas;
  - agentas gavėjas;
  - agentas registratorius;
  - agentas identifikatorius;

Agentų siuntėjo paskirtis yra išsiusti duomenis gavėjo programai supakuotus bei užšifruotus.

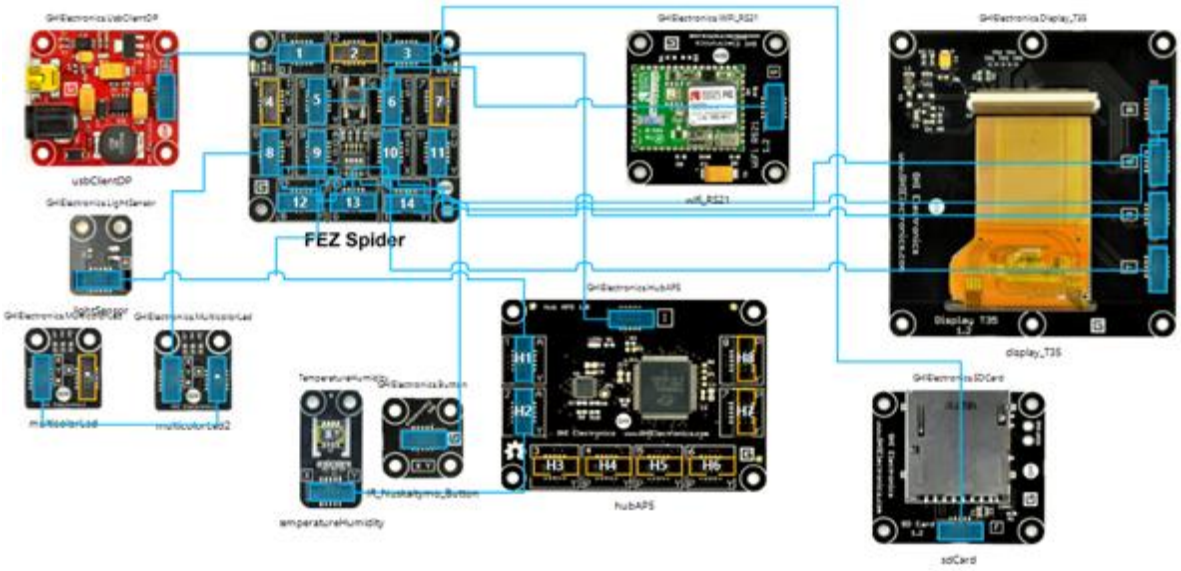
Agentų gavėjo paskirtis yra pasiimti užšifruotus duomenis iš agentų siuntėjo komandos, minėtus duomenis.

Agento identifikatoriaus užduotis yra iš gavėjo programos gautus supakuotus duomenis išsišifruoti ir identifikuoti objektą. Jeigu objektas teisėtas – praleisti siunčiamus duomenis. Jeigu objektas neteisėtas t.y., neatitinka objektų įidentifikavimo algoritmo tuomet identifikavimo programa

siunčia informacija siuntėjo programai, kuri kreipiasi į registravimo programą ir toks objektas yra pašalinamas arba suspenduojamas iš sistemos.

Agentinės programos tarpusavyje sąveikauja siųsdamos gautą informaciją ir į ją reaguodamos. Veikimo principas paremtas šiais aspektais. Agentas identifikatorius autentifikuoja objektus, kurie bando jungtis į sistemą, jeigu objektas yra netikras t.y., atsiųsta informacija netenkina minėtos objektų autentifikavimo architektūros yra siunčiamas atsakymas agento registratoriaus programai, kurios paskirtis yra uždrausti prieigą minėtam objektui. Agentinės siuntėjo programos užduotis yra supakuoti duomenis pagal minėta metodiką iš kelintinės pusės, tuomet agentas gavėjas privalo priimti duomenis iš siuntėjo, juos išpakuoti ir jeigu minėti duomenys yra teisingi įrašyti į duomenų bazę.

Techninės įrangos komponentų sujungimo schema parodyta 22 paveiksle.



22 pav. Techninės įrangos komponentų jungimo schema

2.6. Išvados

Daugybė daiktų interneto objektų šiandien pasaulyje yra sujungti į tinklą. Tačiau vyrauja problemos susijusios su daiktų interneto objektais. Svarbiausia dalis yra ta, kad kaip galima pasitikėti objektų, kaip įsitikinti, kad informacija, kuri ateina iš jutiklio pusės yra teisinga ir nepakeista. To galima pasiekti realizuojant objektų identifikavimo agentinę sistemą, kuri susideda iš keturių agentinių sistemų – agentas registratorius, agentas gavėjas, agentas siuntėjas ir agentas identifikatorius. Agento registratorius - paskirtis atlikti daiktų interneto objektų registravimą.

Objektų identifikavimo modelyje yra siekiama sutalpinti informacijos tiek apie patį vartotoją, kuris naudojasi Sistema, tiek apie pačius įrenginius, kurie komunikuoja tarpusavyje iš kliento ir serverio pusės. Kiekvienas įrenginys (kontroleris) turi gauti iš serverio pusės jam unikalų identifikatorių. Tiek pats įrenginys (kontroleris) tiek prie jo prijungti jutikliai yra identifikuojami naudojant jiems priskirtus identifikatorius. Metodo principas remiasi tuo, kad pranešimo pirmieji baitai yra identifikatoriai, jie apsprendžia ar gauta informacija yra autentiška (pvz., ar ji atitinka tolimesnius apspręstus įrenginių identifikavimo rėžius). Jeigu informacija, kuri atkeliavo neatitinka identifikatoriaus reikalavimų (pvz., įsilaužėlis bando siųsti savo fiktyvią informaciją) ji yra atmetama.

Komunikacijos užmezgimo principas yra paremtas kliento serverio pagrindu. Klientas, tai yra daiktų interneto objektas, kurio paskirtis yra atlikti kokia nors užduotį pvz., siųsti informacija apie kambaryje esančia temperatūrą. Tokiam objektui taikant pateiktą identifikavimo ir autentifikavimo

metodą visų pirma reikia užmegzti komunikacijos sesiją su serveriu. Traktuojame, kad objektas, kuris siekia užmegzti sesiją yra identifikuotas sistemoje, t.y., jam yra suteiktas unikalus identifikatorius. Pirmas etapas iš kliento pusės yra siusti užklausą serveriui pateikiant supakuotą informacijos paketą, kuriame yra identifikatorius, kuris buvo suteiktas unikaliai šiam objektui bei komanda, kuri skirta užmegzti sesijai. Serveris gavęs duomenų paketą jį išpakuoja ir jeigu informacija yra teisinga jis gražina atsakymą objektui apie sėkmingai užmegzta sesiją su serveriu. Toliau yra siunčiamos atitinkamos komandos skirtos objekto valdymui. Komunikacija tarp serverio ir kliento užtikrina agentinės programos, kurių paskirtis yra užtikrinti korektišką duomenų srauto perėjimą tarp serverio ir kliento pusės bei savo paskirties užduočių vykdymą.

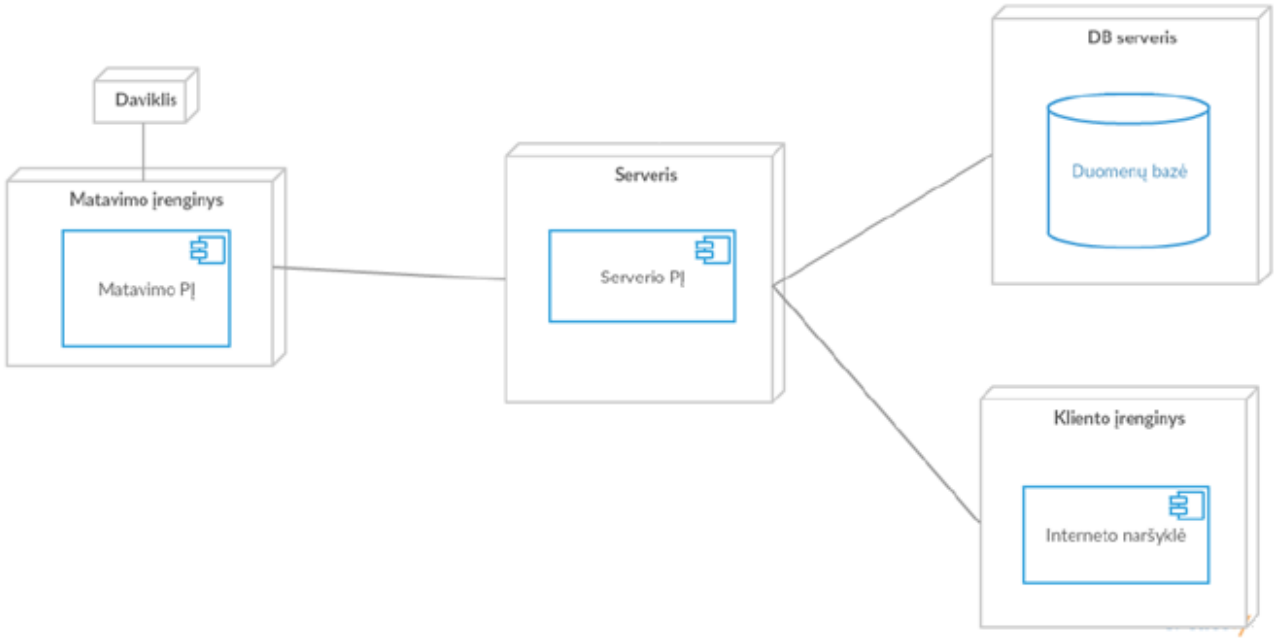
3. DAIKTŲ INTERNETO OBJEKTŲ IDENTIFIKAVIMO PROGRAMINIAME LYGMENYJE SISTEMOS PROTOTIPAS

Projektas yra tradicinė tinkline programa, kuri realizuota naudojant kliento serverio architektūrą. Tinklinė taikomoji programa yra sudaryta iš dviejų dalių: kliento dalies ir serverio dalies, realizuojamos atitinkamuose kliento ir serverio procesuose. Ryšiai tarp kliento ir serverio procesų yra nusakomi tam specifiniu taikomuoju protokolu, kuris numato taisykles, kokia tvarka vyks bendravimas tarp procesų ir skleis šifruotą informaciją tarp kliento ir serverio dalių, apibrėžiant komunikavimo sintaksę bei semantiką. Pati taikomoji programa nusako klientų procesų ir serverio proceso komunikavimo tikslus.

Sistemą (23 pav.) sudaro matavimo įrenginys, kuris siunčia matavimo rezultatus į serverį, naudodamasis šifruojamu protokolu. Duomenų perdavimui yra naudojamas JSON formatas, kuris papildomai yra užšifruotas pagal esamą algoritmą. Serveris apdoroja priimtą pranešimą ir išsaugo gautus duomenis duomenų bazėje. Internetinis puslapis siunčia užklausą serveriui ir gauną atsakymą, kurį privalo iššifruoti siekiant išgauti informaciją apie matavimo rezultatus tam tikru laiko momentu.

Tinklinė taikomoji programa yra sudaryta iš trijų pagrindinių dalių(sluoksnių): vartotojo sąsajos, verslo logikos ir duomenų. Kiekvienas lygis yra griežtai atskirtas nuo kito ir žino tik apie jam gretimo lygio egzistavimą.

3.1.1. Programinės įrangos komponentai.

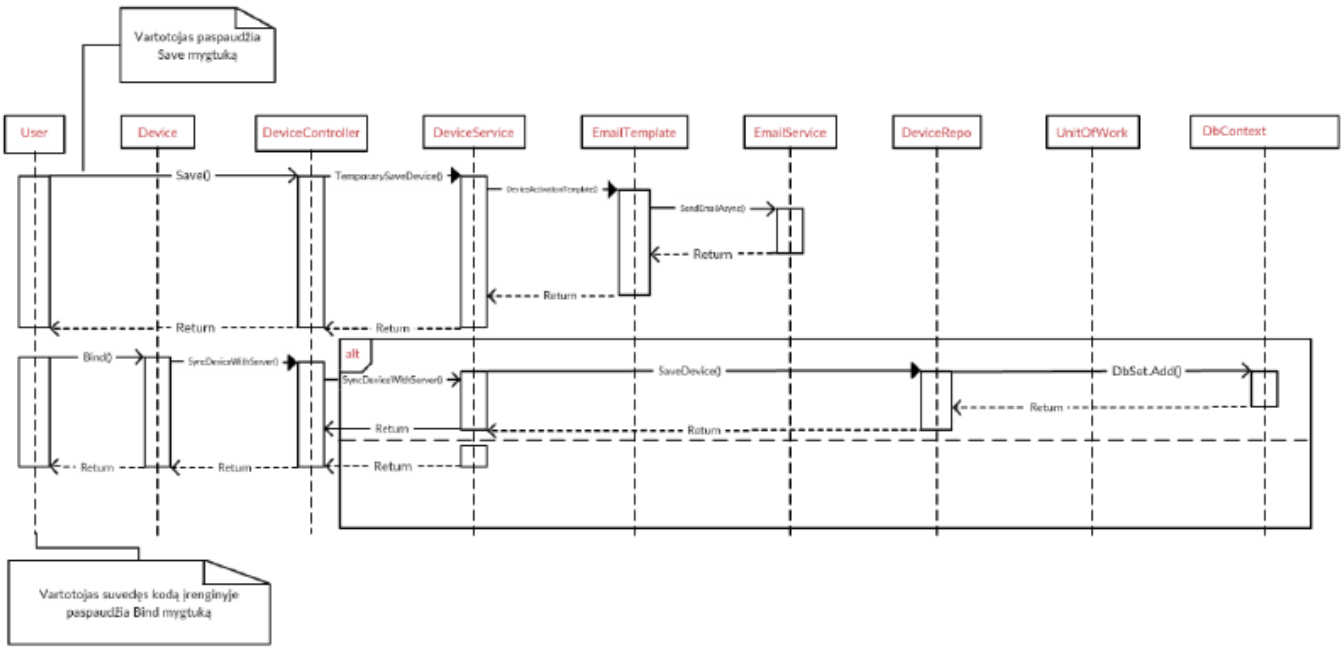


23 pav. Sistemos PĮ įrangos architektūra

Pagrindiniai sistemos programinės įrangos komponentas pavaizduoti 23 paveiksle Sistemos programinę įrangą sudaro:

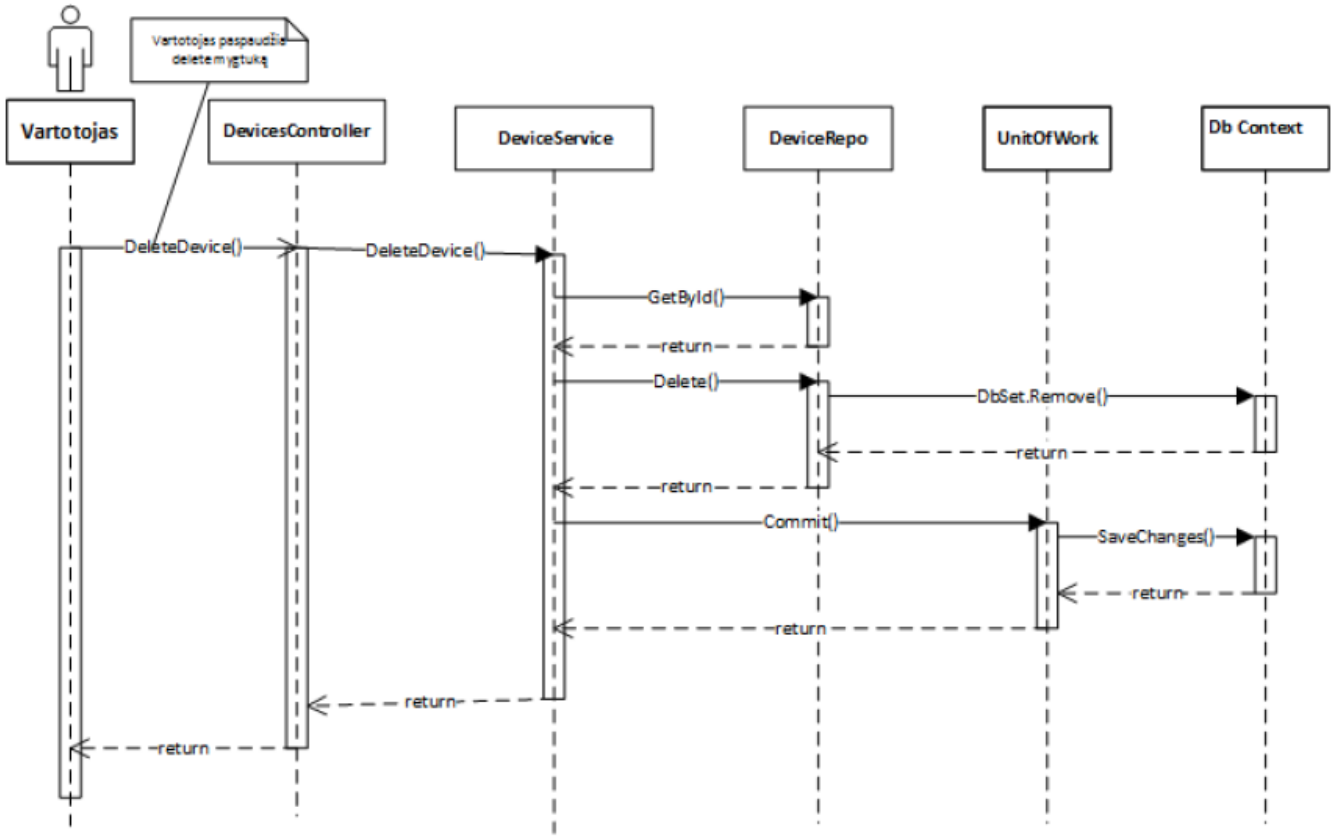
- serverio programinė įranga, kuri priima užklausas;
- kliento (matavimo įrenginio) programinė įranga, kuri siunčia matavimų davinius;
- duomenų bazių valdymo sistema, kuri atsakinga už duomenų saugojimą ir tiekimą duomenų bazėje;
- vartotojo įrenginyje esanti interneto naršyklė, per kurią jis prisijungia prie sistemos valdymo skydo;

Šiame projekte realizuota serverio ir kliento programinė įranga. Žemiau pateikta serverio programinės įrangos sistemos sekų diagrama (24 pav.).



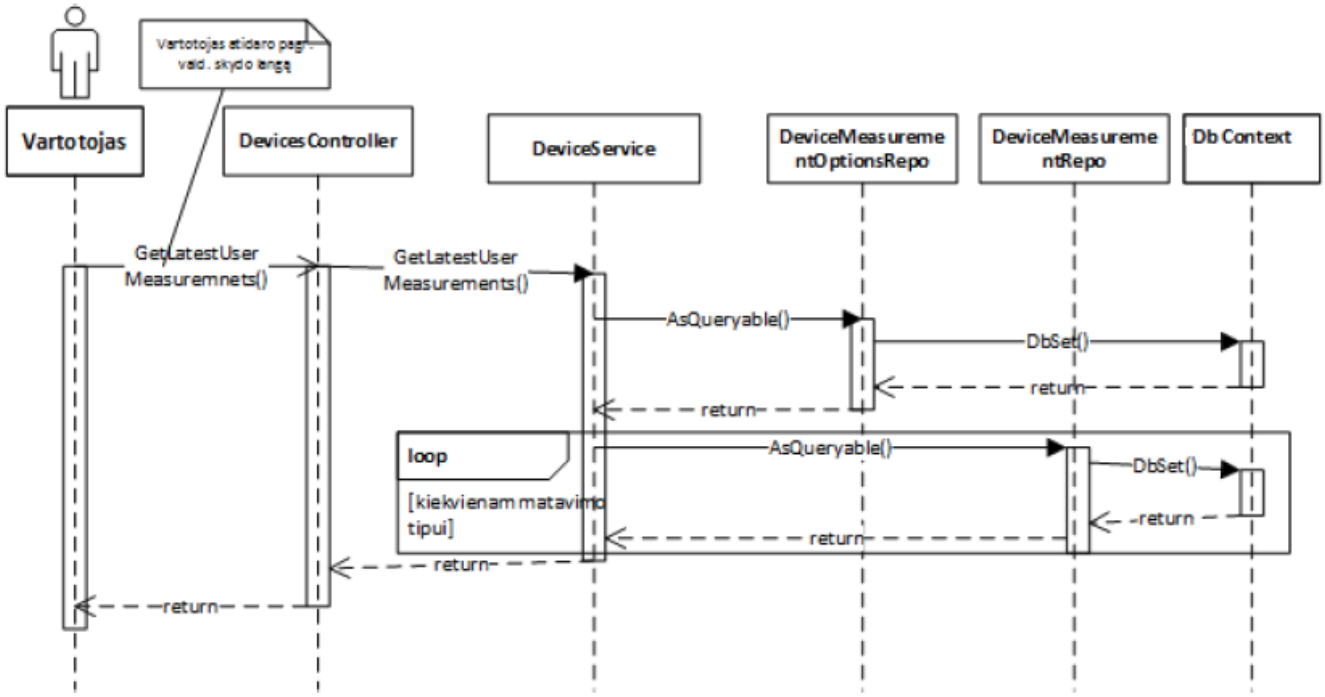
24 pav. Sekų diagrama naujo objekto susiejimui su paskyra

Remiantis pateiktu objektų susiejimo su paskyra sekų diagramos modeliu visų pirma vartotojas siunčia užklausą į objektą, kuris savo paskirtimi suformuluoja komandų seką, kuri turi būti perduodama minėto objekto kontroliniam valdymo blokui. Minėtasis valdymo bloke yra patikrinama, ar toks objektas, kurį bandoma susieti su paskyra nėra jau užregistruotas. Jeigu patikra įvyksta teisingai, tuomet programa kreipiasi į *EmailService* paprograme, kuri siunčia vartotojui papildoma autentifikavimo užklausą, kuria vartotojas turi patvirtinti, siekiant pakartotinai patikrinti, ar veiksmas, kurį vartotojas bando atlikti yra teisingas. Jeigu užklausa yra įvykdyta teisingai, tuomet objektas yra susiejamas su minėta vartotojo paskyra. Jeigu užklausa buvo įvykdyta neteisingai, tarkim tai bandė atlikti kenkėjas, užklausa yra atmeta ir nevykdoma. Apie tai yra informuojamas vartotojas, ir užfiksuojamas minėtas faktas sistemoje. Susiejant paskyrą su objektu trivialus dalykas yra gebėti objektą atskirti nuo paskyros. 25 paveiksle pateikta objekto atsiejimo nuo paskyros diagrama, kuri paremta panašiu principu, kaip ir susiejimas, tačiau veikimo principas dalinai skiriasi.



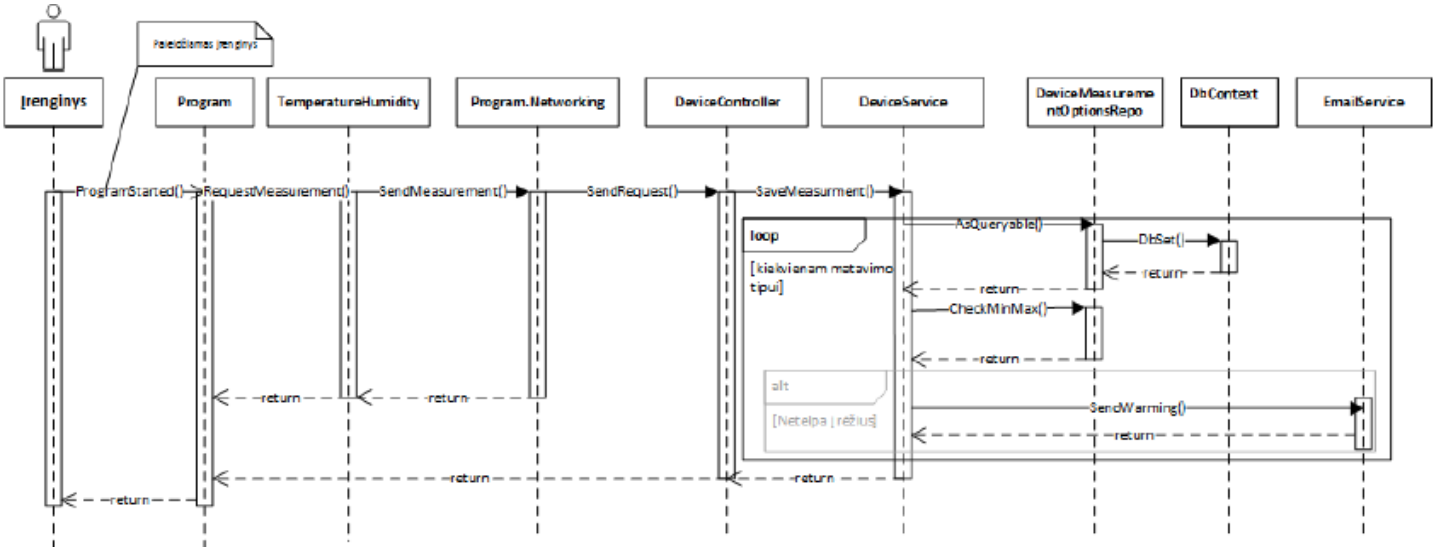
25 pav. Sekų diagrama objekto atsiejimui nuo paskyros iš valdymo skydo

Vartotojas siekiantis pašalinti objektą iš savo paskyroje esančios objektų grupės visų pirma siunčia komandų seką (užklausą) objektų valdymo paprogramei. Minėtas komponentas patikrina gautą informaciją iš kliento pusės ir tada siunčia užklausa į objekto serviso dalinį. Tuomet yra tikrinama ar toks objektas egzistuoja, ir kokia dalį jis užima vartotojo profilyje. Tarkim ganėtinai globalus pavyzdys būtų temperatūros duomenų siuntimo programa. Minėto objekto paskirties duomenys yra surenkami iš duomenų bazės persiunčiami vartotojui ir atvaizduojami grafinėje sąsajoje. Vartotojas gauna pranešimą apie sėkmingai ištrintą objektą ir jo sukauptu duomenų grupę. Priešingų atveju, kada užklausa bando įvykdyti neautentifikuotas vartotojas ir arba objektas, objektų valdymo kontroleris pertikrinęs siunčiamą užklausą atmeta ir informuoja vartotoja, kad prieiga nėra autorizuota.



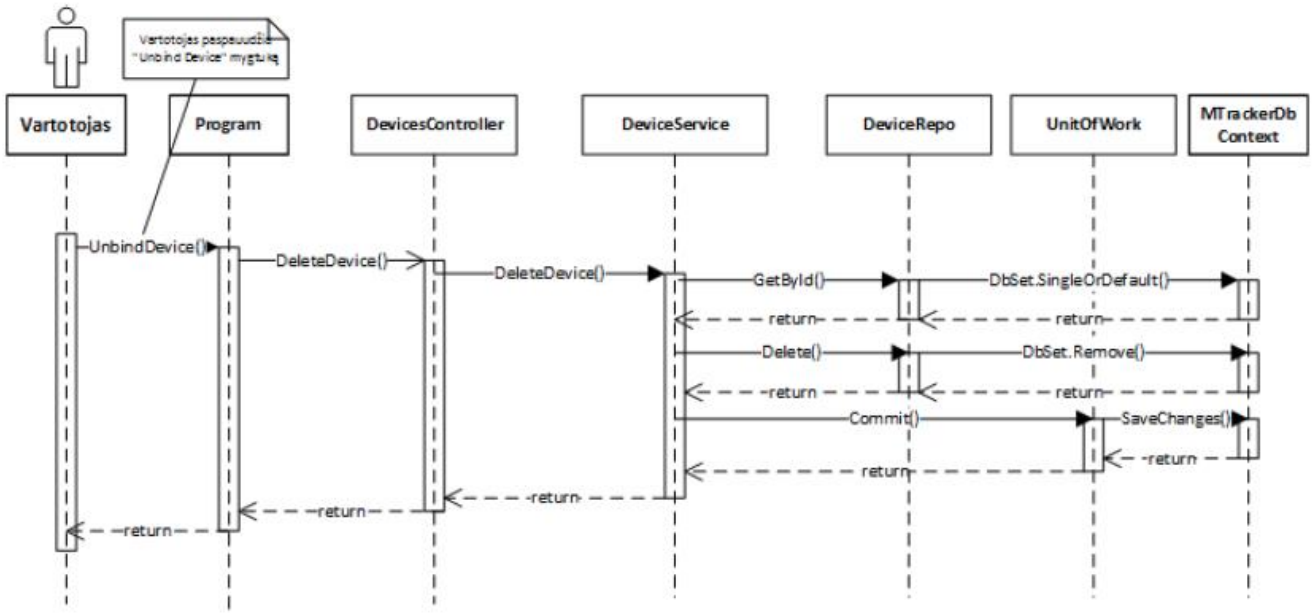
26 pav. Sekų diagrama naujausiems matuojamų dydžių rodmenims gauti

Turint tinkamą susietų objektų grupė yra svarbu išlaikyti tinkamą duomenų apsikeitimo mechanizmą. Svarbus uždavinys yra užtikrinti duomenų integralumą t.y., ar duomenys, kurie atkeliauja iš kelintinės pusės į serverį yra patikimi ir atitinkantys realybę. Pateikta sekų diagrama (26 pav.), skirta atvaizduoti naujų matuojamų dydžiu rodmenų atvaizdavimą atspindi šią veiksmų seką. Pirma vartotojas suformavęs reikiamą komandinę užklausą ja išsiuntęs kreipiasi į objektų valdymo paprogramę. Minėta paprogramė siunčia užklausą į kelintinę dalį. Kelintinėje dalyje minėta užklausa yra apdorojama objektų serviso dalies, kuri yra atsakinga nuolatos tikrinti gaunamų bei siunčiamų duomenų srautus, ir juos pateikti vartotojui.



27 pav. Sekų diagrama periodiniam davinių siuntimui į serverį

Gavus minėtą užklausą iš kelintinės pusės yra prašoma pateikti duomenų grupė (tarkim dabartinius temperatūros daviklio duomenis) minėti duomenis yra suformuojama į atitinkamą duomenų paketą, kuris yra užšifruojamas ir išsiunčiamas, apdoroti serverio dalies programai. Išpakavus persiųstus duomenis jie yra gražinami vartotojui. Analogiškai serveris persiunčia pakartotinę užklausą kelintiniai daliai, kad duomenys buvo persiųsti teisingai, ir procedūra yra kartojama iš naujo, kad išliktu duomenų persiuntimo naujumas.



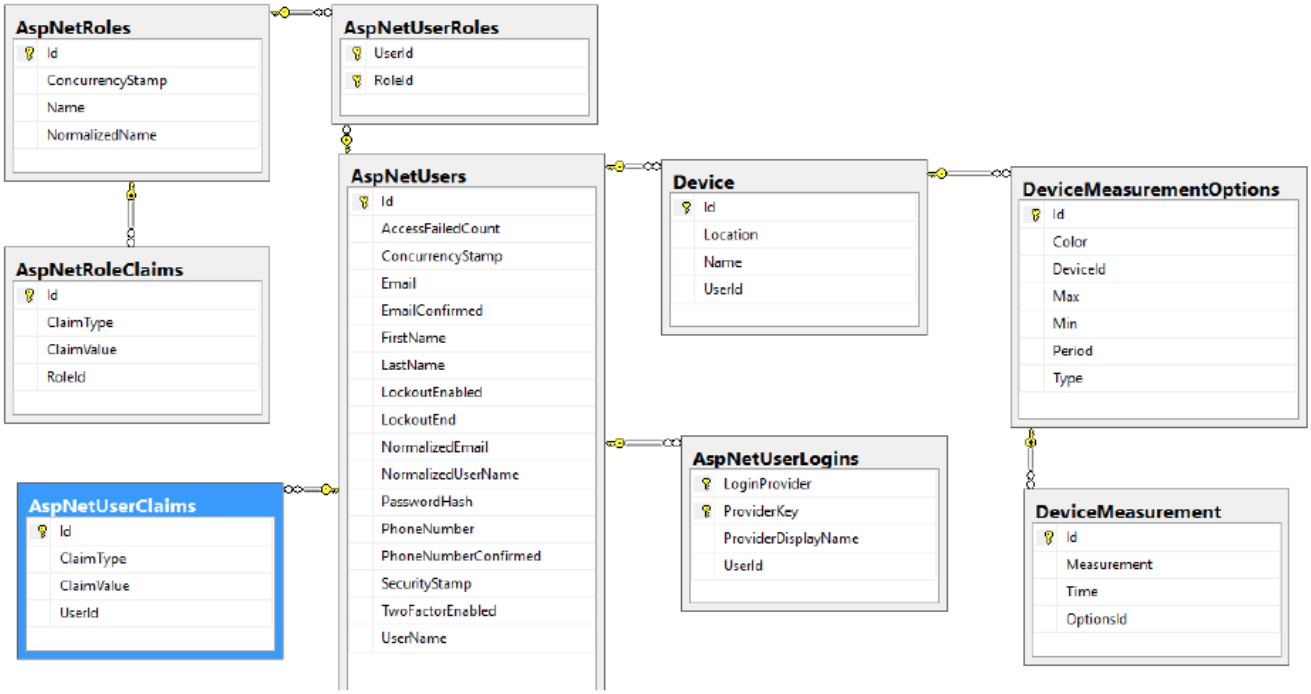
28 pav. Sekų diagrama objekto atsiejimui nuo paskyros

Vartotojas gali atsieti objektą nuo savo paskyros pasinaudodamas įrenginyje įmontuotu lietimams jautrų ekraną. Minėtame ekrane gali būti pasirenkama meniu opcija „Įrenginio atsiejimas“. Pasirinkus

minėtą opciją yra siunčia užklausa iš vartotojo pusės (paspaudžiamas mygtukas) suformuluojama komanda (28 pav.). Minėta komanda yra užšifruojama ir siunčiama į serverį. Serveris identifikavęs objektą papildomai dėl patikros suformuoja 12 skaitmenų kodą, ir jį atvaizduoja vartotojo ekrane (naršyklėje). Pateikus minėtą kodą įrenginiui (jį suvedus) įrenginys yra atsiejamas nuo paskyros ir gali būti pakartotinai priskiriamas iš naujo tai pačiai, arba kitai vartotojo paskyrai ir būti naudojamas.

3.1.2. Programinės įrangos duomenų bazės struktūra

Duomenims saugoti pasirinkta naudoti reliacinę duomenų bazę. Jos schema pateikta 29 paveiksle.



29 pav. Programinės įrangos duomenų bazės struktūra

Pagrindinės duomenų bazės lentelės yra:

- Device – tai lentelė, kurioje saugome vartotojo įrenginius;
- DeviceMeasurementOptions – tai lentelė, kurioje saugome įrenginio matuojamų dydžių aprašus pvz., kokio tipo duomenys iš objekto keliaus į serverį;
- DeviceMeasurement – tai lentelė, kurioje saugome matavimų duomenys.
- AspNetUser – lentelė, kurioje saugomi sistemos vartotojai.
- AspNetUserLogins lentelė saugo vartotojų prisijungimus
- AspNetRoles lentelė saugo galimas vartotojų roles
- AspNetUserRoles – sąryšio lentelė, sauganti kiekvienam vartotojui priskirtas roles
- AspNetUserClaims ir AspNetRoleClaims lentelės skirtos papildomai autentifikuoti vartotojus ar vartotojų grupes.

3.2. Prototipo išvados:

- Projektas yra tradicinė tinkline programa, kuri realizuota naudojant kliento serverio architektūrą. Tinklinė taikomoji programa yra sudaryta iš dviejų dalių: kliento dalies ir serverio dalies, realizuojamos atitinkamuose kliento ir serverio procesuose. Ryšiai tarp kliento ir serverio procesų yra nusakomi tam specifiniu taikomuoju protokolu, kuris numato taisykles, kokia tvarka vyks bendravimas tarp procesų ir skleis šifruotą informaciją tarp kliento ir serverio dalių, apibrėžiant komunikavimo sintaksę bei semantiką.
- Pateiktos objektų identifikavimo ir autentifikavimo prototipo komponentų, sekų, diagramos, komponentų tarpusavio komunikacijos dėsningumas bei operacijų vykdymo seka.
- Pateikta duomenų bazės lentelių struktūra bei sąryšiai tarp lentelių. Detalizuota kiekvienos lentelės paskirtis bei taikymas serverio aplinkoje.

4. DAIKTŲ INTERNETO OBJEKTŲ IDENTIFIKAVIMO SISTEMOS PROTOTIPO TYRIMAS

Remiantis pagal realizuotą Daiktų Interneto Objektų Identifikavimo metodų programiniame lygmenyje modelio prototipą aprašomas atliktas tyrimas:
Tyrimo metu naudota techninė įranga:

- Stacionarus kompiuteris DELL
- Mikrokompiuteris FezSpider
- Maršrutizatorius RB751G-2HnD

Naudota programinė įranga:

- Microsoft Visual Studio 2017 Professional
- Wireshark
- HTTP Analyzer
- AxCrypt Premium
- .NetMicroFrameWork SDK
- GLIDE 2.3

8 lentelė. Tyrimo metu naudotos techninės įrangos detali specifikacija. Kompiuteris DELL.

Stacionarus kompiuteris DELL	
Procesorius	Intel Core i5-3470 3.20 GHz
Operatyvioji atmintis	8 GB DDR3 1600 MHz
Kietasis diskas	512 GB Kingston SSD
	6 TB WD RED HDD
Grafinė plokštė	Radeon ROG Strix RX 580
Tinklo plokštė	4World PCI 10/100 BaseTX (RJ45) chipset Realtek
Operacinė sistema	Windows 10 64-bit

9 lentelė. Tyrimo metu naudotos techninės įrangos detali specifikacija. FEZ Spider mikrokompiuteris.

FEZ Spider mikrokompiuteris	
Procesorius	72MHz. 32-bit ARM7
Operatyvioji atmintis	11 MB
Flash atmintis	2.8 MB
Tinklo plokštė	Wi-Fi 802.11 a/b/g/n
Sistema	.NET Microframework

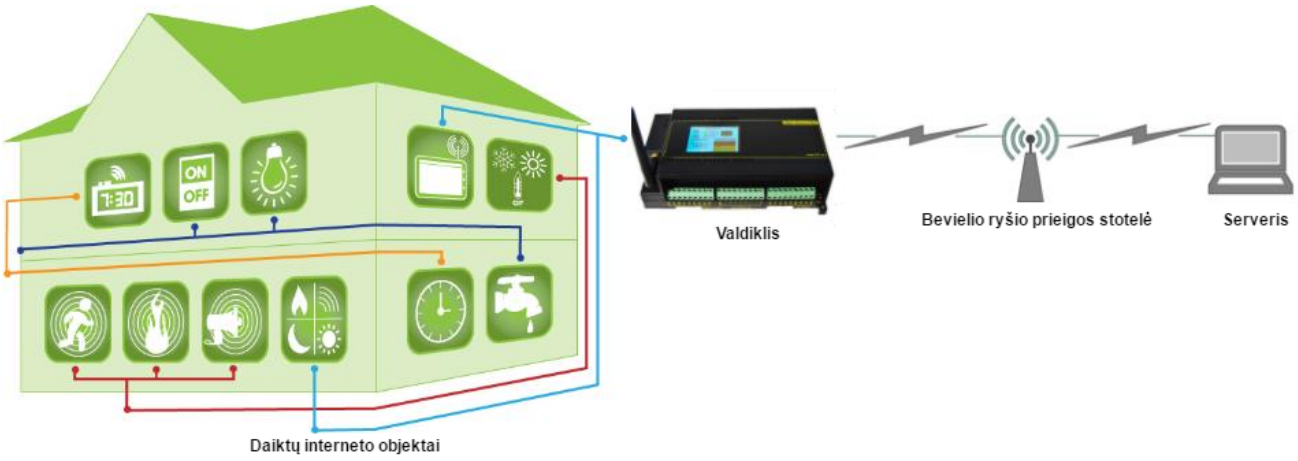
10 lentelė. Tyrimo metu naudotos techninės įrangos detali specifikacija. Maršrutizatorius RB751G-2HnD.

Maršrutizatorius RB751G-2HnD	
Standartas	Wi-Fi 802.11 a/b/g/n
Perdavimo greitis	280 Mb/s
Dažnių juosta	2.4 GHz
Apsaugos protokolas	WPA2

Matavimo įrenginio realizacijai buvo naudojamas .NET Gadgeteer įrenginys. Prie jo buvo prijungtas temperatūros ir drėgmės jutiklis bei bevielio Wi-Fi ryšio modulis.

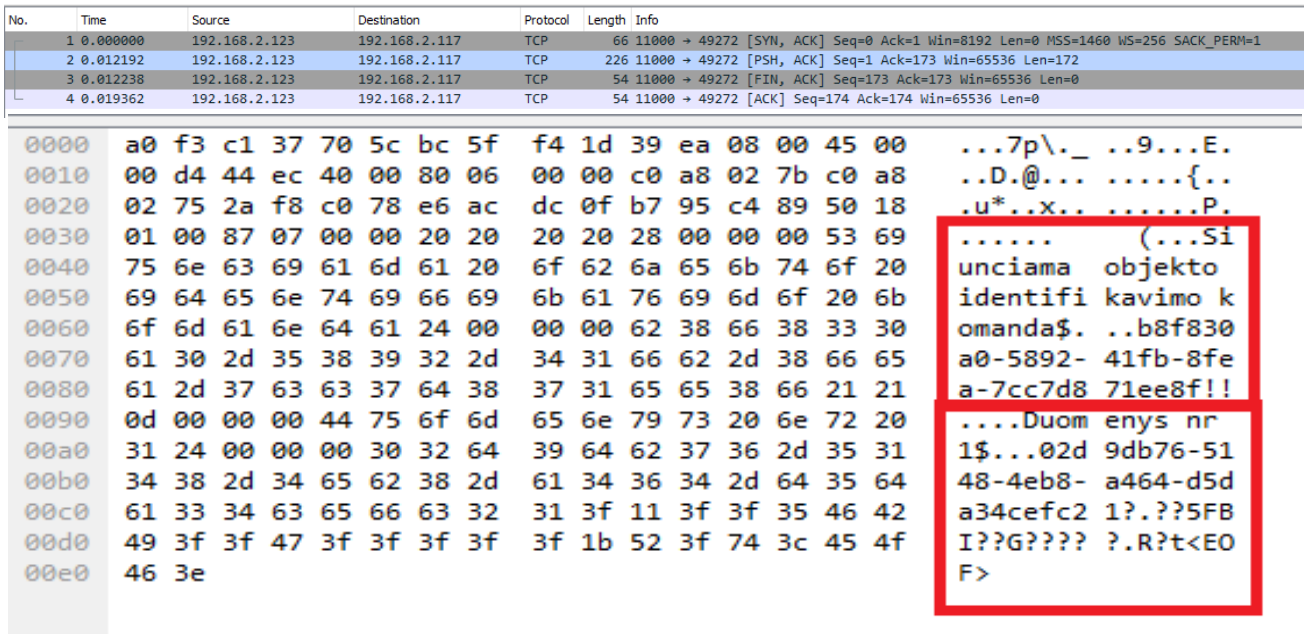
Siekiant įsitikinti ar programinė įranga atitinka konkrečius jai keliamus reikalavimus, ar atitinka savo paskirtį, turi būti atliktas sistemos prototipo testavimas. Programinės įrangos testavimas apima priemones, skirtas programinės įrangos kokybei įvertinti ir užtikrinti bei leidžia išsiaiškinti programinės įrangos defektus. Sistemos testavimui parinkti vienetų testai, nes jie leidžia testuoti tam tikrus programos modulius atskirai. Sistemos testavimui automatizuoti panaudota xUnit biblioteką. Kiekvienam testui yra sukuriama standartinė sistemos pradinė situacija, paduodami įvairūs duomenys ir kviečiami metodai. Gauti rezultatai tikrinami su tikėtinais ir taip stebima, ar sistema veikia korektiškai.

Pagrindinis sistemos servisas yra atsakingas už įrankio, siunčiančio matavimo duomenis, darbą. Pirmasis testas tikrina, ar naujas įrenginys gali būti pridėtas į sistemą.



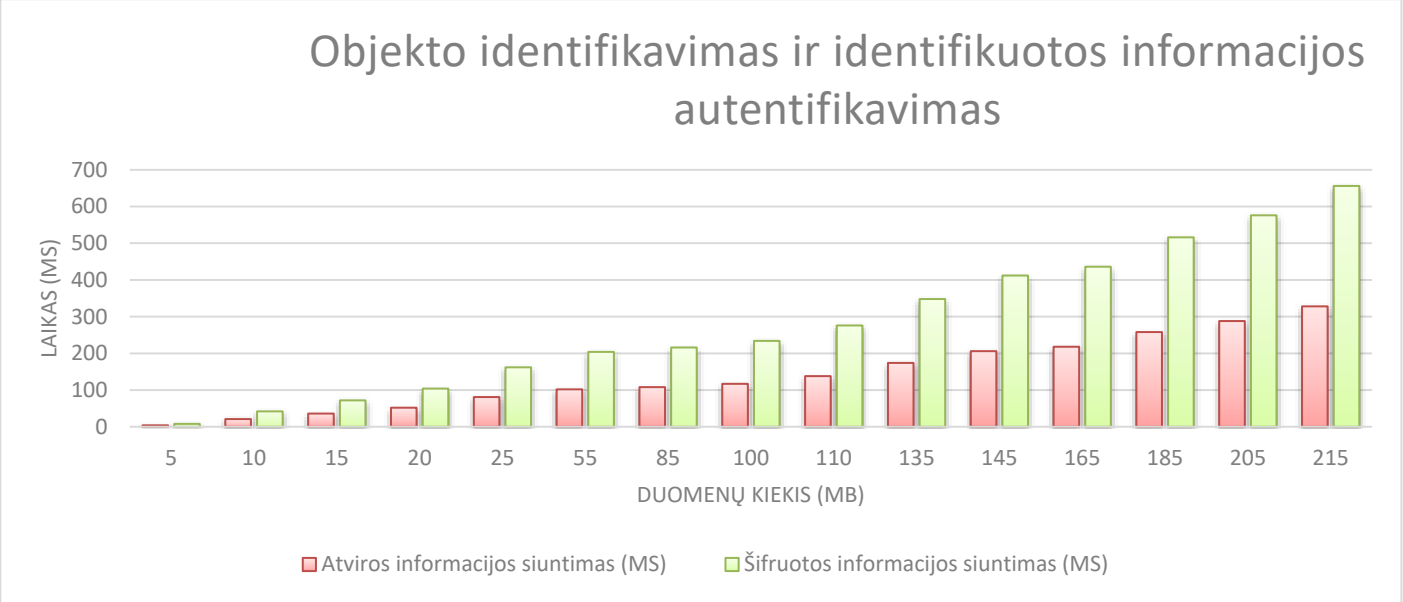
31 pav. Eksperimento vykdymo schema

Eksperimento metu tiriama siunčiamų pranešimų įtaka užklausų greitaveikai. Daiktų interneto objektas jungiamas prie serverio bevielių ryšiu. Tikslui pasiekti naudojama bevielė prieigos stotelė. Tyrimo metu atliekamos užklausos supakuotų duomenų paketų į serverį ir iš serverio į daiktų interneto objektą. Kiekvieno eksperimento metu persiunčiami analogiški duomenų kiekiai. Pagal pateiktus grafikus bei duomenų lenteles yra sulyginama įtaka greitaveikai taikant objektų identifikavimo metodą lyginant su atvirų duomenų siuntimo metodu.



32 pav. Eksperimento vykdymo aplinka

Prieš pradedant vykdyti nuoseklų tyrimo etapą svarbu užtikrinti tikslingą duomenų persiuntimo faktą. Pagal 32 pav. pateiktą paveikslą kontroleris, kuriam suteiktas *192.168.2.123* statinis IP adresas naudodamasis TCP protokolu siunčia pirmąjį duomenų paketa. Pirmasis duomenų paketas skirtas objekto identifikavimui, serveris pagal tai nusprendžia ar jam komunikuoti su objektu, kuris bando į ji kreiptis ar visgi atmesti siunčią informaciją. Informacija sėkmingai pasiekia *192.168.2.117* adresą, kuris yra išskirstas statiškai serveriui. Serveris gavės informaciją ir ją identifikavęs priima siunčiamą duomenų srautą iš kontrolerio. Remiantis eksperimento vykdymo aplinkos rezultatais buvo persiunčiami skirtingų dydžių duomenų blokai (iki 215) ir tiriama įtaka suvartotam laikui taikant skirtingų agentinių programų veikimo principus, 32 pav. pateiktas objektų identifikavimo ir autentifikavimo eksperimentas.

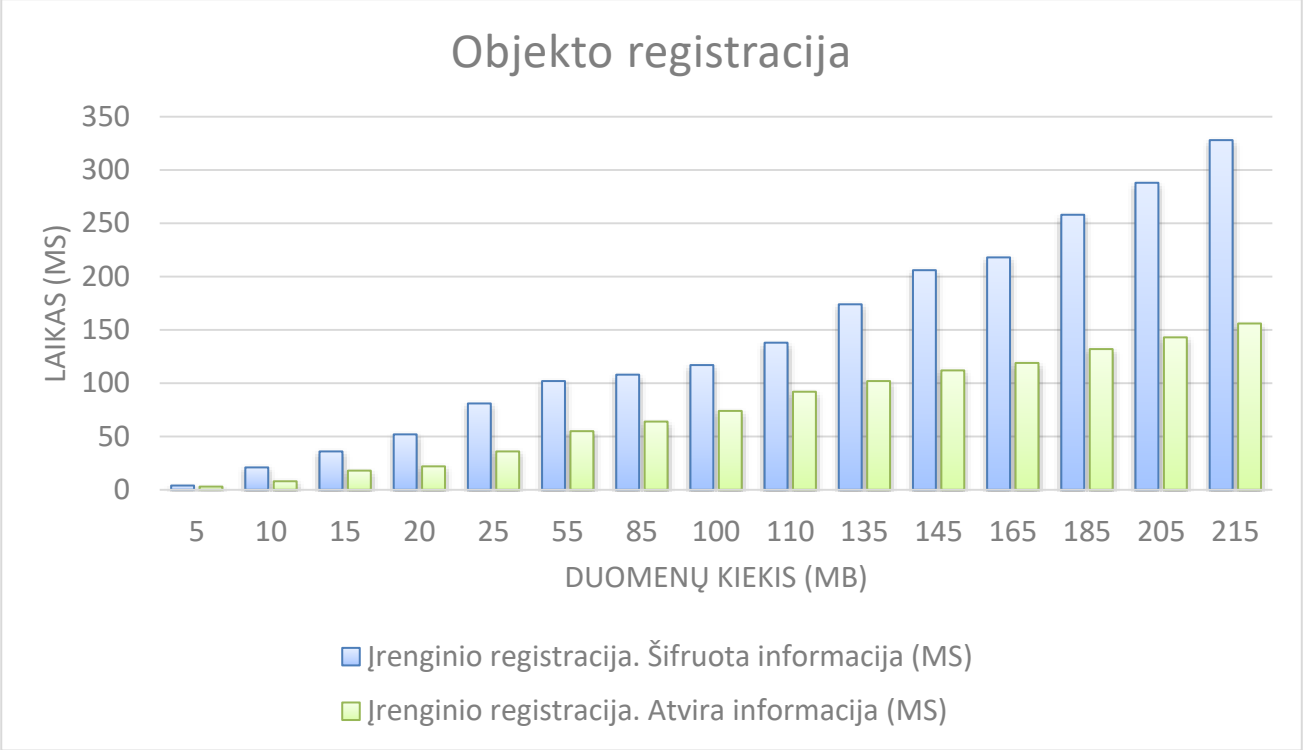


33 pav. Objekto identifikavimo ir autentifikavimo eksperimentas

11 lentelė. Objekto identifikavimas ir autentifikavimo eksperimento duomenys

Šifruotos informacijos siuntimas (MS)	Atviros informacijos siuntimas (MS)	Duomenų kiekis (MB)
8	4	5
42	21	10
72	36	15
104	52	20
162	81	25
204	102	55
216	108	85
234	117	100
276	138	110
348	174	135
412	206	145
436	218	165
516	258	185
576	288	205
656	328	215

Eksperimento metu buvo tiriama objektų identifikavimo ir autentifikavimo įtaka laiko sąnaudų atžvilgiu taikant objektų identifikavimo metodą lyginant su atvirų duomenų persiuntimo būdu. Pagal pateiktą grafika matoma, jog didėjant siunčiamų duomenų kiekiui padidėja ir laiko sąnaudos taikant supakuotų duomenų persiuntimą.

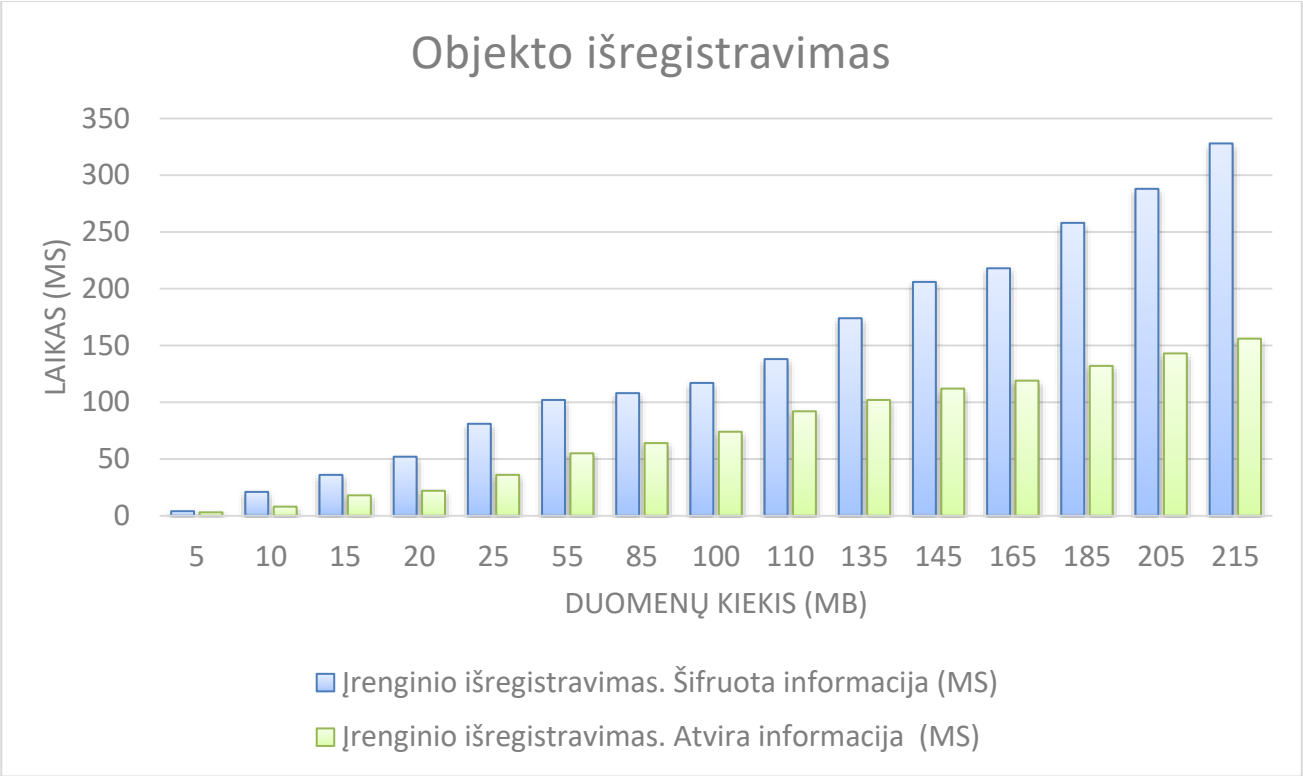


34 pav. Objekto registracijos eksperimentas

12 lentelė. Objekto registracijos eksperimento duomenys

Įrenginio registracija. Šifruota informacija (MS)	Įrenginio registracija. Atvira informacija (MS)	Duomenų kiekis (MB)
4	3	5
21	8	10
36	18	15
52	22	20
81	36	25
102	55	55
108	64	85
117	74	100
138	92	110
174	102	135
206	112	145
218	119	165
258	132	185
288	143	205
328	156	215

Eksperimento metu buvo tiriama objektų registracijos įtaka laiko sąnaudų atžvilgiu taikant objektų identifikavimo metodą lyginant su atvirų duomenų persiuntimo būdų. Pagal pateiktą grafika matoma, jog didėjant siunčiamų duomenų kiekiui padidėja ir laiko sąnaudos taikant supakuotų duomenų persiuntimą analogiškai kaip ir taikant objektų identifikavimą jaučiamas laiko sąnaudų didėjimas.



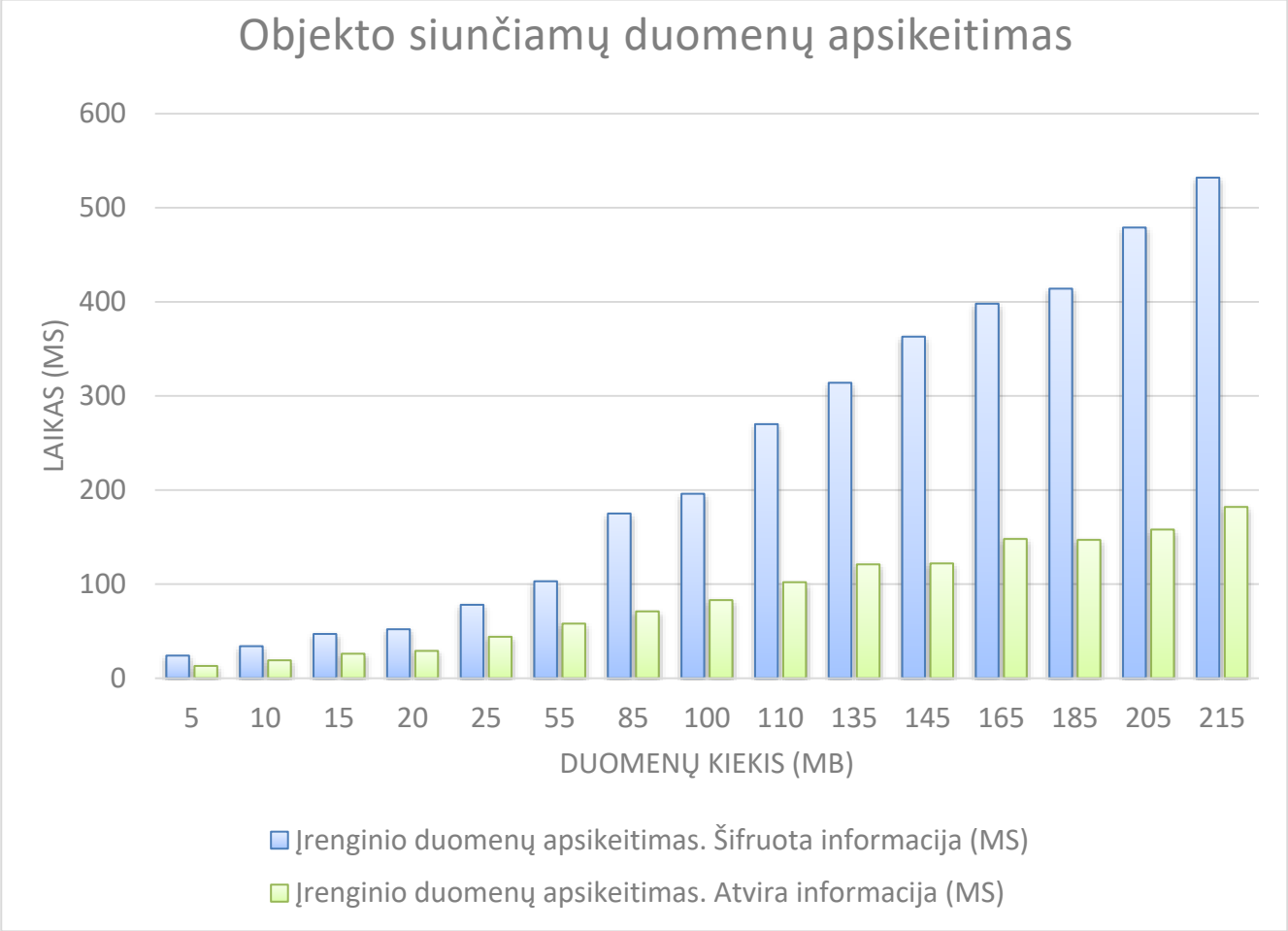
35 pav. Objekto išregistravimo eksperimentas

13 lentelė. Objekto išregistravimo eksperimento duomenys

Įrenginio išregistravimas. Šifruota informacija (MS)	Įrenginio išregistravimas. Atvira informacija (MS)	Duomenų kiekis (MB)
4	3	5
21	8	10
36	18	15
52	22	20
81	36	25
102	55	55
108	64	85
117	74	100
138	92	110
174	102	135
206	112	145
218	119	165
258	132	185
288	143	205
328	156	215

Eksperimento metu buvo tiriama objektų išregistravimo įtaka laiko sąnaudų atžvilgiu taikant objektų identifikavimo metodą lyginant su atvirų duomenų persiuntimo būdų. Pagal pateiktą grafika matoma, jog didėjant siunčiamų duomenų kiekiui padidėja ir laiko sąnaudos taikant supakuotų duomenų persiuntimą. Tačiau didesni laiko sąnaudų skirtumai matomi duomenų apsikeitimo tyrimo metu.

Didėjant siunčiamų duomenų kiekiui net keletą kartų išauga sunaudojamos laiko sąnaudos lyginant su atviru duomenų persiuntimu.

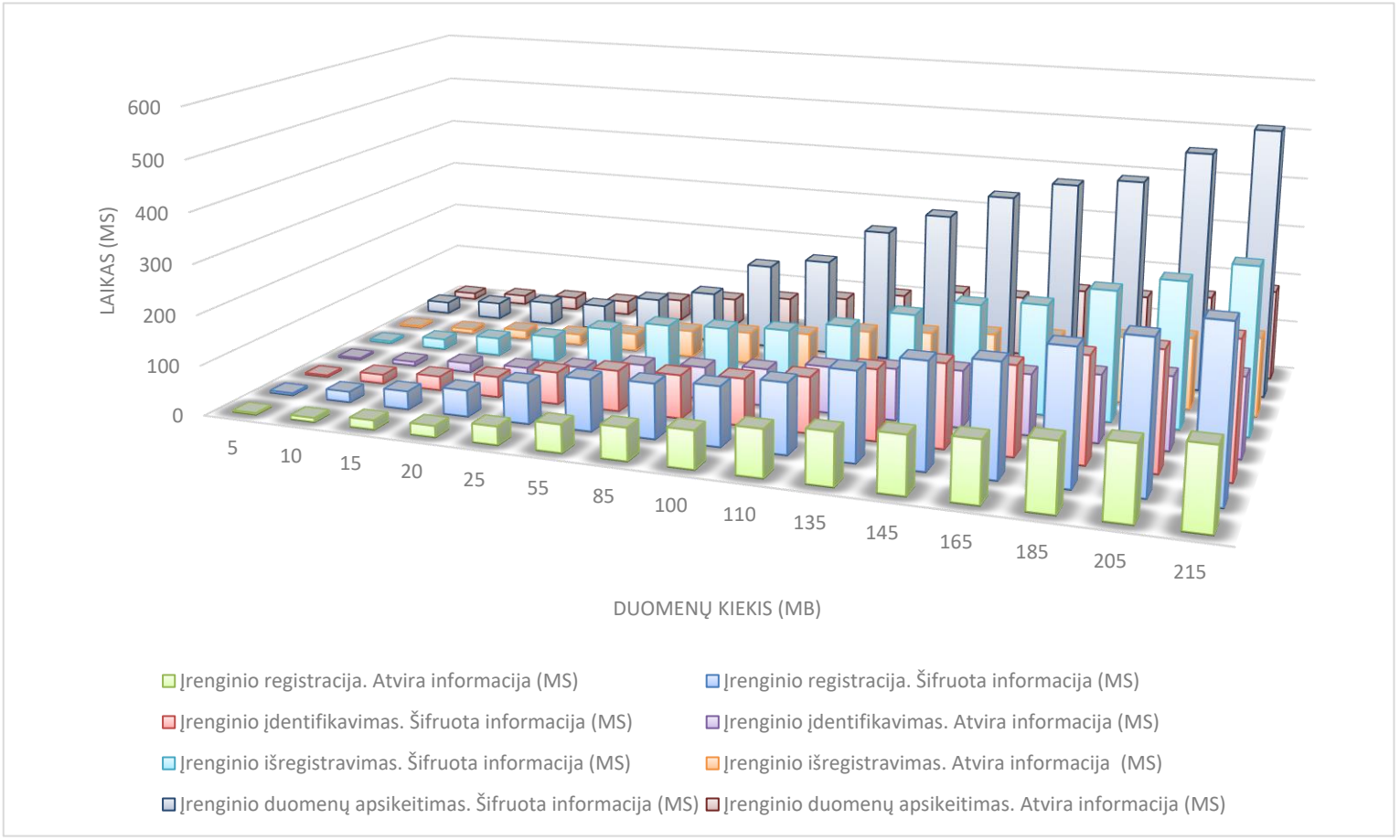


36 pav. Įrenginio siunčiamų duomenų apsikeitimo eksperimentas

14 lentelė. Įrenginio siunčiamų duomenų apsikeitimo eksperimento duomenys

Įrenginio duomenų apsikeitimas. Šifruota informacija (MS)	Įrenginio duomenų apsikeitimas. Atvira informacija (MS)	Duomenų kiekis (MB)
24	13	5
34	19	10
47	26	15
52	29	20
78	44	25
103	58	55
175	71	85
196	83	100
270	102	110
314	121	135
363	122	145
398	148	165
414	147	185
479	158	205
532	182	215

Toks rezultatas yra išsaukiamas todėl, kad tiek serveriui tiek objektui, kuris turi būti identifikuojamas nuolatos tenka išpakuoti siunčiamų duomenų paketus. Paketai turi būti perskaityti ir remiantis išpakuota informacija turi būti siunčiamas atsakymas nurodantis ar galima komunikuoti su objektu ar jo informacija reikia atmesti. Veikimo principas yra paremtas asinchroniniu duomenų perdavimu tai reiškia, kad kiekvienos komunikacijos siunčiamos komandos metu yra užmezgama sesija. Kai persiųsta komanda pasiekia tikslą sesija yra uždaroma. Nuolatinis sesijos užmezgimas sudaro didžiulę įtaka greitaveikai su didėjančiu persiunčiamų duomenų kiekiu.



37 pav. Bendras persiunčiamų duomenų palyginimas taikant objektų identifikavimo metodą

Susumavus visus pateiktus rezultatus įžvelgiamas faktas, kad duomenų persiuntimas kai siunčiami duomenys iš objekto (temperatūros, kuris susidariusi aplinkoje) į serverį taikant objektų identifikavimo ir autentifikavimo metodiką sueikvoja daugiausiai laiko sąnaudų. Mažiausia įtaka sueikvotam laikui turi įrenginių registracija. Tai yra todėl, kad nors ir yra taikomas asinchroninės komunikacijos metodas, tačiau tai yra vienetinis atvejis, todėl persiunčiamų duomenų kiekis nesudaro didelės įtakos laiko lygiu.

4.1. Tyrimo išvados

- Eksperimento metu buvo tiriama objektų registravimo, išregistravimo, identifikavimo ir autentifikavimo įtaka laiko sąnaudų atžvilgiu taikant objektų identifikavimo metodą lyginant su atvirų duomenų persiuntimo būdų. Remiantis pateiktais rezultatais buvo įžvelgta jog didėjant siunčiamų duomenų kiekiui padidėja ir laiko sąnaudos duomenų persiuntimo metu nuo 34.23% iki 84.61% priklausomai nuo užduoties, kuria turi atlikti agentinė programa.
- Didesni laiko sąnaudų skirtumai matomi duomenų apsikeitimo tyrimo metu. Didėjant siunčiamų duomenų kiekiui net iki 84.61% išauga sunaudojamos laiko sąnaudos lyginant su atviru duomenų persiuntimu.
- Susumavus visus pateiktus rezultatus įžvelgiamas faktas, kad duomenų persiuntimas kai siunčiami duomenys iš objekto (temperatūros, kuris susidariusi aplinkoje) į serverį taikant objektų identifikavimo ir autentifikavimo metodiką sueikvoja daugiausiai laiko sąnaudų. Vidutiniškai imant vieno megabaito duomenų persiuntimas netaikant objektų identifikavimo metodo užtrunka iki 2.6 ms. Tačiau kuomet taikomas objektų identifikavimo metodas tuomet vieno megabaito duomenų persiuntimas užtrunka iki 4.8 ms t.y., apie 84.61%. Mažiausia įtaka sueikvotam laikui turi įrenginių registracija. Tai yra todėl, kad nors ir yra taikomas asinchroninės komunikacijos metodas, tačiau tai yra vienetinis atvejis, todėl persiunčiamų duomenų kiekis nesudaro didelės įtakos laiko lygiu. Laiko sąnaudos padidinamos vidutiniškai 34.23% taikant objektų identifikavimo ir autentifikavimo metodą. Kuomet taikomas metodas įrenginio registracijos procese vienas megabaitas informacijos yra persiunčiamas per 1.6 ms. Atsisakius metodo vienas megabaitas informacijos yra persiunčiamas per 1.2 ms. Tendencija išlieka, kad delsimas laiko sąnaudų atžvilgiu išlieka tarp 34.23% - 41.78%.
- Didžiausia įtaka laiko suvartojimui siunčiamų duomenų momentu turi duomenų persiuntimas. Toks rezultatas yra išsaukiamas todėl, kad tiek serveriui tiek objektui, kuris turi būti identifikuojamas nuolatos tenka išpakuoti siunčiamų duomenų paketus. Paketai turi būti perskaityti ir remiantis išpakuota informacija turi būti siunčiamas atsakymas nurodantis ar galima komunikuoti su objektu ar jo informacija reikia atmesti. Veikimo principas yra paremtas asinchroniniu duomenų perdavimu tai reiškia, kad kiekvienos komunikacijos siunčiamos komandos metu yra užmezgama sesija. Kai persiųsta komanda pasiekia tikslą sesija yra uždaroma. Nuolatinis sesijos užmezgimas sudaro didžiulę įtaka greitaveikai su didėjančiu persiunčiamų duomenų kiekiu.

5. IŠVADOS

- Išanalizuotos įvairios daiktų interneto objektų komunikavimo technologijos ir belaidžio ryšio protokolai.
  Išanalizuoti protokolų veikimo principai, pažeidžiamumai ir saugumo užtikrinimo atvejai. Taipogi detalizuota daiktų interneto struktūra, buvo aprašyti ir detalizuoti daiktų interneto koncepciją sudarantys sluoksniai.
  Nors daiktų interneto objektų identifikavimo ir autentifikavimo problema yra žinoma mokslininkai plačiai dirba ties šia problemine sfera ir jau galima aptikti galimų sprendimų problemai spręsti.
  Daiktų interneto objektų identifikavimo sprendimų yra, tačiau nepavyko aptikti sprendimus užtikrinančius autentifikavimą, nors tai yra vienas iš esminių daiktų interneto probleminių sričių, kuria yra būtina tinkamai išspręsti, kad užtikrinti sklandų objektų identifikavimo ir autentifikavimo procesą.
- Daugybė daiktų interneto objektų šiandien pasaulyje yra sujungti į tinklą. Tačiau vyrauja problemos susijusios su daiktų interneto objektais. Svarbiausia dalis yra ta, kad kaip galima pasitikėti objektų, kaip įsitikinti, kad informacija, kuri ateina iš jutiklio pusės yra teisinga ir nepakeista. To galima pasiekti realizuojant objektų identifikavimo agentinę sistemą, kuri susideda iš keturių agentinių sistemų – agentas registratorius, agentas gavėjas, agentas siuntėjas ir agentas identifikatorius. Agento registratorius - paskirtis atlikti daiktų interneto objektų registravimą.
  - Objektų identifikavimo modelyje yra siekiama sutalpinti informacijos tiek apie patį vartotoją, kuris naudojasi Sistema, tiek apie pačius įrenginius, kurie komunikuoja tarpusavyje iš kliento ir serverio pusės. Kiekvienas įrenginys (kontroleris) turi gauti iš serverio pusės jam unikalų identifikatorių. Tiek pats įrenginys (kontroleris) tiek prie jo prijungti jutikliai yra identifikuojami naudojant jiems priskirtus identifikatorius. Metodologijos principas remiasi tuo, kad pranešimo pirmieji baitai yra identifikatoriai, jie apsprendžia ar gauta informacija yra autentiška (pvz., ar ji atitinka tolimesnius apspręstus įrenginių identifikavimo rėžius). Jeigu informacija, kuri atkeliavo neatitinka identifikatoriaus reikalavimų (pvz., įsilaužėlis bando siųsti savo fiktyvią informaciją) ji yra atmetama.
  - Komunikacijos užmezgimo principas yra paremtas kliento serverio pagrindu. Klientas, tai yra daiktų interneto objektas, kurio paskirtis yra atlikti kokia nors užduotį pvz., siųsti informacija apie kambaryje esančia temperatūrą. Tokiam objektui taikant pateiktą identifikavimo ir autentifikavimo metodą visų pirma reikia užmegzti komunikacijos sesiją su serveriu. Traktuojame, kad objektas, kuris siekia užmegzti sesiją yra identifikuotas sistemoje, t.y., jam yra suteiktas unikalus identifikatorius. Pirmas etapas iš kliento pusės yra siusti užklausą serveriui pateikiant supakuotą informacijos paketą, kuriame yra identifikatorius, kuris buvo suteiktas unikaliai šiam objektui bei komanda, kuri skirta užmegzti sesijai. Serveris gavęs duomenų paketą jį išpakuoja ir jeigu informacija yra teisinga jis gražina atsakymą objektui apie sėkmingai užmegzta sesiją su serveriu. Toliau yra siunčiamos atitinkamos komandos skirtos objekto valdymui. Komunikacija tarp serverio ir kliento užtikrina agentinės programos, kurių paskirtis yra užtikrinti korektišką duomenų srauto perėjimą tarp serverio ir kliento pusės bei savo paskirties užduočių vykdymą.
- Eksperimento metu buvo tiriama objektų registravimo, išregistravimo, identifikavimo ir autentifikavimo įtaka laiko sąnaudų atžvilgiu taikant objektų identifikavimo metodą lyginant su atvirų duomenų persiuntimo būdų. Remiantis pateiktais rezultatais buvo įžvelgta jog didėjant siunčiamų duomenų kiekiui padidėja ir laiko sąnaudos duomenų persiuntimo metu nuo 34.23% iki 84.61% priklausomai nuo užduoties, kuria turi atlikti agentinė programa.

- Didesni laiko sąnaudų skirtumai matomi duomenų apsikeitimo tyrimo metu. Didėjant siunčiamų duomenų kiekiui net iki 84.61% išauga sunaudojamos laiko sąnaudos lyginant su atviru duomenų persiuntimu.
- Susumavus visus pateiktus rezultatus įžvelgiamas faktas, kad duomenų persiuntimas kai siunčiami duomenys iš objekto (temperatūros, kuris susidariusi aplinkoje) į serverį taikant objektų identifikavimo ir autentifikavimo metodiką sueikvoja daugiausiai laiko sąnaudų. Vidutiniškai imant vieno megabaito duomenų persiuntimas netaikant objektų identifikavimo metodo užtrunka iki 2.6 ms. Tačiau kuomet taikomas objektų identifikavimo metodas tuomet vieno megabaito duomenų persiuntimas užtrunka iki 4.8 ms t.y., apie 84.61%. Mažiausia įtaka sueikvotam laikui turi įrenginių registracija. Tai yra todėl, kad nors ir yra taikomas asinchroninės komunikacijos metodas, tačiau tai yra vienetinis atvejis, todėl persiunčiamų duomenų kiekis nesudaro didelės įtakos laiko lygiu. Laiko sąnaudos padidinamos vidutiniškai 34.23% taikant objektų identifikavimo ir autentifikavimo metodą. Kuomet taikomas metodas įrenginio registracijos procese vienas megabaitas informacijos yra persiunčiamas per 1.6 ms. Atsisakius metodo vienas megabaitas informacijos yra persiunčiamas per 1.2 ms. Tendencija išlieka, kad delsimas laiko sąnaudų atžvilgiu išlieka tarp 34.23% - 41.78%.
- Didžiausia įtaka laiko suvartojimui siunčiamų duomenų momentu turi duomenų persiuntimas. Toks rezultatas yra išsaukiamas todėl, kad tiek serveriui tiek objektui, kuris turi būti identifikuojamas nuolatos tenka išpakuoti siunčiamų duomenų paketus. Paketai turi būti perskaityti ir remiantis išpakuota informacija turi būti siunčiamas atsakymas nurodantis ar galima komunikuoti su objektu ar jo informacija reikia atmesti. Veikimo principas yra paremtas asinchroniniu duomenų perdavimu tai reiškia, kad kiekvienos komunikacijos siunčiamos komandos metu yra užmezgama sesija. Kai persiųsta komanda pasiekia tikslą sesija yra uždaroma. Nuolatinis sesijos užmezgimas sudaro didžiulę įtaka greitaveikai su didėjančiu persiunčiamų duomenų kiekiu.

6. LITERATŪRA

[1] M. Landman, „Managing smart phone security risks“, įtraukta *InfoSecCD '10 2010 Information Security Curriculum Development Conference*, New York, 2010.

[2] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, C. Wolf, „Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices“, įtraukta *SP '11 Proceedings of the 2011 IEEE Symposium on Security and Privacy*, Washington, 2011.

[3] S. Karsten, „Software Security Aspects of Java - Based Mobile Phones,“ įtraukta *SAC'11 Proceedings of the 2011 ACM Symposium on Applied Computing*, New york, 2011.

[4] M. Mun et.al., „Personal data vaults: a locus of control for personal data streams,“ įtraukta *Co-NEXT '10 Proceedings of the 6th International COnference*, New York, 2010.

[5] „BLURRING BOUNDARIES Trend Micro Security Predictions for 2014 and Beyond“, Trend Micro, 2013

[6] Andy Greenberg, „iOS 7 Bug Lets Anyone Bypass iPhone's Lockscreen To Hijack Photos, Email, Or Twitter“, 2013. [Tinkle]. Prieinama: http://www.forbes.com/sites/andygreenberg/2013/09/19/ios-7-bug-lets-anyone-bypass-iphones-lockscreen-to-hijack-photos-email-or-twitter/

[7] „314 mobile phones 'stolen in London every day“, BBC news London, 2013. [Tinkle]. Prieinama: http://www.bbc.co.uk/news/uk-england-london-21018569

[8] A. Venčkauskas, E. Kazanavičius, Informacinių technologijų saugos metodai, mokomoji knyga, UAB “TEV” 2011.

[9] K. Dunhan, Mobile malware attacks and defence, Burlington: Syngress Publishing, Inc., 2009.

[10] G. Russello, M. Conti, B. Crispo, E. Fernandes, „MOSES: Supporting Operation Modes on Smartphones“, įtrauktą *SACMAT '12 Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, New Tork, 2012.

[11] J. Shin, Y. Chung, K. Sun Ko, Y. Ik Eom, „Design and implementation of the Management Agent for Mobile Devices based on OMA DM“, įtraukta *ICUIMC '08 Proceedings of the 2nd international conference on Ubiquitous information management and communication*, New York, 2008.

[12] „Enterprise Readiness of Consumer Mobile Platforms“, Trend Micro, 2012.

[13] „Security in Evolving Mobile Platforms“, Trend Micro, 2012.

[14] K. Kostiainen, E. Reshetova, J.-E. Ekberg, N. Asokan, „Old, New, Borrowed, Blue – A Perspective on the Evolutionof Mobile Platform Security Architectures“, įtraukta *CODASPY '11 Proceedings of the first ACM conference on Data and application security and privacy*, New York, 2011.

[15] A. Distefano, A. Grillo, A. Lentini, G. F. Italiano, „SecureMyDroid: enforcing security in the mobile devices lifecycle“, įtraukta *CSIIRW '10 Proceedings of the Sixth Annual Workshop on Cyber security and Information Intelligence Research*, New York, 2010.

[16] G. Russello, M. Conti, B. Crispo, E. Fernandes, Y. Zhauniarovich, „DEMO: Demonstrating the Effectiveness of MOSES for Separation of Execution Modes“, įtrauktą *CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security*, New York, 2012.

[17] „OMA Device Management V1.2“, Open Mobile Allience, 2008. [Tinkle]. Prieinama: http://technical.openmobilealliance.org/Technical/release_program/dm_v1_2.aspxPRIEDAI

[18] „Exploring the Weak Links of Internet Security: A Study of WiFi Security in Hong Kong“ 2015 [Tinkle] Prieinama: http://search.proquest.com/openview/7a1805fddadb37ceaee09a232bf0ee42/1?pq-origsite=gscholar

[19] „Wi-Fi Adoption and Security“ 2015 [Tinkle]. Prieinama http://safewifi.hk/files/2015/香港無線網路的使用和安全調查報告2015.pdf

[20] „Malicious WiFi networks: A first look“ [Tinkle]. Prieinama https://www.researchgate.net/publication/261478484_Malicious_WiFi_networks_A_first_look

[21] „An Efficient and Secure RFID Security Method“ 2014 [Tinkle]. Prieinama http://link.springer.com/chapter/10.1007%2F978-0-387-76481-8_7

[22] „Scalable RFID security framework and protocol supportingInternet of Things“ 2014 [Tinkle] Prieinama https://www.researchgate.net/publication/261372890_Scalable_RFID_Security_Framework_and_Protocol_Supporting_Internet_of_Things

[23] „Security Risks With RFID“ 2016 [Tinkle] Prieiga http://www.securitymagazine.com/articles/86954-rfid-the-almost-everything-tool

[24] „New Security Approach for ZigBee Weaknesses“ 2014 [Tinkle] Prieiga http://www.sciencedirect.com/science/article/pii/S1877050914010217

[25] „AES algorithm-based encryption scheme for ZigBee networks“ 2014 [Tinkle] Prieiga http://en.cnki.com.cn/Article_en/CJFDTOTAL-DZJY201404027.htm

[26] „6LoWPAN security: adding compromise resilience to the 802.15.4 security sublayer“ 2013 [Tinkle] Prieiga http://dl.acm.org/citation.cfm?id=2523502

[27] „Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN“ 2014 [Tinkle] Prieiga http://onlinelibrary.wiley.com/doi/10.1002/sec.406/abstract;jsessionid=5A3C61165919C8F6186F401CAB7BF1BB.f04t04?userIsAuthenticated=false&deniedAccessCustomisedMessage=

[28] „WiFi security and testbed implementation for WEP/ WPA cracking demonstration“ 2014 [Tinkle]. Prieiga http://okeanis.lib.teipir.gr/xmlui/handle/123456789/1347

[29] „A Critical Analysis on the Security Concerns of Internet of Things (IoT)“ 2015 [Tinkle] Prieiga http://research.ijcaonline.org/volume111/number7/pxc3901280.pdf

[30] „Identity-Based Authentication Scheme for the Internet of Things“ 2016 [Tinkle] Prieiga http://ieeexplore.ieee.org/document/7543884/?reload=true