KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Marijus Lukša

ASMENINIŲ ĮRENGINIŲ NAUDOJAMŲ ĮMONĖSE INFORMACIJOS SAUGOS METODŲ TYRIMAS

Baigiamasis magistro darbas

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

ASMENINIŲ ĮRENGINIŲ NAUDOJAMŲ ĮMONĖS INFORMACIJOS SAUGOS METODŲ TYRIMAS

Baigiamasis magistro darbas
Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) Doc. dr. Jevgenijus Toldinas
(data)
Recenzentas
(parašas) Doc. dr. Stasys Maciulevičius
(data)

Projektą atliko
(parašas) Marijus Lukša
(data)

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

.....

(Fakultetas)

.....

(Studento vardas, pavardė)

.....

(Studijų programos pavadinimas, kodas)

„Baigiamojo projekto pavadinimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 ___ m. _____ ____ d.

Kaunas

Patvirtinu, kad mano **Marijaus Lukšos** baigiamasis projektas tema „Asmeninių įrenginių naudojamų įmonėse informacijos saugos metodų 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.

_____ _____

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

Lukša, M. „Asmeninių įrenginių naudojamų įmonėse informacijos saugos metodų tyrimas“. Magistro baigiamasis projektas / vadovas doc. dr. Jevgenijus Toldinas; Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra.

Kaunas, 2016. 50 p.

SANTRAUKA

Įmonės, besidominčios naujausiomis technologijomis ir jas naudojančios pradeda taikyti naują koncepciją „atsinešk savo įrenginį (Bring Your Own Device)“. Tai yra sparčiai populiarėjanti technologija, kurios dėka įmonės darbuotojai vietoje įmonės išduotų įrenginių naudoja savo asmeninius. Tai suteikia daug naudos:

- Sumažina įmonės išlaidas, nereikia pirkti naujų įrenginių atėjus naujam darbuotojui,
- Didesnis darbuotojų produktyvumas: darbuotojai gerai išmano savo įrenginius, nereikia pratintis prie naujo įrenginio. Tai leidžia daug greičiau įvykdyti skirtas užduotis.
- Lankstumas. Paprastai darbuotojas, vykstantis į komandiruotę, su savimi pasiima įmonės skirtą įrenginį bei savo asmeniniam naudojimui. Tam reikia daug vietos ir nėra patogu keliauti, o leidus naudoti asmeninį įrenginį darbui ši problema būtų išspręsta.

Tačiau naudojant asmeninius įrenginius įmonėse kyla kitų iššūkių.

- Kaip apsaugoti informaciją pametus įrenginį.
- Kaip apsaugoti įrenginį nuo pavojingų programų.
- Kaip atskirti įmonės informaciją, nuo darbuotojo privačios.
- Kaip uždrausti pašalinėms programoms naudoti įmonės informaciją.

Magistrinio darbo objektas – įmonėse naudojamų mobiliųjų įrenginių duomenų apsaugos sistema.

Šio darbo struktūra:

- Pirmoje darbo dalyje pateikiama asmeninių įrenginių naudojamų įmonėse informacijos saugos metodų ir sistemų analizė. Joje analizuojama įmonių, naudojančių darbuotojų atsineštus asmeninius įrenginius, praktika, su kokiais iššūkiais jos susiduria. Taip pat pateiktos kelios sistemos, kurios padeda apsisaugoti nuo galimų grėsmių.
- Antroje darbo dalyje pateikimas asmeninių įrenginių naudojamų įmonėse informacijos saugos metodų taikymo sistemos modelis. Jame nurodyta šios sistemos architektūra, pavaizduoti kliento ir serverio veikimo algoritmai bei pateiktos būsenų diagramos.
- Trečioje darbo dalyje pateikiami atlikto eksperimentinio tyrimo rezultatai. Šio tyrimo metu ištirta serverio duomenų užšifravimo greitaveika naudojant skirtingus algoritmus. Taip pat buvo parašyta programa, kuri leido naudoti vieną kodą skirtingose platformose (Windows, iOS, Android) ir patikrinti, kaip greitai veikia kliento duomenų iššifravimas skirtingose platformose ir įrenginiuose.
- Darbo pabaigoje pateiktos išvados.

Lukša, Marijus. Research of Information Security Methods in BYOD (Bring Your Own Device). *Master's* thesis / supervisor assoc. prof. Dr. Jevgenijus Toldinas. Department of Computer Science, The Faculty of Informatics, Kaunas University of Technology.

Research area and field:

Key words:

Kaunas, 2015. 50 p.

SUMMARY

Some interested in the newest technologies business companies are starting to use a new conception called „Bring Your Own Device". This new rapidly growing technology gives ability to the employees to use their own devices instead of given by the office. It gives some benefits such as:

- Company's expenses are reduced because of no need to buy new devices when a new employee starts working.
- Employees' efficiency increase. There is no need to get used to a new device. An employee knows its own device best therefore he would complete appointed tasks much faster while using it.
- Versatility. Usually an employee going on business trip has to take two devices: one given by the office and one of his own for personal using. More space is needed and it makes travelling more complicated. This problem would be solved by using personal device for work.

However usage of your own devices in companies makes some other new problems and questions, for example:

- Security of information after the device is lost or stolen.
- Protecting your device against malware.
- Separating company's data and personal data.
- Prohibiting outside sources from using company's data.

The object of this work is the security system of the mobile devices used by bussines companies.

This paper is organized as follows:

- In the first part of the research the analysis of information security methods and systems of personal devices used by companies is presented. There are analyzed the examples of the companies using the BYOD (Bring Your Own Device) practice and the challenges they face because of this practice. Also there are introduced several systems helpful in protection against the possible threats.
- The second part of the research presents the model of information security methods in personal devices used for companies. There is specified the architecture of this system, the algorithms of client and server operations are described and the status diagrams are introduced.
- The third part of the research presents the results of conducted experimental research. The research concentrates on the encryption speed of data in a server using several different algorithms. Also there was written a program which gives an ability to use the same code for various platforms (Windows, iOS, Android) and this way to check the speed of client data encryption in different platforms and devices.
- In the end the conclusion of the research is presented.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

BOYD – „Bring your own device“ atsinešk savo įrenginį.

MĮ – mobilus įrenginys

IT – informacinės technologijos

IM – instaliacijos modulis

MCM – „MOSES Configuration Manager“ MOSES nustatymų valdiklis

MH – „MOSES Hypervisor“

PEM – „Policy Enforcement Module“

MusKRS – „MUSES Knowledge Refinement System“ MUSES žinių tobulinimo sistema

MusCRTEP – „MUSES Continious Real-Time Events Process“ nepertraukiamas realaus laiko įvykių stebėjimas

ĮVADAS

Įmonės, besidominčios naujausiomis technologijomis ir jas naudojančios pradeda taikyti naują koncepciją „atsinešk savo įrenginį (Bring Your Own Device)“. Tai yra sparčiai populiarėjanti technologija, kurios dėka įmonės darbuotojai vietoje įmonės išduotų įrenginių naudoja savo asmeninius. Tai suteikia daug naudos:

- Sumažina įmonės išlaidas, nereikia pirkti naujų įrenginių atėjus naujam darbuotojui,
- Didesnis darbuotojų produktyvumas: darbuotojai gerai išmano savo įrenginius, nereikia pratintis prie naujo įrenginio. Tai leidžia daug greičiau įvykdyti skirtas užduotis.
- Lankstumas. Paprastai darbuotojas, vykstantis į komandiruotę, su savimi pasiima įmonės skirtą įrenginį bei savo asmeniniam naudojimui. Tam reikia daug vietos ir nėra patogu keliauti, o leidus naudoti asmeninį įrenginį darbui ši problema būtų išspręsta.

Tačiau naudojant asmeninius įrenginius įmonėse kyla kitų iššūkių.

- Kaip apsaugoti informaciją pametus įrenginį.
- Kaip apsaugoti įrenginį nuo pavojingų programų.
- Kaip atskirti įmonės informaciją, nuo darbuotojo privačios.
- Kaip uždrausti pašalinėms programoms naudoti įmonės informaciją.

Darbo problematika ir aktualumas

Įmonės duomenų, saugomų darbuotojo mobiliuose įrenginiuose, apsauga už įmonės teritorijos ribų.

Darbo tikslas ir uždaviniai

Sukurti efektyvų duomenų, esančių mobiliuose įrenginiuose, apsaugos metodą, apsaugantį nuo neleistino įmonės duomenų panaudojimo. Šiam tikslui pasiekti buvo iškelti tokie uždaviniai:

- Išanalizuoti dabar naudojamus duomenų apsaugos standartus ir išskirti jų trūkumus.
- Suformuoti duomenų apsaugos funkcinius ir nefunkcinius reikalavimus.
- Pasiūlyti duomenų apsaugos metodą, kuris apsaugotų įmonės duomenys nuo neleistino naudojimo.
- Realizuoti pasiūlytą metodą ir patikrinti jo veikimą.

Darbo struktūra

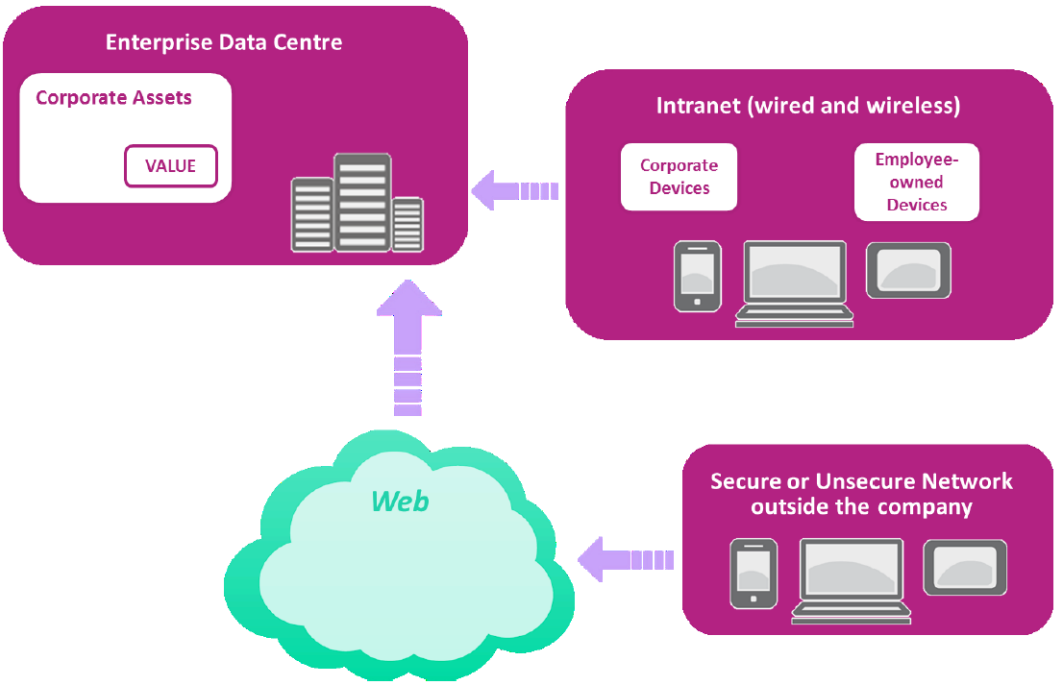
Darbo pirmajame skyriuje aprašoma analizė jau egzistuojančių sistemų, kurios skirtos apsaugoti duomenis mobiliuosiuose įrenginiuose.

1. ASMENINIŲ ĮRENGINIŲ NAUDOJAMŲ ĮMONĖSE INFORMACIJOS SAUGOS METODŲ IR SISTEMŲ ANALIZĖ

Šiame skyriuje išanalizuojama BYOD politikos trūkumai, grėsmės, naudotojai, bei esančios sistemos, kurios padeda apsaugoti svarbius įmonės informacijos išteklius.

1.1. Asmeninių įrenginių naudojamų įmonėse saugos iššūkių analizė

Įmonėse naudojamų mobiliųjų įrenginių (MĮ) kiekis pastaruoju metu aktyviai auga. Šių įrenginių naudojimas naudingas tiek darbdaviui, teik darbuotojui, nes darbuotojų rolės vis dažniau reikalauja dirbti interaktyviai iš bet kur ir bet kada, pasitelkiant naujausius techninius bei programinius sprendimus. Didėjantis resursų kiekis reiškia, jog vis daugiau konfidencialios įmonės bei asmeninės informacijos gali būti talpinama MĮ. Paprastai įmonės, kurios visą informaciją ir įrenginius pirkdavo ir palaikydavo pačios, naudojo vienokią apsaugos politiką, kurioje visi duomenų mainai vyko vidiniame tinkle ir susidorodavo su išorinėmis atakomis. Tačiau populiarėjant darbuotojų asmeninių įrenginių naudojimui, apsaugos politika turi prisitaikyti prie darbuotojų įrenginių pažeidžiamumo ir duomenų nutekėjimo naudojant nesaugų viešą tinklą. Siekiant tai įgyvendinti iškyla įvairius iššūkiai, kurios bendrovės turi apsvarstyti.



1 pav. Naujas modelis naudojant BOYD

1 pav. pavaizduotas naujas įmonės informacinių sistemų struktūros modelis, kai įmonė sutinka naudoti BYOD politiką [1]. Jis skiriasi nuo standartinio modelio tuo, kad jame atsiranda sujungimas su internetu, per kurį darbuotojų nuosavi įrenginiai gali susijungti su įmonės vidine sistema.

Kaip ir visos kitas sistemos, BYOD turi savų trūkumų. Išskiriamos pagrindinės trys problemos:

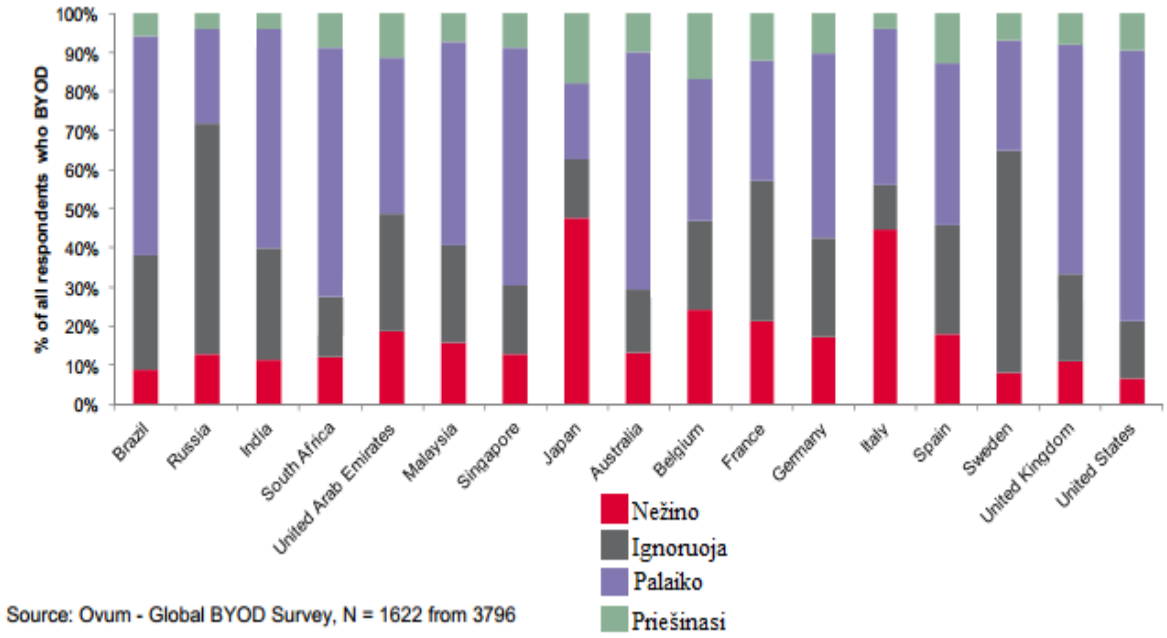
- *Trečiųjų šalių programų prisijungimas prie svarbių duomenų.* Vartotojai atsisiunčiant ir įsirašant programas leidžia joms naudoti telefone esančią atmintį, taip pat ir joje esančius duomenis. Taip piktavaliai gali perimti įmonės duomenis.
- *Duomenų praradimas, kai mobilieji įrenginiai pametami arba pavagiami.* Kadangi mobilieji įrenginiai ne visada gerai apsaugomi nuo pašalinių asmenų naudojimo, praradus įrenginį įmonės svarbūs duomenys gali paplisti.
- *Darbuotojo duomenų atskyrimas nuo įmonės*. Svarbu atskirti vartotojo duomenis, kad atsitikus nelaimingam atsitikimui (įsilaužta į mobilųjį įrenginį ar jis prarastas) būtų galima ištrinti įmonės svarbius duomenis nepakenkiant vartotojo duomenims.

1.2. Įmonių taikančių asmeninių įrenginių naudojimo praktiką analizė

2012 m. „Logicalis Group“ užsakė nepriklausomų analitikų įmonę „Ovum“ ištirti įmonių požiūrį į BYOD politiką ir kaip jos ją priima [6]. Tyrimo metu buvo apklausta 3796 darbuotojų iš 17 skirtingų valstybių. Jie atrinkti pagal vienintelį kriterijų – darbą įmonėje, kurioje yra daugiau nei 50 darbuotojų, pilnu etatu. Apklausoje atkreipiamas dėmesys į įmonių informacinių technologijų skyriaus požiūrį į BYOD politiką, kiek įmonių naudoja BYOD, kiek iš jų naudoja įrenginių valdymo sistemas, kurios apsaugotu įmonės svarbius duomenis.

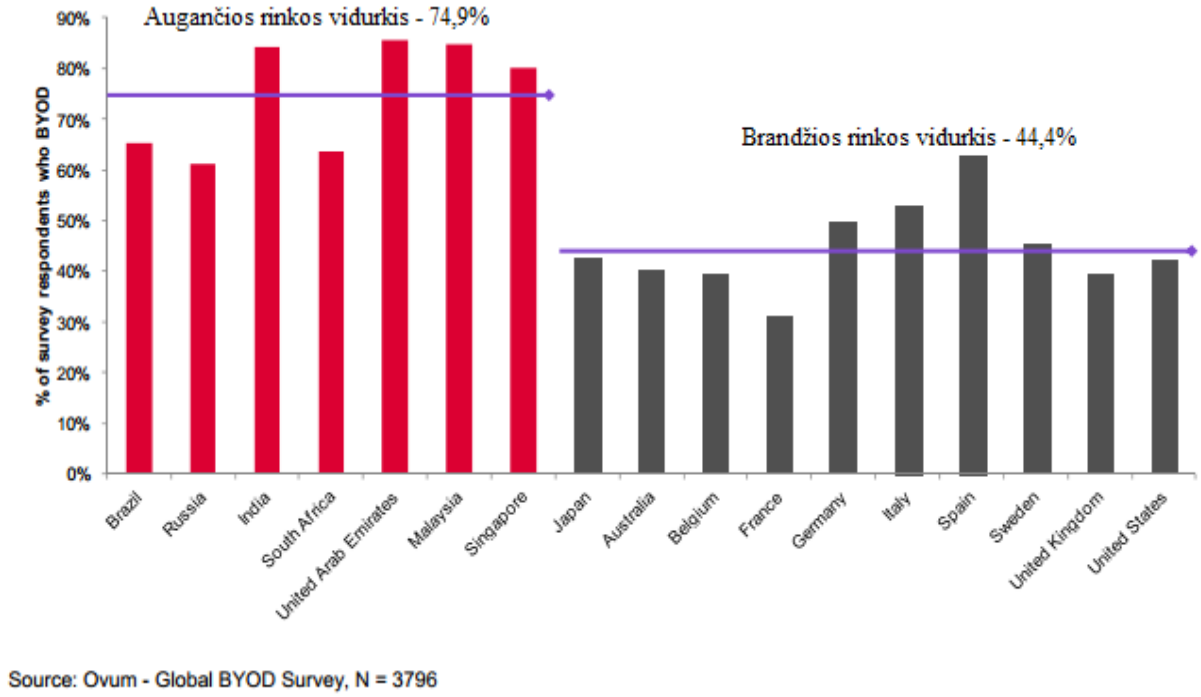
2 pav. pavaizduota įmonių IT skyriaus darbuotojų nuomonė apie BYOD. Raudona spalva reiškia kiek įmonių nieko nežino apie šią politiką. Pilka spalva pažymėta, kiek įmonių ignoruoja BYOD, violetinė – palaiko, o žalia priešinasi šiai politikai. Matome, kad didžioji dalis palaiko asmeninių įrenginių naudojimą

.



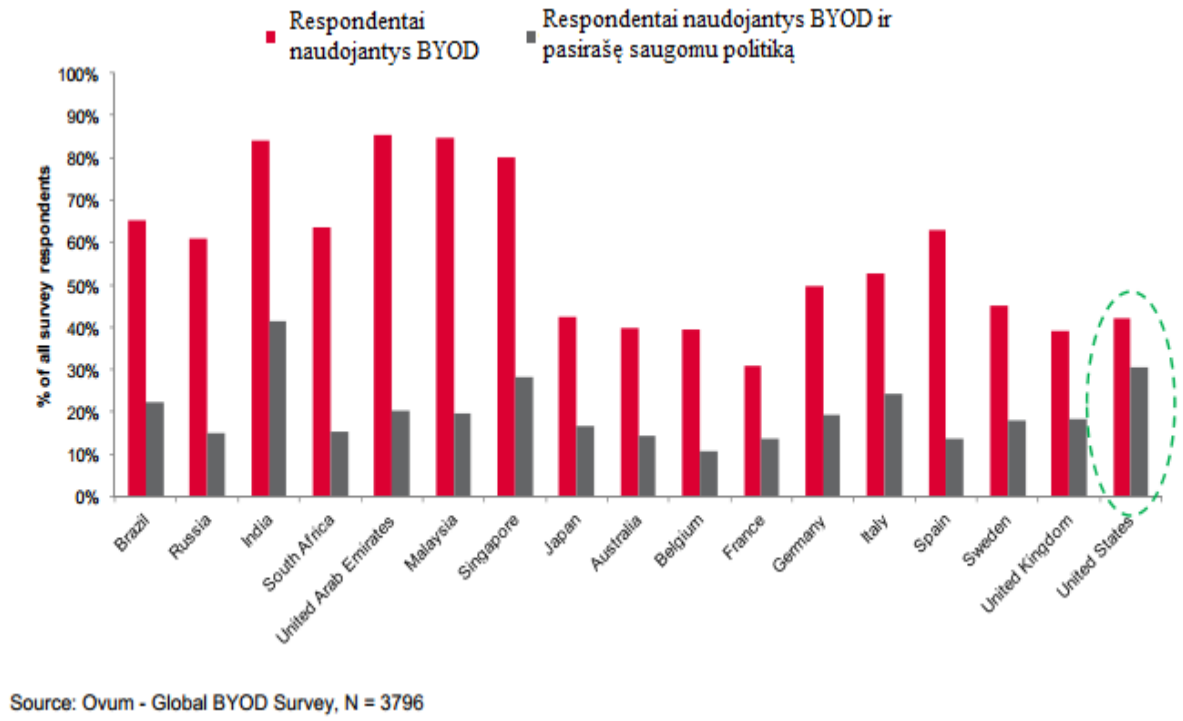
2 pav. IT skyrių darbuotojų nuomonė apie BYOD

3 pav. Pavaizduota kiek įmonių naudoja BYOD politiką įvairiose šalyse. Jos suskirstytos į dvi grupes: augančios rinkos ir brandžios rinkos. Matome, kad augančios rinkos (kaip Brazilija, Pietų Afrika ar Malaizija) labiau linkusios naudoti BYOD, nes jų darbuotojų lankstesnis požiūris į darbo valandas, labiau linkę laisvą laiką naudoti darbui, nei asmeniniams poreikiams.



3 pav. Įmonių naudojančių BYOD politiką kiekis

Nors ir įmonės naudoja BYOD politiką, tačiau ne visos naudoja priemones, leidžiančias apsaugoti įmonės duomenis. 4 pav pavaizduota, kiek apklausoje dalyvavusių įmonių naudoja mobiliųjų įrenginių valdymo sistemas ir pasirašę saugumo politiką. Iš paveiksliuko galime pastebėti, kad tik mažesnioji dalis rūpinasi duomenų sauga (apie 20,1%). Tačiau kai kurios valstybės labiau tuo rūpinasi, kaip pavyzdžiui Jungtinės Amerikos Valstijos (pažymėta žaliu punktyru).



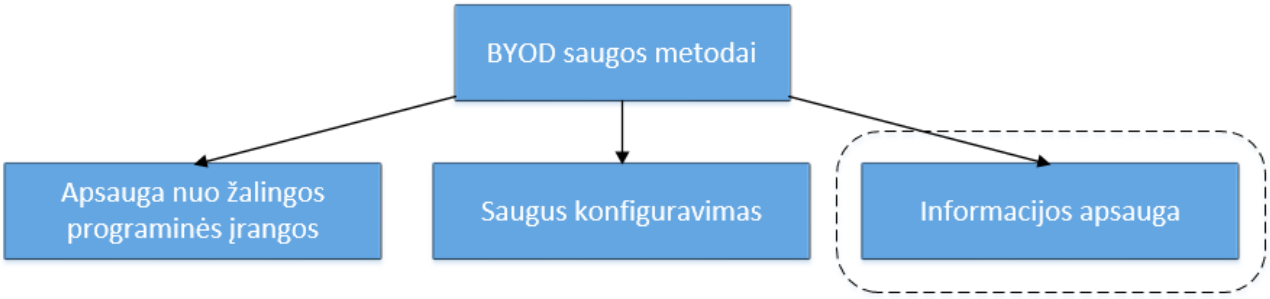
4 pav. Įmonių, pasirašiusių BYOD saugumo politiką, kiekis

1.3. Asmeninių įrenginių naudojamu įmonėse saugos problemų sprendimo metodai

BYOD naudojamas turi trūkumų, dėl kurių iškyla grėsmė įmonių duomenų saugumui. Šios grėsmės atsiranda dėl to, kad įmonės negali visapusiškai reguliuoti, kaip elgiamasi su naudojamais įrenginiais. Pavyzdžiui darbuotojams negalima visiškai uždrausti įsirašyti įvairių nepatvirtintų šaltinių programėlių, kurios gali būti žalingos. Jos gali nuskaityti įrenginyje esančią informaciją, kuri priklauso įmonei ir yra konfidenciali, ir ją perduoti pašaliniams asmenims, kurie gavę ją gali panaudoti blogiems kėslams, taip sugadindami įmonės reputaciją arba padarydami finansinių nuostolių.

Kita grėsmė, kuri kyla naudojant BYOD, yra duomenų praradimas, kai įrenginys pametamas arba pavagiamas. Ši grėsmė labai aktuali, nes neretai naudojamės sąlyginai mažais įrenginiais ir dėl to nepastebime kai įrenginį paliekame ar jis tiesiog iškrenta iš kišenės ar rankinės. Taip pat gyvename pasaulyje, kuriame kiekvieną dieną vyksta nusikaltimai ir vagystės. Mobilieji įrenginiai labai paklausūs ir lengvai pasiekiami, todėl jų pavagiama vis daugiau.

Naudojami keli saugumo metodai, kurie stengiasi sumažinti šias grėsmes arba jų galimą žalą.



5 pav. BYOD saugos metodai

5 pav. pavaizduotos šiuo metu naudojamų apsaugos metodų kategorijos. Jos skirstomos pagal grėsmės tipą ir konfidencialių duomenų išgavimo iš įrenginio tipą.

Apsaugos nuo žalingos programinės įrangos metodas koncentruojasi į tai, kad pašalinės programėlės negalėtų prieiti prie išsaugotų įmonės duomenų. Paprasčiausias būdas tai pasiekti yra uždraudžiant įrašinėti programėles, kurios nėra patikrintos ir aprašytos įmonės saugos politikos nustatymuose. Kitas būdas kaip galima apsaugoti duomenis – tai sukurti profilius ir taip suskaidyti įrenginyje esamą atmintį, kad tik tam tikras profilis galėtų pasiekti tam tikrą vietą atmintyje.

Kitas metodas, skirtas apsaugoti nuo informacijos nutekėjimo, yra „Informacijos apsauga“. Jis taikomas apsisaugoti tais atvejais, kai įrenginys yra pametamas ar pavagiamas iš darbuotojo. Paprasčiausias būdas apsisaugoti nuo to - užšifruoti įmonės duomenis. Taip įsilaužėliai perėmę įrenginį negalėtų lengvai prieiti prie duomenų.

Norint apsaugoti įmonės duomenis nuo pašalinių programų prieinamumo yra kuriamos įvairios sistemos. Nuo paprastų, kaip leisti įdiegti į įrenginį tiktai korporacijos IT administracijos patvirtintų programų (pvz. BOYDroid), iki sudėtingesnių, virtualizacijos būdu sudaryti skirtingas aplinkas įrenginyje, kurios būtų atskirtos viena nuo kitos ir neleistų dalintis svarbiais duomenimis (pvz. MOSES), bei itin sudėtingų, kurios mokės pačios prisitaikyti prie aplinkos ir ieškos darbuotojų elgsenoje anomalijų, rodančių saugumo pažeidimą (MUSES).

1.3.1. Virtualūs privatūs tinklai

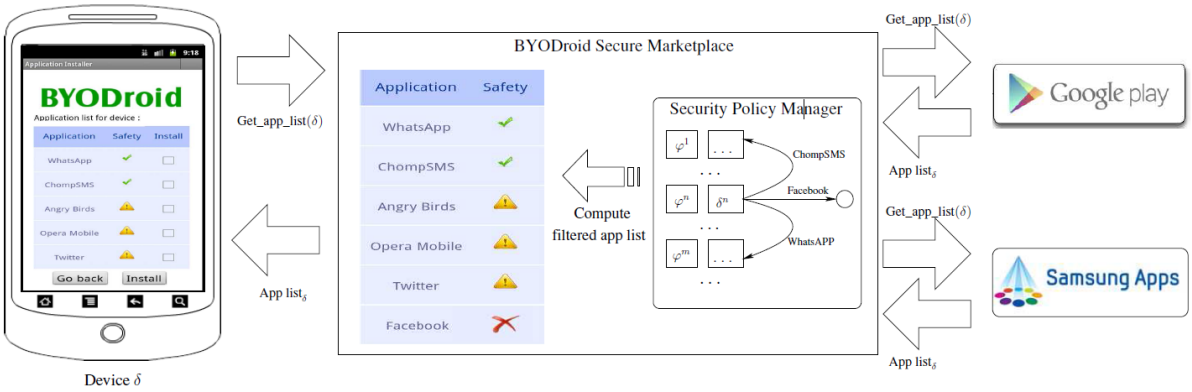
Kiekvienas įmonės darbuotojas besinaudodamas asmeniniu įrenginiu nori turėti galimybę pasiekti įmonės duomenis ne tik iš įmonės tinklo. Vienas svarbiausių BYOD naudojimo aspektų yra kaip saugiai perduoti įmonės tinkle esančius duomenis į darbuotojo įrenginį.

Virtualūs privatūs tinklai (angl. Virtual Private Network, VPN) praplečia įprastinius privačius tinkus tarp viešų tinklų. Tai leidžia vartotojams siųsti ir gauti duomenis internetu imituojant, kad šie įrenginiai sujungti tarpusavyje, taip išnaudojant privataus tinklo saugos politiką. VPN kuriamas naudojant virtualias taškas į tašką jungtis. VPN apimant internetą, yra panašus į globalų tinklą (angl. Wide Area Network, WAN). Iš vartotojo pusės papildomai prijungti tinklo resursai pasiekiami tokiu pačiu būdu kaip ir lokalaus tinklo resursai. Kadangi tradiciniai VPN charakterizuojami kaip taškas į tašką topologija, jie nepalaiko ir nesujungia transliacinių domenų.

1.3.2. Sistema BYODroid

BYODroid – tai sistema, ribojanti programėlių įrašymą pagal įmonės saugumo politiką „Android“ įrenginiuose [2]. Ją sudaro du pagrindiniai komponentai: parduotuvė „BYODroid Market“ ir instaliacijos modulis „BYODroid Installer“(IM). Instaliacijos modulis leidžia pasiekti BYODroid parduotuvę, iš kurios darbuotojas gali atsisiųsti įmonės leidžiamas programėles. IM yra įdiegiamas, kai darbuotojas užregistruoja asmeninį įrenginį įmonėje, jis pakeičia pagrindinį programėlių įrašymo modulį.

Parduotuvė „BYODroid Market“ atsakinga už įrenginio saugumo būsenos palaikymą. Tik įrašyta ji nuskaito visas įrenginyje esančias programas ir patikrina su įmonės leistinomis. Jei randa neleistinų, praneša administratoriui. Kita parduotuvės funkcija - tai leisti vartotojui įsirašyti programas. 2 pav pavaizduotas kaip vyksta programos įrašymas.

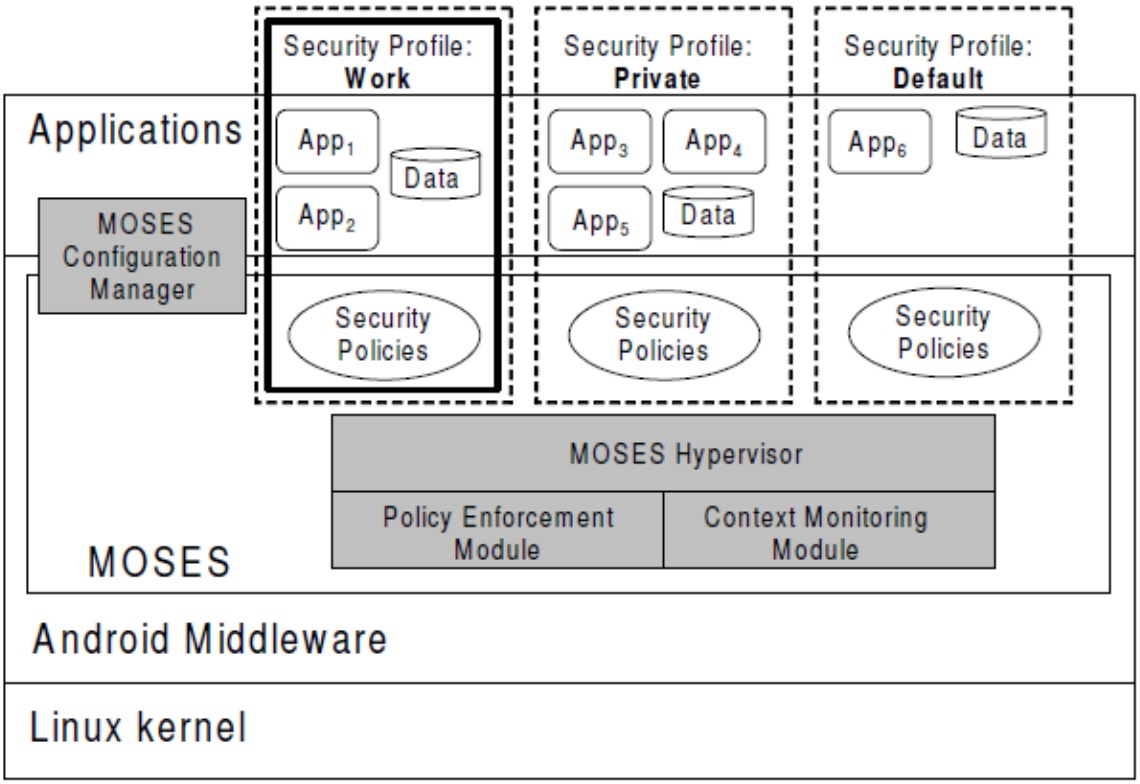


6 pav. BOYDroid programų įrašymas.

1.3.3. Sistema MOSES

MOSES (Mode-of-uses-Separation for Smartphones) yra profiliais grįstas karkasas, kuris apriboja duomenų ir programėlių naudojimą pagal tam tikrą profilį [3, 4]. Vienas svarbiausių

MOSES bruožų yra dinamiškas vieno profilio keitimas kitu. Kiekvienam profiliui priskiriama aplinka. Dėl to įrenginio sensorių dėka MOSES sistema gali aptikti aplinkos pasikeitimą ir pagal tai pakeisti į tinkamą profilį. Įdiegus sistemą ir atlikus su ją bandymus pastebėta, kad jos valdymo išlaidos minimalios ir galutiniam vartotojui visai nepastebimos.



7 pav. MOSES veikimo principas

6 paveikslėlyje pavaizduota apžvalga MOSES karkaso, kuris įgyvendintas naudojant Android tarpinėje perrašant arba praplečiant kai kuriuos modulius. Pagrindinis bruožas yra saugumo profiliai (SP). Juose nurodoma, kokios programėlės ir duomenys leidžiami naudoti bei saugumo polisai.

MOSES gali palaikyti keletą saugumo profilių viename įrenginyje. Sistemoje pagrindinis saugumo profilis yra „Default“. Jame laikomos visos naujai įrašytos programos ir duomenys, kurie nėra nurodyti jokiame kitame profilyje. Vartotojas gali kurti ir redaguoti profilius pasitelkęs „**MOSES Configuration Manager (MCM)**“. Tačiau norint redaguoti kai kuriuos profilius gali reikėti specialių teisių, pvz. Saugumo profilyje – „Work“, kuris skirtas naudoti darbo metu, kai jungiamasi prie įmonės išteklių. Šiuos profilius gali redaguoti tik įmonės IT administratoriai.

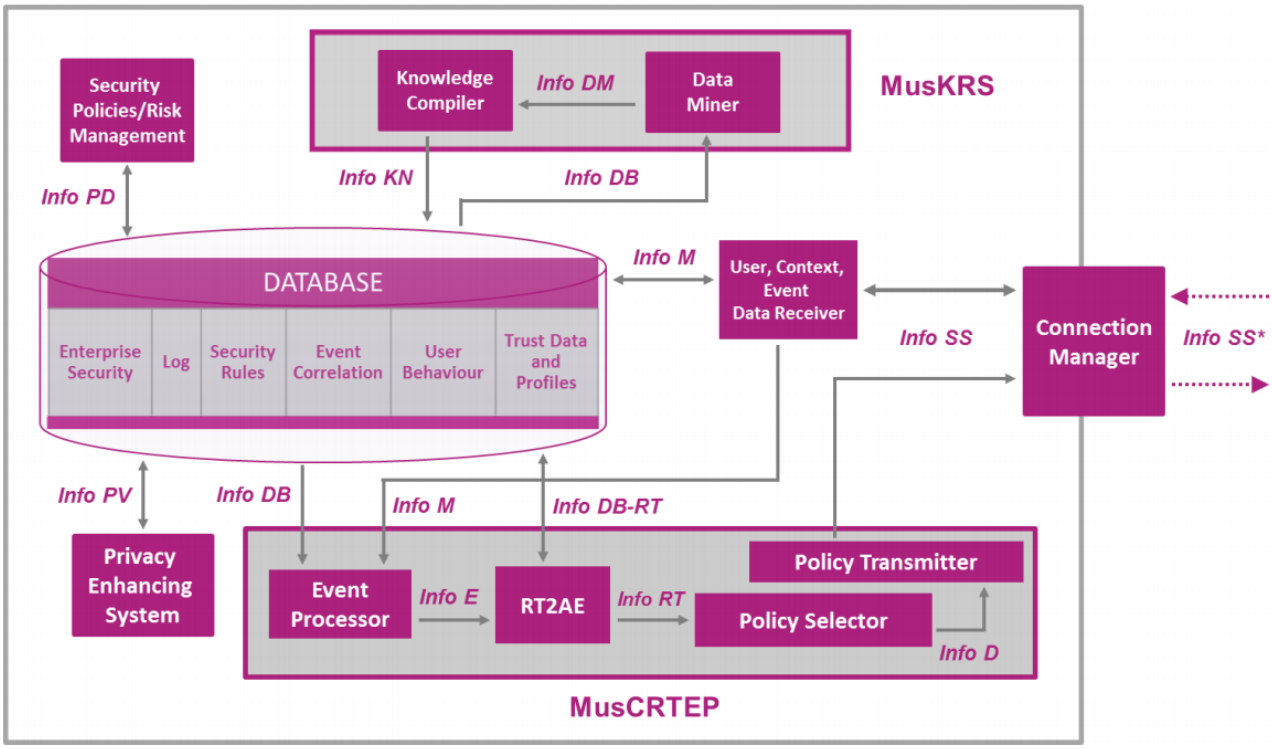
Profilių pakeitimus vykdo „**MOSES Hypervisor(MH)**“. Kai SP aktyvuojamas MH užkrauna to profilio saugumo polisus į „**Policy Enforcement Module(PEM)**“. Kai programa

reikalauja informacijos PEM patikrina, ar aktyvus profilis turi reikalingus polisus. Jei reikiami polisai randami, tai reikalinga informacija perduodama programai. Vartotojas gali pats keisti aktyvius profilius. Tačiau labiau pažengęs MOSES mechanizmas leidžia aptikti aplinkos pasikeitimą ir automatiškai pakeisti profilius. Pavyzdžiui, darbuotojui atėjus į darbą ir prisijungus prie įmonės bevielio tinklo automatiškai pakeičia į darbinį profilį, kuriame leidžiama naudoti įmonės duomenims, bet uždraudžia žaisti žaidimus įrenginyje.

1.3.4. Sistema MUSES

MUSES (Multiplatform Usable Endpoint Security System) - tai įvairių platformų sistema, kuri remiasi kompanijos saugumo politika [1]. Jos pagrindinis bruožas – ji geba „mokintis“ iš vartotojo elgsenos ir prisitaikyti bei sukurti naujus taisyklių rinkinius, kad efektyviau suvaldytų potencialius saugumo incidentus, kurie atsirado dėl vartotojo netinkamo elgesio. Ši sistema analizuos vartotojų įpročius naudodama duomenų išgavimo („Data Mining“) technikas ir mašinų mokymosi metodais.

MUSES architektūra pavaizduota 8 pav. ir 9 pav Tai kliento/serverio modelis, kur klientas bus įrašytas kiekviename mobiliajame įrenginyje, nepriklausomai nuo platformos (operacinės sistemos ir įrenginio tipo), o serverio pusė bus įrašyta korporacijos saugumo operacijų centre. Abi pusės susijungs saugiu kanalu (naudojant HTTPS) per internetą.



8 pav. MUSES serverio architektura

Vienas pagrindinių MUSES sistemos bruožų yra prisitaikymas prie vartotojo ir aplinkos. Tai padeda įgyvendinti komponentas, kuris pavaizduotas 8 pav., pavadintas MusKRS (MUSES

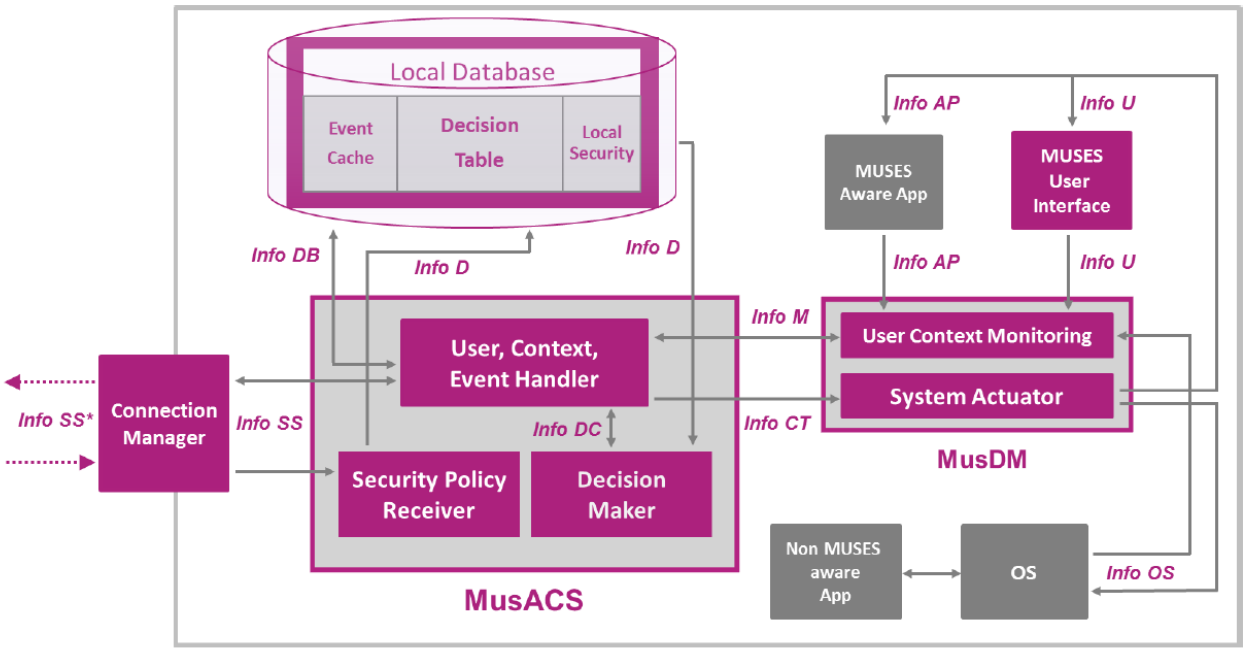
Knowledge Refinement System) – MUSES žinių tobulinimo sistema. MusKRS veikia serverio pusėje ir analizuoja visą surinktą informaciją apie įvykius, konteksto pakeitimus, su vartotojais susijusią informaciją. Išanalizavus duomenis atitinkamai keičiamos saugumo taisyklės.

MUSES serverio architektūra pavaizduota 8 pav. Ji susideda iš trijų pagrindinių komponentų: sistemos duomenų bazė, nepertraukiamas realaus laiko įvykių stebėjimas (MusCRTEP) ir žinių tobulinimo sistema (MusKRS).

Sistemos duomenų bazėje laikoma visa apdorojama informacija, tai saugumo taisyklės, vartotojų elgsenos, patikima informacija ir profiliai, įvykių žurnalai ir t. t.

Nepertraukiamas realaus laiko įvykių stebėjimas - esminis MUSES sistemos komponentas, kuris atsakingas už įvykių surinkimą ir galimų grėsmių identifikavimą.

Žinių tobulinimo sistema atsakinga už duomenų, esančių duomenų bazėje, analizavimą, identifikavimą tinkamos informacijos, tokios kaip svarbių elgsenos šablonų ar saugumo įvykių. Išanalizavus duomenis atitinkamai keičiamos saugumo taisyklės arba sukuriamos naujos.



9 pav. MUSES kliento architektūra

MUSES kliento pusės architektūra pavaizduota 9 pav. Ją sudaro taip pat trys pagrindiniai komponentai: lokali duomenų bazė, įrenginio stebėtojas ir prieigos kontrolės sistema.

Lokali duomenų bazė skirta saugumo duomenims (saugos taisyklių, vartotojo identifikacijos duomenys ir išgauti įvykiai, bei jų informacija).

Įrenginio stebėtojas atsakingas už įvykių ir vartotojo sukurtos informacijos surinkimą. Jis taip pat riboja kontroliuojamas programas.

Prieigos kontrolės sistema reguliuoja, ką daryti pagal surinktą informaciją. Sprendimas gali būti padarytas lokaliai, įrenginyje, jei gautas įvykis atitinka kuria nors saugumo taisyklę, arba siunčiama užklausa į serverį.

Kiti kliento komponentai yra: *vartotojo sąsaja*, kuri leidžia vartotojui bendrauti su sistema, *sujungimo valdytojas*, kuris kontroliuoja komunikaciją tarp kliento ir serverio.

1.1 lentelė. Esamų sprendimų palyginimas

Palyginimo kriterijus	**BYODroid**	**MOSES**	**MUSES**
Operacinė sistema	Android	Android	Multiplatformė
Duomenų atskirimas	-	+	+
Profilių naudojimas	-	+	+
Programų draudimas	-	+	+
Nauju taisyklių pridėjimas	Rankinis	Rankinis	Rankinis ir automatinis

1.4. Šifravimo algoritmai

Šifravimo algoritmų yra simetrinių ir asimetrinių [7]. Simetrinio šifravimo metu naudojamas vienas raktas, kurį žino abi pusės (asmuo, norintis užšifruoti duomenis, ir asmuo, kuris nori šiuos duomenis iššifruoti). Asimetrinio šifravimo metu naudojami du raktai: viešasis ir privatusis. Vienas raktas žinomas visiems, o kitas tik tų raktų poros savininkui. Norint užšifruoti duomenis naudojamas viešasis raktas, iššifruojant juos reikalingas privatus.

Simetrinis šifravimas pranašesnis už asimetrinį tuo, kad užšifravimas ir iššifravimas vyksta daug greičiau, kartais net kelis kartus. O didžiausias minusas - abi pusės turi žinoti tą raktą, iškyla problema, kaip jį saugiai perduoti.

1.4.1. Data Encryption Standard (DES)

DES – blokinis šifravimo algoritmas sukurtas IBM tyrėjų aštunto dešimtmečio pradžioje [8]. Tai buvo pirmasis šifravimo algoritmas patvirtintas Jungtinių Valstijų savivaldybės viešam naudojimui. Šifruojant šiuo algoritmu duomenys skaidomi į 64 bitų blokus. Toliau kiekvienas suskaidytas blokas užšifruojamas tuo pačiu raktu. DES raktas sudarytas iš 64 bitų, tačiau aštuoni bitai naudojami sulyginti, taigi efektyviai naudojamas raktas yra 56 bitų. Šifravimo metu įvykdami 16 ciklų.

1.4.2. Triple Data Encryption Algorithm (3DES)

3DES – blokinis šifravimo algoritmas, kuris skirtas pakeisti pasenusį DES . Jis nuo pirmtako skiriasi tuo, kad užšifruojant naudojami trys raktai ir su jais įvykdomos trys šifravimo iteracijos [7]. Kaip ir paprasto DES šifravimui naudojamai 64 bitų blokai. Pirmos iteracijos metu kiekvienas šifravimo blokas užšifruojamas pirmuoju 64 bitų raktu, antros – gautas užšifruotas blokas iššifruojamas antru raktu, trečios – gautas iššifruotas blokas vėl užšifruojamas trečiu raktu. Kaip ir galima tikėtis, šis algoritmas yra saugesnis nei paprastasis DES, tačiau siekiant saugomo aukojamas šifravimo greitis. Šifravimas šiuo algoritmu gali trūkti iki trijų kartų ilgiau, nei pirmtaku – paprastuoju.

1.4.3. Advanced Encryption Standard (AES)

AES – kitas šifravimo algoritmas, skirtas pakeisti senstanti DES. Jis labiau matematiškai optimizuotas, bet jo pagrindinė stiprybė yra raktų ilgio pasirinkimas [7]. Nes laikui nulaužti užšifruotą tekstą dažniausiai priklauso nuo rakto ilgio. Šis algoritmas yra lankstesnis, nes naudoja skirtingus raktų dydžius (128, 192, 256 bitų). Taip pat, lyginant su pradininku DES algoritmu, kuris šifravo 64 bitų blokus, šis šifravimo metodas gali dirbti su 128, 192, 256 bitų blokais. Šifruojant AES ciklų skaičius priklauso nuo rakto blokų dydžio. Tai parodyta ***1.1*** lentelėje. Vienintelė sėkminga ataka prieš šį algoritmą buvo "Side-chanel attack"

1.1 AES algoritmo vciklų skų skaičiaus prikloasomybė nuo rakto ilgio

	Rakto ilgis	**Bloko dydis**	**Ciklų skaičius**
AES-128	128	128	10
AES-192	192	192	12
AES-256	256	256	14

1.5. Analizės išvados

- Išanalizavus asmeninių įrenginių naudojamų įmonėse saugos iššūkius ir saugos problemų sprendimo metodus pastebėta kad taikant BYOD politiką atsiranda grėsmių paviešinti svarbius duomenis.
- Išanalizavus sukurtas saugos sistemas pastebėjome, kad jos orientuotos į duomenų praradimą piktybiškų programų dėka.
- Analizės rezultatai rodo reikalingumą suprojektuoti ir ištirti sistemą, kuri galėtų apsaugoti duomenis ne tik nuo piktybiškų programų, bet ir nuo duomenų išplatinimo pametus mobilųjį įrenginį.

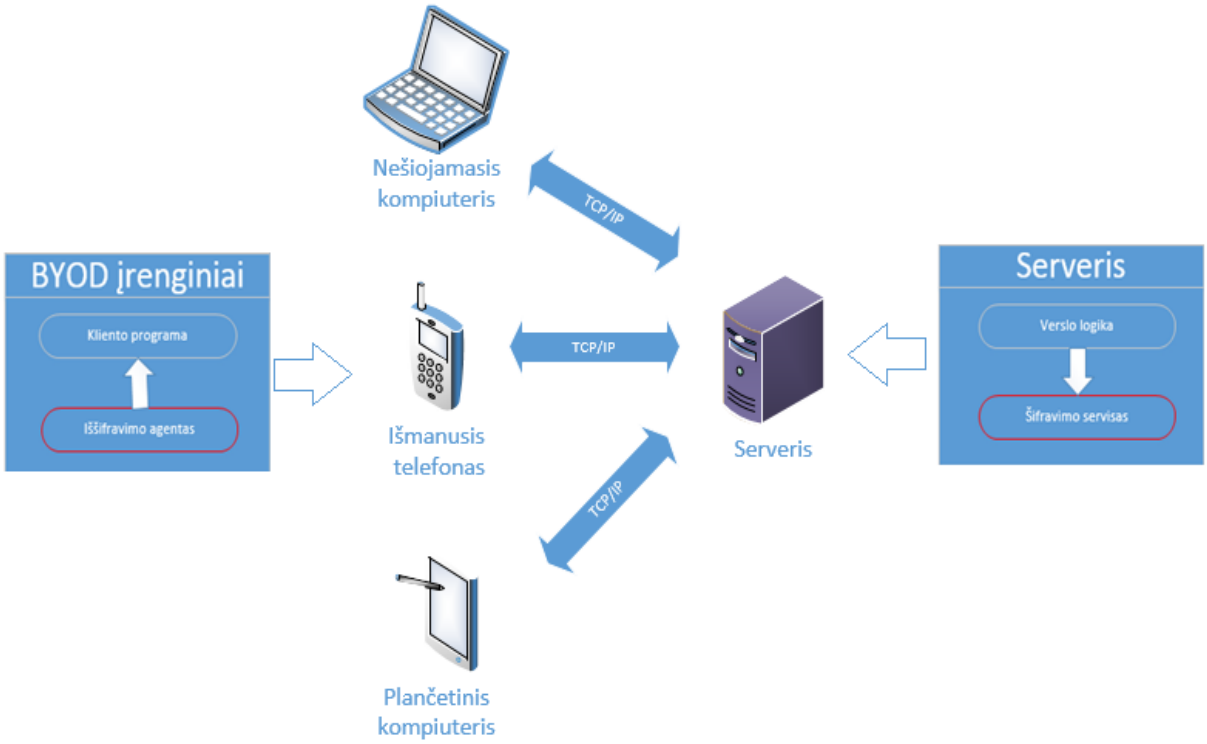
2. ASMENINIŲ ĮRENGINIŲ NAUDOJAMŲ ĮMONĖSE INFORMACIJOS SAUGOS METODŲ TAIKYMAS

Atlikus probleminės srities analizę pastebėta, kad tiriamosios sistemos koncentruojasi į apsaugą nuo kenksmingų programų. Taip pat praradus įrenginį šios sistemos neapsaugo jame esančių duomenų. Todėl atsižvelgiant į šiuos trūkumus siūlomas šis projektas.

2.1. Asmeninių įrenginių naudojamų įmonėse informacijos saugos metodų taikymo sistema

Standartinę įmonės sistemą sudaro du komponentai: serveris ir klientas (mobilus įrenginys). Serverio pusėje vykdomi skaičiavimai ir laikomi duomenys, kurie reikalingi darbuotojui. Kliento pusėje yra apdorojami gauti duomenys. Šie duomenys perduodami laidiniu ar bevieliu ryšiu. Todėl svarbūs įmonės duomenys, atsidūrę mobiliajame įrenginyje, tampa pažeidžiami.

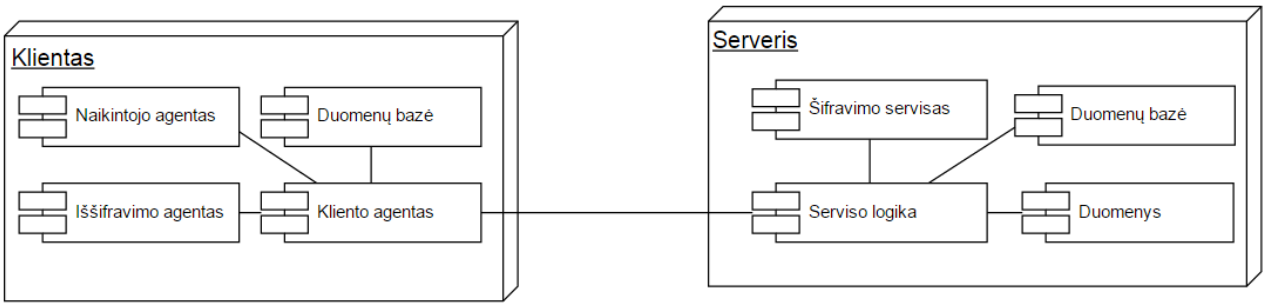
Siūloma informacijos saugos metodų taikymo sistema gali padėti to išvengti. Norint ja naudotis nereikės diegti papildomų serverių, užteks praplėsti jau esamus. Jos veikimo principas pavaizduotas 10 pav. Raudonai pažymėti komponentai yra naujai pridėti. Šifravimo servisas bus diegiamas serveryje. Serviso tikslas - gautus duomenis iš verslo logikos užšifruoti ir perduoti jų reikalaujančiam įrenginiui. Taip pat jis atsakinės į iššifravimo agento užduodamas užklausas, dėl duomenų iššifravimo raktų. Iššifravimo agentas bus diegiamas mobiliajame įrenginyje. Agentas tvarkys gautus duomenys iš serviso. Norint iššifruoti reikiamus duomenis jis sudarys užklausą šifravimo servisui dėl reikiamo iššifravimo rakto ir algoritmo.



10 pav. Informacijos saugos metodų taikymo sistema

2.2. Asmeninių įrenginių naudojamų įmonėse informacijos saugos metodų taikymo sistemos architektūra

Kaip minėta anksčiau, ši sistema susidės iš dviejų dalių: kliento pusės dalis, kuri bus įdiegta įrenginyje ir serverio pusės dalis, kuri bus patalpinta serveryje. Šios sistemos architektūra pavaizduota 11 pav.



11 pav. Informacijos saugos metodų taikymo sistemos architektūra

Serverio pusėje bus keturi komponentai: serviso logika, šifravimo servisas, duomenų bazė ir duomenys.

Duomenys, kuriuos reikia apdoroti (užšifruoti). Jie bus nuskaitomi iš atitinkamos duomenų bazės arba gaunami iš kitų šaltinių.

Šifravimo servisas pagal pateiktus parametrus (slaptą raktą, algoritmą ir t. t.) užšifruos reikiamus duomenis.

Duomenų bazėje bus laikomi raktai, su kuriais bus galima iššifruoti duomenis ir duomenų paketo identifikavimo numeris.

Serviso logika - pagrindinė serverio pusės dalis, kuri atsakinga už bendravimą tarp komponentų, šifravimo raktų talpinimą į duomenų bazę, reikiamų raktų klientui perdavimą bei reikiamų duomenų išgavimą.

Kliento pusėje bus taip pat keturi komponentai: kliento agentas, iššifravimo agentas, naikintojo agentas ir duomenų bazė.

Naikintojo agentas skirtas pašalinti senus įmonės duomenis, taip atlaisvinant įrenginio atmintį. Šalinimo intervalai bus konfigūruojami.

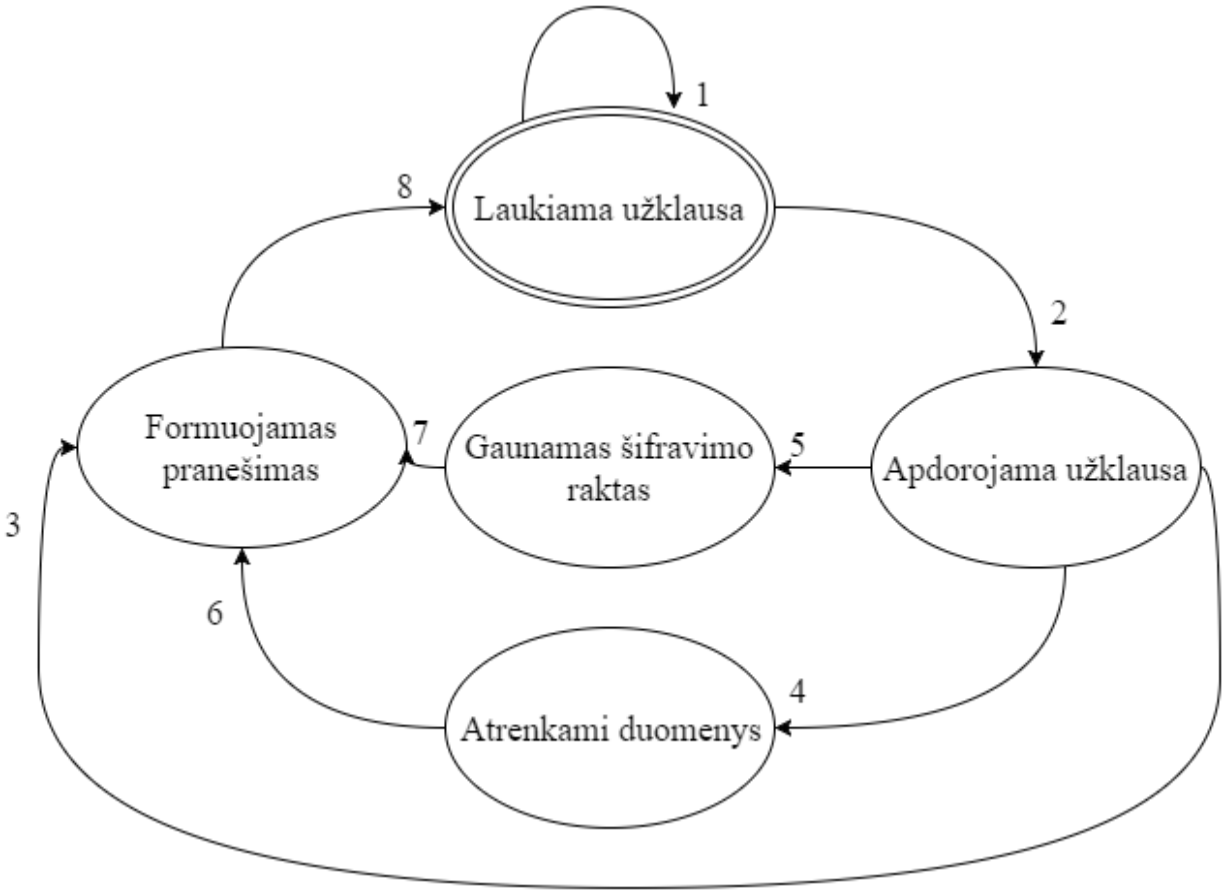
Duomenų bazėje bus talpinama gautų duomenų informacija.

Iššifravimo agentas skirtas pagal gautus parametrus iššifruoti reikiamus duomenis.

Kliento agentas yra pagrindinis kliento pusės agentas, atsakingas už bendravimą su kitais komponentais bei su šifravimo servisu. Jis talpins gautus duomenis į duomenų bazę, perdavinės duomenis ir parametrus šifravimo agentui bei sudarinės užklausas šifravimo servisui dėl reikiamų raktų.

2.3. Asmeninių įrenginių, naudojamų įmonės, informacijos saugos metodų taikymo sistemos būsenų diagramos

Šiame skyriuje pavaizduota asmeninių įrenginių, naudojamų įmonės, informacijos saugos sistemos serverio serviso ir kliento agento būsenų diagramos.

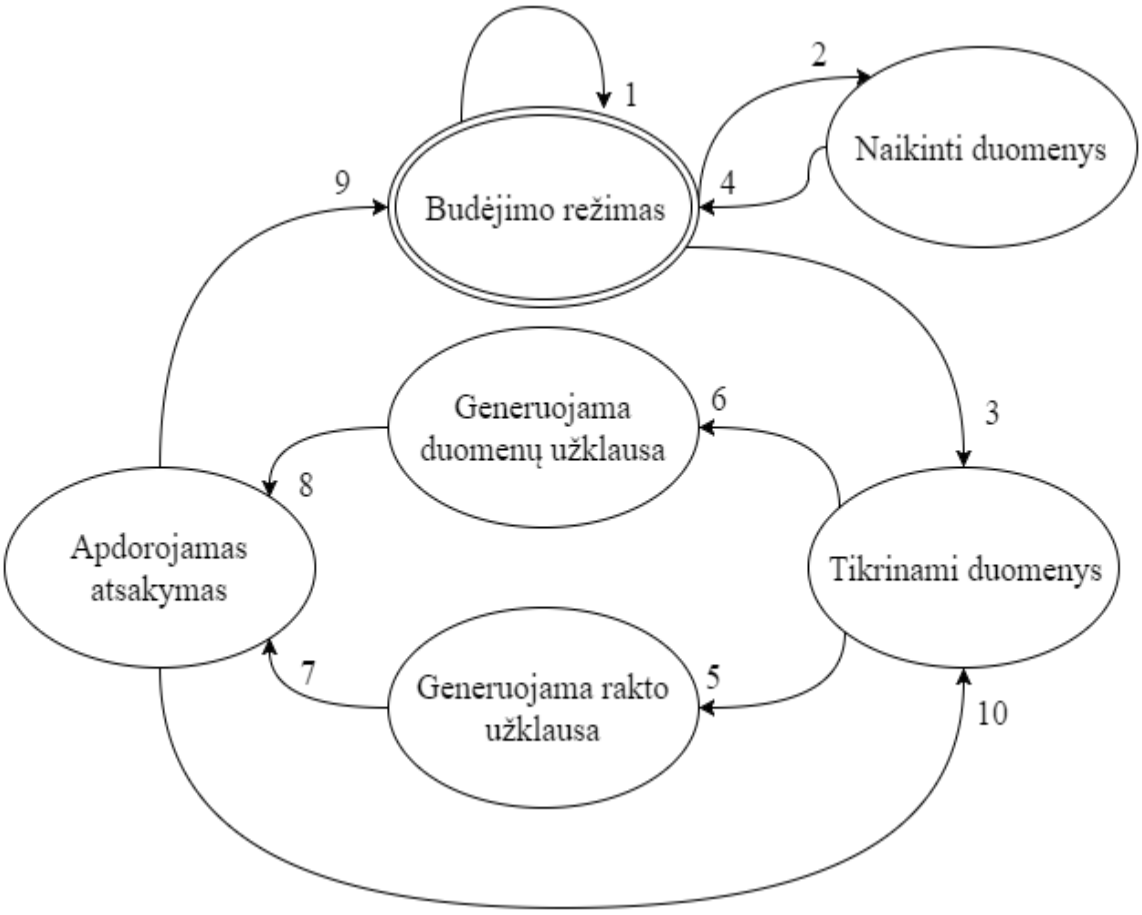


12 pav. Serverio būsenų diagramos

12 pav. pavaizduota serverio būsenų diagrama. Joje matome, kad serveris gali būti vienoje iš 5 būsenų. Pradinė serverio būsena yra „Laukiame užklausos“. Tai būsena, kai serveris dirba laukimo režimu ir nieko nedaro, kol negauna užklausos iš vieno iš klientų. Ši būsena taip pat yra ir paskutinė. Būsenų pokyčiai aprašyti ***2.1*** lentelėje.

2.1 lentelė. Serverio būsenų pokyčiai

Pokyčio nr.	**Pradinė būsena**	**Pokytis**	**Sekanti būsena**	**Rezultatas**
1.	Laukiama užklausa	-	Laukiama užklausa	-
2.		Gaunama užklausa iš kliento	Apdorojama užklausa	Identifikuojamas įrenginys
3.	Apdorojama užklausa	Klientas neturi teisių pasiekti reikiamų duomenų	Formuojamas pranešimas	Perduodama žinutė, kad klientas negali pasiekti šių duomenų
4.		Klientas turi teises pasiekti duomenis, bet jų neturi įrenginyje	Atrenkami duomenys	Klientas patikrintas ir gali pasiekti reikiamus duomenis
5.		Klientas turi teises pasiekti duomenis ir reikalingas iššifravimo raktas	Gaunamas šifravimo raktas	Klientas patikrintas ir gali pasiekti reikiamus duomenis
6.	Atrenkami duomenys	Gautas reikiamų duomenų sąrašas	Formuojamas pranešimas	Reikalingi duomenys užšifruojami ir šifravimo raktas įrašomas į duomenų bazę
7.	Gaunamas šifravimo raktas	Gauta kliento viešasis raktas, identifikacijos numeris ir duomenų nuoroda		Gaunamas duomenų šifravimo raktas ir jis užšifruojamas kliento viešuoju raktu
8.	Formuojamas pranešimas	Gauti duomenys, kuriuos reikia perduoti klientui	Laukiama užklausa	Pranešimas perduodamas klientui



13 pav. Kliento agento būsenų diagrama

13 pav. pavaizduota kliento agento būsenų diagrama. Joje matome, kad kliento agentas gali būti vienoje iš 6 būsenų. Pradinė serverio būsena yra „Budėjimo režimas“. Tai būsena, kai kliento agentas pagal nustatytą laiko tarpą tikrina, ar įrenginys prijungtas prie įmonės tinklo ir duomenų bazės, ar nėra kokio duomenų failo, kurį reiktų ištrinti iš įrenginio. Ši būsena taip pat yra ir paskutinė. Būsenų pokyčiai aprašyti ***2.22.1*** lentelėje.

2.2 Kliento agento būsenų pokyčiai

Pokyčio nr.	**Pradinė būsena**	**Pokytis**	**Sekanti būsena**	**Rezultatas**
1.	Budėjimo režimas	-	Budėjimo režimas	-
2.		Gaunamas įvykis, kad reikia panaikinti duomenis	Naikinti duomenys	Perduodama duomenų nuoroda

3.		Vartotojui reikalingi duomenys	Tikrinami duomenys	Pasirenkami reikalingi duomenys
4.	Naikinti duomenys	Gauta duomenų nuoroda	Budėjimo režimas	Pašalinami duomenys iš įrenginio
5.	Tikrinami duomenys	Patikrinama, ar duomenys įrašyti į įrenginį	Generuojama rakto užklausa	Perduodama duomenų nuoroda
6.		Patikrinama, ar duomenys įrašyti į įrenginį	Generuojama duomenų užklausa	Perduodamas reikalingų duomenų sąrašas
7.	Generuojama rakto užklausa	Gauta nuoroda į duomenis	Apdorojamas atsakymas	Sukuriama užklausa, kurioje nurodama sugeneruotas viešasis raktas ir nuoroda į duomenis. Ji perduodama serveriui.
8.	Generuojama duomenų užklausa	Gautas reikalingų duomenų sąrašas		Sukuriama užklausa, kurioje pateikiamas reikalingų duomenų sąrašas. Ji perduodama serveriui.
9.	Apdorojamas atsakymas	Gautas šifravimo raktas	Budėjimo režimas	Šifravimo raktas iššifruojamas ir su juo iššifruojami reikalingi duomenys.
10.		Gauti užšifruoti duomenys	Tikrinami duomenys	Užšifruoti duomenys įrašomi į įrenginį.

2.4. Asmeninių įrenginių naudojamų įmonėse informacijos saugos sistemos veiklos diagramos

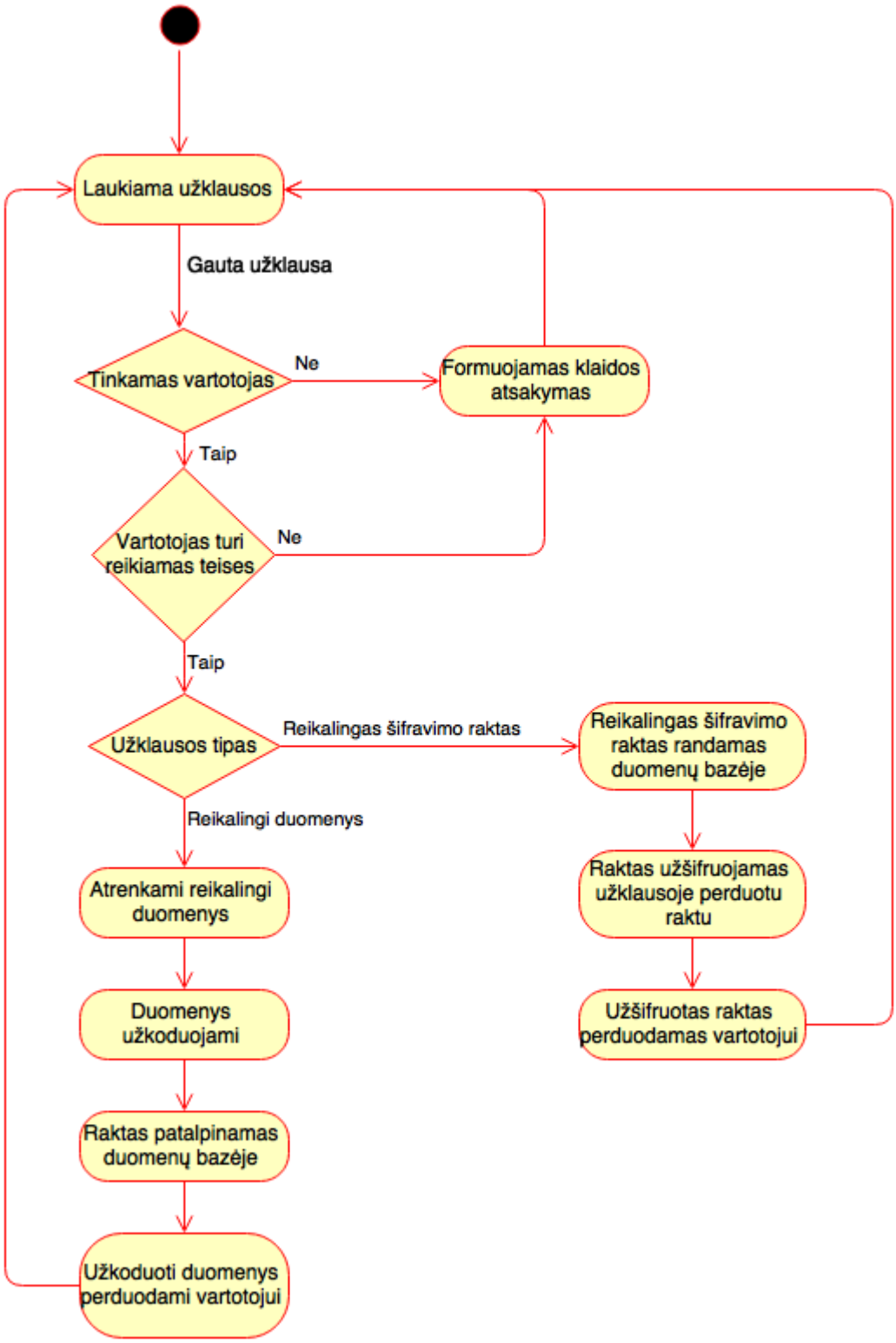
Kliento įrenginys su serveriu bendraus naudodamas užklausas. Užklausos bus dviejų rūšių: vienos skirtos gauti užšifruotiems duomenims, kitos - gauti šifravimo raktą tiems duomenims iššifruoti. Generuojant užklausą į ją bus įrašoma vartotojo įrenginio indentifikavimo numeris (paprastai MAC adresas), užklausos tipas, pagal kurį serveris žinos, ar vartotojui reikia duomenų, ar

šifravimo rakto, ir kurie duomenys reikalingi. Taip pat kuriant užklausą gauti šifravimo raktui bus perduodamas įrenginio sugeneruotas šifravimo raktas, su kurio serveris turės užšifruoti duomenų šifravimo raktą.

14 pav. pavaizduota serverio veiklos algoritmas. Joje matome, kad įjungus serverį jo serviso logika būna užklausos laukimo būsenoje. Iš jos pereinama tik tada, kai gaunama užklausa iš kliento. Gavus užklausą servisas tikrins jos teisingumą ir nustatys, kokių duomenų reikalauja klientas. Tai padarys per tris žingsnius. Pirmuoju žingsniu servisas patikrins, ar duomenų reikalaujantis klientas yra duomenų bazėje, jei užklausoje nurodyto identifikavimo numerio neras duomenų bazėje, tai servisas praneš vartotojui, kad tokio kliento nerado ir grįš į laukimo būseną. Jei ras klientą, tai pereis į kitą žingsnį. Antrame žingsnyje bus tikrinama, ar klientui suteiktos atitinkamos teisės pasiekti jo reikalaujamų duomenų. Jei duomenų bazėje nebus nurodytos atitinkamos teisės, servisas grąžins pranešimą, kad vartotojas neturi reikiamų teisių ir grįš į laukimo būseną. Atlikus vartotojo tikrinimą bus iš užklausos tipo nustatoma, kokių veiksmų reikės imtis: grąžinti užšifruotus duomenis ar duomenims iššifruoti reikiamus raktus.

Norint gauti duomenis servisas turės surasti juos ir sugeneruoti šifravimo raktą. Su šiuo raktu jis užšifruos duomenis ir tą raktą patalpins į duomenų bazę. Taip pat duomenų bazėje bus nurodoma, kokiam vartotojui reikėjo šių duomenų ir nuoroda į duomenis, kad būtų galima nesunkiai grąžinti reikiamą šifravimo raktą. Galiausiai papildžius duomenų bazę šie duomenys bus perduoti vartotojui ir servisas grįš į laukimo būseną.

Norint gauti šifravimo raktą servisas turės iš užklausos pasiimti vartotojo identifikacijos numerį ir nuorodą į duomenis, ir pagal juos iš duomenų bazės išgaus reikiamą raktą. Gavęs raktą servisas užšifruos vartotojo perduotu raktu ir tada perduos reikalingą raktą. Galiausiai servisas grįš į laukimo būseną.

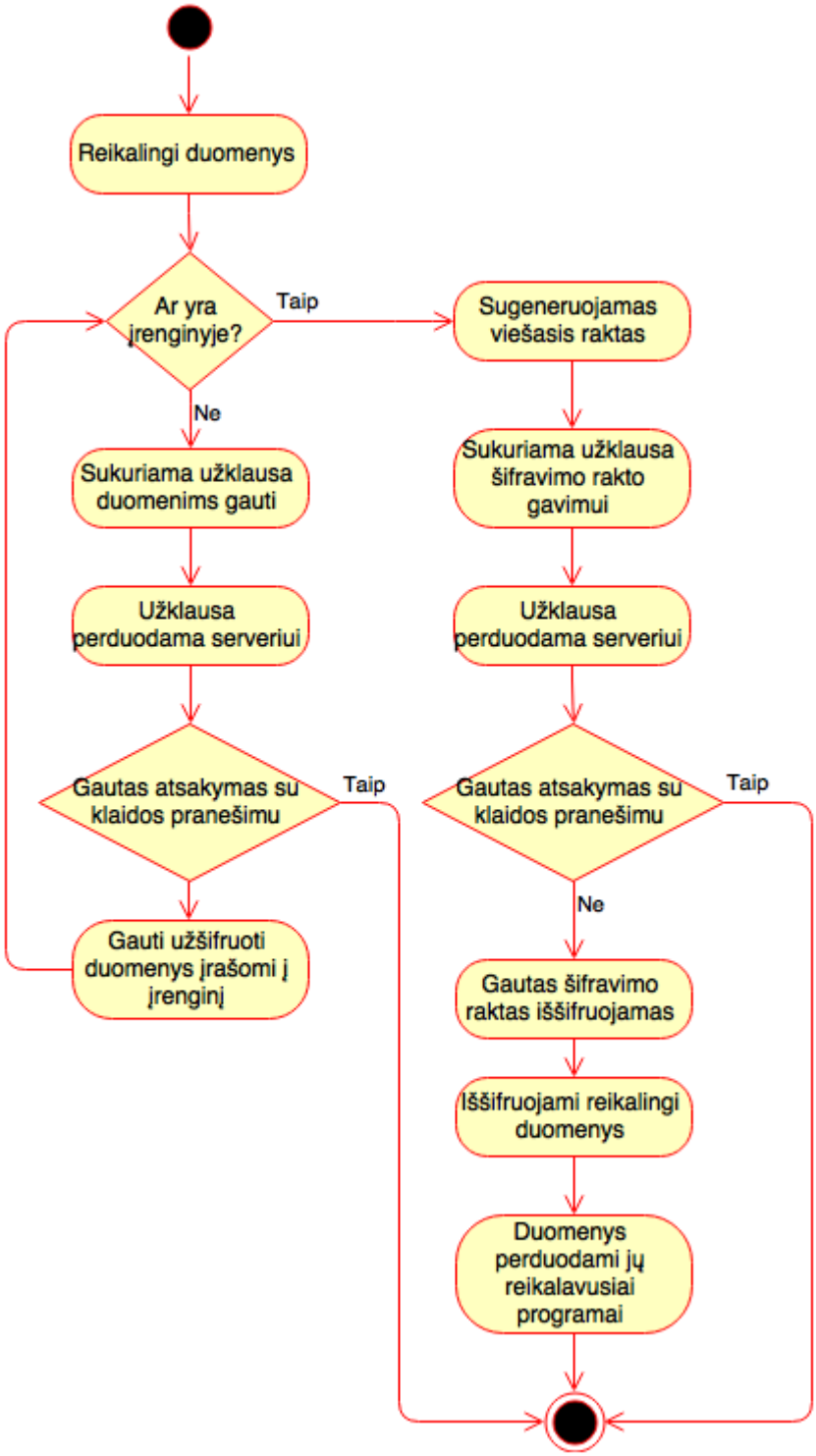


14 pav. Serverio veiklos algoritmas

15 pav. pavaizduota kliento veiklos algortimas. Visi veiksmai prasideda, kai programa pareikalauja jai reikalingų duomenų kliento agento. Jis patikrina, ar reikalingi duomenys jau yra įrašyti į įrenginį, pagal tai agentas generuos užklausą serveriui. Agentas, pamatęs kad reikiamų duomenų įrenginyje nėra, sugeneruos užklausą ir ją perduos serveriui. Jei serveris atsakys be klaidos pranešimo (kurios gali būti dėl netinkamo vartotojo identifikacijos numerio ar nepakankamai teisių) gautus

duomenis įrašys į įrenginį. Tada, kai kliento agentas matys, kad yra reikalingi duomenys, jis galės pareikalauti šifravimo rakto.

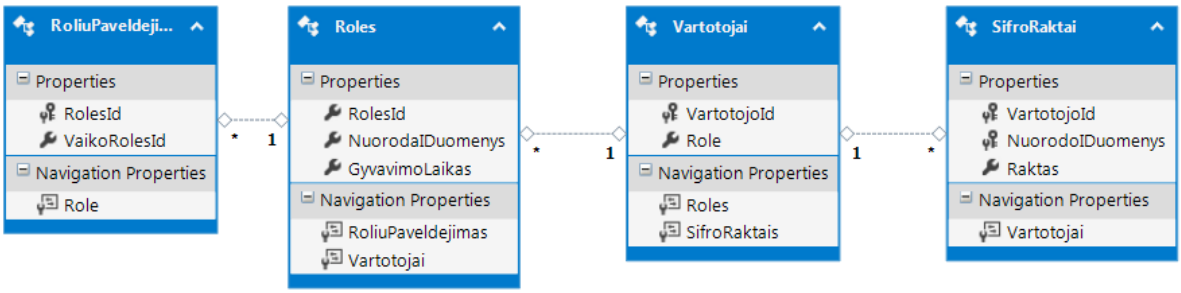
Norint gauti šifravimo raktą agentas sugeneruos savo raktą, kuris skirtas serverio šifravimo raktui užšifruoti. Šį raktą agentas pridės prie sugeneruotos užklausos ir ją perduos serveriui. Gavęs atsakymą be klaidos pranešimos šifravimo agentas iššifruos reikalingą raktą ir su šiuo raktu reikalingus duomenis, kurie bus perduoti jų reikalavusiai programai.



15 pav. Kliento veiklos algoritmas

2.5. Duomenų bazių struktūros

Serverio duomenų bazėje reikalingos keturios lentelės: „Vartotojai“, „SifroRaktai“, „Roles“ ir „RolesPaveldėjimas“. Jos struktūra pavaizduota 16 pav.



16 pav. Duomenų bazės struktūra

„Vartotojai“ lentelėje pildoma informaciją apie vartotojus, jos struktūra pavaizduota ***2.3*** lentelėje.

2.3 lentelė. „Vartotojai“ lentelės struktūra

Laukas	**Lauko aprašymas**
VartotojoId	Vartotojo identifikacijos numeris
Rolė	Vartotojui priskirta rolė

„**SifroRaktai**“ lentelėje saugoma informaciją apie šifravimo serviso užšifruotus duomenis. Vienas vartotojas galės būti susietas su keliais šios lentelės įrašais, t. y. vartotojas galės turėti kelis šifro raktus. Šios lentelės struktūra pavaizduota ***2.4*** lentelėje.

2.4 lentelė. "SifroRaktai" lentelės struktūra

Laukas	**Lauko aprašymas**
VartotojoId	Vartotojo identifikacijos numeris
NuorodaIDuomenys	Nuoroda į duomenys, skirta atpažinti kokie duomenys buvo užšifruoti šiuo raktu
Raktas	Šifravimo raktas kuris reikalingas, kad vartotojas galėtų pasinaudoti gautais duomenimis.

Lentelėje „**Roles**“ laikoma informacija apie sukurtas roles ir prie kokių duomenų tam tikra rolė turi priėjimą. Jos struktūra pavaizduota ***2.5*** lentelėje.

2.5 lentelė. "Roles" lentelės struktūra

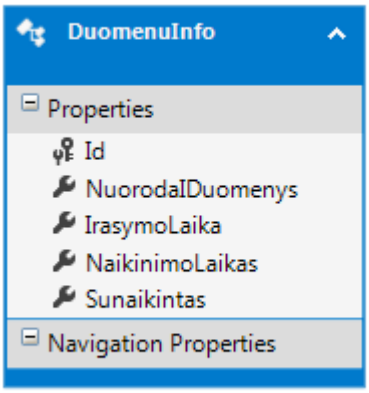
Laukas	**Lauko aprašymas**
RolesId	Rolei identifikuoti skirtas laukas
NuorodaIDuomenys	Nurodomi kokie duomenys gali būti pasiekiami šiai rolei
GyvavimoLaikas	Kliento naikintojo agentui skirtas laukas, nurodantys kiek laiko saugoti duomenys iki jų sunaikinimo

Lentelė „**RoliuPaveldejimas**“ leidžia nurodyti, kokias roles gali paveldėti kitas roles, taip sumažinant duomenų kiekį lentelėje „Roles“ ir palengvina rolių valdymą. Jos struktūra pavaizduota ***2.6*** lentelėje.

2.6 lentelė. "RoliuPaveldejimas" lentelės struktūra

Laukas	**Lauko aprašymas**
RolesId	Rolė, kuri perima kitos rolės teises.
VaikoRolesId	Rolė, kuri perduoda savo teises.

Kliento duomenų bazėje reikalinga viena lentelė. Jos struktūra pavaizduota 17 pav.



17 pav. Kliento duomenų bazės struktūra

Lentelėje „DuomenuInfo“ laikoma informacija apie iš serverio gautus duomenys. Jos struktūra aprašyta ***2.7*** lentelėje.

2.7 lentelė. "DuomenuInfo" lentelės struktūra

Laukas	**Lauko aprašymas**
Id	Duomenų identifikacijos numeris
NuorodaIDuomenys	Nurodoma kur patalpinti atsisiųsti duomenys
IrasymoLaikas	Nurodoma kada buvo gauti duomenys
NaikinimoLaikas	Skirtas naikintojui agentui, kad žinoti kada reikia pašalinti duomenys
Sunaikintas	Vėliavėlė skirta pažymėti, kai duomenys bus pašalinti

2.6. Klasių diagramos

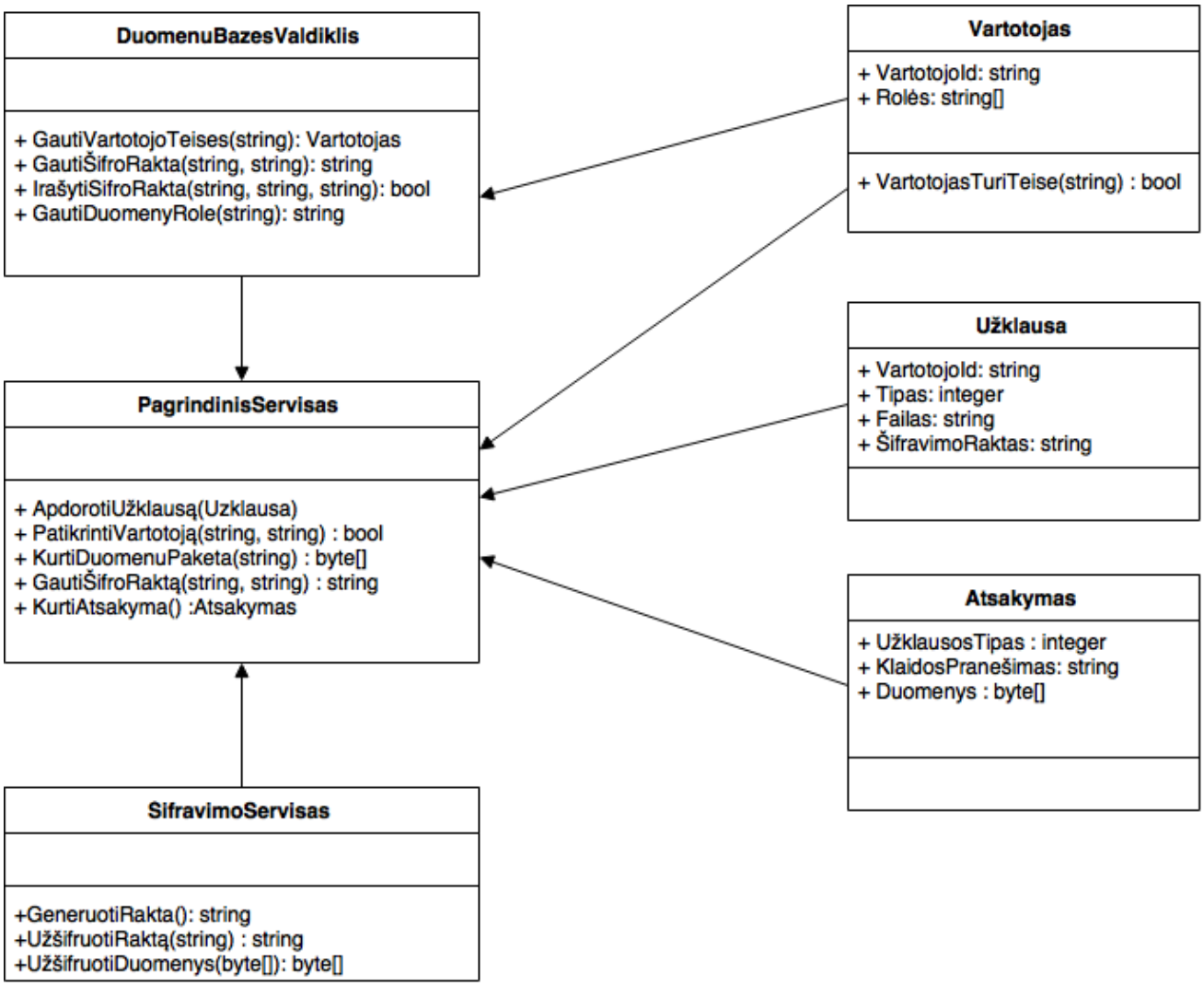
Serverio klasių diagrama aprašyta 18 pav. Serveris naudos tris modulius: „DuomenųBazėsValdiklis“, „ŠifravimoServisas“ ir „PagrindinisServisas“. Šiems moduliams taip pat reikės pagalbinių klasių, kurios saugos visą informaciją apie objektus.

Duomenų bazės modulis atsakingas už pagrindinio serviso bendravimą su duomenų baze. Per jį bus perduodama informacija ir įrašoma į duomenų bazę. Šio modulio naudojami metodai aprašyti ***2.8*** lentelėje.

2.8 lentelė. "DuomenųBazėsValdiklis" metodai

Metodas	**Metodo aprašymas**
GautiVartotojoTeise(string) : Vartotojas	Metodui perduodamas vartotojo identifikacijos numeris. Pagal jį iš duomenų bazės gaunamas vartotojo rolių sąrašas, kuris patalpinamas „Vartotojas“ objekte ir grąžinamas pagrindiniam servisui
GautiŠifroRakta(string, string): string	Metodui perduodami vartotojo identifikacijos numeris ir nuoroda į duomenys, kuriu reikia. Pagal šiuos parametrus iš duomenų bazės gaunamas šifro raktas ir jis grąžinamas pagrindiniam servisui
ĮrašytiŠifroRakta(string, string, string):bool	Metodui perduodami vartotojo identifikacijos numeris, nuoroda į duomenys ir šifro raktas su kuriuo buvo užifruoti duomenys. Šie parametrai įrašomi į duomenų bazę. Jei pavyksta įrašyti grąžinama „True“

GautiDuomenuRole(string): string[]	Metodui perduodama nuoroda į duomenys. Pagal ją iš duomenų bazės gaunamas sąrašas rolių, kurios gali naudotis šiais duomenimis



18 pav. Serverio klasių diagrama

Šifravimo servisas atsakingas už duomenų užšifravimą. Jo naudojami metodai aprašyti ***2.9*** lentelėje.

2.9 lentelė. Šifravimo serviso metodai

Metodas	**Metodo aprašymas**
GeneruotiRaktą(): string	Generuojamas simetrinio šifravimo raktas, su kuriuo bus užšifruoti duomenys ir įrašytas i duomenų bazę
UžšifruotiRaktą(string, string): string	Metodui perduodamas šifro raktas, kuris gautas iš serverio duomenų bazės ir kliento sugeneruotas viešasis raktas. Su

	viešuoju raktu užšifruojamas šifro raktas. Užšifruotas raktas grąžinamas pagrindiniam servisui
UžšifruotiDuomenys(byte[]): byte[]	Metodui perduodamas duomenų masyvas. Kuris bus užšifruotas sugeneruotu raktu. Užšifruotų duomenų masyvas grąžinamas pagrindiniam servisui

Pagrindinis servisas sujungia visus modulius ir paskirsto darbus. Taip pat jis bendrauja su kiekvienu klientu ir priima jų užklausas. Šio serviso metodai aprašyti ***2.10*** lentelėje.

2.10 lentelė. Pagrindinio serviso metodai

Metodas	**Metodo aprašymas**
ApdorotiUžklausą(Užklausa)	Pagrindinis metodas nuo kurio prasideda visi kiti veiksmai. Jam perduodama iš kliento gauta užklausa.
PatikrintiVartotoją(string, string)	Metodui perduodami vartotojo identifikacijos numeris ir nuoroda į duomenys, kuriuos klientas nori pasiekti.
KurtiDuomenųPaketą(string) : byte[]	Metodui perduodama nuoroda į norimus duomenys. Pagal ją atliekami žingsniai išgauti užšifruotus duomenys, kurie ir yra grąžinami
GautiŠifroRaktą(string, string) : string	Metodui perduodami vartotojo identifikacijos numeris ir nuoroda į duomenys. Pagal juos gaunamas reikiamas šifro raktas, kuris ir grąžinamas
KurtiAtsakymą() : Atsakymas	Atlikus visus žingsnius pagal gautus rezultatus generuojamas atsakymas klientui

2.7. Išvados

- Pasiūlyta asmeninių įrenginių naudojamų įmonėse informacijos saugos metodų taikymo sistema ir jos architektūra.
- Pateiktas asmeninių įrenginių naudojamų įmonės informacijos saugos metodų taikymo sistemos veiklos aprašymas naudojant būsenų diagramas ir algoritmus.
- Suprojektuota ir realizuota serverio ir kliento duomenų bazės
- Realizuota asmeninių įrenginių naudojamų įmonėse informacijos saugos metodų taikymo sistema.

3. ASMENINIŲ ĮRENGINIŲ, NAUDOJAMŲ ĮMONĖSE INFORMACIJOS SAUGOS METODŲ TAIKYMO SISTEMOS EKSPERIMENTINIS TYRIMAS

3.1. Eksperimentui naudojama kompiuterinė įranga

Eksperimentui atlikti naudojama įranga:

- Serveris, kurio parametrai:
  - procesorius Intel i7 4790K 4.00Ghz,
  - darbinė atmintis 8Gb
- Nešiojamas kompiuteris:
  - Procesorius Intel i5-3437U 2.40Ghz
  - Darbinė atmintis 8Gb
- Mobilieji įrenginiai:
  - Samsung Galaxy S4
  - Samsung Galaxy S5
  - Apple Iphone 6

Eksperimente serveris naudojamas užšifruoti norimus persiųsti duomenis. Nešiojamas kompiuteris bei mobilieji įrenginiai naudojami patikrinti, kaip greitai jie gali iššifruoti gautus duomenis.

3.2. Eksperimentui naudojama programinė įranga

Kuriant programą eksperimentui naudojama programinė įranga:

- Windows 10
- Xamarin Forms
- Microsoft Visual Studio 2015

3.2.1. Xamarin Forms

Xamarin yra skirtingų mobilių platformų kūrimo sprendimas, kuris leidžia suvienyti programavimo aplinkas. Vietoj to, kad programuotojai, norėdami kurti aplikacijas „iOS“ operacinei sistemai, rašytų kodą Object-C kalba arba „Android“ operacinei sistemai naudotų Java programavimo kalbą, šis sprendimas leidžia naudoti bendrą programavimo kalbą – C#. Kiekviena aplikacija kuriama naudojant bendrą projektą, kuriame nurodoma vienoda vartotojo sąsaja. Tačiau kadangi kiekviena platforma veikia skirtingai su tam tikrais komponentas, galima aprašyti kiekvienai platformai tik jai skirtų komponentų veikimą. Kitas bendro kodo naudojimo privalumas yra tai, kad tarp skirtingų

platformų galima naudoti vieną kodą, kuris aprašo visa verslo logiką, duomenų modelius, debesų prijungimą ar prieigą prie reikiamos duomenų bazės. Tai suteikia galimybę tą patį kodą naudoti ir skirtinguose aplikacijose, taip sumažinant kitų aplikacijų kūrimo laiką.

Aplikacijų, sukurtų naudojant "Xamarin" sprendimą, veikimo greitis panašus į aplikacijų, skirtų tik tam tikroms platformoms, o kartais netgi aplenkia jas. Vidutiniškai aplikacijos, kurtos su "Xamarin", gali panaudoti 75% sukurto kituose projektuose kodo. Kai kūrimo procesas baigtas, projektas gali būti sukompiliuotas ir įkeltas į atitinkamas aplikacijų parduotuves.

3.2.2. Microsoft Visual Studio

Su Microsoft Visual Studio programine įranga kuriamas šifravimo servisas, kuris pagal atitinkamą šifravimo algoritmą sukuria šifravimo raktus ir užšifruoja duomenis. Taip pat ji naudojama sukurti servisą skirtą nešiojamiems kompiuteriams, kuris iššifruos gautus duomenis.

3.2.3. Šifravimo bibliotekos

Šio eksperimento metu nustatoma, kiek laiko trunka duomenų užšifravimas serveryje ir kiek laiko trunka šių duomenų iššifravimas atitinkamuose įrenginiuose. Taip pat tikrinami šifravimo algoritmai ir bandoma nustatyti, kuris algoritmas tik geriausiai mūsų sistemoje.

Testuojami šifravimo algoritmai:

- 3DES
- DES
- RC2
- AES(RijnDael)

Visus šiuos algoritmus siūlo .Net karkasas. Jie aprašyti lentelėje.

3.1 lentelė. Eksperimente naudojami kripgrafinia algoritmai, bai raktū dydžiai

Eil. Nr.	Algoritmas	Rakto Dydis (bit)	.Net karkaso klasės pavadinimas
1.	3DES	192	TripleDESCryptoServiceProvider
2.	DES	128	DESCryptoServiceProvider
3.	RC2	128	RC2CryptoServiceProvider
4.	AES(RijnDael)	128	Rijndeal

Eksperimento metu pastebėta, kad bandant iššifruoti didelius duomenų kiekius mobiliuose įrenginiuose, juose nepakanka atminties ir servisas nulūžta. Todėl atlikus įvarius bandymus

nustatyta, kad norint apdoroti didelius duomenų failus juos reikia skaidyti į mažesnius, optimaliausias duomenų kiekis yra 50Mb.

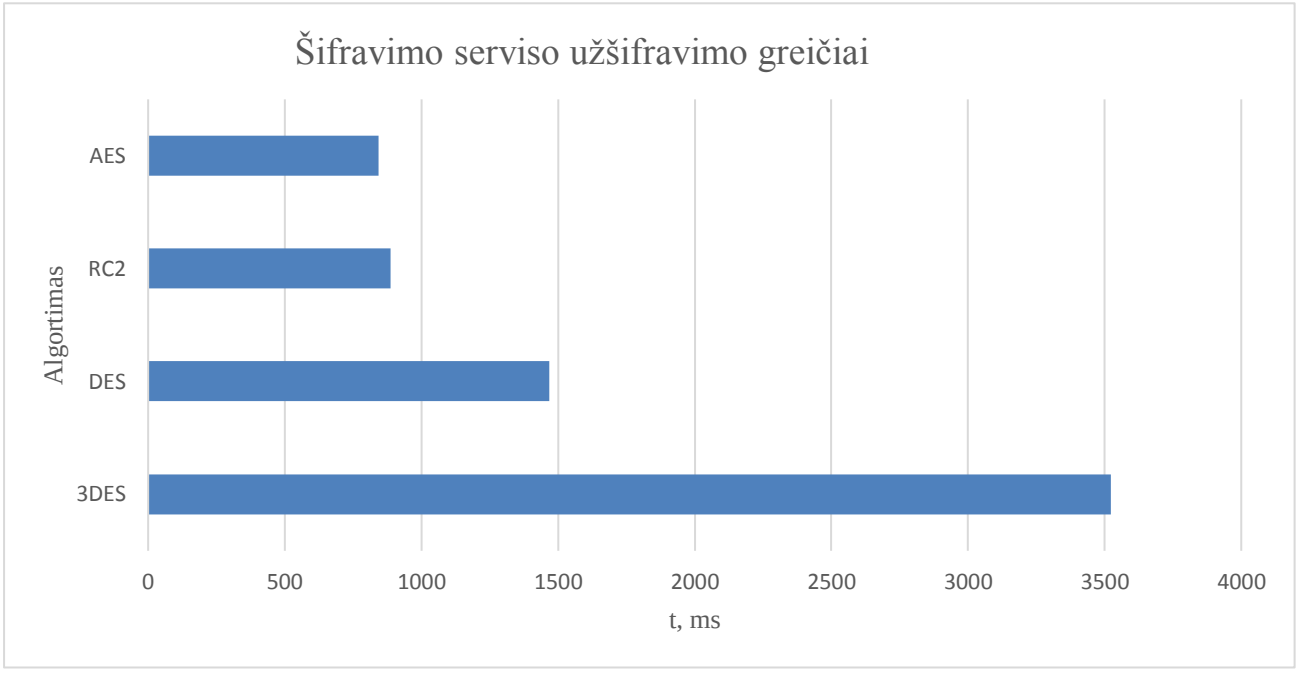
3.3. Serverio duomenų šifravimo algoritmų tyrimas

Tiriant šifravimo servisą pasirinktas nešiojamas kompiuteris ir parašyta programa, kuri naudojo .NET karkaso siūlomas šifravimo bibliotekas. Parašyta programa buvo paleista tris kartus ir nustatyta, kiek laiko trunka šifravimas kiekvienu tikrinamu šifravimo algoritmu. Gauti rezultatai pateikti ***3.2*** lentelėje.

3.2 lentelė. Šifravimo serviso užšifravimo laikai

	1 bandymas	**2 bandymas**	**3 bandymas**
AES	816	868	847
RC2	864	859	943
DES	1512	1425	1468
3DES	3562	3456	3554

0



19 pav. Serverio duomenų užšifravimo greičiai pagal algoritmus

19 pav. pavaizduotas grafikas, kuriame nurodomas vidutinis šifravimo greitis pagal atitinkamus šifravimo algoritmus. Užšifruoti buvo naudojama 50 Mb duomenų paketai. Iš gautų

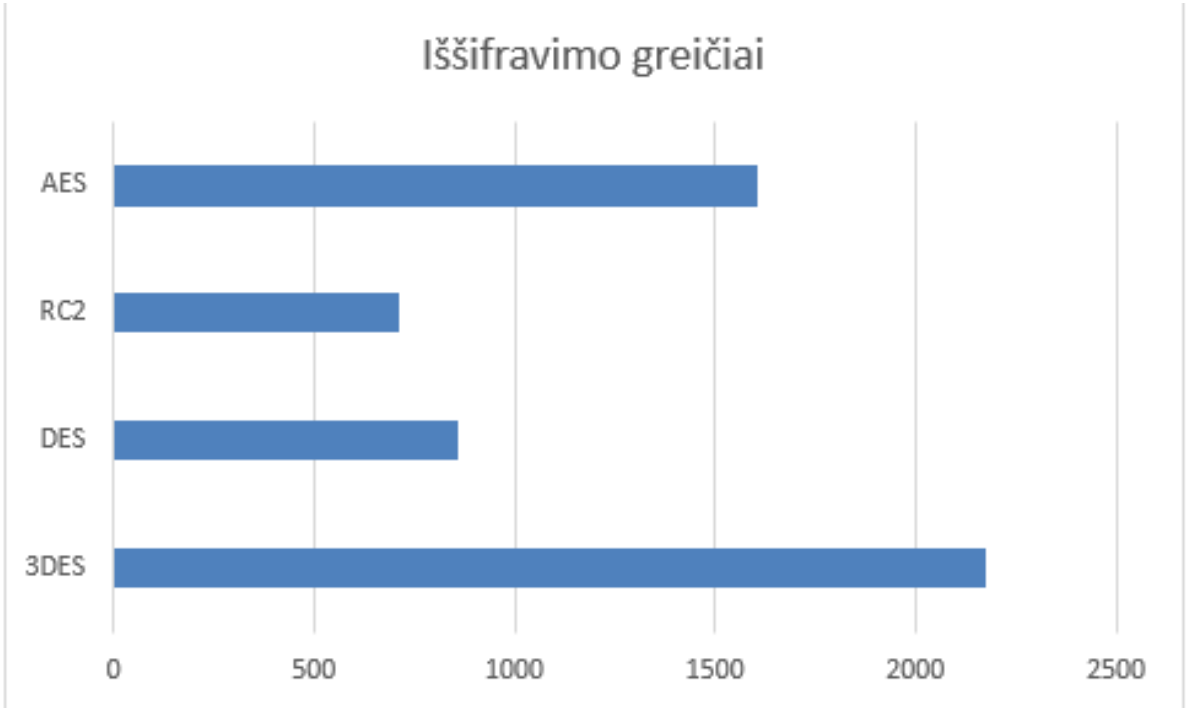
rezultatų matome, kad greičiausiai užšifruojama AES algoritmu. Ne daug nuo jo atsilieka ir RC2 algoritmas. Tačiau DES ir 3DES algoritmai užšifruoja duomenys žymiai liečiau.

3.4. Kliento iššifravimo agento nešiojamame kompiuteryje algoritmų tyrimas

Patikrinti kliento iššifravimo agento greičiams buvo sukurta programa, kuri naudoja .Net karkaso siūlomas šifravimo bibliotekas. Tai atlikus sukurta programa, kuri imitavo kliento iššifravimo agento veikimą nešiojamame kompiuteryje. Ji buvo paleista tris kartus ir gauti iššifravimo greičiai surašyti 3.3 lentelėje.

3.3 lentelė. Kliento iššifravimo agento nešiojamame kompiuteryje veikimo greičiai

	1 bandymas	2 bandymas	3 bandymas
AES	1587	1546	1498
RC2	684	617	649
DES	753	757	724
3DES	2202	2178	2245



20 pav. Nešiojamo kompiuterio duomenų iššifravimo greičiai pagal algoritmus

20 pav. pavaizduota, kiek laiko iššifravimo servisui, įrašytam nešiojamame kompiuteryje, trunka iššifruoti 50Mb duomenų. Pagal gautus rezultatus pastebėta, kad 3DES algoritmas taip pat iššifruoja duomenis lėčiausiai. Tačiau šį kartą RC2 algoritmas aplenkė AES.

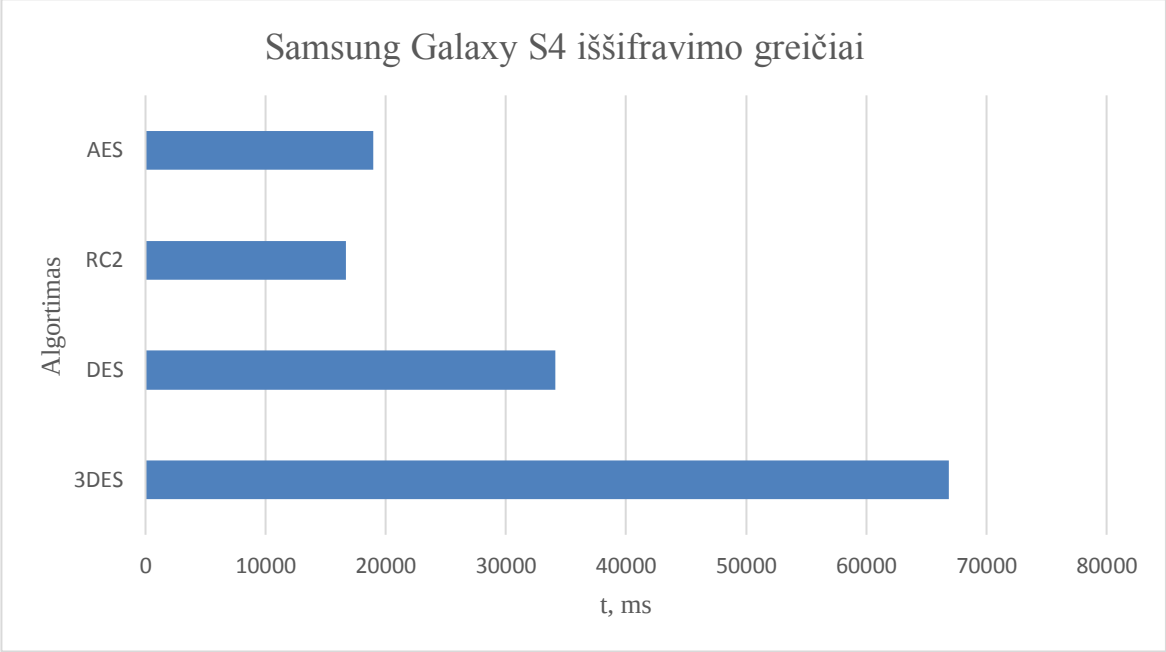
3.5. Kliento iššifravimo agento mobiliuose įrenginiuose algoritmų tyrimas

3.4 lentelėje pavaizduoti gauti rezultatai iš mobiliųjų įrenginių iššifravimo serviso. Joje nurodyta, kiek laiko kiekviename įrenginyje užtrunka iššifruoti 50Mb duomenų paketą su skirtingais algoritmais.

3.4 lentelė. Mobiliųjų įrenginių iššifravimo greičiai

	Galaxy S4	Galaxy S5	iPhone 6
3DES	66885	53548	8299
DES	34116	29958	4407
RC2	16703	13426	3408
AES	18971	14506	1884

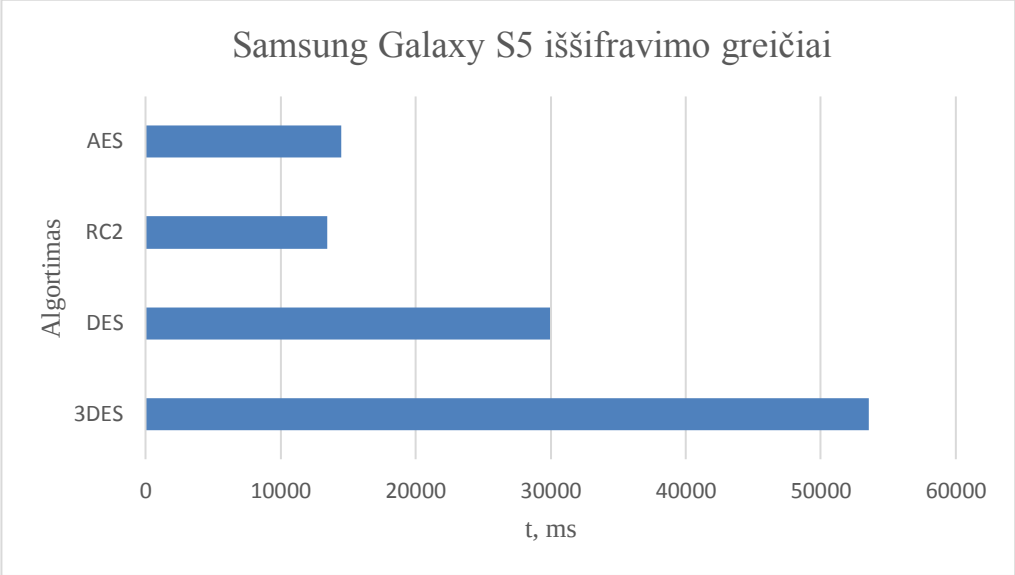
3.5.1. Samsung Galaxy S4 iššifravimo tyrimas



21 pav. Samsung Galaxy S4 iššifravimo greičiai

21 pav. Samsung Galaxy S4 iššifravimo greičiapav. pavaizduotas grafikas, kuriame nurodyta, kaip greitai iššifruojamas 50 Mb duomenų paketas naudojant skirtingus algoritmus. Šiame grafike matoma, kad greičiausiai iššifruojama naudojant RC2 algoritmą, tačiau nuo jo nedaug atsilieka ir saugesnis AES algoritmas. Tačiau senas DES ir patobulinta jo versija (3DES) užtrunka žymiai ilgiau.

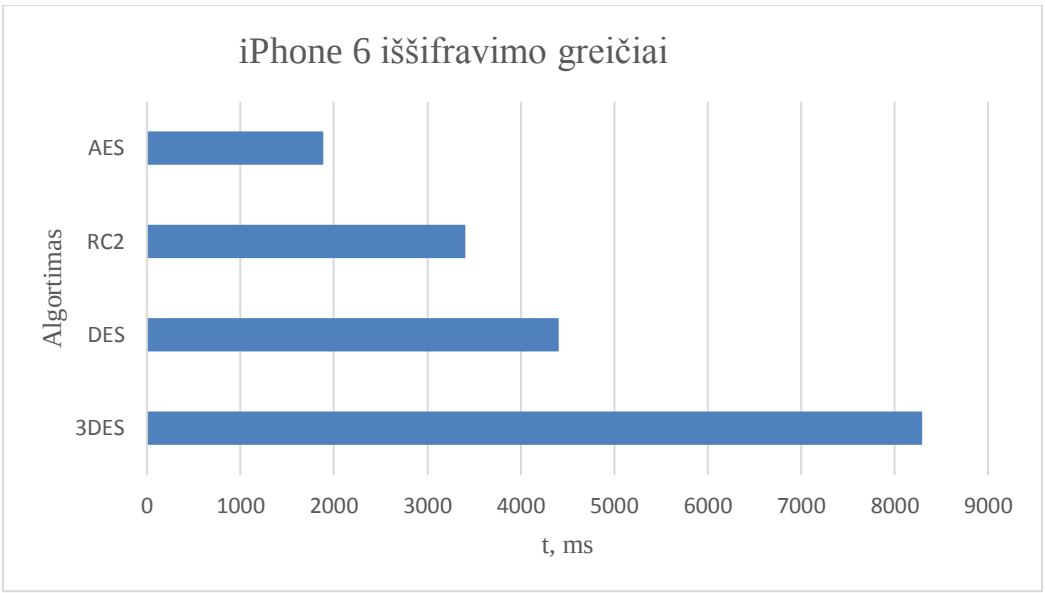
3.5.2. Samsung Galaxy S5 iššifravimo tyrimas



22 pav. Samsung Galaxy S5 iššifravimo greičiai

22 pav. pavaizduotas grafikas, kuriame nurodyta, kaip greitai iššifruojamas 50 Mb duomenų paketas naudojant skirtingus algoritmus. Šiame grafike matoma, kad greičiausiai iššifruojama naudojant RC2 algoritmą, tačiau nuo jo nedaug atsilieka ir saugesnis AES algoritmas.

3.5.3. iPhone 6 iššifravimo tyrimas



23 pav. iPhone 6 iššifravimo greičiai

23 pav. pavaizduotas grafikas, kuriame nurodyta, kaip greitai iššifruojamas 50 Mb duomenų paketas naudojant skirtingus algoritmus. Šiame grafike matoma, kad greičiausiai iššifruojama naudojant AES algoritmą. Tačiau standartinių algoritmų DES ir 3DES iššifravimo greičiai žymiai didesni.

3.6. Rezultatų apibendrinimas

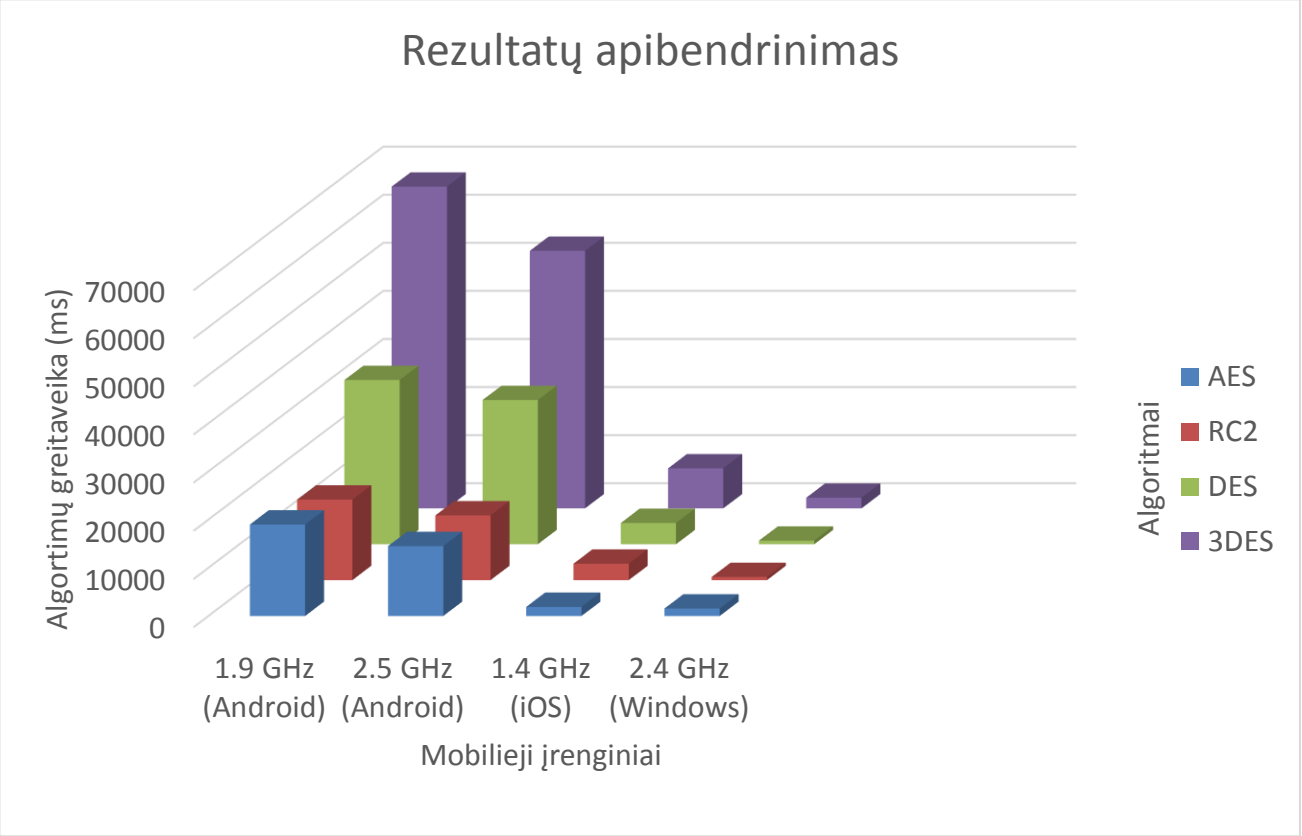
3.5 lentelėje pateikti gauti eksperimento rezultatai. Iš jos matome, kad Windows ir „Android“ platformose greičiausiai duomenys iššifruojami naudojant RC2 šifravimo algoritmą, o „iOS“ platformoje greičiausiai duomenis iššifravo AES algoritmas. Visose platformose 3DES šifravimo algoritmas iššifravo lėčiausiai. Windows platformoje jis buvo 3,4 karto lėtesnis už RC2, „Android“ platformoje jis 4 kartus lėtesnis už greičiausią RC2, o „iOS“ sistemoje net 4,4 karto iššifruoja lėčiau, nei AES.

Kitas pastebėjimas - 3DES šifravimo algoritmas veikia panašiu principu kaip DES, tik užšifruoja tris kartus, būtų galima tikėtis, kad jų greičiai skirsis apie tris kartus. Tačiau atlikus tyrimą pastebėjome, kad „Android“ ir „iOS“ platformose šis pokytis skiriasi tiktai apie 1,9 karto. Bet „Windows“ platformoje atlikto testo metu tas pokytis pakilo iki 2,96 karto.

Taip pat pastebėta, kad duomenų iššifravimas naudojant „Xamarin“ siūlomą karkasą „Android“ platformoje žymiai lėtesnis. Taip yra dėl to, kad neoptimizuotai keičiamas C# kodas į Java kalbą, kuri naudojama Android sistemose. Todėl prieš renkantis šį produktą reiktų į tai atsižvelgti.

3.5 lentelė. Rezultatų apibendrinimas

Modelis	**Proce-sorius**	**Dažnis**	**Bran-duolių sk.**	**Operacinė sistema**	**Iššifravimo algoritmų greitaveika (ms)**			
					AES	**RC2**	**DES**	**3DES**
iPhone 6	Typhoon	1.4 GHz	2	iOS	1884	3409	4407	8299
Samsung Galaxy S4	Krait 300	1.9 GHz	4	Android	18971	16703	34116	66885
Samsung Galaxy S5	Krait 400	2.5 GHz	4	Android	14506	13426	29958	53548
Acer 5750G	Intel i5-3437U	2.40 Ghz	2	Windows	1543	650	744	2208



24 pav. Rezultatų apibendrinimo grafikas

24 pav. pavaizduotas grafikas, kuriame pateikta šifravimų greitaveika pagal procesoriaus dažnį ir operacinę sistemą. Jame aiškiai matoma, kad „Android“ platformoje, nors ir procesoriai galingesni, tačiau jie iššifruoja žymiai lėčiau lyginant su „iOS“ ir „Windows“ platformomis. Lyginant mobiliojo įrenginio „Samsung Galaxy S5“ procesorių su nešiojamojo kompiuterio, jie pagal dažnį nežymiai skiriasi (100Mhz), o jų iššifravimo greičiai skiriasi nuo 9,4 kartų (šifruojant AES algoritmu) iki 40 kartų (šifruojant DES algoritmu).

Išvados:

- Atlikus eksperimentą su šifravimo servisu ir mobilių įrenginių iššifravimo agentu pastebėta:
    - Duomenų šifravimo metu duomenys užšifruojami naudojant DES algoritmą 2,4 kartus greičiau už 3DES ir 1,72 karto lėčiau už AES ir RC2, kurie užšifruoja panašiu greičiu.
    - Duomenų iššifravimo metu „Windows“ platformoje duomenys iššifruojami naudojant AES šifravimo algoritmą 1,43 kartus greičiau už 3DES ir 2 kartus lėčiau už RC2 ir DES algoritmus

- Duomenų iššifravimo metu „Android“ platformoje duomenys iššifruojami naudojant DES algoritmą 1,9 kartus greičiau nei 3DES ir 2,1 kartus lėčiau, už AES ir RC2, kurie veikia panašiu greičiu.
- Duomenų iššifravimo metu „iOS“ platformoje duomenys iššifruojami naudojant DES algoritmą 1,9 kartus greičiau nei 3DES ir 1,8 kartus lėčiau, už AES ir RC2, kurie veikia panašiu greičiu.

- 3DES šifravimo algoritmas veikia panašiu principu kaip DES, tik užšifruoja tris kartus, būtų galima tikėtis, kad jų greičiai skirsis apie tris kartus. Tačiau atlikus tyrimą pastebėjome, kad „Android“ ir „iOS“ platformose šis pokytis skiriasi tiktai apie 1,9 karto. Bet „Windows“ platformoje atlikto testo metu tas pokytis pakilo iki 2,96 karto.
- Žymūs rezultatų skirtumai tarp prietaisų rodo, jog spartesnį iššifravimą ir užšifravimą labiau lemia operacinė sistema, nei procesoriaus galingumas – „Android“ šifravimo procesai vyksta lėčiausiai, tai įtakoja neoptimizuotas C# kodo vertimas į „Android“ aplinką reikalingą Java programavimo kalbą.

4. IŠVADOS:

- Išanalizavus asmeninių įrenginių, naudojamų įmonėse, saugos iššūkius ir saugos problemų sprendimo metodus pastebėta, kad taikant BYOD politiką atsiranda grėsmių paviešinti svarbius duomenis.
- Pasiūlyta ir realizuota asmeninių įrenginių naudojamų įmonėse informacijos saugos metodų taikymo sistema.
- Atliktas asmeninių įrenginių, naudojamų įmonėse, informacijos saugos metodų taikymo sistemos tyrimas parodė:
    - Duomenų šifravimo metu duomenys užšifruojami naudojant DES algoritmą 2,4 kartus greičiau už 3DES ir 1,72 karto lėčiau už AES ir RC2, kurie užšifruoja panašiu greičiu.
    - Duomenų iššifravimo metu „Windows“ platformoje duomenys iššifruojami naudojant AES šifravimo algoritmą 1,43 kartus greičiau už 3DES ir 2 kartus lėčiau už RC2 ir DES algoritmus
    - Duomenų iššifravimo metu „Android“ platformoje duomenys iššifruojami naudojant DES algoritmą 1,9 kartus greičiau nei 3DES ir 2,1 kartus lėčiau, už AES ir RC2, kurie veikia panašiu greičiu.
    - Duomenų iššifravimo metu „iOS“ platformoje duomenys iššifruojami naudojant DES algoritmą 1,9 kartus greičiau nei 3DES ir 1,8 kartus lėčiau, už AES ir RC2, kurie veikia panašiu greičiu.
- 3DES šifravimo algoritmas veikia panašiu principu kaip DES, tik užšifruoja tris kartus, būtų galima tikėtis, kad jų greičiai skirsis apie tris kartus. Tačiau atlikus tyrimą pastebėjome, kad „Android“ ir „iOS“ platformose šis pokytis skiriasi tiktai apie 1,9 karto. Bet „Windows“ platformoje atlikto testo metu tas pokytis pakilo iki 2,96 karto.
- Žymūs rezultatų skirtumai tarp prietaisų rodo, jog spartesnį iššifravimą ir užšifravimą labiau lemia operacinė sistema, nei procesoriaus galingumas – „Android“ šifravimo procesai vyksta lėčiausiai, tai įtakoja neoptimizuotas C# kodo vertimas į „Android“ aplinką reikalingą Java programavimo kalbą.

5. LITERATŪRA

[1] Antonio M. Mora, Paloma De las Cuevas, Juan Julián Merelo, Sergio Zamarripa, Anna I. Esparcia-Alcázar „Enforcing Corporate Security Policies via Computational Intelligence Techniques“. Įtraukta *GECCO Comp '14 Proceedings of the Companion Publication of the 2014 Annual Conference on Genetic and Evolutionary Computation*, 2014. P. 1245-1252.

[2] Alessandro Armando, Gabriele Costa, Alessio Merlo „Bring Your Own Device, Securely“. Įtraukta *SAC '13 Proceedings of the 28th Annual ACM Symposium on Applied Computing*, 2013. P. 1852-1858.

[3] Giovanni Russello, Mauro Conti, Bruno Crispo, Earlence Fernandes, Yury Zhauniarovich „Demonstrating the Effectiveness of MOSES for Separation of Execution Modes“. Įtraukta *CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security*, 2012. P. 998-1000.

[4] Giovanni Russello, Mauro Conti, Bruno Crispo, Earlence Fernandes „MOSES: Supporting Operation Modes on Smartphones“. Įtraukta *SACMAT '12 Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, 2012. P. 3-12.

[5] Mordechai Guri, Gabi Kedma, Buky Carmeli, Yuval Elovici „Limiting Access to Unintentionally Leaked Sensitive Documents Using Malware Signatures“. Įtraukta *SACMAT '14 Proceedings of the 19th ACM symposium on Access control models and technologies*, 2014. P. 129-140.

[6] Adrian Drury, Richard Absalom, „BYOD: an emerging market trend in more ways than one“ [Tinkle]. Available: http://www.us.logicalis.com/globalassets/united-states/whitepapers/logicalisbyodwhitepaperovum.pdf. [Kreiptasi 09 05 2016].

[7] Diaa Salama Abd Elminaam , Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud „Evaluating The Performance of Symmetric Encryption Algorithms“. Įtraukta *International Journal of Network Security*, 2010. P. 213-219.

[8] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks." Įtraukta *IBM Journal of Research and Development*, 1994. P. 243 – 250.

[9] Mason, Andrew G. „*Cisco Secure Virtual Private Network*” (2002).

[10] Dirk Van Bruggen, Shu Liu, Mitch Kajzer, Aaron Striegel, Charles R. Crowell,„Modifying Smartphone User Locking Behavior“, įtraukta *Symposium on Usable Privacy and Security (SOUPS) 2013.*

[11] Diane R Murphy, Richard H. Murphy „Teaching Cybersecurity: Protecting the Business Environment“. Įtraukta *InfoSecCD '13 Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference*, 2013. P. 88.

[12] Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl „Social Engineering Attacks on the Knowledge Worker“. Įtraukta *SIN '13 Proceedings of the 6th International Conference on Security of Information and Networks*, 201. P. 28-35.

[13] M. Landman, „Managing smart phone security risks“. Įtraukta *InfoSecCD '10 2010 Information Security Curriculum Development Conference*, New York, 2010. P. 145-155.

[14] A. B. Garba, J. Armarego ir D. Murray, „Bring your own device organisational information security and privacy“. Įtraukta *ARPN Journal of Engineering and Applied Sciences*, 2015. P. 1279-1287.

[15] K. Kostiainen, E. Reshetova, J.-E. Ekberg ir 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.