

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Paulius Lazauskas

**Audio – video nuotolinio mokymo ir
egzaminavimo sistema**

Magistro darbas

Darbo vadovas
prof. dr. E. Sakalauskas

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Paulius Lazauskas

**Audio – video nuotolinio mokymo ir
egzaminavimo sistema**

Magistro darbas

Recenzentas

doc. dr. Stasys Maciulevičius
2010-05-

Vadovas

prof. dr. E. Sakalauskas
2010-05-

Atliko

IFN-8/3 gr. stud.
Paulius Lazauskas
2010-05-25

Kaunas, 2010

TURINYS

IVADAS	5
1 Nuotolinio mokymo ir egzaminavimo, audio - video perdavimo bei saugumo technologijų analizė	8
1.1 Nuotolinio mokymo ir egzaminavimo problemos	8
1.1.1 ATutor	9
1.1.2 Moodle	12
1.1.3 Virtuali mokymosi terpė WebCT	15
1.1.4 Išvados	16
1.2 Audio - video informacijos perdavimo internetu analizė	18
1.2.1 Vaizdo konferencijos	18
1.2.2 H323 specifikacija	22
1.2.3 Srautinis audio - video informacijos perdavimas	23
1.2.4 Audio - video informacijos perdavimas naudojant P2P technologiją	27
1.2.5 H.264 video standartas	30
1.2.6 Išvados	33
1.3 Saugumo technologijų apžvalga/analizė	33
1.3.1 Autentifikavimas	34
1.3.2 Autorizacija	38
1.3.3 Auditas	38
1.3.4 Apsaugoto kanalo technologijos	38
1.3.5 Informacijos autentifikavimas	39
1.3.6 Išvados	39
1.4 Analizės išvados	40
2 Audio – video nuotolinio mokymo ir egzaminavimo sistemos projektas	41
2.1 Audio – video nuotolinio mokymo ir egzaminavimo sistemos pagrindinės funkcijos ...	42

2.2	Principinis sistemos veikimas ir autentifikacija	44
2.3	Sistemos funkcinė diagrama	45
2.3.1	Sistemai sukurti naudojami video transliacijų komponentai	47
2.4	Saugus autentifikavimas sistemoje	54
2.4.1	OpenID.....	55
2.4.2	Bio-Plugin™	56
2.4.3	TrustBearer OpenID	58
3	Audio – video nuotolinio mokymo ir egzaminavimo sistemos realizacija	60
3.1	Sistemos realizacijos I ir II etapo metu atlikti darbai.....	61
3.2	Autentifikavimui skirta programinė įranga	65
4	Audio – video nuotolinio mokymo ir egzaminavimo sistemos tyrimas.....	69
4.1	Audio-video srauto pasiskirstymo priklausomybė nuo pašnekovų skaičiaus	69
4.1.1	Pirmasis matavimas	70
4.1.2	Antrasis matavimas.....	71
4.1.3	Trečiasis matavimas.....	72
4.1.4	Ketvirtasis matavimas.....	73
4.1.5	Matavimų apibendrinimas	74
4.2	Audio – video nuotolinių sistemų palyginimas.....	76
4.3	SAVIP serverio resursų apkrovimo priklausomybė nuo naudojamo protokolo	77
4.4	Tyrimo išvados.....	78
	IŠVADOS IR REZULTATAI	79
	LITERATŪRA	81
	1 PRIEDAS. „KTU TECHNORAMA 2010“ DIPLOMAS	85
	2 PRIEDAS. AKTAS DĖL BANDOMOJO SISTEMOS DIEGIMO	86
	3 PRIEDAS. RAŠTAS DĖL SISTEMOS KOMERCIALIZACIJOS IR IŠEIGOS KODO NAUDOJIMO.....	Error! Bookmark not defined.

ĮVADAS

Kiekviena nauja technologija skatino naujus lūkesčius ir nutiesė kelią kitoms technologijoms atsirasti. Knygos, kompiuteriai ir kompiuterių tinklai, internetas – kiekviena technologija savo laikmečiu buvo pažangiausia ir priimtinausia besimokantiems bei sukėlė revoliucinius pokyčius mokymesi. R. Katz (2003) išskyrė tris mokymosi technologijų raidos etapus:

- Agrarinis – dominuoja žodinės, rašytinės ir skriptoriumo technologijos
- Industrinis – dominuoja universitetų miesteliai, klasės, auditorijos, laboratorijos ir bibliotekos.
- Žinių - dominuoja universitetų miesteliai, bibliotekos, kompiuteriai, kompiuterių tinklai, daugialypė media, kursų ir mokymosi vadybos sistemos, e.studijų paketai, mokymosi objektai bei modeliavimo programos.[24]

Šią klasifikaciją jau galima papildyti **ketvirtuoju virtualių studijų etapu**, kai universiteto veikla perkeliama į virtualią erdvę, kur studijuojama, kuriama ir kaupiama informacija, administruojami procesai, o studijos jau nebetelpa universiteto miestelio teritorijoje.[24]

Šio laikmečio atradimas – lanksčios ir intelektualios virtualios mokymosi aplinkos (VMA), integruojančios adaptyvią, t. y. studentui pritaikytą, mokymosi medžiagą, savikontrolę, komunikacines galimybes, e. studijų paketo priemones. Pasaulinis žiniatinklis palaiko informacijos paieškos ir e. bibliotekų su visateksčių duomenų bazėmis sistemą, per internetą galima jungtis prie VMA, kur galima išstudijuoti pateiktą medžiagą, atlikti darbus, **pasitikrinti žinias, laikyti egzaminus. Vaizdo konferencijos sudaro tinkamas sąlygas kompiuterių tinklais perduoti vaizdą ir garsą, tarpusavyje bendrauti daugeliui studentų, o dėstytojui – su studentais.** Dažniausiai mokymosi procese naudojamos kelios priemonės, pavyzdžiui, ne tik vaizdo konferencijomis ir VMA, bet ir e. paštu, e. diskusijomis ir kt. Technologijos yra vertinamos pagal tai, kaip jos sukonstruotos perteikti turinį žinioms ir įgūdžiams suformuoti.

Informacijos ir komunikacijos technologijos (IKT) atlieka dvejopą vaidmenį. Viena vertus, palaiko ir išplečia tradicinių mokymosi metodų galimybes, leidžia šiuos metodus perkelti į

naujas sritis. Kita vertus, IKT leidžia sukurti naujus mokymosi metodus, kurie be šių technologijų būtų negalimi (pavyzdžiui, mokymasis kompiuterių tinkluose panaudojant hipertekstų galimybes ar VMA aplinkoje).

IKT – integrali nuotolinių studijų kokybės dalis, todėl jų parinkimo ir taikymo procesas turi būti dinamiškas, kintantis kartu su metodikos naujovėmis, akademinės visuomenės technologinės kultūros bei praktikos pokyčiais, studijų sąlygomis. Paprastai technologijos yra žingsniu toliau nei jų taikymas studijų procese. Kūrybiškas ir lankstus naujų technologijų panaudojimas studijų procese turėtų remtis pasvertais metodais ir geru studijų tikslų bei technologijų galimybių suvokimu.[24]

Šio darbo turinyje keliamos dvi pagrindinės problemos:

- Nuotolinių egzaminų autentiškumo užtikrinimas, panaudojant audio – video ir biometrines technologijas.
- Video transliacijų vykdymas ir kokybė internete - užtikrinti kuo didesnę audio-video medžiagos transliavimo kokybę, naudojant kuo mažesnę interneto srauto kanalą.

Darbo tikslas - sukurti „Audio – video nuotolinio mokymo ir egzaminavimo sistemą“, kurios funkcinis veikimas būtų paremtas srautinės audio - video informacijos perdavimu. Pagrindinis sistemos uždavinys - studentams ir dėstytojams sudaryti palankias sąlygas, kurios leistų virtualioje erdvėje atlikti mokymo bei egzaminavimo procesus. Norint įgyvendinti šį uždavinį, sistemos kūrimo metu, svarbu atsižvelgti į sistemos vartotojų interneto spartos galimybes, kad nebūtų užkirstas kelias studentui mokytis namuose. Taip pat svarbu užtikrinti kuo didesnę egzaminuojamojo asmens autentifikaciją, panaudojant audio-video ir biometrines technologijas.

Efektyviausiai virtualioje aplinkoje yra naudojamos priemonės, kurios būna itin panašios į sutinkamas realybėje. Kuriant sistemą skirtą žmonių bendravimui/mokymui/mokymuisi ši savybė yra būtina, todėl „Audio – video nuotolinio mokymo ir egzaminavimo sistema“, buvo kuriama besilaikant šios nuostatos.

Kuriant sistemą buvo realizuotos studentams ir dėstytojams skirtos funkcijos, kurios padeda išspręsti iškeltas problemas:

- Nauji egzaminavimo (atsiskaitymo) būdai:
 - Video konferencija dėstytojas - studentas (gyva video transliacija paremtas atsiskaitymo būdas, kai dėstytojas pateikia studentui klausimus bei diskutuoja kartu su juo aktualia tema).
 - Egzaminas video įrašo pagalba (studentui atlikus autorizaciją yra suteikiami atsiskaitymo klausimai ,jam susipažinus su jais, inicijuojamas vaizdo įrašas. Video medžiaga realiu laiku yra įrašinėjama į nutolusį serverį, kad jos nebūtų galima modifikuoti. Dėstytojas bet kuriuo metu prisijungęs prie sistemos gali peržiūrėti šią medžiagą bei įvertinti studento žinias.)
 - Daugialypės video konferencijos galimybė. Tokiu būdu galima inicijuoti grupinius darbų atsiskaitymus (pvz.: seminaro forma).
- Dėstytojo terpė, kurioje jis gali transliuoti itin aukštos kokybės video paskaitas, perduoti ne tik savo vaizdo kameros vaizdus, bet ir kompiuterio ekrane atliekamų veiksmų vaizdą.
- Studentas prisijungdamas prie sistemos arba inicijuodamas atsiskaitymą gali būti autorizuojamas biometrinio skaitytuvo bei kitų priemonių pagalba.

„Audio - video nuotolinio mokymo ir egzaminavimo sistemos“ prototipas buvo pristatytas kasmetinėje universiteto jaunųjų mokslininkų darbų parodoje - konkurse KTU technorama 2010. Komisija šiai sistemai skyrė I vietą. Sistemos bendraautoriams buvo įteiktas diplomas (žiūrėti Priedą Nr.1) bei piniginis prizas.

VGTU Viešosios komunikacijos direkcija tiria galimą sistemos pritaikymą universiteto valorizacijos proceso užtikrinimui (žiūrėti Priedą Nr.2).

UAB „Informacinių technologijų organizacija“, atlikto magistrinio darbo medžiagą naudoja komercinio produkto, „Daugiakomponentinė ir multifunkcinė paslaugų tarpininkavimo platforma“, kūrimui (žiūrėti Priedą Nr.3).

1 Nuotolinio mokymo ir egzaminavimo, audio - video perdavimo bei saugumo technologijų analizė

1.1 Nuotolinio mokymo ir egzaminavimo problemos

Nors daugelis universitetų šiandien turi e-mokymosi sistemas, nei viena iš plačiai naudojamų neturi lanksčios nuotoliniams egzaminams skirtos platformos. Pats virtualaus mokymo procesas vyksta gana sklandžiai. Žinoma būtų galima daugiau dėmesio skirti nuotolinių video paskaitų kokybei bei dėstomų paskaitų interaktyvumui, kuris labiau sudomintų klausytoją. Taip būtų pasiekiamas aukštesnis žinių įsisavinimo rezultatas.

Kaip šiuo metu dažniausiai vyksta e-egzaminai?

- Sutartą valandą studentai susirenka į kompiuterių klasę. [jau yra pažeidžiama nuotolinio mokymosi/atsiskaitymų samprata, studentas privalo atvykti į universitetą, kad jis būtų identifiukuotas, kaip asmuo, kuris iš tikrųjų laikys egzaminą ir sieks sau skirto balo.
- Kad nebūtų pažeista taisyklė ir egzaminu nuotoliniu būdu nebūtų galima laikyti ne savo vardu, individualiai yra išdalinami arba dėstytojas pats suveda slaptažodį skirtą egzaminu inicijavimui.
- Taip pat klasėse, kuriose vyksta egzaminai būna naudojama video kamerų stebėjimo sistema. Tai prevencinė priemonė, kuri apriboja studentų nusirašinėjimą bei inicijuoja, kad egzaminai vyktų numatyta tvarka. Tokia praktika taikoma Microsoft sertifikavimo centruose.
- Studentai atlieka žinių patikrinimą ir gauna įvertinimą.

Toks atsiskaitymo būdas yra taikomas naudojant plačiai paplitusias WebCT, Moodle ir kitas atsiskaitymo/mokymo sistema.

Studentui galima leisti laikyti egzaminą namuose, išdavus slaptažodį elektroninio pašto pagalba, tačiau niekas nėra garantuotas, kad egzaminą jis laikys pats ir savarankiškai. Todėl vis labiau didėja nuotolinio autentifikavimo ir video stebėjimo būtinybė.

Šiuo metu dėstytojai studentus konsultuoja el. pašto pagalba arba atvykus į universitetą. Studentams ir dėstytojams būtų žymiai patogiau, konsultacijas ir žinių patikrinimus vykdyti video konferencijų bei seminarų pagalba, nuotoliniu būdu.

Yra nemažai komercinių ir atviro kodo sistemų, kurios skirtos nuotoliniam mokymui. Mūsų tikslas analizuojant kelias klasikines labiausiai paplitusias nuotolinių studijų sistemas išsiaiškinti jų svarbiausius trūkumus. Kuriant „Audio – video nuotolinio mokymo ir egzaminavimo sistemą“, bus atsižvelgiama į sudarytą trūkumų sąrašą.

Virtualios mokymosi aplinkos:

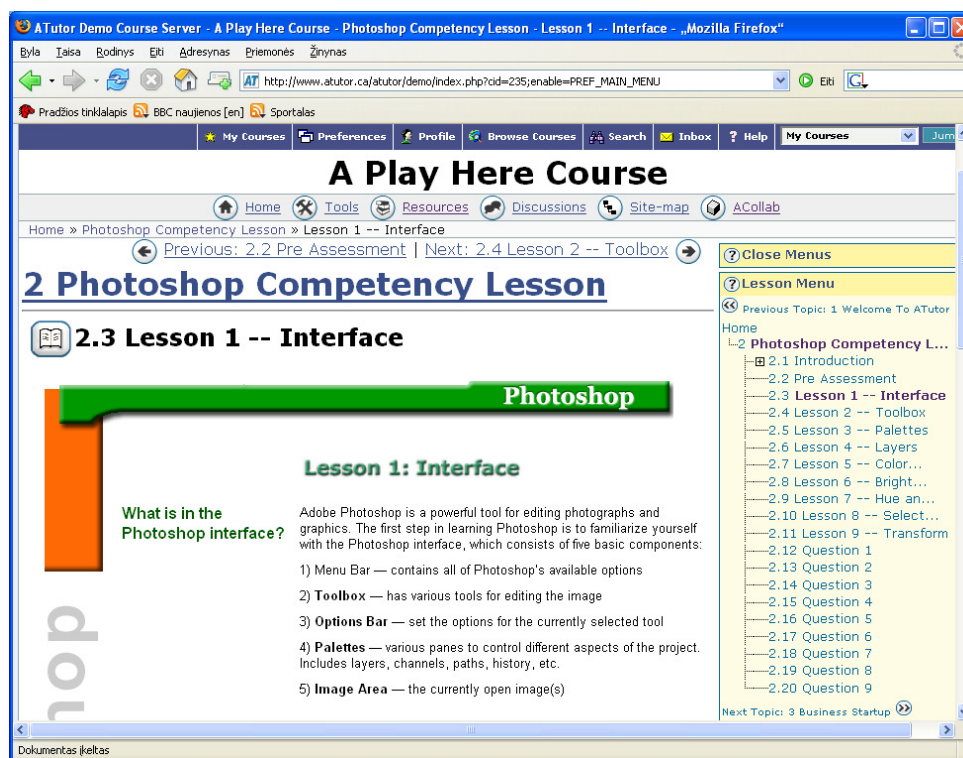
- [ANGEL LMS](#)
- [ATutor](#)
- [Blackboard](#)
- [Claroline](#)
- [Desire2Learn](#)
- [Dokeos](#)
- [eFront](#)
- [Moodle](#)
- [OLAT](#)
- [Sakai Project](#)
- [Scholar360](#)
- [WebCT](#)

Plačiau aptarsime tris sąrašė paminėtas virtualias mokymo aplinkas, tai ATutor , Moodle ir WebCT.

1.1.1 ATutor

Atviroji žiniatinklinė virtualioji mokymosi aplinka (autoriai ją vadina mokymosi turinio tvarkymo sistema). Sistema sukurta Toronto universitete (Kanada). Ji naudojama įvairiuose universitetuose, sėkmingai taikoma ir universitetuose ir vidurinėse mokyklose.

Mokytojas/Dėstytojas gali greitai sutvarkyti, pateikti, persikirstyti mokymosi turinį arba tvarkyti ir prižiūrėti kursų modulius. Mokiniai/studentai gali mokytis savo poreikiams pritaikytoje mokymosi aplinkoje. Bendrą sistemos vaizdą galime matyti 1 pav.[5]



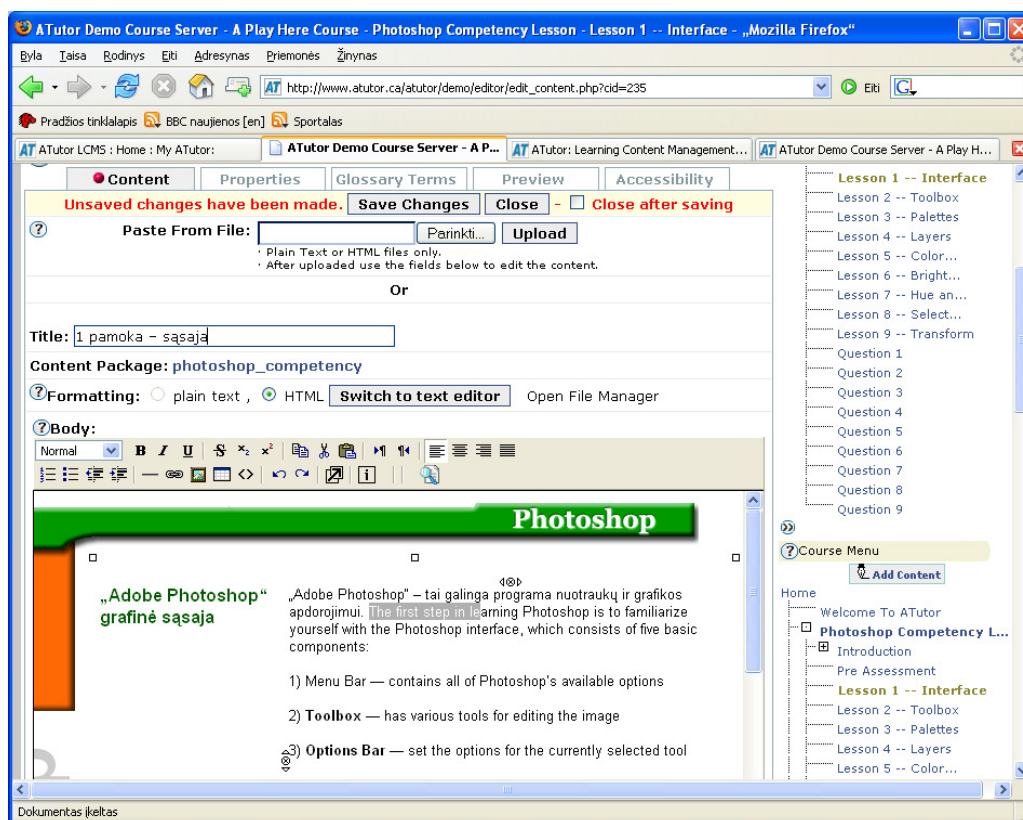
1 pav. „ATutor“ mokymosi sistemos bendras vaizdas

Sistema integruoja pagrindines priemones reikalingam veiksmingam mokytojų/dėstytojų ir mokinių/studentų bendradarbiavimui bei mokymui ir mokymuisi.[5]

Sistemą sudaro: diskusijų forumai, pokalbiai, vidinis elektroninis paštas, pasikeitimo rinkmenomis priemonės (mokiniai/studentai gali persiųsti įvairių formatų dokumentus, dalytis kurso ar grupės biblioteka, gali dalytis savo aplankų turiniu ir kt.), užrašai (mokiniai/studentai gali turėti dalomus arba savo asmeninius užrašus su rinkmenomis), kalendoriai (asmeniniai, grupės arba kurso), žinynas, paieška sistemoje, darbo atsijungus nuo tinklo priemonės (mokiniai gali persiųsti kursų puslapius su peržiūros programa), *darbo grupėse priemonės (administratorius gali sukurti grupes, grupių vadovus, kiekviena grupė gali turėti savo rinkmenų dalijimosi sritis, bendradarbiavimo dokumentus, diskusijas, pokalbių kambarius, el. paštą, kalendorių), savikontrolės priemonės (administratorius gali sukurti savikontrolės testus), mokinių/studentų portfolio (turi savo arba viešus aplankus), saugumo lygio nustatymo priemonės (administratorius gali nustatyti kursų viešumą – laisvai prieinami ar su slaptažodžiu), automatinės testų vertinimo priemonės, kursų tvarkymo priemonės, mokinių/studentų stebėjimo priemonės (pateikiamos ataskaitos apie mokinių/studentų lankytus kursus, prisijungimo laiką, datą ir kt.), kursų šablonai, mokinių apklausos priemonės, mokymosi turinio importo ir eksporto priemonės, integruotos grynojo ir raiškiojo teksto rengyklės.*

„ATutor“ suderinama su IMS/SCORM standartais, todėl sistemoje galima panaudoti mokymosi turinį iš kitų šiuos standartus atitinkančių aplinkų, taip pat eksportuoti turinį ir panaudoti jį kitose aplinkose.[5]

Toliau esančiame paveiksle pavaizduota, kaip mokytojas/dėstytojas gali tvarkyti mokymosi medžiagą: 2 pav. parodytą pamokos/paskaitos turinį, prisijungus su mokytojo/dėstytojo teisėmis, galima keisti naudojant integruotą HTML rengyklę arba įdėti iš anksčiau parengtos rinkmenos.



2 pav. Pamokos turinio tvarkymas „ATutor“ aplinkoje (prisijungus kaip mokytojas)

Sistema dalinai išversta į 40 kalbų, iš jų – į šias Europos Sąjungos šalių kalbas: čekų, danų, olandų, prancūzų, vokiečių, graikų, vengrų, italų, latvių, lietuvių (iš dalies), lenkų, portugalų, slovakų, slovėnų, ispanų, švedų.

Norint įdiegti sistemą „ATutor“, turi būti patenkinti šie reikalavimai:

- HTTP žiniatinklio serveris (rekomenduojama „Apache 1.3.x.“, o ne „Apache 2.x“).
- PHP 4.2.0 arba naujesnė su Zlib ir MySQL (4.3.0 arba naujesnė versija).

- MySQL 3.23.x arba naujesnė, 4.0.12 arba naujesnė (su MySQL 4.1.x ir 5.x oficialiai nesuderinama).

Rekomenduojamos darbui su "ATutor" sistema naršyklės ir jų versijos: *Netscape (7+)* ir kitos *Mozillos* šeimos naršyklės (pvz., *Mozilla*, *Mozilla Firefox*), *Microsoft Internet Explorer 4+*, *Opera 5+*.

1.1.2 Moodle

„Moodle“ pavadinimas - tai pilno angliškojo programos pavadinimo (Modular Object Oriented Dynamic Learning Environment) trumpinys. Pats pavadinimas rodo, kad šioje dinamiškoje, lengvai keičiamoje nuotolinio mokymosi aplinkoje visa informacija yra pateikiama atskirais moduliais, kurie konstruojami iš įvairių lengvai atnaujinamų ir pakeičiamų mokymosi objektų.

Dabar jau visame pasaulyje plačiai akademinuose sluoksniuose žinomu trumpiniu "Moodle" vadinama nuotolinio mokymosi reikmėms sumodeliuota ir pritaikyta nuotolinio (virtuali) mokymosi aplinka, leidžianti ne tik lengvai ir lanksčiai organizuoti mokymo(si) procesą, bet ir organizuoti visai akademinėi bendruomenei aktualios informacijos sklaidą. Šią mokymosi aplinką 1998 m pradėjo kurti pedagogas ir programuotojas Martin Doughiamas iš Australijos Curtin technologijos universiteto.[20]

Pedagoginiu požiūriu „Moodle“ programinė įranga šiuo metu pripažįstama viena iš lanksčiausių. Ji pagrįsta pedagoginėmis socialinio rekonstruktyvizmo ir rekonstrukcionizmo teorijomis. Naudojantis šia programa nėra sunku kurti ar nuotolinėms studijoms adaptuoti studijų kursus, ji reikalauja tik minimalios administratoriaus priežiūros. Pati programa sudaryta taip, kad būtinai skatinamas kūrėjų ir vartotojų bendruomenės aktyvus dalyvavimas šiuolaikiškame mokymo(si), dalijimosi mokymosi patirtimi procese.[20]

Taip pat labai svarbu tai, jog programa "Moodle" atitinka šiuolaikinius techninius tokio pobūdžio programų standartus (LDAP, ADOdb, SCORM, WEB-DAV ir kt.), ir kad akademinės institucijos gali naudotis atvirojo kodo programine įranga.[20]

Privalumas tarp kitų sistemų yra tai, kad ji projektuojama remiantis socialinės konstruktyvistinės pedagogikos principais (bendradarbiavimas, aktyvumas, kritinis vertinimas ir

kt.). Kadangi programa yra atviroji, bet kuris norintysis gali ją išsiversti, pritaikyti savo poreikiams ir naudoti.



3 pav. Kursų tvarkymo sistema „Moodle“

Programa turi modulinę struktūrą. Kiekvienas modulis papildo ją naujomis priemonėmis. Sistemos vaizdą su išsidėsčiusiais moduliais galime matyti 3 pav.

Pagrindiniai „Moodle“ moduliai:

- užduočių tvarkymas (mokinių/studentų atliktų užduočių siuntimas ir priėmimas, pavėluotai atliktų užduočių tvarkymas, tikrinimo rezultatų skelbimas);
- pokalbiai (HTML, paveikslai, grafiniai jaustukai, pokalbių teksto įrašymas, kad jį būtų galima vėliau peržiūrėti);
- pasirinkimas ir balsavimas (kursų skelbimas ir mokinių/studentų kursų pasirinkimai);
- diskusijų forumai (tik mokytojų/dėstytojų diskusijos, kursų naujienų forumai, kelių vartotojų forumai);
- dienyas (privatus tarp mokytojo/dėstytojo ir mokinio/studento);
- *klausimai, testai (pasirenkamų atsakymų klausimai; žodžio ar frazės atsakymų klausimai, „taip“ arba „ne“ atsakymų klausimai, atviro pobūdžio klausimai ir pan.; vaizdus klausimų pateikimas: HTML formatas, paveikslai; klausimų įtraukimas į duomenų bazę);*

- ištekliai (įvairaus formato turinys: tekstų, pateikčių rengyklės, vaizdinė, garsinė ir kt.; rinkmenų atnaujinimas, persiuntimas grynojo teksto arba HTML formatu);
- tyrinėjimai (mokymosi analizės priemonės, skilčių kūrimas, rezultatų skelbimas);
- **studijos (turi įvairias vertinimo skales, mokytojas/dėstytojas gali pateikti bandomąsias užduotis ir kt.).**[5]

Pagrindinės sistemos savybės: tinka ir nuotoliniam mokymui(si), ir naudojimui klasėje, turi paprastą vartotojo sąsają, kursus galima rūšiuoti bei vykdyti jų paiešką, integruotos duomenų saugumą užtikrinančios priemonės, daugumoje tekstų rašymo sričių (ištekliai, forumai, žurnalas) medžiaga gali būti taisoma naudojant HTML rengyklę, sistemos svetainę tvarko administratorius (jis nurodomas diegiant sistemą), administratorius gali keisti sistemos svetainės išvaizdą, net jau įdiegta „Moodle“ gali būti papildoma naujais moduliais, mokiniai/studentai gali kurti savo el. pašto paskyras, el. pašto adresai yra patikrinami ir patvirtinami, vartotojų prisijungimą gali tikrinti LDAP serveris (administratorius nurodo, kuriuos laukus tikrinti), turi išorinę duomenų bazę (bet kuri duomenų bazė, turinti bent du laukus, gali būti naudojama kaip išorinis tapatybės nustatymo šaltinis), darbo su IMAP, NNTP protokolais priemonės, skaitmeniniai liudijimai ir šifravimo priemonės, mokytojas/dėstytojas gali įtraukti studentus į kursą arba išbraukti iš kurso, kiekvienas vartotojas gali nurodyti savo laiko juostą ir kiekviena data „Moodle“ sistemoje yra konvertuojama į vartotojo nurodytąją, kiekvienas vartotojas gali pasirinkti sąsajos kalbą, administratorius (tai gali būti ir mokytojas/dėstytojas) tvarko visus kursus bei kitų mokytojų/dėstytojų registraciją, vartotojų aktyvumo stebėjimas – kiekvieno mokinio/studento aktyvumo ataskaitos gali būti pateikiamos grafiškai, kursų atsarginių kopijų kūrimas (naudojamas *zip* pakavimas). [5]

Sistema išversta arba verčiama į 50 kalbų. Iš jų į šias ES šalių kalbas: čekų, danų, olandų, anglų, estų, suomių, prancūzų, vokiečių, graikų, vengrų, italų, lietuvių (iš dalies), latvių, lenkų, slovakų, ispanų, švedų. Vartoja įstaigos iš 92 šalių. Tarp jų ir ES šalyse: Estija, Graikija, Ispanija, Italija, Kipras, Latvija, Lenkija, Lietuva, Liuksemburgas, Olandija, Portugalija, Prancūzija, Slovakija, Slovėnija, Suomija, Švedija, Vengrija, Vokietija.

Norint įdiegti „Moodle“, turi būti patenkinti šie reikalavimai:

- Žiniatinklio serveris. Daugelis naudoja *Apache*, tačiau veikia ir su kitais serveriais, palaikančiais PHP, pavyzdžiui, IIS operacinėse sistemose *Windows*.

- PHP scenarijų kalba (4.1.0 ar vėlesnė versija). PHP 5 galima naudoti tik su „Moodle“ 1.4 ar naujesnėmis versijomis.

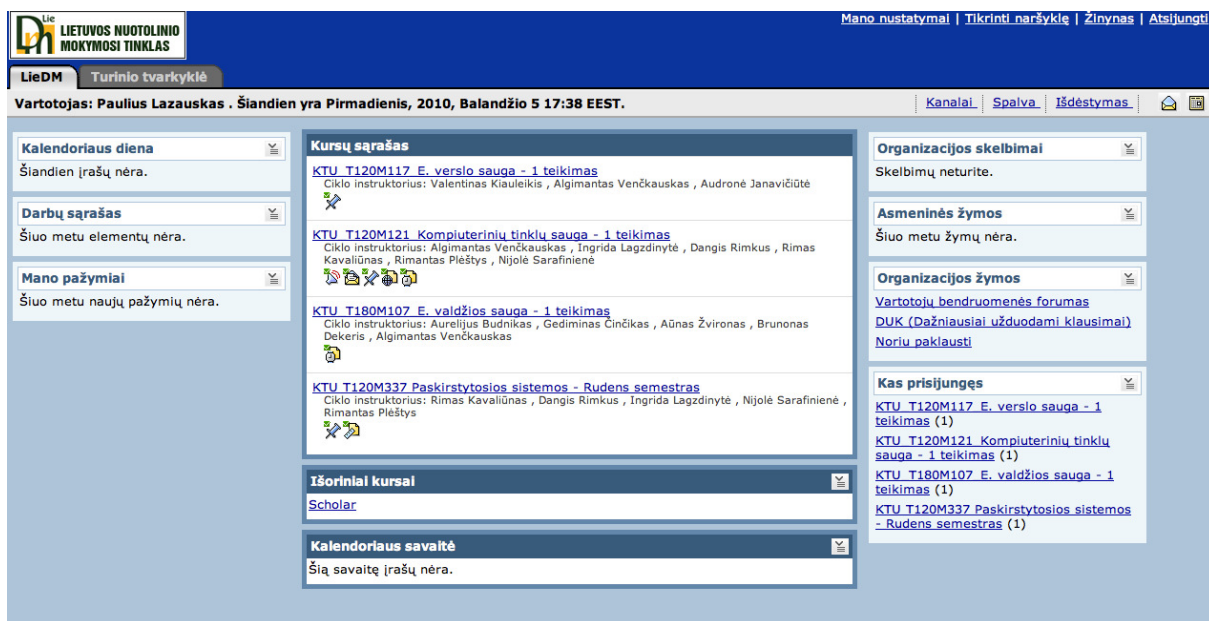
- Duomenų bazių serveris (rekomenduojama *MySQL* arba *PostgreSQL*).

„Moodle“ suderinama su SCORM elektroninio mokymosi turinio pakavimo standartu, todėl sistemoje galima panaudoti mokymosi turinį iš kitų šiuos standartus atitinkančių aplinkų, taip pat eksportuoti turinį ir panaudoti jį kitose aplinkose.[5]

1.1.3 Virtuali mokymosi terpė WebCT

WebCT (Web Course Tools) – plačiausiai pasaulyje naudojama virtuali mokymosi terpė. Pirmą kart pasauliui ji buvo pristatyta 1996 metais. Šią terpę mokymui(si) naudoja virš 6 milijonų pasaulio studentų. WebCT kompanija investavo daugiau kaip 100 milijonų dolerių sistemos plėtrai. Rinkos lyderiu WebCT tapo todėl, kad ji yra lanksčių, lengvai naudojamų ir pedagoginiu požiūriu patogių mokymo ir mokymosi įrankių visuma. Tie įrankiai yra skirti trimis skirtingoms, viena kitą papildančioms funkcijoms vykdyti[26]:

- Kursų kūrimui. WebCT turi priemones, padedančias kursų kūrėjams paruošti ir pradėti teikti naujus kursus.
- Kursų teikimui. Turi įvairias priemones patogiam kursų teikimui nuotoliniu būdu. Be to ši terpė tinka ir dieninių studijų modernizavimui. Taikymo funkcijos skirstomos į:
 - **Komunikavimo ir bendravimo įrankius;**
 - **Atestavimo (įvertinimo) įrankius.**
- Kursų valdymui. Pradėjus teikti kursą WebCT valdymo įrankiai leidžia efektyviai jį administruoti. Be to, kuratorius bet kada gali gauti statistinę informaciją apie besimokančiųjų aktyvumą bei atestavimų rezultatus. Suasmeninti terpės vartai leidžia studentams dėstytojams bei administratoriams įeiti į daugialypių kursų aplinką ir turėti bendrus kursų kalendorius ir mokyklos pranešimus[26]. Kaip atrodo sistemos aplinka vartotojui galima pamatyti 4 pav.



4 pav. Bendras WebCT sistemos vaizdas

WebCT terpė yra gausi pagalbinių įrankių. Terpėje patogu naudotis elektroniniu paštu, išoriniais išvesties įrenginiais, pagalbomis ir pan.

Techniniai kompiuterio reikalavimai darbui **WebCT** aplinkoje:

- Personalinis kompiuteris pastoviu interneto ryšiu.
- Kompiuteryje turi būti įdiegta Netscape Navigator 4x, Netscape Communicator 4x arba Internet Explorer 5 ar naujesnės šių interneto naršyklių versijos.

1.1.4 Išvados

Atlikus egzistuojančių, labiausiai paplitusių nuotolinio mokymo ir egzaminavimo sistemų analizę sudarėme apibendrinimui skirtą lentelę Nr. 1. Šioje lentelėje išvardinti kriterijai ir statusai, kurie nurodo sistemų privalumus ir trūkumus.

Vertinimo kriterijai:

Egzaminavimo įrankių lygis – vertinama ar sistemose įdiegti atsiskaitymo būdai yra pritaikyti studentams laikyti egzaminus nuotoliniu būdu, bei jų gausa.

Video paskaitų lygis – jei sistema turi nuotolinių video paskaitų transliacijos galimybę, vertinama perduodamos audio-video medžiagos kokybė.

Video seminarų lygis - jei sistema turi video seminarų transliacijos galimybę, vertinama perduodamos audio-video medžiagos kokybė.

Autentifikacijos lygis – vertinamas saugių duomenų perdavimo protokolų naudojimas bei naujos kartos autentifikavimo priemonių palaikymas (autentifikacija biometrinių skaitytuvų arba e-parašo pagalba).

Paplitimas – vertinamas sistemos populiarumas mokymo įstaigose.

Trečiųjų šalių modulių palaikymas – atkreipiamas dėmesys ar sistema palaiko papildomus modulius, kuriuos kuria kitos kompanijos ar asmenys. Kuriant „Audio – video nuotolinio mokymo ir egzaminavimo sistemą“ yra aktualu atkreipti dėmesį į kitų sistemų platformiškumą ir galimybę, kuriamą sistemą suprojektuoti taip kad ji galėtų tarnauti kaip papildomas funkcijų rinkinys kitose sistemose.

Lentelė Nr. 1 Išnagrinėtų sistemų skirtų nuotolinėms studijoms apibendrinimas

Kriterijus	Nuotolinio mokymo ir egzaminavimo sistemos		
	ATutor	Moodle	WebCT
Egzaminavimo įrankių lygis	Žemas	Žemas	Žemas
Video paskaitų lygis	Nėra	Nėra	Nėra
Video seminarų lygis	Nėra	Nėra	Nėra
Autentifikacijos lygis	Vidutinis	Vidutinis	Vidutinis
Paplitimas	Vidutinis	Didelis	Didelis
Trečiųjų šalių modulių palaikymas	Yra	Yra	Yra

Nei viena iš nagrinėjamų sistemų neturi mokymo įrankių paremtų video transliacijomis. Video apdorojimo terpė palikta trečiųjų šalių programinei įrangai (įskiepiams). Visose sistemose realizuoti labai primityvūs atsiskaitymo būdai. Autentifikacijai taip pat nėra skiriamas didelis

dėmesys. Nei vienoje sistemoje nėra realizuota autentifikacija nei biometrinio skaitytuvo ar e-parąšo pagalba.

1.2 Audio - video informacijos perdavimo internetu analizė

Kuriamoje „Audio – video nuotolinio mokymo ir egzaminavimo sistemoje“ didžiausias dėmesys yra skiriamas mokymo procesams paremtiems vaizdo konferencijomis. Pasaulyje egzistuoja sistemų, kurių pagalba galima vykdyti video transliacijas iš nutolusios vietos ar inicijuoti daugialypes vaizdo konferencijas. Kauno technologijos universitetas video paskaitų transliacijoms naudoja ViPS programinį sprendimą. Plačiai visiems žinomos programinės įrangos Skype mokama versija turi daugialypių vaizdo konferencijų palaikymą. Tačiau dauguma sistemų turi tam tikrų trūkumų. Svarbiausias trūkumas yra tai, kad sistemos vartotojas negali vykdyti video konferencijos į savo kompiuterį neįdiegęs papildomos programinės įrangos. Dar vienas iš trūkumų yra tai, kad dėstytojams norint transliuoti aukštos kokybės video paskaitas reikia naudotis video studijomis, kurioms įkurti reikalingos didelės investicijos.

Vykdamt nuotolinius seminarus ar egzaminus yra reikalingas „dvipusis“ audio – video ryšys. Reikia atkreipti dėmesį, kad dažnas „namų“ vartotojas turi nedidelės spartos internetą. Mūsų uždavinys sukurti sistemą, kuri nustačiusi vartotojo interneto pralaidumą, jam siųstų atitinkamos kokybės video medžiagą.

Analizuojant audio-video informacijos perdavimą internetu didelis dėmesys bus skiriamas aukštos kokybės (HD) video perdavimui. Tai gali būti naudinga vykdamt video paskaitas medicinos srityje, nes mokomoji medžiaga dažnai būna realios rentgeno nuotraukos bei kita.

1.2.1 Vaizdo konferencijos

Tai būdas kompiuterių tinklais perduoti dinaminį vaizdą ir garsą. Vaizdo konferencijoje gali dalyvauti keletas abonentų. Kiekvienam jų reikia vaizdo kameros ir kompiuterio. Abonentai per savo kompiuterį transliuoja į kompiuterių tinklą vaizdo kameros signalus (vaizdą ir garsą), o kiti abonentai juos priima. Galima priimti tik kitų abonentų siunčiamus signalus (pasyviam vaizdo konferencijos dalyviui kamera nebūtina), priimti atskirų abonentų signalus, demonstruoti priimamą vaizdą ir garsą televizorių ekranuose arba projektuoti vaizdą į sieninius ekranus ir t.t.

Vaizdo konferencijos tinka distancinėms studijoms. Iš studijų centro gali būti transliuojamos mokomosios laidos pagalbiniais studijų centrams. Galimas realaus laiko atgalinis ryšys su studijų centru tais pačiais kompiuterių tinklais, tačiau atgalinio ryšio tipas ir būdas priklauso nuo turimų ryšio kanalų ir technikos.

Vaizdo konferencijas taikant distancinėse studijose, paprastai būna dvipusis asimetrinis ryšys, nes be atgalinio ryšio edukologiniu požiūriu studijos yra nevisavertės. Ryšys gali būti asimetrinis, nes atgalinio ryšio reikalavimai paprastesni negu mokomųjų laidų transliacijos. Kokybiškų mokomųjų laidų transliacijai pageidautina turėti bent 2 Mbps laidumo ryšio kanalą. Atgaliniam vaizdo ryšiui pakanka 256 kbps laidumo ryšio kanalo, o jei pakanka garsinio atgalinio ryšio, tuomet pakanka 64 kbps laidumo ryšio kanalo. Jei yra iki dešimties studijų pagalbinių centrų, patenkinamą rezultatą galima gauti, sujungus juos 2 Mbps laidumo ryšio kanalais, atgalinį ryšį turint tais pačiais kanalais.

Su vaizdo konferencijomis perduodamos informacijos įvairumu ir kokybe negali lygintis jokie kiti distancinių studijų organizavimo metodai. Vaizdo konferencijos suteikia daugiau galimybių negu kitos komunikacijų sistemos ir kompiuterinio ryšio lygiai, ir atstoja jų teikiamas galimybes, išskyrus paštą, nes negali būti perduodami materialūs daiktai. Tačiau perduoti mokomąją medžiagą čia sudėtingiau, todėl dažnai kartu su vaizdo konferencijomis distancinėse studijose naudojamos ir kitos kompiuterinio ryšio priemonės, pavyzdžiui, elektroninis paštas, pasaulinio voratinklio aplinkos priemonės ir t.t.

Palyginti su kitomis priemonėmis ir sistemomis, edukologiniu požiūriu vaizdo konferencijos garantuoja efektyviausias distancines studijas. Gali būti pasitelkta beveik visa tradicinių studijų patirtis ir metodikos, išskyrus laboratorinius darbus, nors kai kuriuos procesus galima demonstruoti vaizdo filmais. Be to, vis daugiau procesų galima modeliuoti kompiuteriu; t.y. pigiau negu naudojant kitą laboratorinę įrangą. Todėl kai kuriais atvejais laboratorinius darbus galima iš dalies kompensuoti darbu modeliavimo programų paketais arba vaizdo įrašų peržiūra.

Šiuo metu vaizdo konferencijos yra viena efektyviausių priemonių organizuoti grupines distancines studijas, šioje srityje intensyviai dirbama visame pasaulyje, todėl jos ateityje neabejotinai populiarės.

1.2.1.1 Vaizdo konferencijų paplitimą ribojantys veiksniai

Dar pakankamai brangūs ryšio kanalai, užtikrinantys pakankamą vaizdo ir garso kokybę. Bet labiausiai, ko gero, platų vaizdo konferencijų naudojimą stabdo inercija ir jų galimybių bei galimų taikymo sričių nežinojimas, rečiau – lėšų stygius, nes daug kur vaizdo konferencijos gali apsimokėti.[23]

1.2.1.2 Vaizdo konferencijų kokybė

Vaizdo konferencijos tikslas – sukurti tiesioginio, be technikos tarpininkavimo, tarpusavio bendravimo iliuziją. Žmogus privalo jausti, kad jo pašnekovai yra kažkur greta toje pačioje erdvėje, o televizorius, monitorius ar vaizdo projektorius turi taip susieti jį su aplinka, kad vaizdas būtų matomas tarsi pro langą.

Svarbiausias dalykas, leidžiantis arba neleidžiantis sudaryti tiesioginio bendravimo iliuziją – vaizdo ir garso kokybė. Garsas bus geras, jei sklis be trikdžių ir aido, bus aiškus, netrūkčiojantis, be pauzių ir erdvinis. Garso kokybė priklauso nuo garso kanalo pločio bei techninės įrangos – mikrofonų, garsiakalbių ir kt. Vaizdas turi būti spalvotas, aiškus, netrūkčiojantis ir nevėluojantis. Vaizdo kokybė priklauso nuo kadru (piešinių) keitimosi dažnio, skiriamosios gebos (taškų skaičiaus) ir monitoriaus dydžio.[23]

Garsas ir vaizdas, paversti skaitmeniniais kodais, sudaro didelius duomenų blokus, kuriuos sunku ir brangu saugoti bei perduoti ryšių linijomis. Todėl praktikuojamas garso ir vaizdo suspaudimas, leidžiantis atsisakyti perteklinės informacijos ir sumažinti duomenų blokų apimtį. Tačiau suspaudimo metu prarasta perteklinė informacija keičia garsą ir vaizdą, blogina kokybę, gali iškraipyti juos. Ypač pavojinga suspaustą vaizdą ir garsą perduoti nepakankamai patikimomis bei riboto pralaidumo ryšio linijomis, nes, atsisakius perteklinės informacijos, praradimų ryšio kanale kompensuoti nebegalima.[23]

Vaizdo konferencijų kokybė tiesiogiai proporcinga įrangos ir kanalų nuomos kainoms. Vargu ar galima tikėtis pakankamos kokybės, pasirinkus pigiausius variantus. Tačiau papildomai įdėti pinigai taip pat ne visuomet leis pakelti vaizdo konferencijų kokybę. Šiuo metu sparčiai plėtojasi telekomunikacijų tinklai, todėl įsigyta įranga turi būti adaptyvi, lanksti ir leisti dirbti su įvairiais duomenų perdavimo protokolais, palaikyti Tarptautinės telekomunikacijų sąjungos parengtus standartus, nusakančius vaizdo konferencijų garso ir vaizdo suspaudimo algoritmus,

duomenų perdavimo būdus, kanalo pločius ir jų valdymo metodus. Standartų laikymasis įgalina derinti skirtingų firmų įrangą, nuolat ją atnaujinti, nuosekliai plėtoti, didina sistemos lankstumą.[23]

1.2.1.3 Audio-video srautų organizavimas bei pralaidumo įvertinimas e-studijų sistemoje

Kuriant E-studijų sistemas, esant bendravimo modeliui: nutolęs dėstytojas ↔ studentų klasė, iškyla specifinės problemos kaip optimizuoti Audio-Video srautų transliacijas tarp dėstytojo ir studentų. Taip pat būna poreikis audio-video srautų transliavimą susieti su kitomis standartinėmis e-studijų funkcijomis, kaip dalinimasis programomis, greiti atsakymai, pokalbiai, dalinimasis failais ir pan. Analizuojama, kaip išspręsti šias problemas laikantis H323 specifikacijos

1.2.1.4 Tiesioginis sujungimas prieš centralizuotą sistemą

Tiesioginio sujungimo video konferencijos planuojamos tokiu principu, kad kiekvienas konferencijos dalyvis siunčia video informaciją visiems likusiems konferencijos dalyviams, bei tuo pačiu metu klausosi kitų audio-video srautų per atskirai sukurtus kanalus. Tokių konferencijų vykdymas kai kuriais aspektais yra techniškai lengvesnis, be to klientas įgauna daugiau laisvės, nes nereikia prisirišti prie centrinio serverio, o tiesiog galima jungtis prie konkretaus vartotojo ir taip organizuoti konferenciją. Vis tik tokia sistema turi pakankamai minusų, esminis tame, kad ją bus sudėtinga išplėsti ir pridėti papildomų funkcijų. Tokios funkcijos kaip konferencijos žurnalo vedimas bei saugojimas ar unifikuoti testai naudojami e-studijų sistemose daug lengviau realizuojamos naudojant centralizuotą serverį. Be to yra dažnai pasitaikantis atvejis, kad klasės, kurioje sėdės studentai, kompiuteriai gali turėti lokalius IP numerius ir stovėti už ugniasienės. Taip pat dažnai pasitaiko, kad dėstytojo darbo vieta būna nutolusi (per internetą) nuo studentų klasės, taigi gali būti apribota duomenų perdavimo sruto apimtis. Jeigu kompiuteriai, esantys klasėje, stovi už ugniasienės, iškyla Audio-Video srautų praėjimo pro ugniasienę problema, kurią įmanoma išspręsti tik naudojant tarpinį serverį (nebūtinai centrinį, bet jis galėtų susikalbėti su centriniu). Net jeigu klasė nestovi už ugniasienės yra neefektyvu transliuoti Audio-Video srautą keliems vartotojams esantiems vienoje vietoje per internetą, nes taip didės duomenų perdavimo

srautas, kuris gali būti ribotas. Daug efektyviau priimti viena srautą viename iš klasės kompiuterių ir išdalinti jį 'netoli' esantiems. Tai taip pat gali atlikti tarpinis serveris. Taigi galima daryti išvadą, kad e-studijų sistemoms nenaudinga naudoti tiesioginio sujungimo sprendimą. Visom e-studijų funkcijom realizuoti bei techninėm problemom spręsti geriau naudoti centralizuotą sistemą, kur veiktų vienas ar keli serveriai.[4]

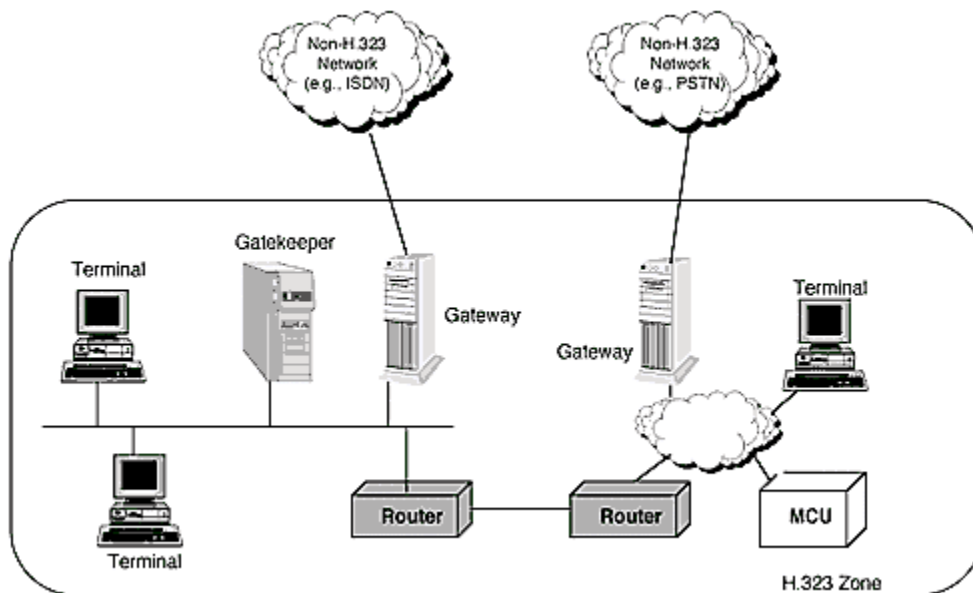
1.2.2 H323 specifikacija

1.2.2.1

H323 standartas tai aibė protokolų skirtų vaizdo-garso konferencijoms rengti paketų perdavimu pagrįstuose tinkluose, tokiuose kaip IP tinklai(internetas). Šiuo metu H323 standartas yra pagrindinis tam skirtas standartas turintis tik vieną konkurentą – SIP. Bet šiuo metu SIP yra dar labai jaunas standartas, ir praktiškai testavimo fazėje. H.323 rekomendacija apibrėžia terminalus ir kitus objektus dirbančius tinkluose, kurie negarantuoja kokybiško paslaugų atlikimo. H.323 objektai gali komunikuoti realiu laiku ir perduoti garsą, vaizdą bei duomenis. Bendravimas garsu yra privalomas, kai tuo tarpu vaizdo ir duomenų perdavimas yra nebūtinas. Tačiau jei vaizdo ir duomenų perdavimas yra įmanomas, tada pageidaujama, kad visi terminalai palaikytų šių duomenų apsikeitimą ir galėtų tarpusavyje komunikuoti. H323 apibrėžia keturis komponentus: Gateway, Gatekeeper, Terminal ir MCU(Multipoint Control Unit).

- Terminal yra galinis tinklo taškas, kuris teikia realaus laiko komunikacijas su kitu Terminal, Gateway arba MCU. Terminal turi palaikyti tam tikrus Audio bei Video kodekus.
- Gateway teikia pakeitimo tarp protokolų servisą. Panaudojant juos, H323 numato galimybę komunikuoti su terminalais atitinkančiais H320(ISDN), H321(ATM) ir pan. standartais.
- Gatekeeper tikslas yra atlikti visos sistemos kontrolę, teikti autorizacijos paslaugas, kontroliuoti audio-video perdavimo resursus ir pan.
- MCU tai komponentas suteikiantis galimybę konferencijoje dalyvauti daugiau nei dviems sistemos komponentams, jis atlieka paskirstymo darbą. [4]

Šių komponentų bendrą sąveiką galime matyti 5 pav.



5 pav. Bendra H323 schema

1.2.2.2 H323 specifikacijos laikymasis e-studijų sistemoje

1.2.2.3

Konkrečiai e-studijų sistemai, jai esant gan specializuotai ir nenumatant ryšių su kitomis sistemomis Gateway komponentas praleidžiamas, tuo tarpu Gatekeeper realizuojamas, kaip centrinis sistemos serveris, tuo pačiu metu galintis aptarnauti vartotojų autorizaciją bei atlikti specialias e-studijų funkcijas, tokias kaip failų dalinimasis, testavimas ir pan. MCU realizuojamas kaip tarpinis serveris-paskirstytojas.

1.2.3 Srautinis audio - video informacijos perdavimas

Srautinės audio - video informacijos perdavimo (angl. Streaming) metu audio - video informacija iš serverio per tinklą siunčiama klientams realiu laiku. Serveris, kuris šią informaciją apdoroja vadinamas srautinės audio video informacijos perdavimo (SAVIP) serveriu. Klientų interneto spartos amplitudė maksimali nuo modemu perduodamo iki plačiajuosčio. Nei vienas failas nėra persiunčiamas į kliento standų diską. Audio - vieo informacija atkuriamą kliento turimomis programomis.

1.2.3.1 SAVIP serveris

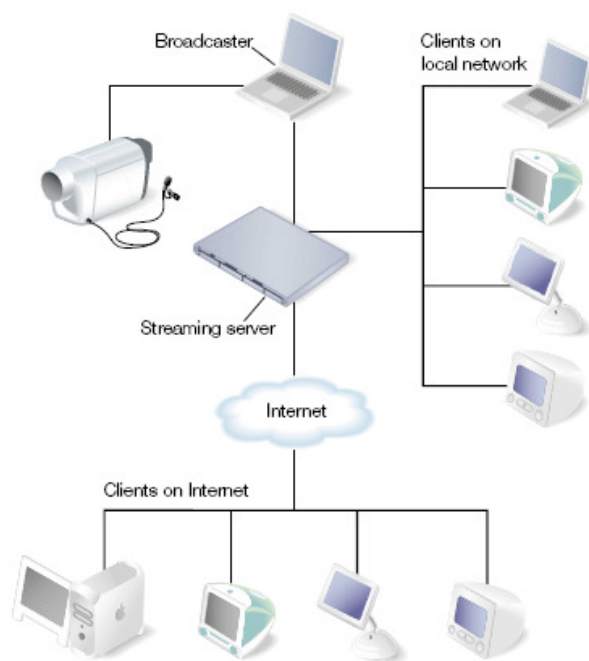
Norint naudoti srautinį audio - video informacijos siuntimą, tam, kad informacija internetu pasiektų vartotojai būtinai reikalingas SAVIP serveris. [7] Kaip vartotojams reikia web

serverio jų interneto svetainėms, mail serverio – pašto žinutėms, taip SAVIP serveris reikalingas realaus laiko transliacijoms.

Smulkiems projektams tame pačiame kompiuteryje gali būti paleistos visų serverių web, mail ir SAVIP programinės įrangos. Kuriant stambius projektus reikėtų atsižvelgti į vartotojų kiekius ir naudoti dedikuotus serverius kuriuose atskirai būtų valdomos skirtingi programų rinkiniai. Taip pat yra taikomas virtualių mašinų principas.

1.2.3.2 Realus laiko transliacijų veikimo principas naudojant srautinės audio – video informacijos perdavimo technologiją

Filmuojama medžiaga retransliuojama į kompiuterį (mobilią darbo vietą), kuriame video medžiaga apdorojama ir siunčiama į SAVIP serverį. Klientai internetu gali pasiekti realaus laiko transliacijas, kurios yra vykdomos serveryje. (6 pav.) pateikta veikimo principinė schema. Ši schema aptinkama visų srautinės audio – video informacijos perdavimo technologijomis pagrįstų produktų aprašymuose. (pvz. Darwin Streaming server, Adobe Flash Media Server 3, VLC ir kt.).



6 pav. Realus laiko transliacijų veikimo principo schema

1.2.3.3 Srautinės audio – video informacijos perdavimo privalumai

“Progressive download”, tai paprastas metodas video medžiagos atkūrimui su labai mažai kontrolės.[18] SAVIP – tai metodas, kuris leidžia transliuotojui kontroliuoti visus aspektus susijusius su video medžiagos atkūrimu.

SAVIP privalumai [2]:

- **Greitas startas** – SAVIP yra greičiausias būdas paleisti video transliaciją interneto svetainėje.
- **Pažangi video kontrolė** – srauto matavimas; paslaugos kokybės stebėjimas/monitoringas; automatinis pristatančių paveikslėlių formavimas; serverio pusės grojaraštis.
- **Efektyvus tinklo resursų panaudojimas** – Vartotojai kurie moka už savo video medžiagos talpinimą serveryje arba už srauto suvartojimą, video klipų transliacijos metu yra registruojamas kiekvienas persiųstas bitas ir už tam tikrą srauto suvartojimą klientas moka nustatytą kainą. Vartotojui žiūrint srautinės audio-video informacijos transliaciją yra parsiončiami tik tie bitai kurie aktualūs žiūrimos video medžiagos atkūrimui, tai reiškia, kad yra taupomas srautas.
- **Saugumas, saugus audio-video informacijos perdavimas** – audio-video informacija SAVIP atveju nėra kešuojama (saugoma) kliento kompiuteryje, todėl nei video nei audio failų negalima rasti „temporary Internet files“ kataloge ar kur kitur. Taip pat audio-video informacijos atkūrimo metu, ji yra apsaugota nuo neleistinų kopijų („ripping“).
- **Minimalus kliento resursų naudojimas** – Tokie resursai kaip atmintis ir kietoje disko vieta yra beveik nenaudojami, nes video failas nėra parsiončiamas į kliento kompiuterį.
- **Statistika ir veiksnų registravimas** – Kadangi „progressive download“ yra paprasčiausias failo parsisiuntimas, todėl neįmanoma rinkti statistikos apie tam tikrus veiksmus. Pavyzdžiui: kiek laiko video medžiaga buvo žiūrima; ar vartotojas navigavo po žiūrimą video medžiagą (pirmyn ar atgal); ar medžiaga buvo sustabdyta; kiek kartų vartotojas paleido groti video medžiagą; ar kai vartotojas uždarė naršyklės langą, video failas buvo peržiūrėtas pilnai; ir kiti

įvairūs statistiniai aspektai. SAVIP leidžia registruoti visą informaciją apie tokius veiksmus.[18]

- **Pilnas pareikalavimas ir navigacija** – Vartotojas gali pasirinkti bet kurią video vietą kaip pradžios atskaitos tašką ir po paspaudimo iškart matyti video transliaciją nuo pasirinktos vietos. Tai šaunus SAVIP sprendimas ilgiems video failams (paskaitų medžiaga, konferencijų atskiri pranešimai), kai reikia video medžiagą stebėti ne nuo pradžių, o nuo tos vietos kur yra dominantanti informacija.
- **Gyva transliacija (Live video)** – SAVIP technologija leidžia realiu laiku iš įvykio vietos web kameros arba DV kameros pagalba filmuoti ir retransliuoti gyvą video medžiagą. Taip pat galima retransliuoti gaunamą medžiagą tiesiogiai iš video plokštės.
- **Video filmavimas ir įrašymas** – yra galimybė filmuojant tam tikrą įvykį vienu metu jį rodyti realiu laiku bei įrašinėti į nutolusį serverį. Taip iškart suformuojamas video archyvo failas.
- **Daugiavartotojiškumo galimybė** – Yra galimybė realiu laiku atlikti ne vieną, o keletą transliacijų. Taip netgi įmanoma suprojektuoti komunikacijos sistemą.

SAVIP technologija programuotojams suteikia daugiau galimybių sukurti interaktyvią video sistemą su įvairiomis panaudojimo galimybėmis. Kaip patį didžiausią minusą galima išskirti, kad norint realizuoti srautinį duomenų perdavimą yra būtina serverio pusės programinė įranga. SAVIP serveris yra diegiamas kartu su web serveriu, šiuolaikinių serverių aparatūrinis pajėgumas tai leidžia. [2]

1.2.3.4 SAVIP naudojimas

SAVIP patartina naudoti esant tokioms situacijoms:

- Atkuriant ilgos trukmės failus (daugiau nei 30 sekundžių) arba aukštos kokybės failus (daugiau nei 100 Kbps)
- Atlikus pralaidumo matavimą, leisti perduoti aukštesnės kokybės video failą
- Kai reikalingas paslaugos kokybės monitoringas
- Kai reikalingas statistikos rinkimas realiu laiku
- Kai yra reikalingos video/audio realaus laiko transliacijos

- Kai reikia įrašinėti video/audio medžiagą
- Kai reikia taupyti srauto sąnaudas ne video kokybės mažinimo kaina.

Jeigu interneto svetainė yra paremta informaciją vartotojui pateikti video, audio medžiagos pavidalu bei realaus laiko transliacijomis, tada neišvengiamai yra būtina naudoti SAVIP technologiją. Norint tai įgyvendinti yra būtina serverio pusės programinė įranga. [1]

1.2.4 Audio - video informacijos perdavimas naudojant P2P technologiją

1.2.4.1 RTMFP(Real Time Media Flow Protocol)

liet. Realaus Laiko Audio-Video Srauto Protokolas

RTMFP –tai privatus protokolas, kurį sukūrė Adobe kompanija. RTMFP leidžia tiesiogiai peer-to-peer ryšiu tarp Adobe Flash grotuvu ir programų sukurtų naudojant "Adobe AIR" vykdyti realaus laiko komunikaciją. RTMFP galutiniams vartotojams suteikia galimybę prisijungti ir bendrauti tiesiogiai viena su kitu naudojantis savo kompiuterio mikrofonu ir kamera. Tačiau RTMFP nepalaiko failų ar dokumentų dalinimosi funkcijos. Šis sprendimas padidina esamą Flash Player funkcionalumą bei suteikia didesnes galimybes kuriant kokybiškesnius sprendimus.[19]

1.2.4.1.1 RTMFP Privalumai

Kadangi RTMFP duomenų srautas skirstomas tiesiogiai tarp galutinių vartotojų, nenaudojant jokių serverio resursų, taip yra taupomas didelis kiekis duomenų srauto tuo pačiu taupomi ir finansai. RTMFP protokolas veikia UDP protokolo pagrindu todėl informacijos pristatymo greitis didesnis. UDP yra veiksmingesnis (bet mažiau patikimas) būdas video ir audio informaciją perduoti internet, taip yra nes pamesti ar sugadinti paketai nėra pakartojami. RTMFP turi dvi ypatybes, kurios gali padėti sumažinti ryšio klaidų poveikį:

- **Greitas sujungimo atkūrimas.** Sujungimas yra atkuriamas akimirksniu po trumpo ryšio sutrikimo. Pvz. Po bevielio tinklo sujungimo persikrovimo.
- **IP mobilumas** Aktyvi sesija veiks nepertraukiamai net jeigu vieno iš klientų pasikeistų IP adresas. Pvz. Kai nešiojamasis kompiuteris gauna naują IP adresą nes belaidžio interneto jungtis buvo pakeista laidine jungtimi.



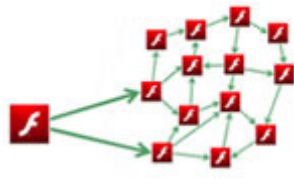
1.2.4.2 Stratus

RTMFP – tai revoliucija audio-video informacijos perdavimui realiu laiku internete. Stratus technologija labai siaurai buvo pristatyta 2008. Ši technologija leido klientui siųsti duomenis kitam klientui nenaudojant serverio. Pasirodžius 10 versijai FlashPlayer, kuri palaiko P2P technologiją, atsivėrė naujos galimybės. Šis grotuvas yra itin paplitęs kompiuterių vartotojų tarpe. Be to jau daugiau nei 90% vartotojų yra susidiegę naująją grotuvo versiją.[21]

Patys svarbiausi RTMFP privalumai:

- Mažas vėlavimas,
- End to end peering'as,
- Saugumas bei paslankumas.

Lentelė Nr. 2 Adobe priemonių skirtų audio-video informacijos perdavimui raida [21]

Tradiciniai SAVIP / Komunikacija pagrįsta Unicast modeliu	RTMFP Flash player 10.0 / Stratus 1,0	RTMFP Flash player 10,1 / Stratus 2,0
		
<p>Tradicinis SAVIP reikalauja, kad klientas parsisiųstų duomenis iš centralizuoto serverio. Norint plėsti vartotojų kiekį reikia diegti kuo daugiau serverių.</p>	<p>Pirmosios kartos RTMFP naudojant Flash player 10.0 palaiko srauto dalinimąsi. Audio – video informacija visuomet buvo prieinama per viešai skelbiamą informacijos šaltinį.</p>	<p>Antrosios kartos RTMFP palaikantis grupavimą Flash player 10,1 palaiko taikomąjį lygmenį multicast ir sumažina informacijos šaltinio apkrovą.</p>

2 lentelėje pateikta kaip struktūriškai kito audio-video informacijos perdavimas naudojant Adobe kompanijos priemones. Tačiau tai visiškai nereiškia, kad SAVIP technologija bus išstumta. Norint transliuoti aukštą audio-video informaciją internete neišvengiamai būtina naudoti SAVIP technologija pagrįstus įrankius.

Norint naudotis RTMFP, Flash Player teikimais privalumais, privalote prisijungti prie RTMFP palaikančio serverio, pvz. Stratus paslaugos. Stratus yra paruošę beta versija. Yra viešai patalpinta pristatomoji paslauga, kuri padeda užmegzti ryšį tarp Flash Player galutinių vartotojų.

Skirtingai nei "Adobe Flash Media Server", Stratus nepalaiko audio – video informacijos, naudojamų objektų, skriptų ir t.t. Taigi, naudojant Stratus, galite tik sukurti programas, kurios Flash Player parametrų pagalba tiesiogiai bendrautų tarpusavyje.

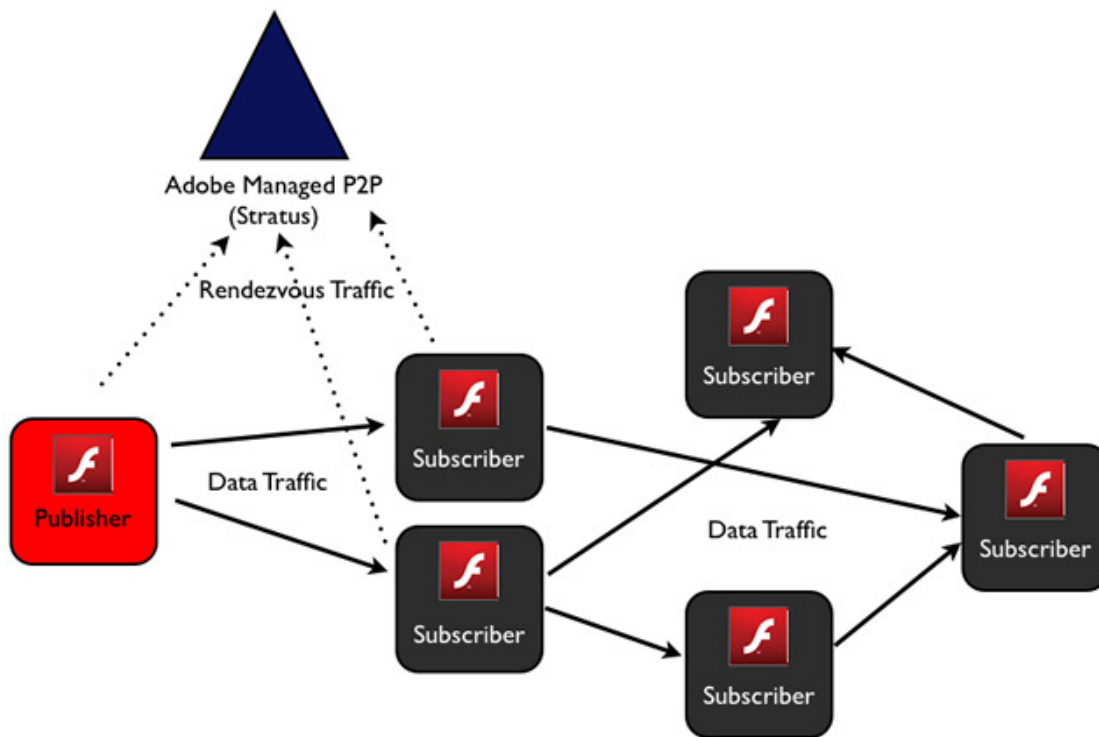
Flash Player yra rinkos lyderis vaizdo paskirstymo per www srityje. Su RTMFP ir pažangia audio - video informacijos suspaudimo technologija, Flash Player 10,1 yra realaus laiko komunikacijos lyderis taip pat.

Stratus tai ateityje pasirodysiančios technologijos pristatymas talpinamas Adobe serveriuose.

Stratus nepalaiko serverio pusės programavimo, audio - video informacijos užlaikymo bei objekcinio programavimo modelių. Ši technologija bus paskelbta su naujai išleidžiamu Adobe Flash Streaming Server programiniu paketu. Tačiau jau dabar galima naudotis šios technologijos teikiamomis paslaugomis. [21]

1.2.4.2.1 Realus laiko taikomasis lygmuo „multicast“

Visi prijungti įrenginiai gali užmegzti ryšį su kontroliuojančiu servisu, kuris naudojamas tik teikti autentifikavimo paslaugą ir kaupti informacijai apie prisijungusius prietaisus. Nuo to taško tolyn, visi duomenys bus nukreiptas per P2P tinklą kuo efektyviau kaip parodyta 7 pav. Kiti šios topologijos privalumai yra tai, kad srautas yra naudojamas efektyviau, nes P2P taškai pasirinktinai ima turinį iš kitų taškų, kad kuo greičiau pristatyti informaciją, o ne iš informacijos tiesioginio skleidėjo.[17]



7 pav. Taikomasis lygmuo multicast [17]

1.2.5 H.264 video standartas

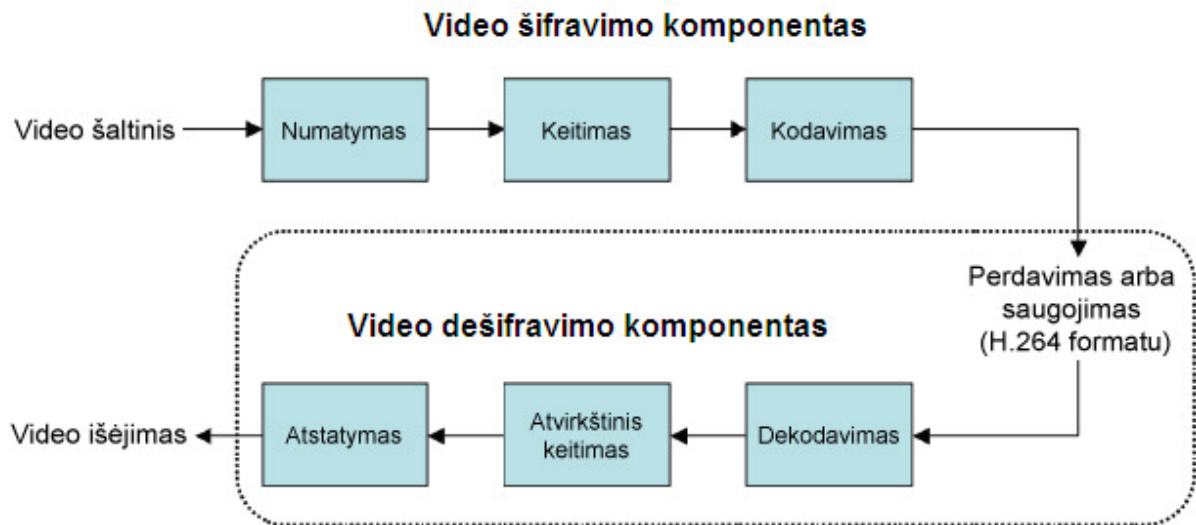
H.264 tai pramoninis video medžiagos suspaudimo standartas, skaitmeninės video medžiagos konvertavimo procesas į formatą, kuris saugojimo ar perdavimo metu užima mažiau talpos. Video suspaudimas (ar video kodavimas) yra svarbi technologija tokiems taikymams kaip skaitmeninė televizija, DVD-video, mobili TV, video konferencijos ir audio - video transliavimui srautinės informacijos pagrindu internete.

Video suspaudimo standartizavimas leidžia naudoti skirtingų gamintojų produktus. **Kodavimo įrenginys** konvertuoja video medžiagą į suspaustą video formatą, o **dekoduotojas** - priešingai.

Pažangus video kodavimas (Advanced Video Coding (AVC)) yra dokumentas paskelbtas tarptautinių standartų organo ITU-T (Tarptautinė telekomunikacijų sąjunga) ir ISO/IEC (Tarptautinė standartizacijos organizacija/Pasaulinė elektrotechnikos komisija). Dokumentas apibrėžia formatą (sintaksę) suspaustai video informacijai ir metodą šios sintaksės dekodavimui. Standartinis dokumentas iš tikrųjų neapibrėžia, kaip užkoduoti (suspausti) skaitmeninę video

medžiagą – tai išspręsti paliekama video kodavimo įrenginio gamintojui – praktiškai kodavimo įrenginys parodo dekodavimo procesą. 8 iliustracija rodo kodavimo bei dekodavimo procesus ir svarbiausias dalis, kurios yra apimtos H.264 standarto. [3]

H.264/AVC standartas buvo iš pradžių publikuotas 2003. Jis remiasi ankstesnių standartų, tokių kaip MPEG-2 ir MPEG-4 Visual, sąvokomis ir siūlo geresnį suspaudimo efektyvumą, lankstesnį suspaudimą, perdavimą ir video medžiagos kaupimą. [13]



8 pav. Video medžiagos kodavimas, perdavimas arba saugojimas bei atkūrimas naudojant H.264 formatu

1.2.5.1 H.264 veikimo principas

H.264 video kodavimo įrenginys atlieka numatymo, keitimo ir kodavimo procesus (8 pav.), kad pagamintų suspaustą H.264. H.264 video dekoderis atlieka dekodavimo, priešingo keitimo ir atstatymo procesus, kad pagamintų iššifruotą video seką. [13]

1.2.5.2 H.264 našumas ir taikymas

Galbūt didžiausias pranašumas H.264 [3, 13] nuo ankstesnių standartų yra savo suspaudimo našumas. Palyginti su standartais tokiais kaip MPEG-2 ir MPEG-4 Visual, H.264 gali atgabenti:

- geresnės kokybės atvaizdus tame pačiame suspaudime

- mažesnis suspaudimas esant tai pačiai atvaizdo kokybei.

Pavyzdžiui, vienasluoksnis DVD gali sukaupti kino filmą apytiksliai 2 valandų ilgio MPEG-2 formate. Naudojant H.264, turi būti galima sukaupti 4 valandas ar daugiau kino filmo kokybės tame pačiame diske. Arba kitaip, H.264 suspaudimo formatas gali tiekti geresnę kokybę esant tam pačiam suspaudimui lyginant su MPEG-2 ir MPEG-4 Visual (9 pav.).

H.264 yra labiau pažengęs negu ankstyvesni suspaudimo metodai, ir tai reiškia, kad gali reikėti žymiai daugiau apdirbimo galios suspaudžiant ir išskleidžiant H.264 video medžiagą.



9 pav. Suspaustų video kadro kokybė esant tokiai pat kodavimo spartai naudojant: MPEG-2 (kairėje), MPEG-4 Visual (viduryje), H.264 (dešinėje)

Kaip ir pagerintam suspaudimo našumui, H.264 siūlo didesnę lankstumą išreiškiant suspaudimo variantams ir perdavimo palaikymams. H.264 kodavimo įrenginys gali išrinkti iš didelės suspaudimo įrankių įvairovės, darydamas tinkamas taikymams nuo žemos kokybės ir mažo užlaikymo iki aukštos kokybės. Standartas aprūpina integruotą palaikymą perdavimui ar laikymui, apimdamas suspaustą formatą ir ypatybės, kurios padeda sumažinti perdavimo klaidų padarinį.

H.264/AVC yra priimamas didėjančiam paraiškų diapazonui, apimdamas:

- aukštos kokybės DVD (HD-DVD)
- aukštos kokybės televiziją, transliuojamą Europoje
- Apple produktai, apimdamas iPod video ir MacOS
- mobilios televizijos laidas
- internete atkuriami video įrašai
- video konferencijas

1.2.6 Išvados

Šioje darbo dalyje buvo išnagrinėtos technologijos leidžiančios realizuoti audio – video medžiagos perdavimą interneto linijomis. „Audio – video nuotolinio mokymo ir egzaminavimo sistema“ bus kuriama remiantis šių technologijų privalumais:

- Srautinės audio – video informacijos perdavimas (angl. Streaming) – naudojant šią technologiją galima reguliuoti siunčiamų audio – video duomenų kokybę. Skirtingą interneto greitį turintiems vartotojams bus transliuojama atitinkamos kokybės audio - video medžiaga. Kuo vartotojo interneto pralaidumas didesnis tuo didesnės kokybės audio – video transliaciją jis galės stebėti.
- Audio – video informacijos perdavimas naudojant P2P technologiją – tai Stratus technologijos paremtos RTMFP protokolu revoliucija audio-video informacijos perdavimui realiu laiku internete. Ši technologija leidžia klientui siųsti duomenis kitam klientui nenaudojant serverio. Tai itin svarbu komerciškai, nes audio – video transliacijų paslaugos tiekėjui nebereikia mokėti už sunaudojamą interneto srautą. Kuriamoje sistemoje šiuo technologiniu principu bus realizuota audio – video konferencija (vienas su vienu). Ateityje video archyvų peržiūros metodai.
- H.264 video standartas – didžiausias šio standarto pranašumas lyginant su kitais yra suspaudimo našumas.

H323 specifikacija nebus naudojama, kuriant sistemą dėl labai paprastai suprantamų priežasčių. Ši technologija yra ganėtinai pasenusi ir neturi lankstaus pritaikymo, kuriant programinį sprendimą.

1.3 Saugumo technologijų apžvalga/analizė

Atsižvelgiant į egzistuojančių nuotolinio mokymo sistemų trūkumus, kuriamai sistemai išskelėme saugumo reikalavimus:

- Stipri autentifikacija – būtina užtikrinti kuo didesnę saugumą egzaminų vykdymo metu;
- Asmens duomenų apsauga – asmens privatūs duomenys turi būti apsaugoti laikantis įstatymų numatytos tvarkos;

- Perduodamų duomenų šifravimas – jeigu sistema būtų naudojama institucijose kur perduodami duomenys yra konfidencialūs.

Įvairiuose programiniuose ir aparatiniuose duomenų apsaugos produktuose dažnai naudojami vienodi vertinimai, veiksmai ir techniniai sprendimai.

Prie tokių bazinių saugumo technologijų priskiriama:

- ▶ autentifikavimas,
- ▶ autorizacija,
- ▶ auditas,
- ▶ apsaugoto kanalo technologija.

1.3.1 Autentifikavimas

Autentifikavimas (authentication) užkerta priegą prie tinklo nepageidaujamiems asmenims ir leidžia priegą legaliems naudotojams.

Autentifikavimą reikia skirti nuo identifikavimo. Identifikavimas - tai vartotojo savo identifikatoriaus pranešimas sistemai, tuo tarpu **autentifikavimas – tai vartotojo įrodymo procedūra, kad jis yra tas kuo skelbiasi, konkrečiai įrodymas, kad būtent jam priklauso jo įvestas identifikatorius.**

Autentifikuojamasis gali pademonstruoti kokios nors bendros abiem pusėm paslapties žinojimą: žodžio (slaptažodžio) arba fakto (įvykio datos ir mėnesio, žmogaus pravardės ir pan.);

Autentifikuojamasis gali pademonstruoti, kad jis disponuoja koku unikaliu daiktu (fiziniu raktu), kuriuo gali būti, pavyzdžiui, elektroninė magnetinė kortelė;

Autentifikuojamasis gali įrodyti savo identiškumą, naudodamas savo biocharakteristikas: akies rainelės piešinys ar pirštų atspaudai, kurie iš anksto buvo įtraukti į autentifikatoriaus duomenų bazę.[25]

1.3.1.1 Biometrinės autentifikavimo sistemos

Biometrija – tai automatiniai asmens atpažinimo metodai, pagrįsti fiziologinėmis arba elgsenos charakteristikomis. Tarp charakteristikų ir savybių tiksliausios yra šios sistemos: veido, pirštų atspaudų, plaštakos geometrijos, akies rainelės, akies ragenos, balso bei kapiliarų (kraujagyslių). Biometrinės technologijos tampa vis platesne erdve aukšto lygio saugumo sistemose asmens tapatybės patvirtinimo bei identifikavimo sprendimams. Šie biometrine technologija pagrįsti sprendimai yra pajėgūs apsaugoti nuo konfidencialių bankų finansinių transakcijų iki asmeninių duomenų slaptumo. Biometrinės technologijos poreikis itin svarbus valstybiniam, valdžios, armijos bei komerciniams objektams. Verslas tinklų saugumo srityje, saugi elektroninė bankininkystė, finansinių operacijų saugumo sritis, mažmeninė prekyba, teisėsauga, sveikatos bei visuomeninės organizacijos jau turi naudos iš šios technologijos.[27]

1.3.1.1.1 Aktualumas

Biometrine technologija pagrįstas autentifikacijos taikytinumas valdymo kompiuteriuose, tinkluose, organizacijos darbuotojų kompiuteriuose (pakeičiantis įprastinius slaptažodžius), nuotolinio autorizavimo, prisijungimo, pereinant prie duomenų ir baigiant pasaulinio žiniatinklio saugumu. Pasitikėjimas šiomis elektroninėmis, nuotolinėmis identifikavimo priemonėmis yra svarbus aspektas globalios ekonomikos palankiam augimui. Pavienės ar integruotos su kitomis technologijomis, tokiomis kaip banko kortelės, kodavimo raktai ir skaitmeniniai parašai, biometrinės sistemos artimiausiu metu pakeis nemažą dalį autorizacijos sistemų versle bei kasdieniniame gyvenime. Šios technologijos naudojimas tampa daug patogesnis negu esami metodai, naudojant slaptažodžius ar PIN kodus. Taip yra todėl, jog, panaudojus biometrinius duomenis, galima tiksliai ir konkrečiai autorizuoti asmenį (slaptažodis ar kortelė gal būti pavogti ar naudojami kito asmens). Patogumas – nereikia nieko prisiminti ar nešiotis. Tikslumas – tai užtikrina autorizaciją. Ši technologija tampa vis priimtinesnė visuomenei ir vis pigesnė.

1.3.1.1.2 Technologija, identifikavimas

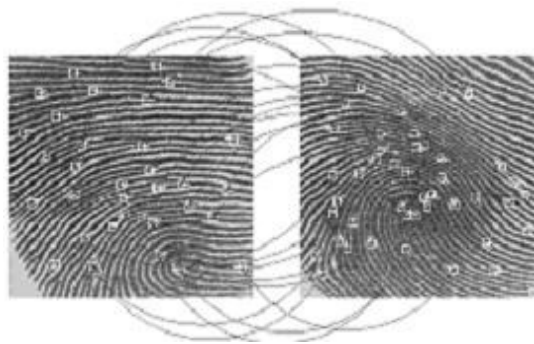
Tarp visų biometrinių technologijų pirštų atspaudais pagrįstas metodas yra vienas iš seniausių, jis buvo sėkmingai naudojamas ir įvairiai pritaikomas. Iki šiol yra sukurta daug technologijų atspaudui nuskaityti: optiniai skaitytuvai (angl. optical readers), reflektoriniai skaitytuvai (angl. reflection with sweep; reflection touches), TFT jutikliai, elektrooptiniai jutikliai (angl. electro-optical), talpinės varžos jutikliai (angl. capacitance) ir kiti. Dabar – tai viena pigiausių biometrijos technologijų, leidžianti nuskaitymo įrenginius įmontuoti net nešiojamuose atminties įrenginiuose (angl. memory stick).

Kiekvienas turime unikalius, nepasikartojančius pirštų atspaudus, kuriuos sudaro daugybė iškilimų bei griovelių piršto paviršiuje. Kiekvienas piršto atspaudas gali būti skirstomas pagal savo raštą, kurį nusako „apibūdinamieji“ taškai (angl. minutiae points) (10 pav.), į tam tikrus pogrupius (angl. fingerprint patterns).[27]



pav. 10 „Apibūdinamieji“ taškai

„Apibūdinamieji“ taškai – tai rašto raukšlių susikirtimai, nutrūkimai (pradžia arba pabaiga) ar išsišakojimai.



11 pav. Taškų metaduomenų informacijos palyginimas

„Apibūdinamieji“ taškai iš piršto atspaudu atvaizdu yra gaunami, pasitelkiant grafikos algoritmus.

Duomenų bazėje dažniausiai yra saugoma tik metaduomenys apie piršto atspaudą – „apibūdinamieji“ taškai, t.y. taško padėtis kitų taškų atžvilgiu, linijos kryptis, taško tipas.

Lyginant tarp savęs pirštų atspaudus, lyginama metaduomenų (taškų) informacija (11 pav.).[27]

1.3.1.1.3 AFIS

Pirštų atspaudai yra naudojami „vienas su daugeliu“ (angl. one-to-many) paieškos sistemose, duomenų bazėse (kurios dydis gali siekti iki keleta milijonų pirštų atspaudų). Šios paieškos rezultatus galime gauti trumpiau nei per valandą (iš kelių milijonų), ši identifikavimo sistema kitaip vadinama – AFIS (Automated Fingerprint Identification Systems). AFIS dar vadinamas kaip „AFIS Systems“ – šis terminas apibrėžia didelės apimties, „vienas su daugeliu“ paiešką (identifikaciją). Pirštų atspaudų technologija gali būti naudojama AFIS'e ir su mažiau nei 100,000 pirštų atspaudų duomenų baze, tai kur kas dažniau naudojama „vienas su vienu“ (angl. one-to-one) tikrinimui.[10]

Straipsnyje aprašoma realios sistemos veikimo principas, pagrįstas pirštų atspaudų sulyginimu „vienas su daugeliu“ (angl. one-to-many). Naudojama technologija – optinis (lazerinis) nuskaitymo įrenginys.

Lentelėje Nr. 3 pateikiama keletas realių situacijų palyginimui su kitomis sistemomis.

Lentelė Nr. 3 Situacijų palyginimas

	Slaptažodis	Kortelė	Kontrolė (asmuo)	Pirštų atspaudų skaitytuvas
Galimybė piknaudžiauti	+	+	+	-
Laiko sąnaudos	+	-	-	-
Nuolatinės išlaidos	-	-	+	-
Papildomi reikalavimai	+	+	-	-
Autorizacijos klastojimas	+	+	-	-
Autorizacijos klastojimas vidaus tinkle	+	+	+	-

Vienas iš problemos sprendimo būdų – taikyti pirštų atspaudų identifikavimo sistemą. Naudojant identifikavimo sistemą prarandama galimybė piknaudžiauti (kiekvienas pasižymi tik už save), tai neužtrunka, nėra jokių tikslinių eksploatacinių išlaidų, nereikia nieko atsiminti ar turėti su savimi. Niekas nebus paimta ar padaryta vietoj atsakingo žmogaus.[10]

1.3.2 Autorizacija

Prieigos autorizacijos priemonės (*authorization*) kontroliuoja legalių vartotojų prieigą prie sistemos išteklių, suteikdamos kiekvienam iš jų būtent tas teises, kurios jam buvo nustatytos administratoriaus.

Be vartotojų prieigos prie katalogų, failų ir spausdintuvų teisių suteikimo, autorizacijos sistema gali kontroliuoti vartotojų galimybę atlikti įvairias sistemines funkcijas, tokias kaip lokali prieiga prie serverio, sisteminio laiko nustatymas, duomenų rezervinių kopijų sukūrimas, serverio išjungimas ir panašiai.[25]

1.3.3 Auditas

Auditas (*auditing*) – tai įvykių, susijusių su prieiga prie saugomų išteklių, fiksavimas sisteminiame žurnale.

Šiuolaikinių web ir kitų sistemų audito posistemės leidžia diferencijuotai nurodyti administratorių dominančių įvykių sąrašą. Stebėjimo ir apskaitos priemonės užtikrina galimybę aptikti ir užfiksuoti svarbius įvykius, susijusius su saugumu, arba bet kokius bandymus sukurti, gauti prieigą ar pašalinti sisteminius išteklius. Auditas naudojamas tam, kad susektumėme net nesėkmingus „įsilaužimo“ į sistemą bandymus.[25]

1.3.4 Apsaugoto kanalo technologijos

Duomenų saugumui užtikrinti perduodant juos viešais tinklais naudojamos įvairios apsaugoto kanalo technologijos.

Apsaugoto kanalo technologija skirta užtikrinti duomenų perdavimo atviru transporto tinklu, **pavyzdžiui internetu, saugumą.**

Apsaugoto kanalo pagrindinės funkcijos:

- abonentų tarpusavio autentifikavimas inicijuojant sujungimą, kuris gali būti įvykdytas, pavyzdžiui, apsikeičiant slaptažodžiais;

- kanalu perduodamų pranešimų apsauga nuo nesankcionuotos prieigos, pavyzdžiui, šifruojant duomenis;
- kanalu ateinančių pranešimų vientisumo patvirtinimas, pavyzdžiui, su pranešimu perduodant jo maišos reikšmę.

1.3.5 Informacijos autentifikavimas

Informacijos autentifikavimas kompiuterinėse sistemose – tai duomenų, gautų tinklu ar koku nors kiti būdu, tikrumo nustatymas.

Jeigu informacijos šifravimo tikslas yra užtikrinti apsaugą nuo nesankcionuoto susipažinimo su šia informacija, tai informacijos autentifikavimo tikslas yra užtikrinti informacijos apsikeitimo dalyvių apsaugą nuo klaidingos informacijos primetimo.

Autentifikavimo koncepcija plačiau prasme numato informacijos tikrumo nustatymą kaip esant apsikeitimo dalyvių tarpusavio pasitikėjimui taip ir jo (pasitikėjimo) nesant.[25]

Informacijos autentifikavimo formos:

- saugomų duomenų masyvų ir programų autentifikavimas – tai nustatymas to fakto, kad duomenys ar programos nebuvo modifikuotos;
- pranešimų autentifikavimas – tai gautų pranešimų tikrumo nustatymas, tame tarpe pranešimų autorystės ir priėmimo fakto nustatymas.
- Informacijos autentifikavimui naudojamas skaitmeninis (elektroninis) parašas.[25]

1.3.6 Išvados

Šioje darbo dalyje trumpai aptarėme saugumo užtikrinimo galimybes informacinėse sistemose. Mūsų kuriamos sistemos vienas iš uždavinių – užtikrinti kuo didesnę saugumą egzaminų vykdymo metu. Atsižvelgiant į šį reikalavimą galima daryti išvadą, kad mūsų kuriamai sistemai labiausiai tiktų biometrinis autentifikavimas pirštų antspaudų pagalba. Norint atlikti biometrinių autentifikavimą asmuo privalo lokaliai dalyvauti procese, kitų autentifikacijos priemonių atveju, asmuo gali perduoti slaptus duomenis ir jo vardu autentifikaciją atliks kitas

asmuo. Norint užtikrinti asmens duomenų apsaugą, galima naudoti apsaugoto kanalo technologijas. Ateityje plečiant sistemos funkcionalumą reikėtų naudoti ir daugiau saugos technologijų. Studentams ir dėstytojams įdiegti funkciją, kurios pagalba jie galėtų e-parąšu pasirašinėti elektroninius dokumentus. Perduodama susirašinėjimo bei audio-video informacija turėtų būti šifruojama. Apie audio-video informacijos šifravimą skaityti 4.3. skyriuje.

1.4 Analizės išvados

Išanalizavus kelias klasikines labiausiai paplitusias nuotolinių studijų sistemas buvo išsiaiškinta, kad nei viena iš sistemų neturi mokymo įrankių paremtų video transliacijomis. Visose sistemose realizuoti labai primityvūs atsiskaitymo būdai. Autentifikacijai nėra skiriamas didelis dėmesys.

Atsižvelgiant į skirtingas kuriamos sistemos funkcijas, išanalizavus audio – video medžiagos perdavimui internete skirtas technologijas, realizacijai įgyvendinti buvo pasirinktos šios:

- Srautinės audio – video informacijos perdavimas (angl. Streaming);
- Audio – video informacijos perdavimas naudojant P2P technologiją;
- H.264 video standartas.

Mūsų kuriamos sistemos vienas iš uždavinių – užtikrinti kuo didesnę saugumą egzaminų vykdymo metu. Išanalizavus saugumo technologijas buvo pasirinktas biometrinis autentifikavimas. Norint atlikti biometrinių autentifikavimą asmuo privalo lokaliai dalyvauti procese. Taip pat egzaminuojamojo tapatybės patvirtinimui viso egzamino metu yra vykdomas veido srities video įrašas.

2 Audio – video nuotolinio mokymo ir egzaminavimo sistemos projektas

Šios darbo dalies uždavinys suprojektuoti „Audio – video nuotolinio mokymo ir egzaminavimo sistemą“, kurios funkcinis veikimas būtų paremtas srautinės audio - video informacijos perdavimu. Pagrindinis sistemos uždavinys sudaryti studentams ir dėstytojams palankias sąlygas, kurios leistų virtualioje erdvėje atlikti mokymo bei egzaminavimo procesus. Pagrindiniai reikalavimai keliami projektuojamai sistemai:

- Sistema turi būti realizuota Linux operacinės sistemos aplinkoje;
- Srautinis audio-video informacijos perdavimas;
- Galimybė sistemos vartotojams inicijuoti video konferencijas į kompiuterį papildomai neįdiegus jokios papildomos programinės įrangos.

Pagrindinės sistemos funkcijos:

- Atsiskaitymas(egzaminas) video konferencijos pagalba;
- Atsiskaitymo(egzamino) forma paliekant video įrašą nutolusiame sistemos;
- Daugialypė video konferencija;
- Autentifikacija pagrįsta biometriniais duomenimis (pirštų antspaudai);
- Galimybė dėstytojams transliuoti aukštos kokybės video paskaitas.

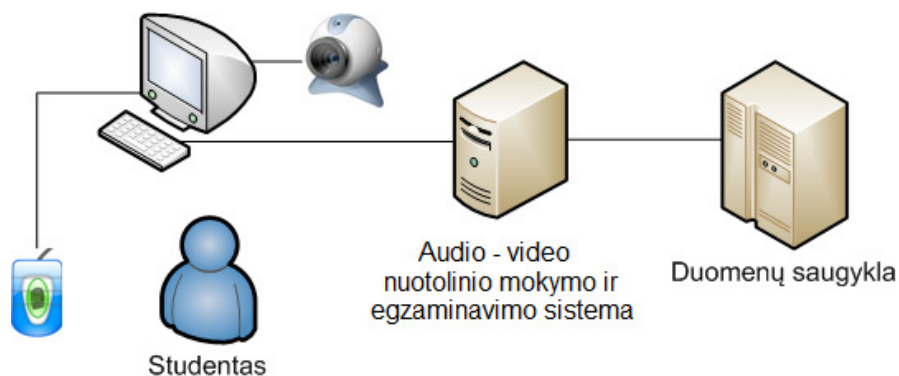
2.1 Audio – video nuotolinio mokymo ir egzaminavimo sistemos pagrindinės funkcijos

Atsiskaitymas(egzaminas) video konferencijos pagalba (12 pav.), tai egzaminavimo būdas kai dėstytojas pateikia studentui klausimus bei diskutuoja kartu su juo aktualia tema nuotoliniu būdu virtualioje erdvėje.



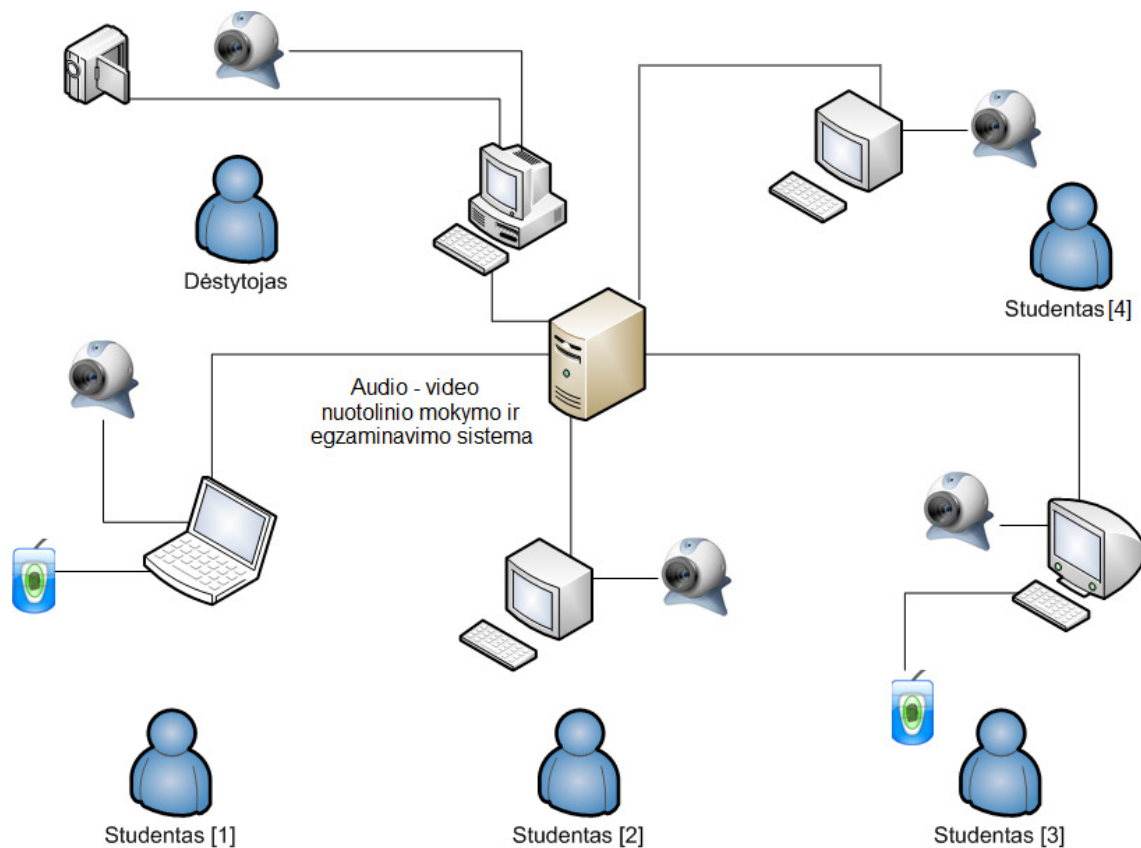
12 pav. Atsiskaitymas(egzaminas) video konferencijos pagalba

Atsiskaitymo(egzamino) forma paliekant video įrašą nutolusiame sistemos serveryje (13 pav.) - studentui prisijungus prie sistemos naudojant pasirinktą autentifikacijos būdą yra pateikiami egzamino klausimai, jam susipažinus su jais, inicijuojamas vaizdo įrašas. Video medžiaga realiu laiku yra įrašinėjama į nutolusį serverį, kad jos nebūtų galima modifikuoti. Dėstytojas bet kuriuo metu prisijungęs prie sistemos gali peržiūrėti šią medžiagą bei įvertinti studento žinias.



13 pav. Atsiskaitymo(egzamino) forma paliekant video įrašą nutolusiame sistemos serveryje

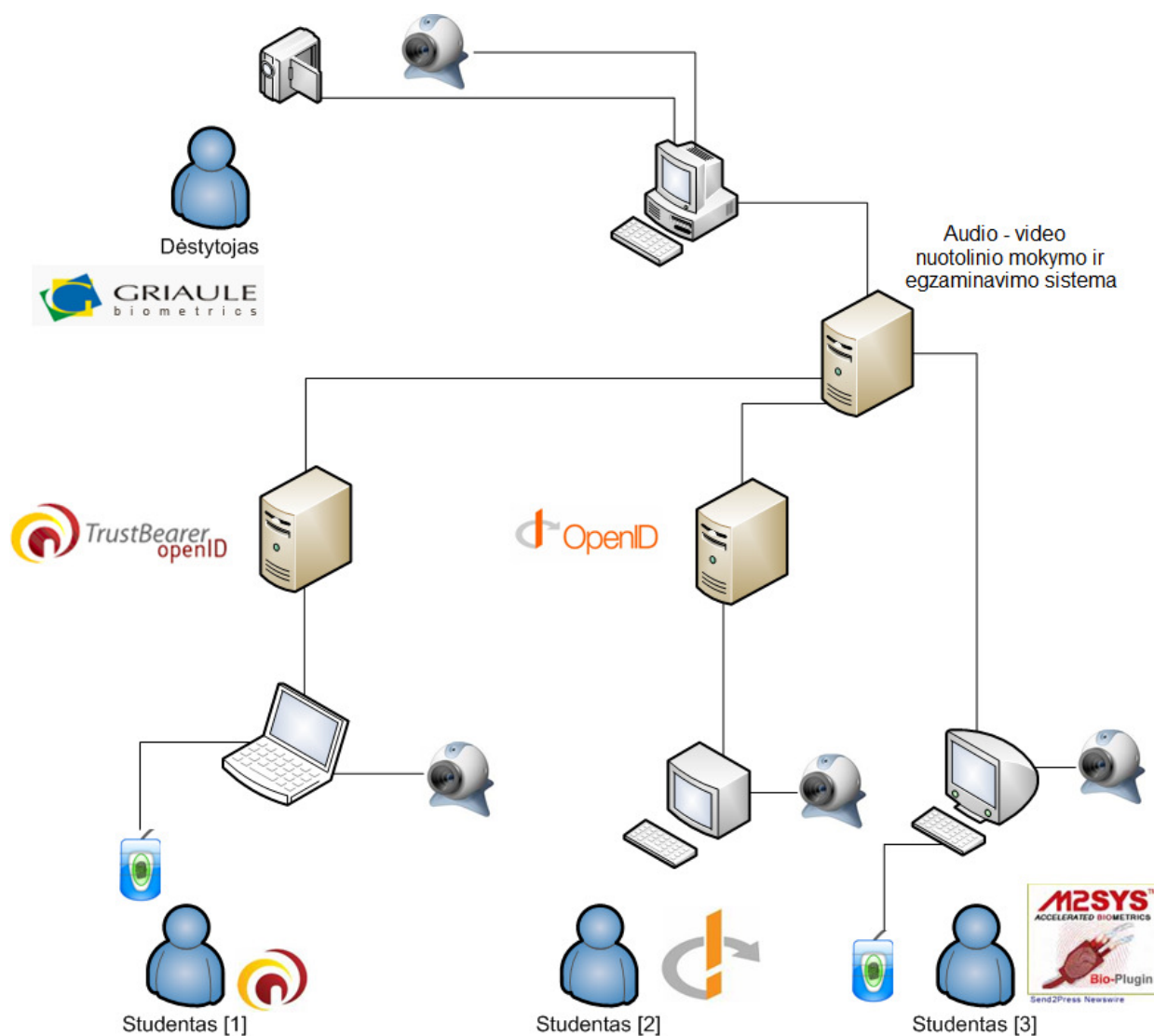
Daugialypė video konferencija (14 pav.) – tai video konferencija kurioje gali dalyvauti nuo dviejų iki penkių pašnekovų vienu metu.. Tokiu būdu galima inicijuoti grupinius darbus atsiskaitymus (pvz.: seminaro forma).



14 pav. Daugialypė video konferencija (skirta maksimaliai 5-iems vartotojams vienoje diskusijoje)

2.2 Principinis sistemos veikimas ir autentifikacija

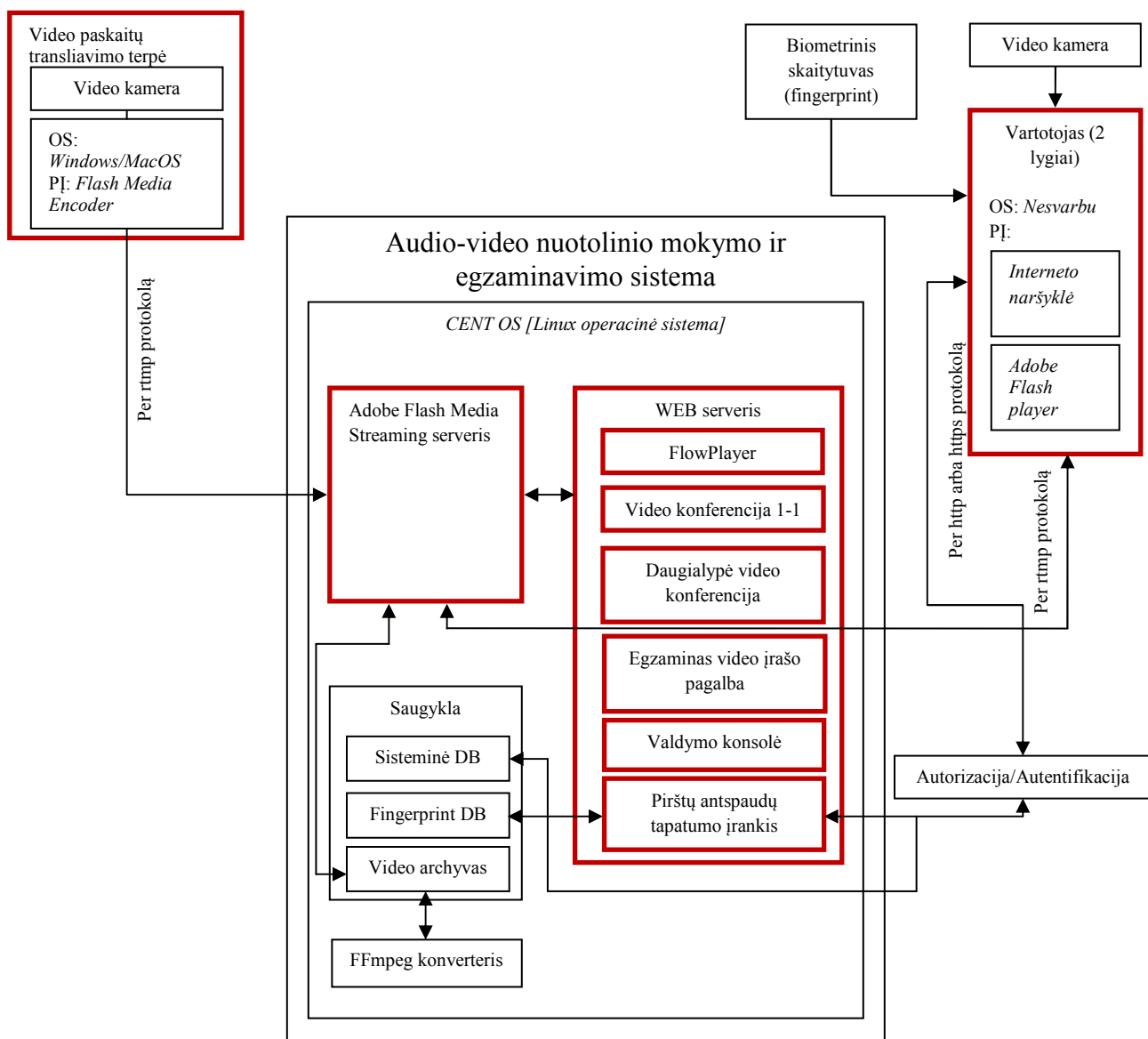
Schemoje (15 pav.) pateikti skirtingi autentifikavimo būdai, kurie suteikia vartotojams prieigą prie nuotolinio mokymo ir egzaminavimo sistemos. Realizuotoje sistemoje vartotojas galės pasirinkti jam priimtinausią autentifikavimo būdą. Atlikus autentifikaciją vartotojas yra prijungiamas prie sistemos ir gali naudotis sistemos teikiamomis paslaugomis. Tolimesnėje darbo dalyje išanalizuosime ir aptarsime, kurias autentifikavimo priemones tikslinga diegti kuriamoje sistemoje.



15 pav. Principinė sistemos veikimo schema

2.3 Sistemos funkcinė diagrama

Kuriamos „Audio – video nuotolinio mokymo ir egzaminavimo sistemos“ funkcinė diagrama pateikta 16 paveikslėlyje. Ši sistema yra projektuojama Linux operacinės sistemos aplinkoje. Siekiant sistemos lankstumo ir patogumo tobulinimui, ji sudaryta iš atskirų komponentų. Komponentai sąveikauja tarpusavyje per tam skirtas sąsajas.



16 pav. Audio – video nuotolinio mokymo ir egzaminavimo sistemos funkcinė diagrama

Šioje darbo dalyje plačiau aptarsime 16 paveikslėlyje raudonai pažymėtus pagrindinius sistemos komponentus ir jų privalumus.

1. **Video paskaitų transliavimo terpė** – dėstytojas gali atlikti gyvą video paskaitų transliaciją. Šios paskaitos transliavimo metu iškart yra įrašinėjamos į saugyklą. Todėl studentai jas gali peržiūrėti jiems patogiu laiku. Video paskaitų kokybė gali būti reguliuojama pagal poreikį ir tinklo galimybes. Galima pasiekti HD (High definition) kokybę.
2. **Adobe Flash Media Streaming serveris** – tai serveris, kuris apdoroja video medžiagos transliavimą, įrašymą bei atkūrimą.
3. **Saugykla** – čia yra saugomi video paskaitų įrašai, vartotojų pirštų antspaudų skaitinės reikšmės, sisteminė duomenų bazė bei įvairūs sistemos dokumentai ir failai.
4. **WEB serveris**- tai vieta kurioje yra programiškai realizuotos sistemos veikimo funkcijos:
 - FlowPlayer – video grotuvas skirtas video archyvų atkūrimui.
 - Video konferencija 1-1 – komponentas skirtas dviejų asmenų video konferencijai. (Atsiskaitymas dalyvaujant dėstytojui ir studentui).
 - Daugialypė video konferencija - komponentas skirtas video konferencijoms, kuriose gali dalyvauti iki penkių pašnekovų vienu metu. (Seminaras dalyvaujant dėstytojui ir studentams).
 - Egzaminas video įrašo pagalba– komponentas, kurio pagalba studentas gali išlaikyti egzaminą. Visa egzamino video įrašo medžiaga yra patalpinama sistemos saugykloje. Dėstytojas prisijungęs prie sistemos, saugykloje esančią egzamino video medžiagą gali peržiūrėti bei įvertinti atitinkamu pažymiu.
 - Valdymo konsolė – tai sistemos branduolys, kuriame programiškai aprašyti galimi studentų ir dėstytojų veiksmai dirbant sistemoje.
 - Pirštų antspaudų tapatumo įrankis – programinis įskiepis sistemai leidžiantis vartotojus autentifikuoti biometrinio(pirštų antspaudų) skaitytuvo pagalba. Šis įskiepis sulygina vartotojo autentifikacijos metu siunčiamą piršto antspaudo skaitinę reikšmę su esančia duomenų bazėje.
5. **Vartotojas** – bet kuriam iš vartotojų (studentui ar dėstytojui) prisijungus prie sistemos automatiškai bus inicijuojamas web kameros atpažinimas. Taip sistemos vartotojas galės naudotis visomis sistemos funkcijomis ir dalyvauti video konferencijose, neįdiegęs jokios.

2.3.1 Sistemai sukurti naudojami video transliacijų komponentai

Adobe Flash Media Server (uždaro kodo serverio pusės programinė įranga (turinti nemokamą programuotojams skirtą versiją - Adobe Flash Media Development Server) ši serverio pusės programinė įranga skiriasi nuo kitos RTMP protokolą palaikančios serverio pusės programinės įrangos tuo, kad lengvai suderinamas su Linux OS bei turi daug profesionaliai išdirbtų opcijų, tiesiogiai atitinkančių mūsų sistemos modelį) [1]

Adobe Flash Media Encoder (kliento-pusės programinė įranga skirta tiesioginių transliacijų video medžiagos perdavimui iš mobilios darbo vietos į SAVIP serverį; ši programinė įranga yra pateikiama viename pakete su **Adobe Flash Media Server**) [11]

Flowplayer (populiariausias FLV leistuvus, kuris palaiko Adobe Flash Media Server bei kitas RTMP protokolu pagrįstas serverio pusės programines įrangas. Tai tik įrankis leidžiantis **Adobe Flash Player** atkurti video medžiagą.) [12]

Adobe Flash Player (tai įskiepis leidžiantis vartotojo kompiuteryje atkurti RTMP protokolu transliuojamą video medžiagą) [14]

FFmpeg (tai serverio pusės įrankis leidžiantis kelti bet kokio formato video medžiagą per http protokolą į saugyklą, o įkėlimo metu konvertuojantis tą medžiagą į nustatytą formatą) [8]

2.3.1.1 Adobe Flash Media Streaming serveris

Adobe Flash Media serverio pagalba video medžiaga yra perduodama saugiau ir efektyviai, negu bet kokia kita technologija. Panaudojimo galimybės nuo vartotojų sukurtų video klipų iki filmų ir nuo televizijos laidų iki kooperatyvinių mokymų. Tai tikrai aukšto lygio sprendimas video medžiagos perdavimui ir gyvoms transliacijoms.

Privalumai:

- **Geresnis pateikimas vartotojams**
 - Greitesnis video atkūrimas
 - Gyvas video palaikymas
- **Kokybė**
 - On2 VP6 ir H.264/AAC aukštos video kokybės kodekų palaikymas.
 - Automatinis interneto linijos pralaidumo matavimas ir dinamiškas užkrovimas.

- **Paslaugos pateikiamumas ir pasiekiamumas**

- Klientų kompiuterių operacinė sistema (Windows,® Mac, Linux®) paslaugos pasiekiamumui neturi įtakos.
- Didžiausią įtaką pasiekiamumui turi Adobe Flash Player. Kiekvieną dieną yra daugiau nei 8 milijonai vartotojų parsisiunčia šį įskiepi, ir jo paplitimas pasaulio vartotojų kompiuteriuose siekia 99%.
- Serverio operacinė sistema gali būti arba Linux arba Windows.

- **Interaktyvumas**

Remiantis ActionScript programavimo kalba galima modifikuoti serverio programinės įrangos architektūra naujais savo sukurtais įskiepiais.

- **Saugumas**

Perduodama medžiaga koduojama, įmanomas priėjimo ribojimas, o svarbiausia informacija nėra saugoma vartotojo kompiuteryje.

Šie bei kiti privalumai leidžia Flash Media Server 3 įvertinti, kaip šaunų pasirinkimą - gyvoms video transliacijoms arba video su pareikalavimu (video archyvų) transliacijoms. Adobe sukūrė serverį, kuris yra efektyvus, ir konkurencingai įvertintas versle. Šio produkto plėtojimas pagal savo poreikius leidžia lengvai sukurti įvairias sistemas, kurios versle padėtų uždirbti pinigus. [1]

Adobe Flash platforma leidžia video medžiagą atkurti ne tik kompiuterių, ekranuose, bet ir kituose įrenginiuose (pvz.: telefonuose), tai labai didelis privalumas. Flash Media Serveris leidžia atkurti srautinę audio - video informaciją interneto naršyklėje pasitelkiant Flash Player įskiepi, kompiuterio ekrane tai leidžia įgyvendinti Adobe AIR platforma, o mobilaus telefono ekrane tai yra atliekama Flash Lite programinės įrangos pagalba. Tai leidžia išplėsti vartotojų skaičių.

Adobe Flash Media Streaming Server 3 ekonomišką sprendimą, kuris leidžia sparčiai pradėti aukštos kokybės, saugų srautinės video informacijos perdavimą. Šis sprendimas turi visas pagrindines savybes reikalingas video ir audio perdavimui internete inicijuoti. Pagrindinės savybės:

- Nedidelė technologijos kaina
- Lengvas ir greitas diegimas

- HD kokybė (remiantis H.264 standartu)
- Statistikos rinkimo galimybė
- Perduodamos medžiagos kodavimas
- Lengvai suvokiama kontrolė
- Aukštos kokybės gyvos transliacijos
- Didelis našumas – 1Gbps sąsaja
- Įvairi kodavimo sparta
- Tinklo efektyvumas

Flash Media Streaming Server 3 turi dvi skirtingas galimybes transliuoti video medžiagą:

- **Gyvos video transliacijos (Live video streaming)** — Norint pradėti gyvą transliaciją reikia klientiniame kompiuteryje, prie kurio prijungta video kamera, įdiegtos Adobe Flash Media Encoder programinės įrangos. Remiantis šia programine įranga filmuojama medžiaga yra nukreipiami į nutolusį serverį, kuriame įdiegta Flash Media Streaming Server programinė įranga. Šios serverio programinės įrangos pagalba video medžiaga realiu laiku yra retransliuojama į stebėtojų kompiuterius. Stebėtojo kompiuteryje yra reikalingas nesenesnis nei 8 versijos Flash Player įskiepis kuris atkuria srautinę video medžiagą.
- **Video su pareikalavimu (Video on demand (VOD))** — Standartiniai VOD taikymo privalumai: tarp serverio ir vartotojo esančios interneto linijos pralaidumo nustatymas (kad galima būtų parinkti video kokybę, kuri be trukdžių bus ištransliuota), domenu paremta autentifikacija (kad jūsų turimą video medžiagą galėtų publikuoti tik nustatytų interneto svetainių administratoriai), visos transliacijos paremtos FLV atkūrimu, todėl stebėtojo kompiuteryje pakanka nesenesnio nei 8 versijos Flash Player įskiepio. Veikimo principas labai paprastas: web serveryje yra patalpinta video medžiaga, kuri yra transliuojama į vartotojo kompiuterį Flash Media Streaming Server 3 programinės įrangos pagalba. [2]

Kokie turi būti minimalūs serverio parametrai bei operacinė sistema, norint į ją diegti Flash Media Streaming Server 3 programinę įrangą yra pateikta 4 lentelėje.

Lentelė Nr. 4 Flash Media Serverio reikalavimai sistemai [1]

Windows	Linux
Microsoft® Windows Server® 2003 su Service Pack 1 (visos 32-bit versijos/leidimai) Microsoft Windows XP(tiktai Flash Media Development Server – programuotojų versija)	Linux Red Hat® 4 (32-bit tiktai)
Aparatūrinės įrangos reikalavimai	
<ul style="list-style-type: none"> • 3.2GHz Intel® Pentium® 4 processor (dual Intel Xeon® arba rekomenduotinas greitesnis) • 2GB of RAM (4GB RAM rekomenduotina) • 1GB tinklo plokštė 	

2.3.1.2 Adobe Flash Media Encoder 2

Adobe® Flash® Media Encoder 2 yra sukurtas įrašinėti realaus laiko audio ir video transliaciją tuo pat metu, kai ši medžiaga realiu laiku yra transliuojama Flash Media Server (FMS) pagalba. Kai prioritetas yra realiu laiku transliuoti (24 x 7, 365 dienas per metus) kuo aukštesnės kokybės audio/video medžiagą, Flash Media Encoder 2 yra tikrai geras sprendimas šiai medžiagai retransliuoti iš įvykio vietos. [11]

Galimi Flash Media Encoder 2 panaudojimo atvejai

- Sporto varžybos
- Koncertai
- Internetinės konferencijos
- Mokomosios medžiagos transliavimas ir kt.

Flash Media Encoder 2 privalumai

- Nesunkiai suprantama programos sąsaja

- Plug and play video ir audio įrenginių palaikymas
- Flash video (VP6) technologija, perduoda aukštos kokybės medžiagą bei yra lanksti failo dydžio ir perdavimo greičio atžvilgiu.
- Flash Media Encoder 2 yra lengvai integruojamas į SAVIP juostą (pipeline) komandinių eilučių pagalba lokaliame arba nutolusiame tinkle.
- Automatinis persikrovimas po elektros energijos pertrūkimo ar kitokių sistemos persikrovimų, dėl nenustatytų priežasčių. Tai užtikrina 24 x 7, 365 dienų per metus paslaugos pateikiamumą.[11]

2.3.1.3 Flowplayer – nemokamas Flash (FLV) leistuvus interneto svetainėms

FlowPlayer [12] yra Flash(FLV) leistuvus. Jį galima naudoti HTML interneto puslapiuose video failams atkurti.

Palaikomi formatai

FLV, SWF, MP3, MP4, H.264 video, JPG ir PNG

Lankstus konfigūravimas

FlowPlayer turi daugybę konfigūravimo parinkčių. Su šiuo produktu galima pradėti dirbti iškart su standartiniais nustatymais, o pasigilinus galima išbadyti ir kitas įvairias parinktis. [12]

Progressive download

Flowplayer pagalba galima žiūrėti Flash video failus „progresive download“ būdu, taip kaip YouTube.

Srautinės audio-video informacijos perdavimas

FlowPlayer palaiko SAVIP serverius tokius kaip Flash Media Server, Wowza and Red5 (visi RTMP protokolu pagrįsti serveriai). Jis leidžia permetinėti laiko slankjuostės kursorių į bet kurią video medžiagos vietą beveik be užlaikymo.

Momentiniai vaizdai

Leidžia greitą perėjimą nuo vieno rodomo video kadro prie kito net ir ilgame video klipe.

Grojaraštis

Galima valdyti keletą video klipų viename leistuve. Arba derinti keletą video klipų kaip vieną "stream'ą" pasitelkiant SAVIP serverį.

API programavimas

Flowplayer leistuvas interneto svetainėse integruojamas JavaScript pagalba.[12]

Reklamos plėtimo galimybės/palaikymas

Leistuvas turi galimybę į video siužetą įterpti reklaminį klipą. Video kontrolė gali būti apribota specifiniams klipams (pvz. kad reklamos metu nebūtų galima jos prasukti). Reklaminiuose klipuose galima integruoti nuorodą (hyperlink) į svetainę susijusią su reklamuojamu gaminiu ar paslauga.

Pilno ekrano parinktis

Pilno ekrano (fullscreen) parinktis veikia nedidinant (maximize) naršyklės lango. Tai pat galima individualiai susiprogramuoti in-window fullscreen. [12]

Licencijavimas

FlowPlayer yra nemokamas ir platinamas pagal GPL 3 licenciją, ne komerciniams tikslams. Komerciniam naudojimui būtina įsigyti komercijai skirtą licenciją. [12]

2.3.1.4 Flash player

Adobe į savo populiariaus Flash Player 9 grotuvo versiją įtraukė suderinamumą su didelės raiškos (HD) vaizdu. Tai video revoliucija. Internete dabar yra galima talpinti itin geros kokybės ir mažai vietos bei duomenų srauto reikalaujančius vaizdo klipus, užkoduotus H.264/MPEG-4 AVC algoritmu. Garsas koduojamas AAC būdu. Tai aukštesnės kokybės garso kodavimas nei mp3. AAC garso kodavimas gali būti naudojama kartu su vaizdu arba atskirai. H.264 – tai tas pats kodavimas, kuris naudojamas Blu-Ray, HD-DVD grotuvuose bei skaitmeninės antžeminės televizijos transliacijoms (taip pat Lietuvoje). Geriausia yra tai, kad H.264 yra atviras standartas, o ne kažkokios vienos bendrovės licencijuojamas kodavimas. Be to, nuo 9 Adobe grotuvo versijos yra išnaudojamas aparatinis spartinimas ir kelių branduolių procesorius rodant vaizdą visame ekrane.

Abu šie audio-video medžiagos kodavimai leidžia vartotojui transliacijas paremtas SAVIP būdu žiūrėti esant nedideliam srauto pralaidumui. [13, 15]

98 procentai viso pasaulio kompiuterių turi įdiegtus Flash grotuvus (įskiepius). Tokios svetainės kaip YouTube, ABC ar NBC pirmenybę teikia Flash technologijai, o ne Apple QuickTime ar Microsoft Windows Media formatams, nes Flash yra sąlygiškai lengva naudoti ir pateikti tinklalapiuose.

Naudojant tą patį API, kuris padeda užkrauti Sorenson ar On2 VP6 video turinį, dabar galima užkrauti H.264 video MPEG-4 formate. Tai reiškia, kad galima pasinaudoti gausiais įrankiais ir technologijomis, kurias palaiko H.264, net neformuojant SWF.

Flash Player gali atkurti MPEG-4 formato video medžiagą, remiantis H.264 turiniu. Tai reiškia, kad galima paimti egzistuojančią video medžiagą kaip 3GP, MP4, ir MOV rinkmenas ir atkurti jas kaip SWF turinį.

Kyla klausimas ar naujasis MPEG-4 ir H.264 kodavimas pakeis ir išstums iš užimamų pozicijų On2 VP6 kodavimą? Žinoma, kad ne. Tai programuotojams tik leis pasirinkti geresnį sprendimą, kuri technologija jiems yra tinkamesnė, kuriamo produkto atžvilgiu. Abu kodekai turi savų privalumų ir trūkumų. On2 VP6 yra geresnis pasirinkimas projektams kurie yra pilnai paremti aukštos kokybės Flash video medžiaga. Tačiau platesnes galimybes platinti, aukštos kokybės ir HD video medžiagą turi H.264 kodeku paremti projektai, nes H.264 turi didesnę parinkčių bagažą.[15]

Apple prieš kelerius metus išleido su H.264 suderinamą QuickTime versiją. Microsoft (kaip dažniausiai būna) naudoja savo uždarą didelės raiškos vaizdo standartą, vadinamą Windows Media VC-9. Visgi Adobe Flash grotuvas yra pats populiariausias, tad H.264 suderinamumas mums yra labai svarbus: galėsime tikėtis televizinės kokybės vaizdo internete.

Naujausia Adobe Flash Player versija 10.1. Tai dar vienas perversmas video medžiagos perdavimo internetu srityje.

Kompanija „Adobe“ jau padarė didelį darbą, nes sukūrė „Flash“, skirtą kelioms mobiliųjų telefonų platformoms. Mobilųjų telefonų pastangos yra susijusios su kompanijos „Adobe“ vykdomu projektu „Open Screen Project“, kuriuo siekiama pasiūlyti platformą mobiliesiems telefonams, kompiuteriams, „netbook“ kompiuteriams ir netgi televizoriams. „Open Screen“ remia beveik 50 prietaisų gamintojų, turinio kūrėjų bei kitų partnerių.

Tačiau šiame darbe daugiausiai reiktų atkreipti dėmesį į tai, kad ši naujoji Flash Player versija įgalina naudoti P2P, Stratus serviso pagalba (Apie tai aprašyta ankstesnėje darbo dalyje 1.2.4)

2.3.1.5 Konverteris Ffmpeg

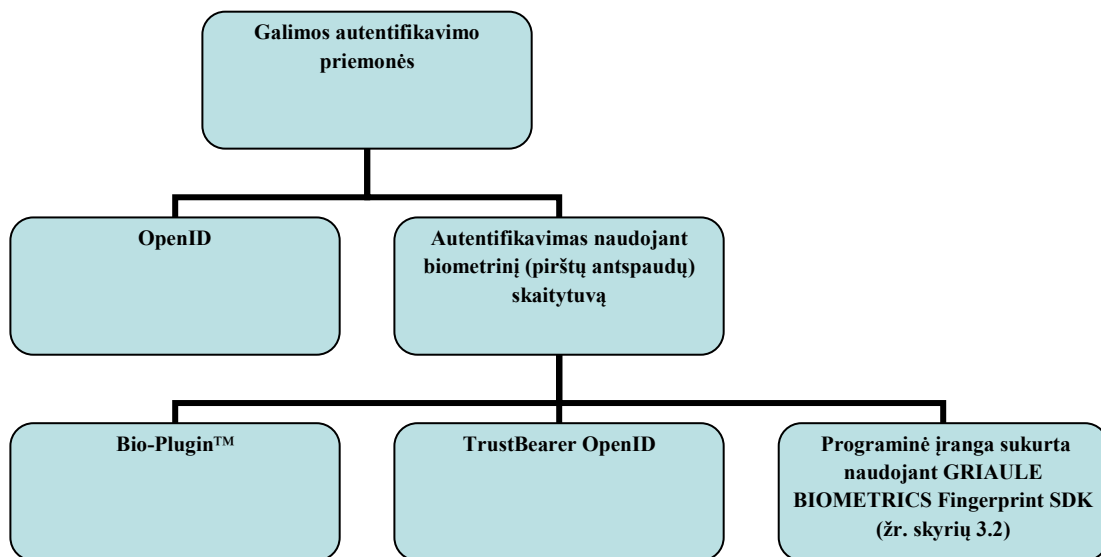
FFmpeg yra greičiausias video ir audio konverteris. Taip pat gali įrašinėti realiu laiku transliuojamą audio/video medžiagą. Komandinės eilutės sąsajas yra suprojektuota būti intuityvia, ta prasme, kad FFmpeg suvoktų visus parametrus, kurie gali būti gauti automatiškai. Tikrai turite apibrėžti tikslią kodavimo spartą. [8]

FFmpeg taip pat gali paversti iš bet kokios normos į bet kokią kitą, ir pakeisti video dydį (iš didesnės į mažesnę). [8]

2.4 Saugus autentifikavimas sistemoje

„Audio – video nuotolinio mokymo ir egzaminavimo sistemoje“, norint užtikrinti nuotolinių egzaminų autentiškumą, kaip viena iš saugos priemonių yra pasirinkta vartotojų autentifikacija biometrinių duomenų (piršto antspaudų) pagalba. Šioje darbo dalyje išsiaiškinsime geriausią biometrinės autentifikacijos realizacijos būdą. Kaip alternatyvą biometriniai autentifikacijai panagrinėsime OpenID standarto įdiegimo galimybes į kuriamą sistemą.

Žemiau 17 paveikslėlyje pateiktos visos autentifikavimo priemonės, kurias būtų galima realizuoti, kuriamoje sistemoje. Kiekviena iš šių priemonių tolimesnėje darbo dalyje bus aptarta atskirai bei pateiktos išvados. Remiantis išvadomis bus nuspręsta kurias iš priemonių realizuoti veikiančioje sistemoje.



17 pav. Galimos autentifikavimo priemonės kuriamoje sistemoje

2.4.1 OpenID



„OpenID“ - vieningas ir atviras interneto tapatybės standartas, kurio pagalba turint vieną „OpenID“ identifikatorių galima prisijungti prie visų internete esančių tinklalapių, kurie suteikia tokią galimybę. Būdamas atviras ir dokumentuotas, „OpenID“ suteikia galimybę kiekvienam tinklalapiui turėti įdiegtą „OpenID“ vartotojų prisijungimo sistemą. Taip gali būti sutaupomos lėšos, kurios turėtų būti skirtos vartotojų prisijungimo sistemos saugumui užtikrinti. Be to, toks tinklalapis bus patrauklus vartotojui, turinčiam „OpenID“ identifikatorių, kadangi prisijungimo ir registracijos į „OpenID“ palaikantį tinklalapį procesas gali būti pusiau arba pilnai automatizuotas ir greitas[16].

„OpenID“ - decentralizuota sistema. Tai reiškia, jog vartotojas gali rinktis iš daugybės skirtingų „OpenID“ tiekėjų, tarp kurių yra ir IT milžinai: „Google“, „Verisign“, „Yahoo“ ir kt.

Pagrindinės sąvokos:

- Vartotojas - interneto vartotojas (pvz.: Jūs);
- „OpenID“ tiekėjas - interneto servisas, suteikiantis vartotojams „OpenID“ identifikatorius;
- „OpenID“ identifikatorius - interneto adresas (URL), identifikuojantis vartotoją. „OpenID“ tiekėjai kiekvienam vartotojui suteikia atskirą „OpenID“ adresą, kuris naudojamas prisijungiant prie „OpenID“ palaikančių interneto svetainių. „OpenID“ identifikatorių pavyzdžiai: <http://vartotojo-vardas.myopenid.com>, <http://www.kitas-openid-tiekejas.com/vartotojo-vardas>;
- Tinklalapis - interneto svetainė, kuri naudoja „OpenID“, leidžiančią vartotojams prisijungti prie to tinklalapio sistemos.

Kai kurie skeptikai teigia, jog „OpenID“ turi saugumo pažeidžiamumą duomenų vagystės atžvilgiu. Vartotojas, įvedęs savo „OpenID“ identifikatorių žalingame tinklalapyje gali būti perkeliamas ne į savo „OpenID“ tiekėjo tinklalapį, bet į vizualiai panašų kenksmingą tinklalapį. Suvedęs savo prisijungimo duomenis vartotojas juos perduoda sukčiams. [16]

Tam, kad apsisaugoti nuo galimos duomenų vagystės, reikia rinktis patikimą ir saugų „OpenID“ tiekėją ir naudotis jų siūlomais saugumo sprendimais (pvz.: asmeninė iliustracija, kuri rodoma prisijungus TIK prie tikrojo tinklalapio).

„OpenID“ yra valdomas ir prižiūrimas „OpenID“ fondo. Šio fondo tarybos nariai yra „Google“, „Microsoft“, IBM, „Verisign“, „Yahoo“ ir kt. kompanijų atstovai. [16]

Išvados

Pastaruoju metu internetas tampa vis atviresnis ir labiau orientuotas į vartotoją, jo poreikius, asmens duomenų apsaugą. „OpenID“ neabejotinai prisidės prie šio veiksnio ir bus plačiai naudojamas kaip vartotojų tapatybės sistema. Tai patvirtina didžiausių informacinių technologijų kompanijų veiksmai: „Google“ (turintiems tinklaraštį blogspot.com sistemoje) ir „Yahoo“ jau įdiegė „OpenID“ į savo servisus.

Kitas panašaus pobūdžio projektas „OAuth“ veikia panašiu principu, tačiau yra skirtas ne vartotojo identifikavimui, o atitinkamų vartotojo duomenų perdavimui tarp įvairių interneto (ir ne tik) tarnybų. Abu šie standartai turėtų sukurti vieningą sąsają plisti socialiniams veiksniams internete.

Šį standartą nuspręsta realizuoti kuriamoje sistemoje.

Priežastys:

- *Ateityje numatomas gausus šio standarto paplitimas elektroninėje erdvėje.*
- *Patogus ir greitas naudojimas.*

2.4.2 Bio-Plugin™

Programinės įrangos **Bio-Plugin™** gamintojas teigia, kad tai revoliucingas pirštų antspaudų atpažinimo sprendimas, leidžiantis programuotojams labai greitai integruoti „server-based“ biometrinę sistemą. Taip pat pabrėžiama, kad tai nėra „fingerprint SDK“ ir nereikalauja aukštų programavimo įgūdžių. [6]

Bio-Plugin™ tai “**fingerprint sdk**” alternatyva, kuri leidžia sklandžiai atlikti pirštų antspaudų nuskaitymo įrankio integravimą į bet kokią Windows ar žiniatinklio programinę įrangą, per keletą valandų.

Kuriant autentifikuotą nuotolinio mokymo video atsiskaitymų sistemą svarbiausia dalį yra, kad įrankiai būtų pritaikyti žiniatinklio platformoms. **Bio-Plugin™** programinė įranga, tai palaiko. Kaip tai realizuojama pavaizduota 18 paveikslėlyje.



18 pav. Bio-Plugin žiniatinklio serveris: Tai būdas kaip pirštų antspaudų nuskaitymo įrankį integruoti į žiniatinklio platformas.

Sistemos privalumai:

- Palaiko šias duomenų bazes: MS SQL Server, Access, MySQL, Oracle 9i, DB2, Informix
- Saugomi įrašai gali būti suspaudžiami naudojant skirtingus algoritmus.
- Piršto antspaudų atitikmuo randamas tarp 25000 įrašų per 1 sekundę, jei naudojamas suspaudimo algoritmas. Naudojant skirtingus algoritmus paieškos laikas truputėlį gali kisti.
- Nuskaicius piršto antspaudą yra gaunamas paveikslėlis. Jei jis yra su pašaliniais „triukšmais“ jie yra eliminuojami.
- Užkoduotas piršto antspaudų atvaizdas yra siunčiamas tinklu į serverį ir duomenų bazėje ieškoma jo atitikmens.
- Piršto antspaudų pozicija nuskaitymo metu nedaro įtakos.[6]

Sprendimo aktualumas:

- Integravus Bio-Plugin įrankį žiniatinklio platformoje, pirštų antspaudų atpažinimo sistema gali pakeisti tradicinį vartotojo vardo ir slaptažodžio mechanizmą.

Išvados

Kruopščiai išnaginėjus aprašytą sprendimą paaiškėjo, kad jis veikia tik su vienos rūšies pirštų antspaudų skaitytuvais, kuriuos kuria ta pati kompanija. Dėl šios priežasties, sprendimas buvo įvertintas kaip itin nelankstus globalios vartotojų visuomenės atžvilgiu bei nuspręsta jo nenaudoti kuriamoje sistemoje. Tačiau pats veikimo/realizacijos principas gali būti naudojamas kaip itin geras pavyzdys.

2.4.3 TrustBearer OpenID

Ko Jums prireiks norint naudotis TrustBeare OpenID:

- Bet kurios iš išvardintų naršyklių: Internet Explorer 6 arba naujesnio, Firefox 2, Safari 2 arba naujesnio.



- Asmenybę identifikuoti leidžiančio USB rakto (USB token), kortelės su saugos čipu (smart card) arba biometrinio (pirštų antspaudų) skaitytuvo



TrustBearer OpenID palaiko labai platų skirtingų gamintojų autentifikacijai skirtų produktų asortimentą.[22]

Sąvoka OpenID jau girdėta ir aptarta ankstesnėje šio darbo dalyje 2.4.1. OpenID panaikina būtinybę naudoti daug skirtingų vardų ir slaptažodžių norint prisijungti prie skirtingų paskirų skirtinguose interneto tinklapiuose. Vienu iš atvejų jums tereikia prisiminti vieną svetainės adresą ir turėti vieną iš autentifikavimosi priemonių. Standartiniu atveju tai būtų vienas vartotojo vardas ir vienas slaptažodis.

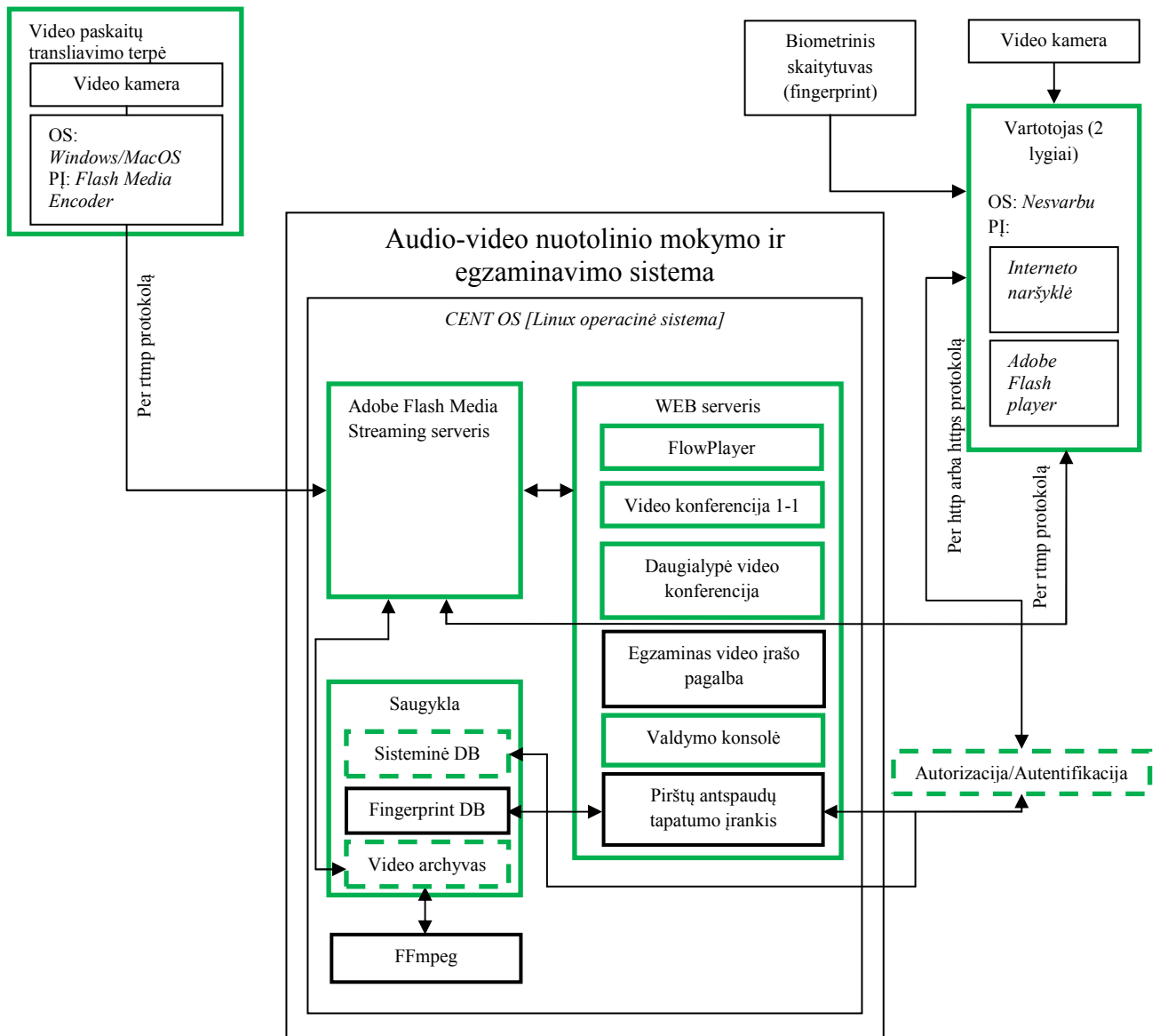
Kas pasikeičia naudojant TrustBearer OpenID? Šiuo atveju yra naudojamas stipraus autentifikavimo būdas. Vartotojas norėdamas autentifikuotis turi naudoti aparatinę įrangą (USB raktas (USB token), kortelė su saugo čipu (smart card) arba biometrinis (pirštų antspaudų) skaitytuvas). Be viso šito vartotojas turi užsiregistruoti sistemoje bei susiinstaliuoti naršyklės įskiepi leidžiantį atpažinti naudojamą įrangą. Norint autentifikuotis sistemoje belieka įjungti sistemos palaikomą aparatinę įrangą ir jos pagalba nusiųsti jus identifikuojančią informaciją.

Projektuojamoje sistemoje realizacijos metu bus išbadyta autentifikacija naudojant biometrinių pirštų skaitytuvą kuris yra integruotas daugelyje nešiojamų kompiuterių. TrustBearer OpenID sistema palaiko Wave-Enabled TPM (Trusted Platform Module), kuris ir yra diegiamas šiuolaikiniuose nešiojamuose kompiuteriuose. Ši platforma taip pat palaiko kortelių su saugos čipu (smart card) nuskaitymą ir autentifikacijos duomenų panaudojimą.[22]

Išvados

TrustBearer OpenID buvo įdiegtas, kuriamoje sistemoje, tačiau išbandyti tikrojo veikimo principo nepavyko. Priežastis: Sistemos gamintojas teigia, kad ji yra suderinama su Wave-Enabled TPM (Trusted Platform Module) aparatine įranga, kuri ir buvo naudojama realizacijos metu. Tačiau bandant suderinti sistemos darbą su šia aparatine įranga pasipylė sistemos gamintojo spragos. Spragų sąrašas buvo perduotas sistemos gamintojui, tačiau nebuvo gautas atsakymas, kuris padėtų išspręsti problemą. Kūrėjai tik patvirtino, jog stengsis, kad ateityje šių problema pavyktų išvengti.

3 Audio – video nuotolinio mokymo ir egzaminavimo sistemos realizacija



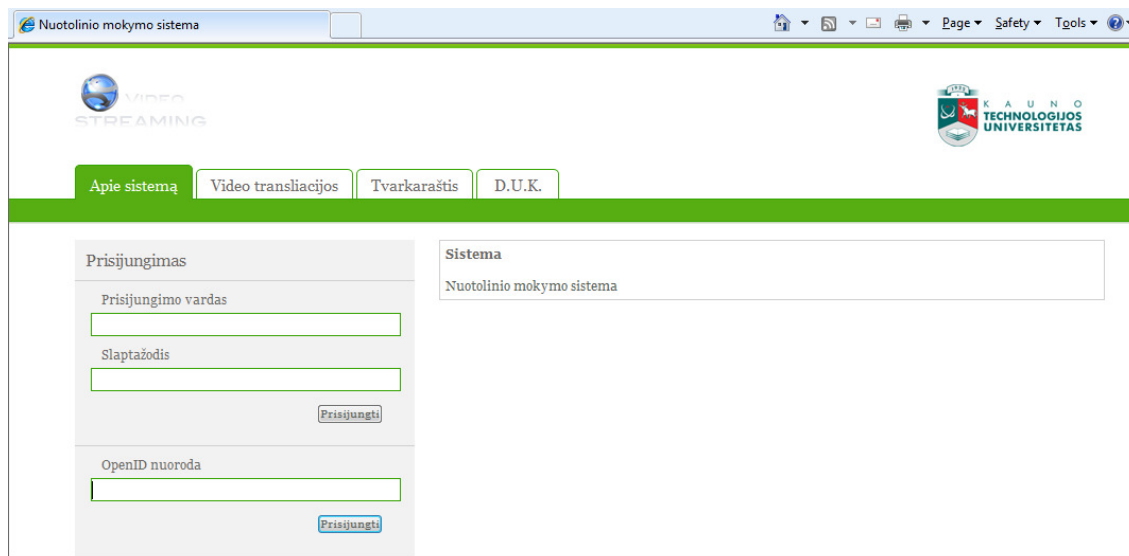
19 pav. Sistemos funkcinė diagrama (sužymėtos realizuotos funkcijos)

19 paveikslėlyje pateikta sistemos funkcinė diagrama, kurioje sužymėti pilnai realizuoti, dalinai realizuoti ir nerealizuoti sistemos komponentai.

- Žalia vientisa linija žymimi pilnai realizuoti sistemos komponentai.
- - - - - Žalia punktyrine linija žymimi dalinai realizuoti sistemos komponentai.
- Juoda vientisa linija žymimi nerealizuoti sistemos komponentai.

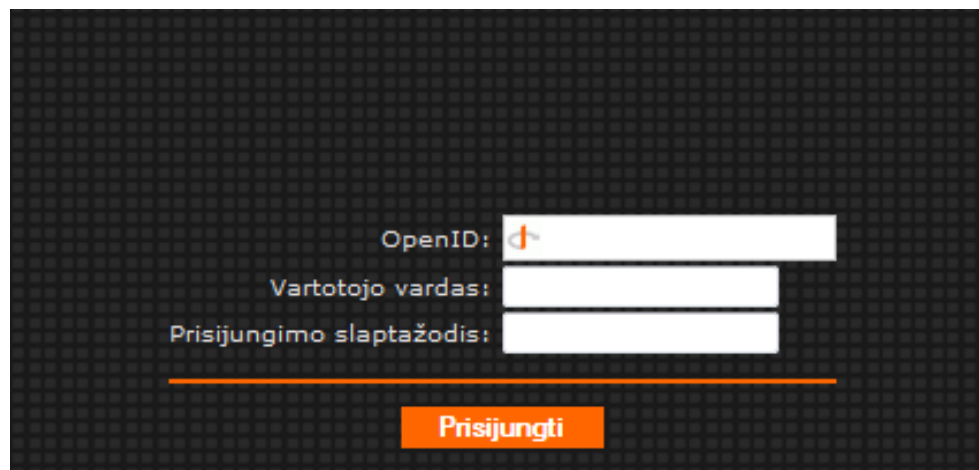
3.1 Sistemos realizacijos I ir II etapo metu atlikti darbai

Realizacija buvo vykdoma dviem etapais. Pirmojo etapo metu buvo sukurtas prototipas kuriame buvo atliekami įvairūs bandymai, diegiami ir testuojami papildomi įskiepai. Preliminariai viską ištestavus ir atlikus eksperimentus antrojo etapo metu palaipsniui buvo pradėta kurti audio - video nuotolinio mokymo ir egzaminavimo sistema. 20 paveikslėlyje pateikta sistemos vartotojo grafinė sąsaja.



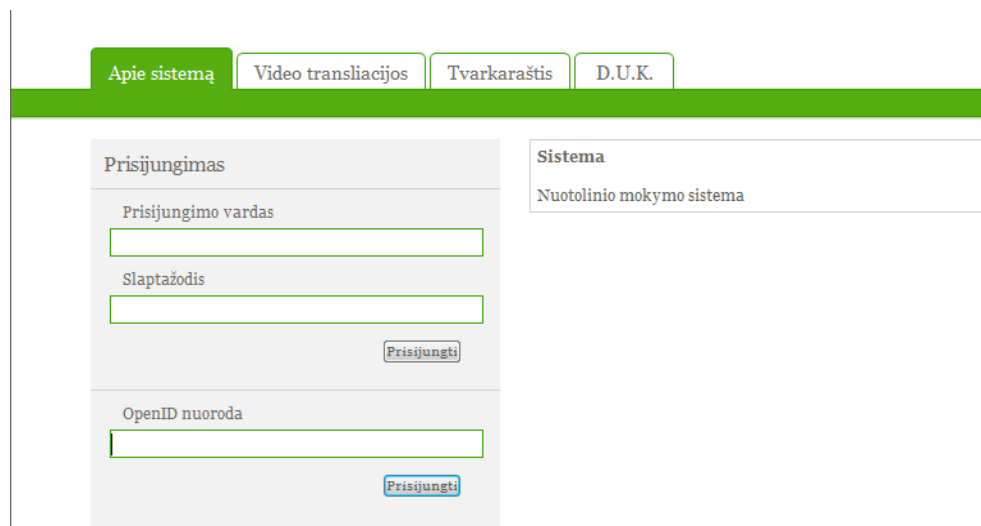
20 pav. Audio - video nuotolinio mokymo ir egzaminavimo sistemos vartotojo grafinė sąsaja

I etapo metu buvo išbandytas OpenID veikimo principas naudojant vieno vartotojo OpenID nuorodą(21 pav.).



21 pav. Sistemos vaizdas atliekant autentifikaciją naudojantis openID privalumais (I etapas)

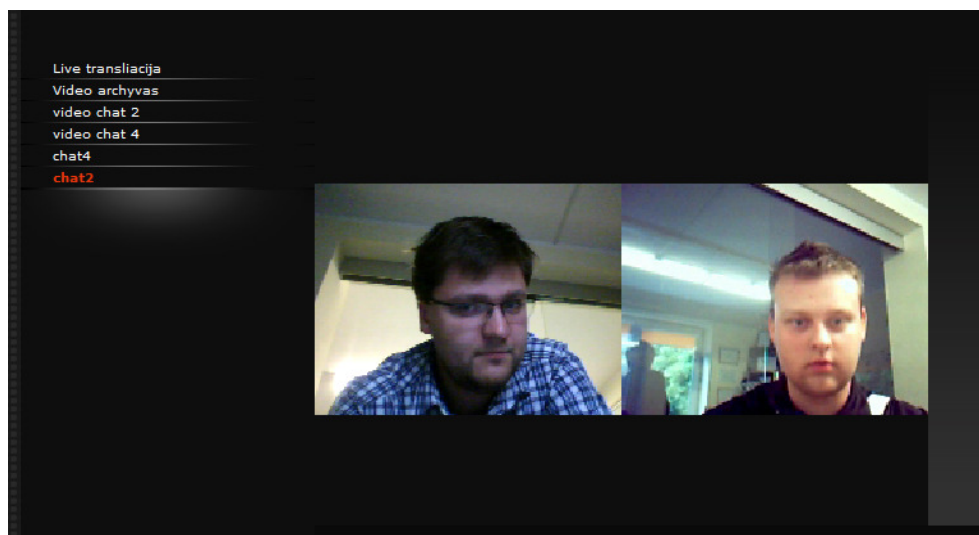
II etapo metu buvo patobulinta ne tik sistemos grafinė sąsaja, buvo suprogramuota galimybė administratoriui kurti naujus sistemos vartotojus ir priskirti jiems roles (22 pav.). Kiekvienam sistemos vartotojui yra galimybė priskirti jo OpenID nuorodą. Taip pat realizuota programinė įranga, kurios pagalba sistemos vartotojai gali autentifikuotis pirštų antspaudų pagalba.



The screenshot shows a web interface with a green header. The header contains four tabs: 'Apie sistemą', 'Video transliacijos', 'Tvarkaraštis', and 'D.U.K.'. Below the header, there are two main sections. The left section is titled 'Prisijungimas' and contains two login forms. The first form has fields for 'Prisijungimo vardas' and 'Slaptažodis', with a 'Prisijungti' button below. The second form has a field for 'OpenID nuoroda' and a 'Prisijungti' button below. The right section is titled 'Sistema' and displays 'Nuotolinio mokymo sistema'.

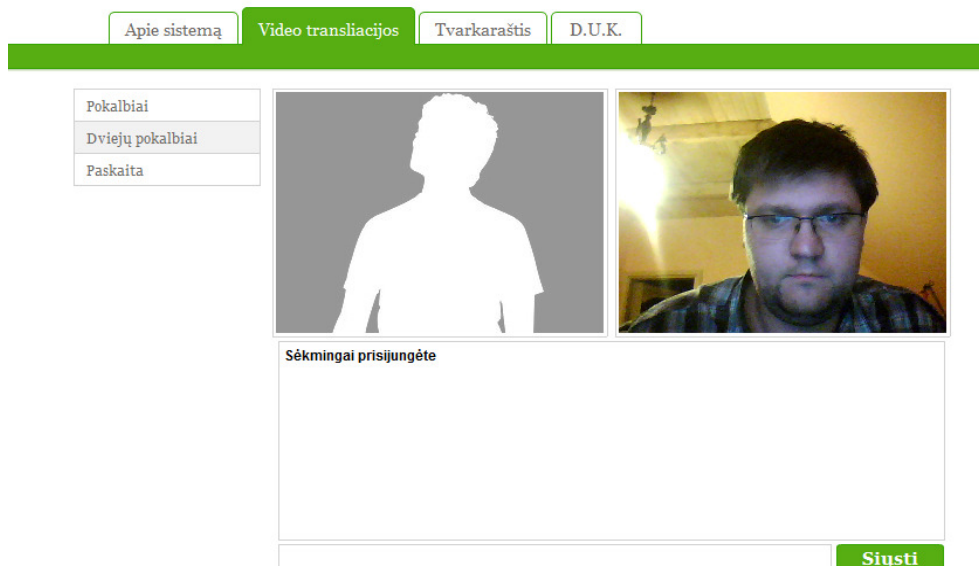
22 pav. Sistemos vaizdas atliekant autentifikaciją naudojantis openID privalumais (II etapas)

I etapo metu buvo išnagrinėta ir įdiegta automatinė video kameros atpažinimo funkcija, kuri leidžia vartotojui nediegiant jokios papildomos programinės įrangos, vieno mygtuko paspaudimu transliuoti savo norimą video, sistemos ribose (23 pav.).



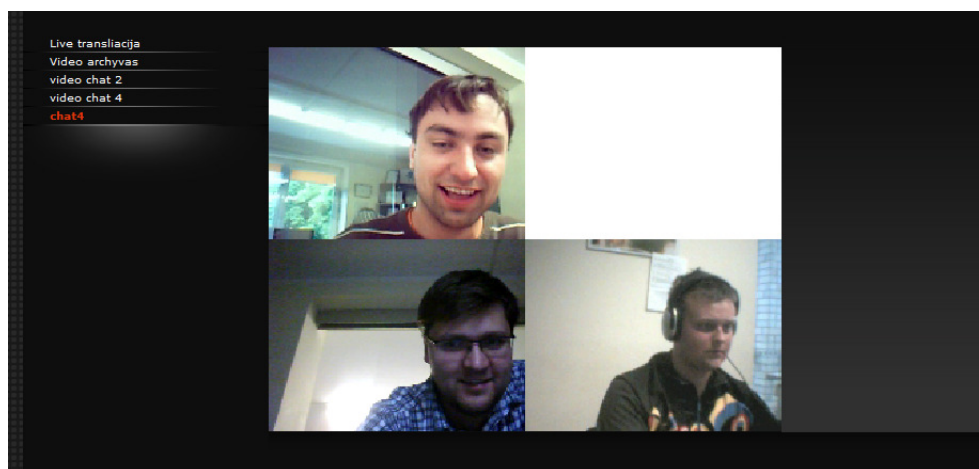
23 pav. Sistemos vaizdas vykdant dviejų asmenų video konferenciją (I etapas)

II etapo metu buvo padidinta perduodamos video medžiagos raiška, papildoma suprogramuota ir įdiegta elektroninių žinučių siuntimo funkcija (24 pav.).



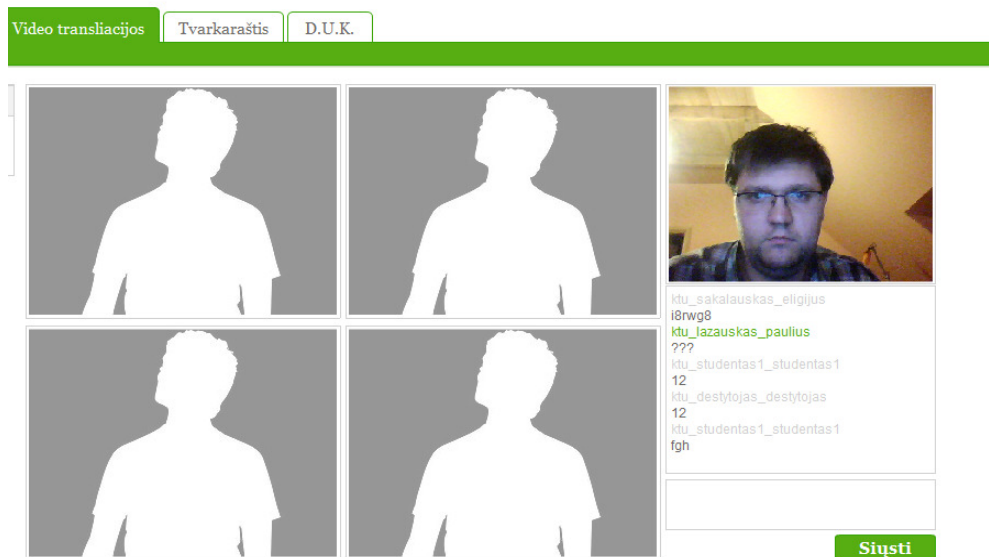
24 pav. Sistemos vaizdas vykdant dviejų asmenų video konferenciją (II etapas)

I etapo metu buvo tik ištestuota galimybė įgyvendinti video pokalbių kambarį, išnagrinėtų technologijų pagalba, skirtą daugiau nei dviem pašnekovam (25 pav.).



25 pav. Sistemos vaizdas vykdant daugialypę video konferenciją (I etapas)

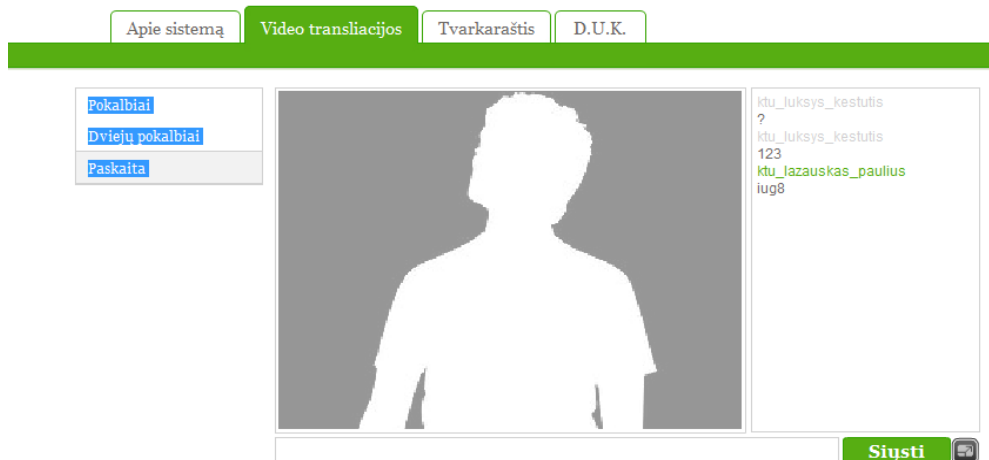
II etapo metu buvo pilnai suprogramuota galimybė vykdyti video konferenciją 5 pašnekovam. Kiekvienas iš pašnekovų video pokalbių kambaryje gali stebėti 4 savo pašnekovus, bei matyti kokia video medžiaga yra transliuojama iš jo pasirinkto video įrenginio (video kamera, ekrano klonavimo programinė įranga ir kt.) (26 pav.).



26 pav. Sistemos vaizdas vykdant daugialypę video konferenciją (II etapas)

I etapo metu buvo išnagrinėta itin aukštos video kokybės perdavimo technologija internetu, sukonfigūruotas serveryje video medžiagos srautą priimantis iš retransliuojantis servisas.

II etapo metu buvo realizuota dėstytojui skirta video paskaitų dėstymo terpė, kurioje galima transliuoti pasirinktos kokybės video medžiagą, naudojantis papildoma programine įranga Adobe Flash Media Encoder 2 (žr. 2.3.1.2 skyriuje). Suprogramuota galimybė stebintiems video paskaitą studentams uždavinėti klausimus elektroninių žinučių pagalba (27 pav.). Realizuota galimybė video paskaitą stebėti ne tik sistemos lange, bet ir pilnai išdidinus kompiuterio ekrano rėmuose.



27 pav. Paskaitų dėstymui skirtas modulis su galimybe užduoti klausimus elektroninių žinučių pagalba

3.2 Autentifikavimui skirta programinė įranga

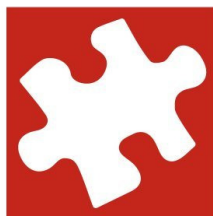
Nepavykus sistemoje panaudoti jau sukurtų sprendimų - Bio-Plugin™ (žr. 2.4.2 skyriuje) ir TrustBearer OpenID (žr. 2.4.3 skyriuje) - buvo nuspręsta sukurti autentifikavimui skirtą programinę įrangą, kuri leistų sistemoje autentifikuotis pirštų antspaudų pagalba.

Kuriant savo autentifikavimo programinę įrangą, kuri vartotoją automatiškai prijungia prie jo norimos tinklaraščio sistemos, buvo naudojamas 28 paveikslėlyje pavaizduotas Microsoft Fingerprint Reader DG2-00002.



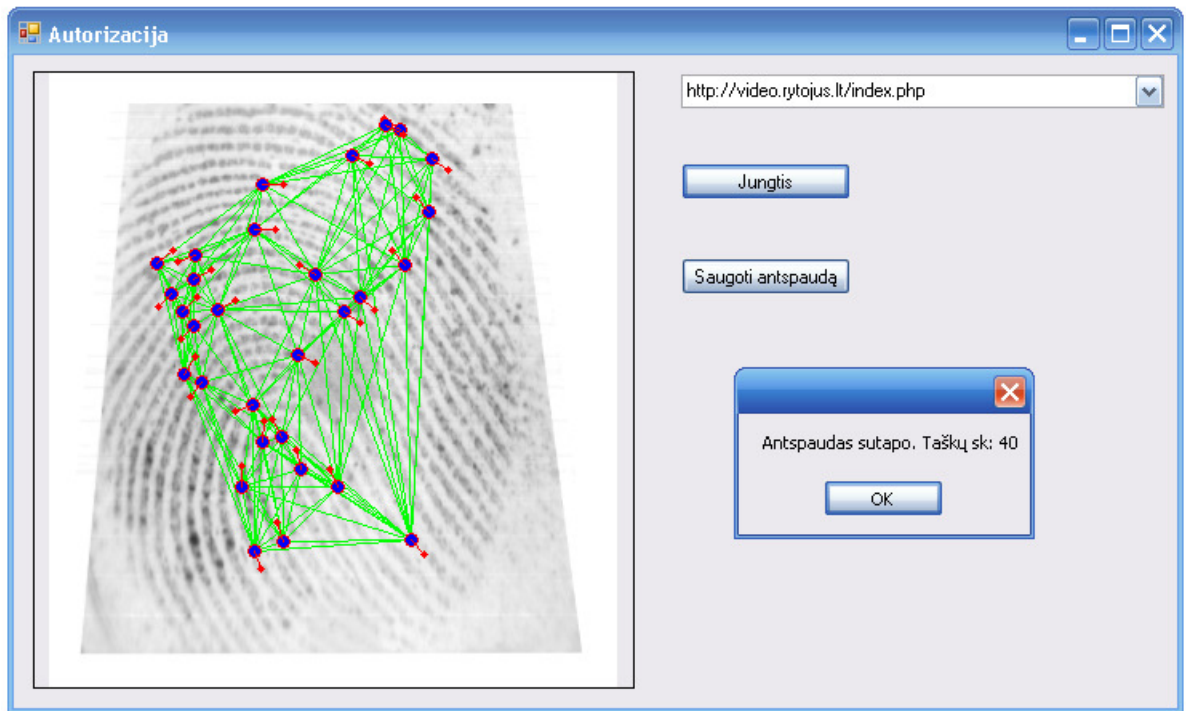
28 pav. Microsoft Fingerprint Reader DG2-00002

Kuriant programinę įrangą buvo naudojamas GRIAULE biometrics Fingerprint SDK. Tai bibliotekų rinkinys skirtas programų kūrėjams integruoti pirštų antspaudų nuskaitymo bei sulyginimo metodus.[9]

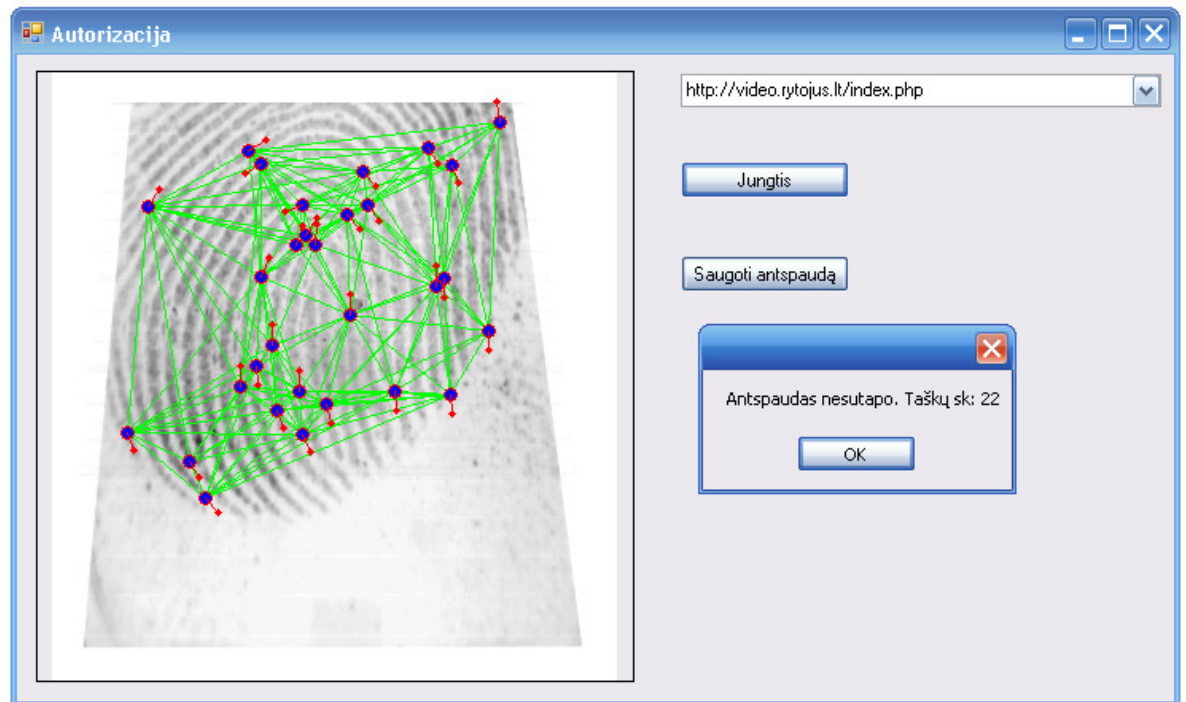


Fingerprint **SDK**

Kaip veikia realizuota autentifikacijai skirta programinė įranga pavaizduota 29 ir 30 paveikslėliuose.

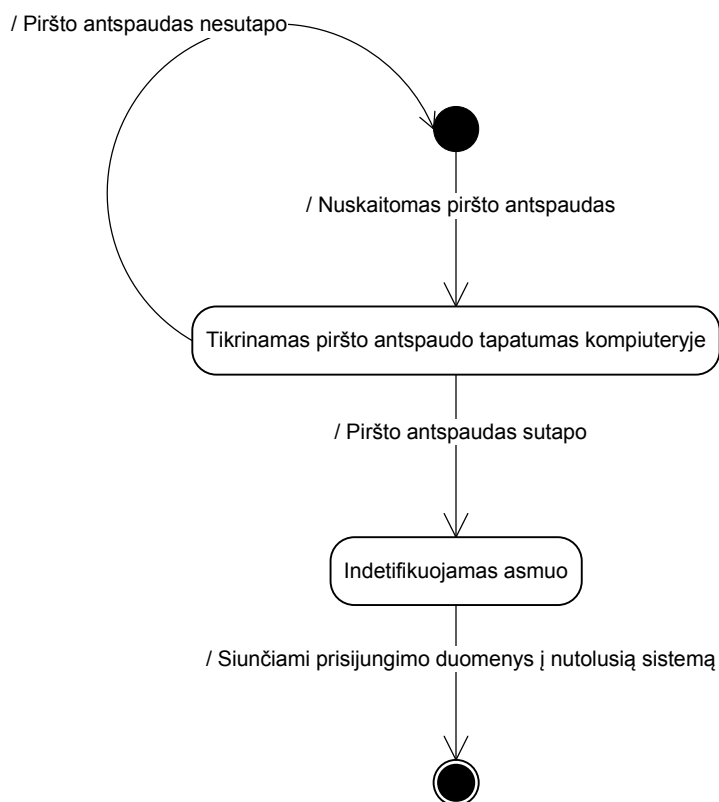


29 pav. Programinės įrangos veikimas sutapus piršto antspaudui



30 pav. Programinės įrangos veikimas nesutapus piršto antspaudui

Kaip šiuo metu yra vykdomas biometrinių duomenų (piršto antspaudo) tapatumo nustatymas ir vartotojo prijungimas prie sistemos yra pavaizduota 31 paveikslėlyje.



31 pav. Autentifikavimui skirtos programinės įrangos veikimo principas

Ižvelgiamos problemos

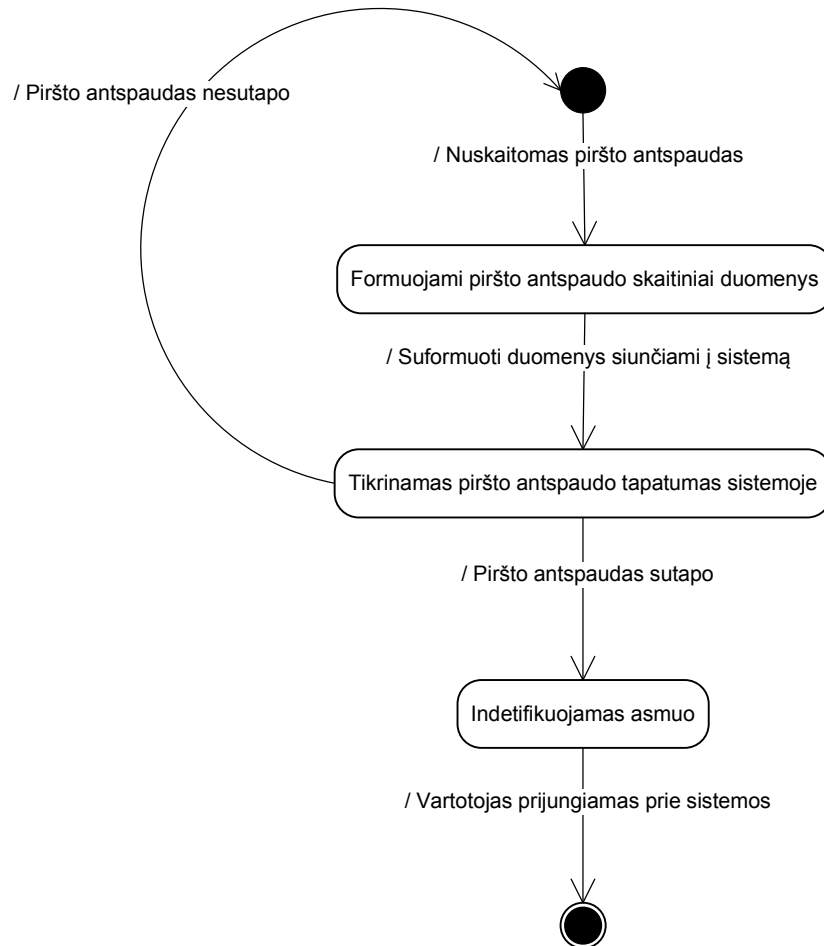
- Naudojant šį sprendimą pirštų antspaudas yra sulyginamas kliento kompiuteryje, o ne serverio pusėje. Tai nėra patogu, nes autorizacijai skirta informacija saugoma už sistemos ribų.
- Šiuo metu autentifikavimui skirta programinė įranga patikrina ar vartotojo piršto antspaudas sutampa su nustatytuoju ir tada inicijuoja vartotojo vardo ir slaptažodžio siuntimą nuotolinio mokymo sistemai. Tokiu būdu vartotojas yra autorizuojamas.
 - Nesaugu vartotojo vardą bei slaptažodį saugoti kompiuterio laikmenoje.
 - Autorizacijos duomenis reiktų siųsti saugiu SSL protokolu.

Problemų sprendimo būdas

- Numatoma patobulinta autentifikavimui skirtos programinės įrangos realizacija:
 - Vartotojų pirštų antspaudai turėtų būti saugomi serveryje.

- Nuskaičius piršto antspaudą biometriniu skaitytuvu, jo skaitiniai duomenys SSL protokolu turėtų būti siunčiami į serverį sulyginimui.
- Serverio pusėje būtina realizuoti pirštų antspaudų skaitinių reikišmių sulyginimo metodą.

Ateityje autentifikavimui skirtos programinės įrangos veikimo principas turėtų būti realizuotas, kaip pavaizduota 32 paveikslėlyje.



32 pav. Patobulintas autentifikavimui skirtos programinės įrangos veikimo principas

4 Audio – video nuotolinio mokymo ir egzaminavimo sistemos tyrimas

Sistemos tyrimą sudaro trys atskiros dalys:

- Interneto srauto matavimai, kurių metu bus išsiaiškinta ar paprastas „namų“ vartotojas galės naudotis sistemos teikiamomis paslaugomis ar šią sistemą bus galima naudoti tik specialiai paruoštose kompiuterių klasėse.
- Sistemos palyginimas su naujai atsiradusiomis video perdavimo sistemomis, kurios gali būti pritaikytos ir nuotoliniam mokymui. Atlikto tyrimo metu bus nustatyta, kuo sukurta sistema yra pranašesnė prieš kitas bei kokių papildomų įrankių jai trūksta.
- SAVIP serverio resursų apkrovimo priklausomybė nuo naudojamo protokolo. Tyrimo rezultatai turėtų parodyti kokią įtaką serverio resursų panaudojimui turi audio - video srauto šifravimas.

4.1 Audio-video srauto pasiskirstymo priklausomybė nuo pašnekovų skaičiaus

Bendra informacija apie matavimus:

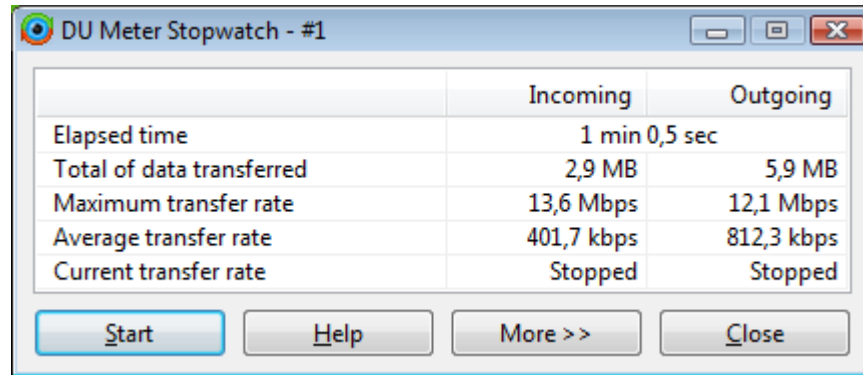
- Kiekvieno matavimo trukmė ~ 1 min.
- Matavimai buvo atlikti naudojantis DU Meter 4.16 ir ProteMac Meter 3.4.6 programine įranga.
- Žemiau pateikti keturių matavimų rezultatai, kurių metu buvo pasijungę 2, 3, 4 ir 5 pašnekovai vienoje video konferencijoje.

Vertinkime, kad „namų“ vartotojas turi interneto liniją kurios parametrai tokie:

- Įeinantis srautas 2Mbps;
- Išeinantis srautas 1Mbps.

4.1.1 Pirmasis matavimas

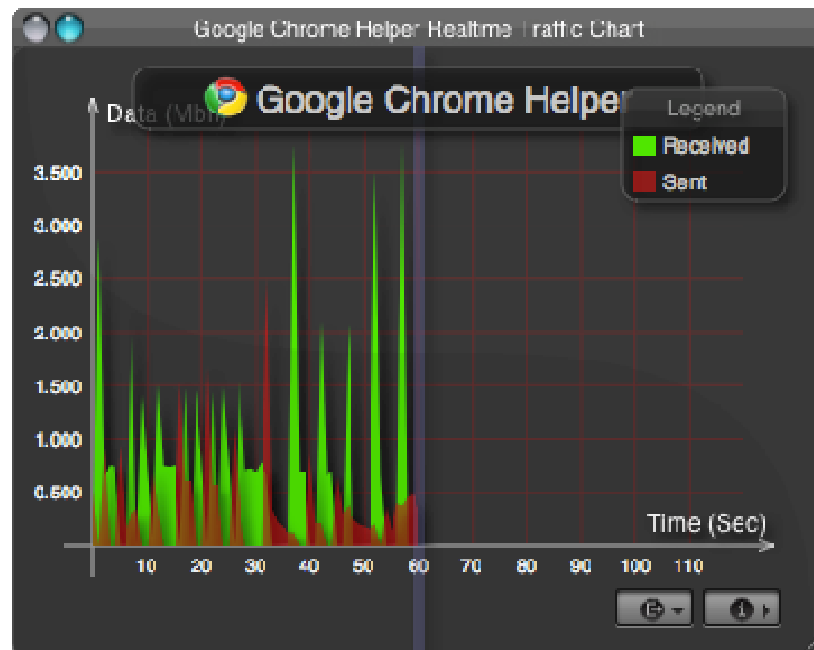
Pirmojo matavimo metu prie sistemos buvo prijungti **du** aktyvūs vartotojai. Matavimo rezultatai pateikti 33 ir 34 paveikslėliuose.



	Incoming	Outgoing
Elapsed time	1 min 0,5 sec	
Total of data transferred	2,9 MB	5,9 MB
Maximum transfer rate	13,6 Mbps	12,1 Mbps
Average transfer rate	401,7 kbps	812,3 kbps
Current transfer rate	Stopped	Stopped

Start Help More >> Close

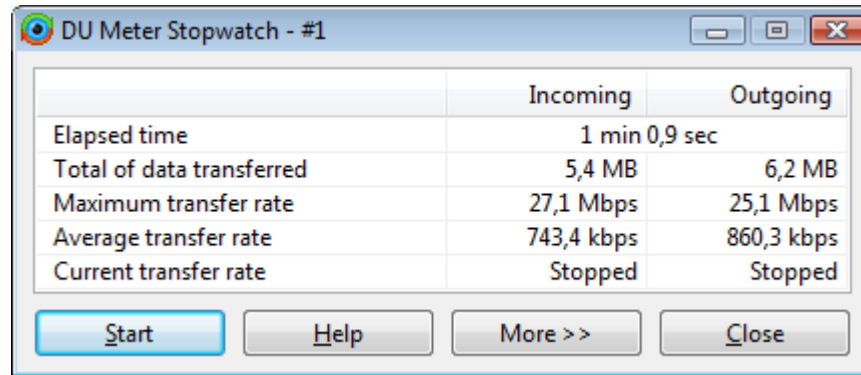
33 pav. Pirmojo matavimo skaitiniai rezultatai



34 pav. Pirmojo matavimo grafiniai rezultatai

4.1.2 Antrasis matavimas

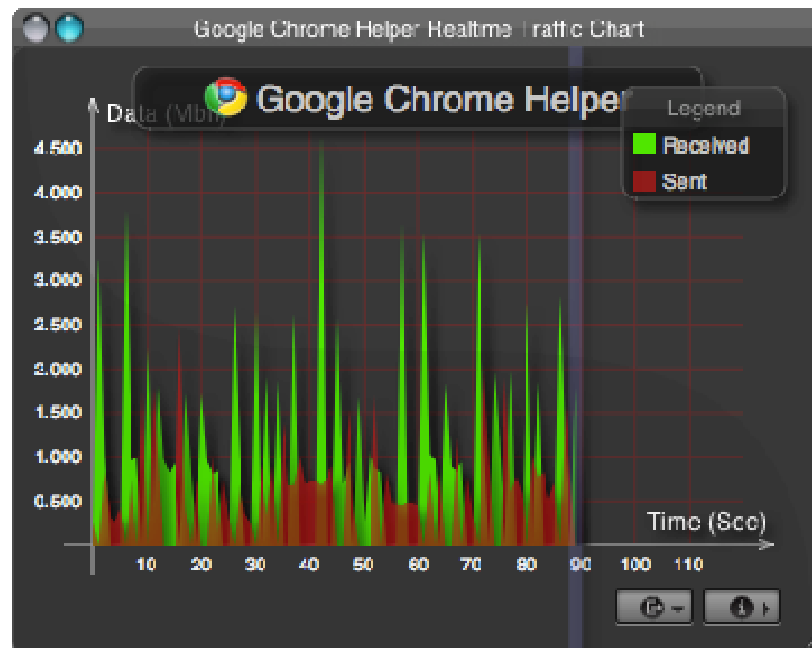
Antrojo matavimo metu prie sistemos buvo prijungti trys aktyvūs vartotojai. Matavimo rezultatai pateikti 35 ir 36 paveikėliuose.



The screenshot shows a window titled "DU Meter Stopwatch - #1". It contains a table with network statistics and four buttons at the bottom: "Start", "Help", "More >>", and "Close".

	Incoming	Outgoing
Elapsed time	1 min 0,9 sec	
Total of data transferred	5,4 MB	6,2 MB
Maximum transfer rate	27,1 Mbps	25,1 Mbps
Average transfer rate	743,4 kbps	860,3 kbps
Current transfer rate	Stopped	Stopped

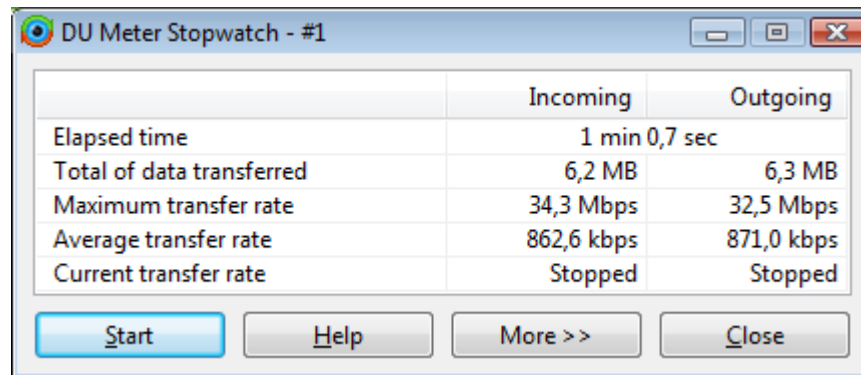
35 pav. Antrojo matavimo skaitiniai rezultatai



36 pav. Antrojo matavimo grafiniai rezultatai

4.1.3 Trečiasis matavimas

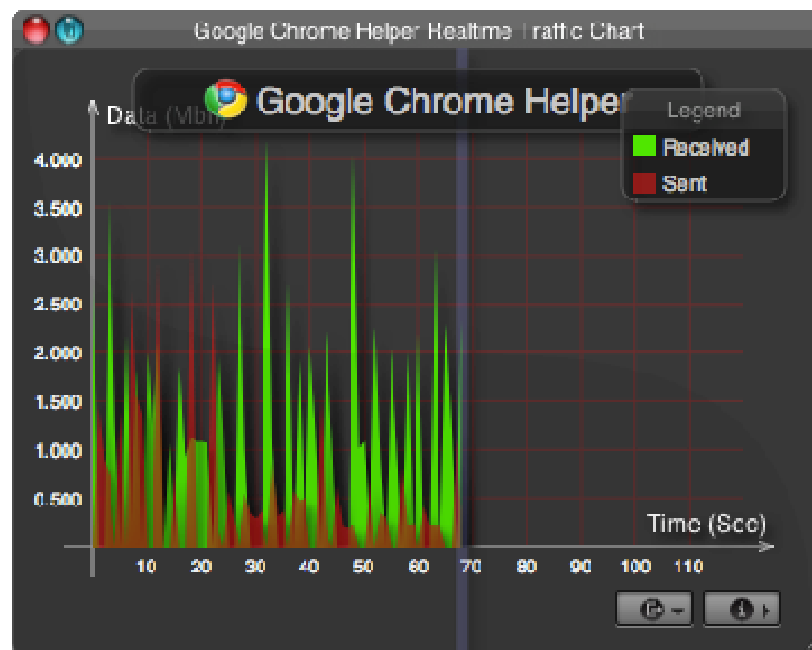
Trečiojo matavimo metu prie sistemos buvo prijungti **keturi** aktyvūs vartotojai. Matavimo rezultatai pateikti 37 ir 38 paveikėliuose.



	Incoming	Outgoing
Elapsed time	1 min 0,7 sec	
Total of data transferred	6,2 MB	6,3 MB
Maximum transfer rate	34,3 Mbps	32,5 Mbps
Average transfer rate	862,6 kbps	871,0 kbps
Current transfer rate	Stopped	Stopped

Buttons: Start, Help, More >>, Close

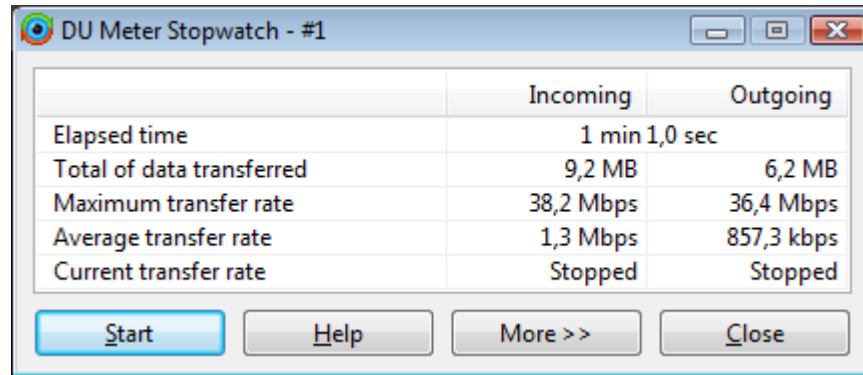
37 pav. Trečiojo matavimo skaitiniai rezultatai



38 pav. Trečiojo matavimo grafiniai rezultatai

4.1.4 Ketvirtasis matavimas

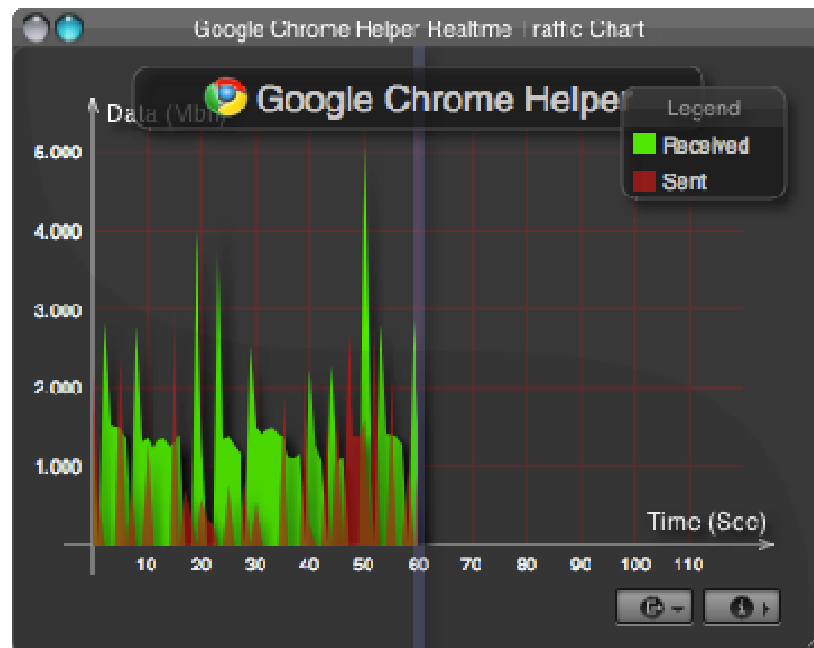
Ketvirtojo matavimo metu prie sistemos buvo prijungti **penki** aktyvūs vartotojai. Matavimo rezultatai pateikti 39 ir 40 paveikėliuose.



	Incoming	Outgoing
Elapsed time	1 min 1,0 sec	
Total of data transferred	9,2 MB	6,2 MB
Maximum transfer rate	38,2 Mbps	36,4 Mbps
Average transfer rate	1,3 Mbps	857,3 kbps
Current transfer rate	Stopped	Stopped

Start Help More >> Close

39 pav. Ketvirtojo matavimo skaitiniai rezultatai

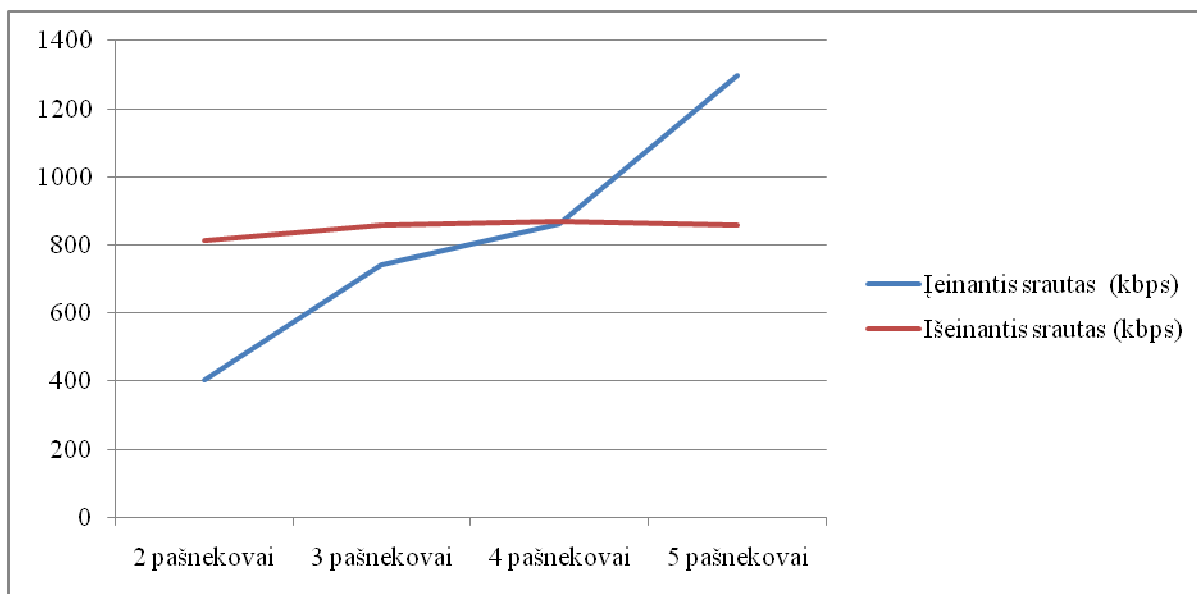


40 pav. Ketvirtojo matavimo grafiniai rezultatai

4.1.5 Matavimų apibendrinimas

Lentelė Nr. 5 Bendri matavimo rezultatai

	Įeinantis srautas (kbps)	Išeinantis srautas (kbps)
2 pašnekovai	402	812
3 pašnekovai	743	860
4 pašnekovai	863	871
5 pašnekovai	1300	857



41 pav. Įeinančio ir išeinančio srauto priklausomybė nuo pašnekovų skaičiaus

Pagal matavimo rezultatus pateiktus lentelėje Nr. 5 bei 41 paveikslėlyje matome, kad:

- Išeinantis srautas yra pastoviai stabilus, mažus jo pokyčius įtakoja transliuojamo vaizdo spalvų gamos pakitimai bei pašnekovo judesiai konferencijos metu. Atlikus šiek tiek daugiau papildomų matavimų buvo pastebėta kad prieš kamera palikus vien tik statinį nejudantį vaizdą generuojamo srauto kiekis sumažėjo 300 kbps. Nedidelę ~ 30 kbps įtaką turi perduodamo balso signalas (audio srautas).
- Įeinančio srauto priklausomybė nuo pašnekovų kiekio yra labai artima tiesiniai. Įeinančio srauto kiekį įtakoja visų pašnekovų išeinantis srautas. Svyruojant

išeinančio srauto kiekiui (svyravimai, kaip aptarėme anksčiau priklauso nuo spalvų gamos ir judesių kiekio) kinta ir įeinančiojo srauto kiekis.

Tyrimo rezultatai rodo, kad sistemos vartotojas gali dalyvauti 5 asmenų video konferencijoje, jei interneto prieigos parametrai nėra žemesni nei 1,5 Mbps įeinančio srauto ir 0,9 Mbps išeinančio srauto. Pagal mūsų darytą prielaidą, kad „namų“ vartotojo interneto prieigos parametrai yra 2 Mbps įeinančio srauto ir 1 Mbps išeinančio srauto, galima teigti, kad „namų“ vartotojai galės naudotis sistemos teikiamomis paslaugomis.

4.2 Audio – video nuotolinių sistemų palyginimas

Norėdami palyginti savo sukurtos sistemos funkcionalumą ir konkurencingumą su jau egzistuojančiomis rinkoje sistemomis, sudarėme Lentelę Nr. 6. Pagal skirtingus kriterijus sistemoms buvo skiriami balai nuo 0 iki 3. Kuo atitinkamos sistemos funkcija labiau pritaikyta nuotoliniam mokymui ar egzaminavimui tuo jai balų buvo skiriama daugiau.

Lentelė Nr. 6 Sistemos palyginimas su rinkoje egzistuojančiomis audio-video transliacijų sistemomis

KRITERIJUS	SISTEMOS PAVADINIMAS						
	AVNMIES*	AlmostMeet	ViPS	DimDim	Eluminate	MegaMeeting	GoToMeeting
Autentifikacija pagrįsta biometriniais duomenimis	3	0	0	0	0	0	0
Video paskaitų transliacija	2	2	2	2	2	2	2
Video konferencija 1-1	2	2	0	2	1	2	2
Daugialypė video konferencija	2	2	0	0	0	3	0
Bendras konferencijos dalyvių darbalaukis	0	2	0	0	1	0	1
Aukštos kokybės video medžiagos perdavimas	3	1	1	1	0	1	1
Ekrano vaizdo perdavimas	1	3	1	0	2	3	3
Galimybė transliuoti paskaitas iš pasirinkto failo (pvz. *.ppt)	1	2	2	3	2	1	1
Egzaminas pagrįstas video įrašu	3	0	0	0	0	0	0
Papildomos programinės įrangos diegimas norint paleisti sistemos funkcijas	2	3	1	3	1	3	0
Balų suma:	19	17	7	11	9	15	10

*AVNMIES – Audio-video nuotolinio mokymo ir egzaminavimo sistema

Kriterijų sąrašas buvo sudarytas pagal tai, kokios sistemos funkcijos yra labiausiai aktualios norint vykdyti nuotolinį mokymą ir egzaminavimą. Mūsų sukurtoje sistemoje nėra funkcijos „Bendras konferencijos dalyvių darbalaukis“, nėra itin patogų perduoti ekrano vaizdą, tačiau ji surinko didžiausią balų skaičių lyginant su kitomis sistemomis. Tai leidžia daryti išvadą, kad patobulinus ir praplėtus sistemos funkcijas ją būtų galima pradėti publikuoti ir platinti kaip komercinį produktą.

4.3 SAVIP serverio resursų apkrovimo priklausomybė nuo naudojamo protokolo

Tyrimo metu prie vienodo klientų skaičiaus (20) bus tiriamas serverio resursų apkrovimas naudojant šiuos audio - video informacijos perdavimo protokolus:

- RTMP
- RTMPT
- RTMPS

Real Time Messaging Protocol (RTMP) tai patentuotas protokolas, kurį sukūrė Adobe Systems kompanija. Šis protokolas skirtas audio, video medžiagą perduoti internete realiu laiku. Informacija yra perduodama iš serverio į Flash Player grotuvą.

RTMP protokolas turi 3 variacijas:

1. Tai paprastas protokolas veikiantis TCP protokolo pagrindu (prievaro numeris 1935).
2. RTMPT yra enkapsuliuotas HTTP sujungime, kad siunčiamų duomenų neblokėtų ugniasienės.
3. RTMPS tai tas pats RTMP, kuris apsaugotas saugiu HTTPS (HTTP + SSL) sujungimu.

Serverio, kuris naudojamas tyrimo metu parametrai:

- Procesorius(CPU): 2,0 Ghz [AMD];
- Operatyvinė atmintis(RAM): 2GB.

Lentelė Nr. 7 Serverio apkrovimo tyrimo rezultatai

PROTOKOLAS	CPU APKROVIMAS (%)	RAM IŠNAUDOJIMAS (MB)
RTMP	5	368
RTMPT	5	368
RTMPS	7	376

Pagal lentelėje Nr. 7 pateiktus duomenis matome, kad vykdant šifruotos audio-video informacijos perdavimą RTMPS protokolu serverio resursų panaudojimas nežymiai padidėjo. Naudojant RTMPT protokolą, pakitimų serverio resursų panaudojime neatsirado.

4.4 Tyrimo išvados

Buvo atliktos visos trys tyrimą sudarančios dalys ir apibendrinti gauti rezultatai.

Audio-video srauto pasiskirstymo priklausomybė nuo pašnekovų skaičiaus

Prieš atliekant matavimus buvo daryta prielaida, kad „namų“ vartotojo interneto prieigos parametrai yra 2 Mbps įeinančio srauto ir 1 Mbps išeinančio srauto. Matavimai parodė, kad „namų“ vartotojai galės naudotis sistemos teikiamomis paslaugomis.

Audio- video nuotolinių sistemų palyginimas

Vykdamas sistemų palyginimą kriterijų sąrašas buvo sudarytas pagal tai, kokios sistemos funkcijos yra labiausiai aktualios norint vykdyti nuotolinį mokymą ir egzaminavimą. Mūsų sukurta sistema surinko didžiausią balų skaičių. Tai leidžia daryti išvadą, kad patobulinus ir praplėtus sistemos funkcijas ją būtų galima pradėti publikuoti ir platinti kaip komercinį produktą.

SAVIP serverio resursų apkrovimo priklausomybė nuo naudojamo protokolo

Tyrimo rezultatai parodė, kad serverio resursų panaudojimui audio - video srauto šifravimas neturi didelės įtakos. Vykdamas šifruotos audio-video informacijos perdavimą RTMPS protokolu serverio resursų panaudojimas nežymiai padidėjo.

IŠVADOS IR REZULTATAI

1. Egzistuojančių klasikinių nuotolinio mokymo ir egzaminavimo sistemų analizė parodė, kad nuotolinių egzaminų autentiškumo užtikrinimo problema yra aktuali, nes šiuo metu studentams vykdant žinių patikrinimus nuotoliniu būdu, nėra priemonių, kurios užtikrintų, kad egzaminą laiko asmuo, kuriuo dedasi esąs.

2. Pažangių audio - video informacijos perdavimo technologijų analizės metu buvo iškelti du svarbūs reikalavimai kuriamai sistemai:

- užtikrinti audio-video transliacijų kokybę, esant mažai interneto spartai – taip siekiama užtikrinti, kad sistemos teikiamomis paslaugomis galėtų naudotis „namų“ vartotojai;
- egzamino metu vykdyti studento veido srities video įrašą į nutolusį serverį, kad dėstytojais vertinimo metu matytų ar studentas egzaminą laikė savo vardu bei nesinaudojo kitų asmenų pagalba.

3. Saugos technologijų analizė parodė, kad norint užtikrinti stiprų egzaminuojamų asmenų tapatybės patvirtinimą, kurioje sistemoje reikia realizuoti autentifikavimo priemonės biometrinių duomenų pagalba.

4. Remiantis audio-video srauto pasiskirstymo priklausomybės nuo pašnekovų skaičiaus tyrimo rezultatais, užtikrintai galima teigti, kad sistemos teikiamomis paslaugomis galės naudotis „namų“ vartotojai. Tyrimo rezultatai rodo, kad sistemos vartotojas gali dalyvauti 5 asmenų video konferencijoje, jei interneto prieigos parametrai nėra žemesni nei 1,5 Mbps įeinančio srauto ir 0,9 Mbps išeinančio srauto. Šių parametrų taip pat užtenka, video paskaitų stebėjimui, nuotolinių egzaminų laikymui bei dviejų asmenų video konferencijos vykdymui.

5. Atlikus audio video nuotolinių sistemų palyginimą didžiausią balų skaičių surinko „Audio – video nuotolinio mokymo ir egzaminavimo sistema“. UAB „Informacinių technologijų organizacija“, atlikto magistrinio darbo medžiagą naudoja komercinio produkto, „Daugiakomponentinė ir multifunkcinė paslaugų tarpininkavimo platforma“, kūrimui (žiūrėti Priedą Nr.3). Remiantis šiais rezultatais galima teigti, kad patobulinus ir praplėtus sistemos funkcijas ją būtų galima pradėti publikuoti ir platinti kaip komercinį produktą.

6. Darbe sukurta „Audio – video nuotolinio mokymo ir egzaminavimo sistema“ naudojama praktikoje. VGTU Viešosios komunikacijos direkcija tiria galimą sistemos pritaikymą universiteto valorizacijos proceso užtikrinimui (žiūrėti Priedą Nr.2). Sistemos prototipas buvo pristatytas kasmetinėje universiteto jaunųjų mokslininkų darbų parodoje - konkurse KTU technorama 2010. Komisija sistemai skyrė I vietą (žiūrėti Priedą Nr.1). Remiantis šiais rezultatais galima teigti, kad darbas yra pilnai išbaigtas ir atliktas kokybiškai.

7. Darbo metu realizuotos sistemos funkcijos:

- Autentifikacija biometrinių duomenų (pirštų antspaudų) pagalba;
- Atsiskaitymas (egzaminas) video konferencijos pagalba;
- Atsiskaitymo (egzamino) forma paliekant video įrašą nutolusiame sistemos serveryje;
- Daugialypė video konferencija (skirta maksimaliai 5-iems vartotojams vienoje diskusijoje);
- Aukštos kokybės video paskaitų transliacijos modelis.

Sukurta sistema gali būti plečiama. Rekomenduojami tobulinimai:

- Ekranų vaizdo perdavimas nenaudojant papildomai diegiamos programinės įrangos. Visas procesas turėtų būti vykdomas vieno mygtuko paspaudimu.
- Bendras video konferencijos dalyvių darbalaukis. Kiekvienas pašnekovas darbalaukyje galės pakoreguoti kito asmens pateiktą informaciją, nubrėžti grafiką ir kt.
- Individualios dėstytojų interneto svetainės. Sistemoje kuriant dėstytojo vartotoją automatiškai bus sugeneruojama jam priklausanti asmeninė svetainė. Jose bus pateikiama bendra informacija apie dėstytoją, jo dėstomus modulius, kiekvieno modulio skirsnyje automatiiniu būdu formosis nuotoliniu būdu dėstytojų video paskaitų archyvas.
- Sistemos pagrindines funkcijas apjungti į lengvai diegiamą įskiepi. Tai trečiųjų šalių programinės įrangos modelis, kuri būtų galima diegti į plačiai paplitusias klasikines nuotolinio mokymo sistemas (Moodle, WebCT ir kt.)
- Įvairių dokumentų ir failų pasirašymas elektroniniu parašu.

LITERATŪRA

1. Adobe® Flash® Media Server 3. *Technical white paper - Adobe Systems Incorporated* [interaktyvus]. 2008, vasaris [žiūrėta 2008-05-05]. Prieiga per internetą: <http://www.adobe.com/support/documentation/en/flashmediaserver/3_5/FMS_3_5_Release_Notes.pdf>.
2. Advantages of streaming video. *WebsynergiDesign* [interaktyvus]. 2008 [žiūrėta 2008-05-10]. Prieiga per internetą: <http://www.websynergi.com/video_streaming_audio_streaming.asp>.
3. An Overview of H.264 Advanced Video Coding. *White paper – Iain Richardson* [interaktyvus]. 2007 [žiūrėta 2008-04-15] Prieiga per internetą: <http://www.ebu.ch/trev_302-sunna.pdf>.
4. AREŠKA, N. Audio-video srautų organizavimas bei pralaidumo įvertinimas e-studijų aplikacijoje. Mokslinės techninės konferencijos pranešimų medžiaga. Kaunas, 1997, p. 7-12.
5. BALBIERIS, G.; KRISČIŪNIENĖ, N.; ir kt. Virtualioji mokymosi aplinka mokyklai. *Mokyklų tobulinimo programa* [interaktyvus]. 2005 [žiūrėta 2009-10-10]. Prieiga per internetą: <<http://www.mtp.smm.lt/>>.
6. Bio plug-in™ fingerprint sdk alternative. *M2SYS* [interaktyvus] 2009 [žiūrėta 2009-11-16]. Prieiga per internetą: <<http://www.m2sys.com/bioplugin.htm>>.
7. Dr. HUANG, E.; SISK, J.; KIRK, T.; CORYELL, G.; IR STEWART, J. Searching for an Live Streaming Technology. *Indiana University-Purdue University Indianapolis* [interaktyvus]. 2007 [žiūrėta 2008-05-09]. Prieiga per internetą: <<http://www.iupui.edu/~nmstream/live/introduction.php>>.
8. FFmpeg General Documentation. *FFmpeg* [interaktyvus] 2009 [žiūrėta 2009-09-12]. Prieiga per internetą: <<http://ffmpeg.mplayerhq.hu/general.html>>.
9. Fingerprint SDK. *GriauleBiometrics* [interaktyvus] 2009 [žiūrėta 2010-01-16]. Prieiga per internetą: <http://www.griaulebiometrics.com/page/fingerprint_sdk>.
10. Fingerprint System Technology. *AFIS* [interaktyvus] 2007 [žiūrėta 2008-05-12]. Prieiga per internetą: <<http://www.east-shore.com/product.html>>.
11. Flash Media Encoder 2. *Adobe* [interaktyvus] 2008 [žiūrėta 2008-03-12]. Prieiga per internetą: <<http://www.adobe.com/products/flashmediaserver/flashmediaencoder/>>.

12. Flowplayer - Free video player for web. *Flowplayer* [interaktyvus] 2008 [žiūrėta 2008-03-13]. Prieiga per internetą: <<http://www.flowplayer.org/player/index.html>>.
13. H.264. *Adobe*. [interaktyvus] 2007 [žiūrėta 2008-05-12]. Prieiga per internetą: <http://www.adobe.com/products/hdvideo/supported_technologies/h264.html>.
14. Hassoun, D. Exploring Flash Player support for high-definition H.264 video and AAC audio. *RealEyes Media* [interaktyvus] 2008 [žiūrėta 2008-04-10]. Prieiga per internetą: <http://www.adobe.com/devnet/flashplayer/articles/hd_video_flash_player_print.html>.
15. JONAITIS, A. High Definition vaizdas internete – jau greitai. *Kompiuterija*, 2007, Nr. 8, p. 9-10.
16. OpenID - vieninga asmens tapatybė internete. *Lecinskas* [interaktyvus] 2008 [žiūrėta 2009-09-20]. Prieiga per internetą: <<http://www.lescinskas.lt/openid-vieninga-asmens-tapatybe-internete>>.
17. Peer-assisted networking using RTMFP groups in Flash Player 10.1. *Adobe* [interaktyvus]. 2010 [žiūrėta 2010-03-10]. Prieiga per internetą: <http://www.adobe.com/devnet/flashmediaserver/articles/p2p_rtmfp_groups_03.html>.
18. Progressive Download. *RichMediaProject* [interaktyvus] 2008 [žiūrėta 2008-10-12]. Prieiga per internetą: <<http://www.rich-media-project.com/progressive-download-products/progressive-download/>>.
19. Real Time Media Flow Protocol. *Wikipedia* [interaktyvus]. 2009 [žiūrėta 2009-01-10]. Prieiga per internetą: <http://en.wikipedia.org/wiki/Real_Time_Media_Flow_Protocol/>.
20. SAUGENIENĖ, N. Nuotolinių studijų aplinka. *Teismo medicinos institutas* [interaktyvus]. 2010 [žiūrėta 2010-04-05]. Prieiga per internetą: <http://www.tmi.lt/lt/padaliniai/centrai/nuotoliniu_s_centras/nuotoliniu_s_aplinka/>.
21. Startus. *Adobe Labs* [interaktyvus]. 2010 [žiūrėta 2010-03-10]. Prieiga per internetą: <<http://labs.adobe.com/technologies/stratus/>>.
22. Strong Authentication & OpenID. *Trustbearer* [interaktyvus] 2009 [žiūrėta 2009-11-14]. Prieiga per internetą: <<http://openid.trustbearer.com>>.
23. ŠILEIKIENĖ, I. Kompiuterinės mokymo sistemos. Paskaitų mokomoji medžiaga. Vilnius, 2002.
24. TARGAMADŽĖ, A.; ir PETRAUSKIENĖ, R. Nuotolinių studijų kokybė technologijų kaitos sąlygomis = the quality of distance learning in the situation of technological change. Tarptautinės konferencijos pranešimų medžiaga. Kaunas 2008 gegužė, p. 74-93.

25. VENČKAUSKAS, A.; ir TOLDINAS, E. Kompiuterių ir operacinių sistemų sauga. Paskaitų mokomoji medžiaga. Kaunas, 2007.
26. WebCT. *Wikipedia* [interaktyvus]. 2009 [žiūrėta 2009-01-10]. Prieiga per internetą: <<http://en.wikipedia.org/wiki/WebCT/>> .
27. ZABAVIČIUS, P. Biometrinės autentifikavimo sistemos. Lietuvos IX - sios jaunųjų mokslininkų konferencijos pranešimų medžiaga. Kaunas, 2008.

Audio – video distance learning and examination system

Summary

One of the great discoveries of our times is flexible and sophisticated virtual learning systems. Using remote services student can study the provided material, complete exercises, test the knowledge and take exams. Video conferencing provides the means to transfer sound and video, for students to communicate with each other and for teachers to communicate with students using computer networks. Most of the common remote learning systems do not have an ability to provide interactive remote studying and knowledge testing based on audio and video streaming.

Two main problems are raised in this work:

- Authenticity during remote examination is ensured by using audio - video and biometric technologies.
- Raising the quality of video streaming over the internet - to ensure as high quality audio and video streaming as possible by using as low bandwidth as possible.

The purpose of this work is to create audio - video distance learning and examination system, which would be based on streaming audio - video information and will have biometric authentication method. The main goal of the system is to provide students and teachers convenient means for providing virtual learning and examination. The more real-world learning means will be migrated to this virtual system, the more perfect it will be and that will enable it to compete with conventional means of studying.

JAUNŲJŲ
MOKSLINIKŲ
DARBŲ
PARODA



KTU
TECHNORAMA
2010

DIPLOMAS

Nuoširdžiai sveikiname

**Paulių Lazauską
Mantą Lenzą
Paulių Vitkų**

laimėjus

I vieta

už darbą

„Telekonferencijų sistema nuotoliniam mokymui“

Rektorius
R. Šiaučiūnas

2010 m. gegužės 4 d.

2 PRIEDAS. AKTAS DĖL BANDOMOJO SISTEMOS DIEGIMO



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Viešosios komunikacijos direkcija

Saulėtekio al. 11, LT-10223 Vilnius, tel.: (8 5) 274 5025, (8 5) 274 4936, el. p. ird@adm.vgtu.lt

Kauno technologijos universiteto
Informatikos fakulteto
Kompiuterių katedrai

AKTAS
DĖL BANDOMOJO SISTEMOS DIEGIMO
2010-05-21

Vilnius

VGTU Viešosios komunikacijos direkcija pažymi, kad Pauliaus Lazausko magistrinio darbo metu sukurtos „Audio-video nuotolinio mokymo ir egzaminavimo sistemos“, galimybės yra testuojamos. VGTU VKD tiria galimą sistemos pritaikymą universiteto valorizacijos proceso užtikrinimui.

VKD direktoriaus pavaduotojas
Justas Nugaras

Kauno technologijos universiteto
Informatikos fakulteto
Kompiuterių katedrai

**RAŠTAS
DĖL SISTEMOS KOMERCIALIZACIJOS IR IŠEIGOS KODO NAUDOJIMO**

2010-05-17

Kaunas

UAB „Informacinių technologijų organizacija“ pažymi, kad Pauliaus Lazausko magistrinio darbo „Audio-video nuotolinio mokymo ir egzaminavimo sistema“ turinys yra glaudžiai susijęs su įmonės vykdomu projektu „Daugiakomponentinės ir multifunkcinės paslaugų tarpininkavimo platformos kūrimas“ pagal veiksmų programos prioriteto priemonę Intelektas LT. Ateityje sukurta sistema bus naudojama komerciniams tikslams. Dėl šios priežasties studentas Paulius Lazauskas negali Kauno technologijos universitetui atiduoti sistemos išieigos kodo.

(Parašas)

Įmonės akcininkas
Petras Bieliauskas

UAB „Informacinių technologijų organizacija“
Įmonės kodas: 300558136
PVM kodas: LT100003405813

Beršausko 47-13, LT -51420, Kaunas
Tel.: +370 671 139 58
El.paštas: info@iTo.lt
www.iTo.lt

A.s. LT947300010094426312
AB bankas HANSABANKAS
Banko kodas: 73000