ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

ЗОКИРОВ ОДИЛЖОН ЁҚУБЖОН ЎҒЛИ

БУЛУТЛИ ҲИСОБЛАШ ТИЗИМЛАРИДА ФОЙДАЛАНУВЧИЛАРНИ АУТЕНТИФИКАЦИЯЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ

Тошкент-2020

УДК: 004.056.53

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси автореферати мундарижаси

Оглавление автореферата диссертации доктора философии (PhD) по техническим наукам

Contents of dissertation abstract of the doctor of philosophy (PhD) on technical sciences

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.13/30.12.2019.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

ЗОКИРОВ ОДИЛЖОН ЁҚУБЖОН ЎҒЛИ

БУЛУТЛИ ҲИСОБЛАШ ТИЗИМЛАРИДА ФОЙДАЛАНУВЧИЛАРНИ АУТЕНТИФИКАЦИЯЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ6

Тошкент-2020

Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссиясида B2020.3.PhD/T1892 рақам билан рўйхатга олинган.

Диссертация Тошкент ахборот технологиялари университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгаш веб-саҳифасида (www.tuit.uz) ва «Ziyonet» Ахборот таълим порталида (www.ziyonet.uz) жойлаштирилган.

Илмий раҳбар:	**Ганиев Салим Каримович** техника фанлари доктори, профессор
Расмий оппонентлар:	**Каримов Маджит Маликович** техника фанлари доктори, профессор
	Норматов Шербек Бахтиярович техника фанлари бўйича фалсафа доктори (PhD)
Етакчи ташкилот:	**«UNICON.UZ» – фан-техника ва маркетинг тадқиқотлари маркази**

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.13/30.12.2019.T.07.01 Илмий кенгашнинг 2020 йил «30» декабр соат 14:00 даги мажлисида бўлиб ўтади. (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университети Ахборот-ресурс марказида танишиш мумкин (1630 рақам билан рўйхатга олинган.). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-ўй. Тел.: (99871) 238-65-44).

Диссертация автореферати 2020 йил « 18 » декабр да тарқатилди.
(2020 йил « 16 » декабр даги 18 рақамли реестр баённомаси.)

Р.Х. Хамдамов
Илмий даражалар берувчи илмий кенгаш раиси, т.ф.д., профессор

Ф.М. Нуралиев
Илмий даражалар берувчи илмий кенгаш илмий котиби, т.ф.д., доцент

Б.Ф. Абдурахимов
Илмий даражалар берувчи илмий кенгаш кошидаги илмий семинар раиси ўринбосари, ф-.м.ф.д., профессор

КИРИШ (фалсафа доктори (PhD) диссертациясининг аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Жаҳонда булутли ҳисоблаш тизимларидан фойдаланиш ҳажмининг кескин суръатлар билан ортиши, булутли тизимлар билан боғлиқ хавфсизлик муаммоларини олдинги ўринга чиқарди. Бу булутли тизимларнинг заифлиги, нафақат фойдаланувчиларнинг шахсий маълумотларининг, балки, муҳим коорпоратив сирлар ва мулкка оид маълумотларининг ҳам ошкор қилиниши билан изоҳланади. Хусусан, Statista компаниясида “2019-2020 йилларда ташкилотнинг булутли ҳисоблаш тизимидаги муаммолар рўйхатида 85% кўрсаткич билан хавфсизлик муаммоси етакчилик қилган”[1]. Булутли ҳисоблаш тизимларида маълумотлар ва ресурслардан рухсатсиз фойдаланишни олдини олишда аутентификация усулларининг ўрни муҳим. Булутли тизимларни татбиқ этиш, булутли ҳисоблаш тизимларида маълумотларни ҳимоялаш, фойдаланувчиларни кафолатли аутентификациялаш усулларини ишлаб чиқиш соҳасига АҚШ, Япония, Германия, Жанубий Корея, Ҳиндистон ва бошқа ривожланган давлатларда катта эътибор қаратилмоқда.

Жаҳонда булутли ҳисоблаш тизимларида маълумотларни сақлаш, ишлаш ва узатиш ҳамда ресурслардан ишончли фойдаланишдаги муаммоларни ечишга қаратилган усул ва алгоритмларни яратиш бўйича кўплаб илмий тадқиқотлар олиб борилмоқда. Шу ўринда, фойдаланувчиларнинг булутли ҳисоблаш тизими ресурсларидан қонуний фойдаланишларини кафолатли амалга оширувчи, криптографик алгоритмларга ва кўп омилли аутентификация усуллари ва воситаларига бағишланган илмий-амалий тадқиқотларга алоҳида эътибор қаратиш зарур ҳисобланади.

Республикамизда давлат ва хўжалик бошқарув органлари томонидан тақдим этилаётган булутли ҳисоблаш тизимларига асосланган хизматларда фойдаланувчиларнинг ҳақиқийлигини текшириш ва жараён хавфсизлигини таъминлашга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан «...ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоялаш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга қарши ўз вақтида ва муносиб қаршилик кўрсатиш»[2] вазифалари белгиланган. Ушбу вазифаларни амалга оширишда булутли ҳисоблаш тизимларида фойдаланувчиларнинг ҳақиқийлигини текширишнинг самарали ва хавфсиз усуллари ҳамда воситаларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича

[1] https://www.statista.com/statistics/511283/worldwide-survey-cloud-computing-risks/

[2] Ўзбекистон Республикаси Президенти 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида» ги Фармони

Ҳаракатлар стратегияси тўғрисида»ги, 2018 йил 14 мартдаги ПФ-5379-сон «Ўзбекистон Республикасининг давлат хавфсизлиги тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги, 2018 йил 19 февралдаги ПФ-5349-сон «Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида»ги Фармонлари ва Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2018 йил 5 сентябрдаги 707-сон «Бутунжаҳон Интернет тармоғида ахборот хавфсизлигини янада такомиллаштириш чора-тадбирлари тўғрисида»ги Қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишда мазкур диссертация тадқиқоти маълум даражада хизмат қилади.

Тадқиқотнинг республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги. Мазкур тадқиқот республика фан ва технологиялар ривожланишининг IV. «Ахборотлаштириш ва ахборот-коммуникация технологияларини ривожлантириш» устувор йўналиши доирасида бажарилган.

Муаммонинг ўрганилганлик даражаси. Булутли ҳисоблаш тизими ресурсларидан кафолатли фойдаланишни амалга оширувчи, криптографик алгоритмларга ва кўп омилли аутентификация усуллари ва воситаларини ишлаб чиқиш соҳасида кўплаб олимлар илмий-амалий тадқиқотлар олиб бормоқдалар.

Жаҳонда, М.Ализадех, Х.Фарук, С.Дежамфар, С.Лим булутли ҳисоблаш тизимларида аутентификация усулларини таснифлаш, С.Ҳафизул, Ю.Лиао, С.Калра, С.Чанг, С.Кумарилар томонидан эллиптик эгри чизиқларга асосланган фойдаланувчиларни аутентификациялаш усулларини ишлаб чиқиш, Й.Чон, С.Дей, Ф.Омри, К.Бензекки, Д.Шваб, С.Жегадесанлар томонидан мобил булутли ҳисоблаш тизимлари учун аутентификация усулларини ишлаб чиқиш, Auth0, AMD Telecom, OpenID, IBM, iSM, WatchGuard каби халқаро ташкилотлар томонидан булутли ҳисоблаш тизимлари учун фойдаланишларни назоратлаш ва аутентификация воситаларини яратиш бўйича илмий-тадқиқот ишлари олиб борилмоқда.

Республикамизда, П.Ф.Хасанов, М.Орипов, С.К.Ганиев, М.М.Каримов, Д.Е.Акбаров, З.Т.Худойкулов ва бошқалар бошчилигидаги илмий жамоалар томонидан ахборот тизимларининг ҳимояланганлигини таҳлиллаш, криптографик ҳимоя усулларини яратиш, фойдаланувчиларни аутентификациялаш усуллари ва воситаларини ишлаб чиқиш усуллари ўрганилган.

Шу билан бир қаторда, булутли ҳисоблаш тизимларида фойдаланувчилар ҳақиқийлигини текширишда мобиль қурилмалар имкониятларидан фойдаланишга ва эллиптик эгри чизиқларга асосланган аутентификация усулларига етарлича эътибор қаратилмаган.

Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация тадқиқоти Тошкент ахборот технологиялари университетининг

илмий-тадқиқот ишлари режасининг №БВ-Ф4-023 – “Тақсимланган ахборот-коммуникация тизимларида инцидентлар ва киберхужумларга қарши харакатларни бошқариш муаммоларини тадқиқ этиш (Исследование проблем управления инцидентами и противодействия кибератакам в распределенных информационно-коммуникационных системах)” (2017-2020) мавзусидаги лойиҳа доирасида бажарилган.

Тадқиқотнинг мақсади булутли ҳисоблаш тизимларида икки омилли ва криптографик алгоритмларга асосланган фойдаланувчиларни аутентификациялаш усул ва алгоритмларини ишлаб чиқишдан иборат.

Тадқиқотнинг вазифалари:

булутли ҳисоблаш тизимлари учун биргина фойдаланишли аутентификация протоколини такомиллаштириш;

булутли ҳисоблаш тизимлари учун эллиптик эгри чизиқларга асосланган икки томонлама аутентификациялаш протоколини ишлаб чиқиш;

мобиль булутли ҳисоблаш тизимлари учун фойдаланувчиларни хавфсиз аутентификациялаш протоколини ишлаб чиқиш;

ишлаб чиқилган аутентификация протоколлари асосида биргина фойдаланишли аутентификация тизимини қуриш.

Тадқиқотнинг объекти сифатида булутли ҳисоблаш тизимларида фойдаланувчиларни ҳақиқийлигини текшириш жараёни олинган.

Тадқиқотнинг предметини булутли ҳисоблаш тизимларидаги эллиптик эгри чизиқларга асосланган ва икки омилли аутентификациялаш усуллари ва алгоритмлари ташкил этади.

Тадқиқотнинг усуллари. Тадқиқот жараёнида алгоритмлаш, сонлар назарияси, қиёсий таққослаш, хавфсизликка таҳлиллаш ва объектга йўналтирилган дастурлаш усулларидан фойдаланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

шахсий маълумотларни шифрлаш ва бардошли аутентификация усуллари асосида биргина фойдаланишли аутентификация протоколи такомиллаштирилган;

эллиптик эгри чизиқлар афзалликларини инобатга олган холда булутли ҳисоблаш тизимларида фойдаланувчиларни икки томонлама аутентификациялаш протоколи ишлаб чиқилган;

мобиль булутли ҳисоблаш тизимлари учун “савол – жавоб” механизмига асосланган икки томонлама аутентификация протоколи ишлаб чиқилган;

ишлаб чиқилган протоколлар асосида биргина фойдаланишли аутентификация тизими такомиллаштирилган.

Тадқиқотнинг амалий натижаси қуйидагилардан иборат:

OpenID Connect протоколида хавфсизлик муаммоларини бартараф этиш учун хавфсизлик чоралари ишлаб чиқилган;

эллиптик эгри чизиқлар афзалликларини қўллаган ҳолда, булутли ҳисоблаш тизимларида фойдаланувчиларни ҳақиқийлигини текширишнинг хавфсиз структураси ишлаб чиқилган;

мобиль булутли ҳисоблаш тизимларида “савол – жавоб” механизмига асосланган икки томонлама аутентификация тизими ишлаб чиқилган;

ишлаб чиқилган аутентификация усулларини OpenID Connect биргина фойдаланишли назоратлаш тизимига киритиш асосида такомиллаштирилган.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги булутли ҳисоблаш тизимларида, эллиптик эгри чизиққа ва мобиль қурилмалар имкониятига асосланган, биргина фойдаланишли аутентификация тизими учун ишлаб чиқилган усуллар ва алгоритмлардан олинган реал ҳамда тажрибавий таҳлиллар билан изоҳланади.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Тадқиқот натижаларининг илмий аҳамияти булутли ҳисоблаш тизимларида, эллиптик эгри чизиққа ва мобил қурилмалар имкониятига асосланган, биргина фойдаланишли аутентификация тизими учун усул ва алгоритмларни ишлаб чиқиш ва такомиллаштириш билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти булутли ҳисоблаш тизимларида фойдаланувчиларни ҳақиқийлигини тасдиқлашга қаратилган таҳдидларни камайтириш ва кўп сонли қайд ёзувлар учун аутентификация жараёнини ягона парол асосида амалга ошириш имконияти билан изоҳланади.

Тадқиқот натижаларининг жорий қилиниши. Ишлаб чиқилган булутли ҳисоблаш тизимларида фойдаланувчиларни ҳақиқийлигини текшириш усуллари, алгоритмлари ва дастурий воситалари бўйича олинган натижалар асосида:

эллиптик эгри чизиққа асосланган фойдаланувчиларни аутентификациялаш протоколларнинг дастурий воситаси “UNICON.UZ” ДУК – Фан-техника ва маркетинг тадқиқотлари марказининг амалий фаолиятида жорий қилинди (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 01 декабр № 33-8/7322-сон маълумотномаси). Таклиф этилган аутентификация протоколи ҳар иккала томонда ҳисоблашлар вақти бўйича, мавжудларига нисбатан 1,16 марта юқори самарадорликни қайд этган;

ишлаб чиқилган аутентификация усуллари асосида такомиллаштирилган OpenID Connect биргина фойдаланишли аутентификация “COSCOM” МЧЖнинг амалий фаолиятига жорий қилинди (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 01 декабр № 33-8/7322-сон маълумотномаси). Илмий тадқиқот натижасида OpenID Connect биргина фойдаланишли аутентификация тизими ташкилот ходимлари томонидан юритилаётган кўплаб паролга асосланган тизимни ягона махфий параметр асосида бошқариш ва паролни ёдда сақлаш билан боғлиқ муаммоларни 4 марта камайтириш имконини берган;

мобил қурилмалар имкониятига асосланган аутентификация усулининг дастурий воситаси Давлат Хизматлари Агентлигининг амалий фаолиятида жорий қилинди (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2020 йил 01 декабр № 33-8/7322-сон

маълумотномаси). Ишлаб чиқилган аутентификация протоколи SCRAM протоколига нисбатан ҳисоблашлар сони бўйича 2,5 марта юқори самарадорликни қайд этган.

Тадқиқот натижаларининг апробацияси. Мазкур тадқиқот натижалари 1 та халқаро ва 6 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Диссертациянинг мавзуси бўйича жами 18 та илмий иш чоп этилган, жумладан, Ўзбекистон Республикаси Олий аттестация комиссиясининг диссертацияларнинг асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларида 8 та мақола, 6 таси хорижий ва 2 таси республика журналларида нашр этилган ҳамда ЭҲМ учун яратилган 3 та дастурий воситаларни қайд қилиш гувоҳномалари олинган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертация ҳажми 107 бетни ташкил этади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация мавзусининг долзарблиги ва зарурияти асосланган, тадқиқотнинг Ўзбекистон Республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги кўрсатилган, мақсад ва вазифалари белгилаб олинган ҳамда тадқиқот объекти ва предмети аниқланган, олинган натижаларнинг ишончлилиги асослаб берилган, уларнинг назарий ва амалий аҳамияти, тадқиқот натижаларини амалда жорий этилиш ҳолати, нашр этилган ишлар ва диссертациянинг тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг «**Булутли ҳисоблаш тизимларида хавфсизлик муаммолари»** деб номланган биринчи боби булутли ҳисоблаш тизимлари, уларнинг имкониятлари, уларда мавжуд хавфсизлик муаммолари, хусусан, фойдаланувчиларни аутентификация усулларининг таҳлилига бағишланган.

Маълумотларни сақлаш технологияларининг жадал ўсиши ва Интернетнинг ривожи натижасида компьютер ресурслари аввалгига қараганда арзонроқ ва кучлироқ бўлди, ҳамда ихтиёрий жойда фойдаланиш имконияти яратилди. Ушбу тенденция “Булутли ҳисоблаш” (Cloud Computing) деб номланувчи янги мавзунинг шаклланишига олиб келди. Булутли ҳисоблашда ресурсларни (масалан, процессор ва хотира), фойдаланувчилар ва Интернет томонидан талабларни ҳисобга олган ҳолда, жамоа воситаси сифатида ишлатиш мумкин.

АҚШнинг стандарт ва технологиялар миллий институти (National Institute of Standards and Technology, NIST) томонидан булутли ҳисоблаш технологиясининг талаб бўйича ўзи-ўзига хизмат кўрсатиш, тармоқдан кенг фойдаланиш, ресурсларни тўплаш, тезкор мослашувчанлик ва ўлчовли хизмат каби асосий хусусиятлари алоҳида санаб ўтилган. Булутли ҳисоблаш провайдерлари томонидан фойдаланувчиларга қатор хизматлар тақдим

этилади ва улар илова хизмати (Software as a Service, SaaS), платформа хизмати (Platform as a Service, PaaS) ва инфратузилма хизмати (Infrastructure as a Service, IaaS) моделларига асосланади.

Булутли ҳисоблаш тизимлари харажатларни камайтириш, кенг қамровлилик/эгилувчанлик, ишончлилик, мобил фойдаланиш каби афзалликларга эга бўлсада, махфийликни таъминлашдаги муаммолар, стандартлардаги камчиликлар, доимий ривожланиш ва мослашишдаги қийинчиликлар илмий изланишларни талаб қилувчи жиҳатлари ҳисобланади.

Булутли ҳисоблаш тизимларидаги таҳдидларнинг STRIDE методологияси бўйича таҳлил натижалари уларнинг асосан ахборотнинг ошкор бўлиши, имтиёзнинг ортиши ва ўзгартириш хусусиятига қаратилганини кўрсатди. Бундан ташқари, булутли тизимларда мавжуд ҳужумлар асосан аутентификация тизимини, рухсатларни назоратлаш тизимини бузишни ва махфий ахборотни ошкор бўлишини мақсад қилиниши таҳлиллар натижасида аниқланди. Мазкур таҳдид ва ҳужумларни олдини олишда рухсатларни бардошли ва самарали назоратлаш, фойдаланувчиларни аутентификациялаш ва шахсий ахборотни ҳимоялаш усулларидан фойдаланиш зарурияти олиб борилган изланишлар натижасида аниқланди.

Булутли ҳисоблаш тизимларида фойдаланиладиган мавжуд аутентификация усулларининг таҳлили паролга асосланган аутентификация усулларига нисбатан бардошли ҳамда самарали янги аутентификация усулини ишлаб чиқиш заруриятини кўрсатди. Бундан ташқари, мобил булутли тизимлар учун яратилган мавжуд аутентификация усулларида ҳам амалга ошириш, хавфсизлик ва самарадорлик билан боғлиқ очиқ муаммолар мавжудлиги аниқланди. Бу эса, мобил булутли ҳисоблаш тизимлари учун самарали ва бардошли янги аутентификация усулини ишлаб чиқиш заруриятини кўрсатди.

Диссертациянинг **«Булутли ҳисоблаш тизимларида фойдаланишларни назоратлаш усуллари»** деб номланган иккинчи бобида биргина фойдаланишга асосланган протоколларнинг хавфсизлик таҳлили амалга оширилган ва танлаб олинган OpenID Connect протоколи, мавжуд муаммоларни бартараф этиш мақсадида, такомиллаштирилган.

Ҳозирда булутли ҳисоблаш тизимларида ва корпоратив ташкилотларда айнан биргина фойдаланиш (Single Sign-On, SSO) асосида фойдаланувчиларни аутентификациялаш ва авторизациялаш амалга оширилмоқда. Мазкур технология фойдаланувчиларга кўплаб хизматлардан ёки тизимлардан фойдаланиш учун ягона қайд ёзувини ишлатиш имкониятини тақдим этади. Ҳозирда кенг қўлланилувчи SSO протоколларига OAuth2, OpenID Connect, SAML, LDAP, CAS, CoSign ва бошқаларни киритиш мумкин (1-жадвал).

Таҳлил натижалари OAuth2, CAS ва CoSign протоколларида авторизация ёки аутентификация муолажаларининг мавжуд эмаслигини кўрсатмоқда. LDAP протоколдан локаль тармоқда SSO хизматини қуришда фойдаланилсада, веб иловаларда қўлланилмаганлиги сабабли, кам қизиқарли

соҳа ҳисобланади. SAML 2.0 протоколи ўзида XML форматига токенни тақдим қилиши сабабли, ҳисоблаш имконияти чекланган муҳитлар учун ноқулайдир. Шунинг учун, булутли ҳисоблаш тизимларда аутентификацияни, авторизацияни турли муҳитларда амалга ошириш имкониятини тақдим этувчи OpenID Connect протоколи танлаб олинди.

1-жадвал

SSO технологиясини амалга ошириш протоколларининг таҳлили

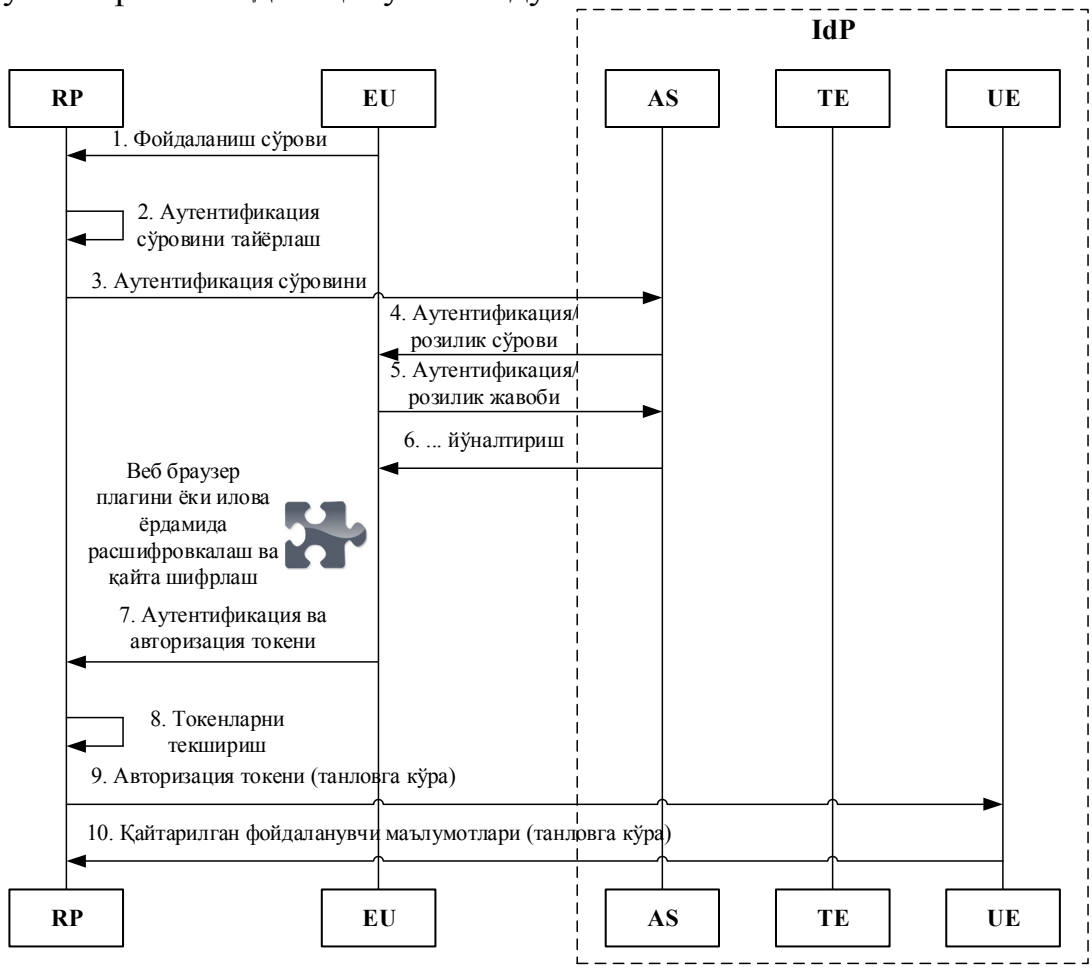
	Аутентификация	**Авторизация**	**Токен формати**	**Фойдаланувчи розилигини сўраш**	**Токен муддати**
OAuth2	Йўқ*	Бор	XML ёки JSON	Бор	Танловга кўра
OpenID Connect	Бор	Бор	JSON	Бор	Бор
SAML 2.0	Бор	Бор	XML	Йўқ	Бор
LDAP	Бор	Бор	?	Йўқ	Йўқ
CAS	Бор	Йўқ	XML	Йўқ	?
CoSign 3	Бор	Йўқ	XML	Йўқ	?

Изоҳ: *жадвалдаги ? белгиси - маълумот номаълумлигини англатса, * белгиси авторизация учун аутентификациядан ўтказилиши, лозимлигини яъни алоҳида аутентификация муолажасининг мавжуд эмаслигини кўрсатади.*

OpenID Connect протоколи OAuth2 протоколига асосланган ва ундан аутентификациялаш ва шахсий маълумотларни алмашиниш имконияти мавжудлиги билан фарқ қилади. OpenID Connect протоколи 3 та қисмпротоколдан (протокол тавсифида “flow” деб аталган) иборат: асос қисмпротокол (Authorization Code Flow), яширин қисмпротокол (Implicit Flow) ва гибрид қисмпротокол (Hybrid Flow).

OpenID Connect протоколини таҳлиллаш соҳа изланувчилари томонидан бир неча ҳолатлар бўйича амалга оширилган. OpenID Connect протоколи тавсифида одатда аутентификация усули сифатида “бирор нарсани билишга” асосланган ёндашув ёритилган. Бироқ, ушбу аутентификация усули ISO/IEC 29115 стандартида келтирилган 4 даражали тизимда, иккинчи даражага тегишлидир. Олинган таҳлил натижаларига кўра эса фойдаланилган усул учинчи ёки тўртинчи сатҳга тегишли бўлишлиги талаб этилади. Диссертациянинг 3 ва 4 боблари айнан OpenID Connect протоколи учун аутентификация протоколларини ишлаб чиқишга бағишланган. Бундан ташқари, фойдаланувчиларнинг шахсий маълумотлари (исми, фамилияси, профил маълумоти, расми, кредит карта рақами ва бошқалар) IdP провайдерига хавфсиз тарзда узатилиши амалга оширилмаган. Ушбу хавфсизлик муаммосини олдини олиш учун фойдаланувчи шахсий маълумотларини шифрлаш талаб этилади. Ушбу талабни амалга оширувчи

OpenID Connect протоколининг яширин қисмпротоколида шахсий маълумотларни шифрлаш тартиби 1-расмда келтирилган. Бу ерда, RP (Relying Party) – хизматлар провайдери, EU (End User) – (хизматдан) фойдаланувчи, IdP (Identity Provider) – идентификация провайдери, AS (Authorization Server) – авторизация сервери, TE (Token Endpoint) – токенларни генерациялаш модули, UE (UserInfo Endpoint) – фойдаланувчилар маълумотларини тақдим қилувчи модул.



1-расм. Яширин қисмпротоколда шахсий маълумотларни шифрлаш

OpenID Connect протоколини ҳужжатлаштириш ва амалга ошириш жараёнида кузатилган таҳдидларни олдини олиш учун таклиф этилган ёндашувлар ва тавсиялар 2-жадвалда келтирилган омиллар бўйича таснифланди.

2-жадвал

Таклиф этилган ёндашувларнинг мавжудлари билан қиёсий таҳлили

№	Манбалар	Протокол	Хавфсизлик таҳлили	Шахсийлик таҳлили	Токен	Крипто-графия	Протокол-лар	Такомил-лаштириш	Сиёсат, тавсия
1	2	3	4	5	6	7	8	9	10
1.	Ҳу ва бошқалар	OAuth	+						
2.	Янг ва манохаран	OAuth	+						

3.	Бансал ва бошқалар	OAuth	+						
4.	Чари ва бошқалар	OAuth	+						
5.	Фетт ва бошқалар	OAuth	+						
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
6.	Янг ва бошқалар	OAuth	+		+			+	
7.	Биррел ва Шнеидер	Кўплаб		+					
8.	Маинка ва бошқалар	OIDC	+		+			+	
9.	Маинка ва Счвенк	OIDC	+						
10.	Вернер ва Вестҳалл	OIDC				+			+
11.	Фетт ва бошқалар	OIDC	+		+		+	+	
12.	Ҳалпин Ҳ.	OIDC				+	+		
13.	Вайнгертнер ва Вестфалл	OIDC		+		+	+		
14.	Li ва бошқалар	Кўплаб	+					+	
15.	Li ва бошқалар	OIDC	+	+					+
16.	Навас Й., Бельтран М.	OIDC	+	+	+	+	+	+	+
17.	Таклиф этилган ёндашув	OIDC	+	+	+	+	+	+	+

Қиёсий таҳлил натижалари таклиф этилган ёндашувнинг амалий ва назарий ҳимоя чораларига эгалигини кўрсатди.

Диссертация ишининг «**Булутли ҳисоблаш тизимларида фойдаланувчиларни аутентификациялаш усуллари ва алгоритмлари**» номли учинчи боби булутли тизимларда ISO/IEC 29115:2013 стандартига мос, эллиптик эгри чизиқларга асосланган аутентификация усулини ишлаб чиқишга ва уни хавфсизликка баҳолашга бағишланган.

Очиқ калитли криптографик алгоритмлар амалда фойдаланувчиларни аутентификациялаш, хабар яхлитлиги таъминлаш ва DDoS хужумларидан ҳимоялаш учун қўлланилади. Очиқ калитли криптографик алгоритмлар орасида эллиптик эгри чизиққа (Elliptic curve cryptography, ECC) асосланганлари бардошлигини йўқотмасдан юқори ҳисоблаш самарадорлигига эгалиги билан ажралиб туради. Чекли Z_q $(q > 2^{160})$ майдонда $E_q(a,b)$ эллиптик эгри чизиқ тенгламаси $y^2 mod q = x^3 + ax + b(mod q)$ билан ифодаланиб, бу ерда q – катта туб сон ва a ва b лар икки ўзгармас $(a, b \in Z_q)$ бўлиб, $4a^3 + 27b^2 \neq 0$ шартни қаноатлантириши шарт. Агар P эллиптик эгри чизиқдаги n $(n > 2^{160})$ тартибга эга асос нуқта ва $\emptyset$ - чексизликдаги нуқта бўлса, у ҳолда $n \times P = \emptyset$ шарт ўринли. Бу ерда, P – ЕССдаги нуқта бўлиб, (x, y) координата қийматлари билан характерланади. × - нуқтани скалярга кўпайтириш амали.

Теорема. Фараз қилинсин $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ нуқталар $E_q(a,b)$ эллиптик эгри чизиқда ётсин. У ҳолда $E_q(a,b)$ эллиптик эгри чизиқда ётувчи $P_3 = P_1 + P_2 = (x_3, y_3)$ нуқта қуйидагича ҳисобланади:

$$P_1 + P_2 = \begin{cases} O_\infty \text{ агар } x_1 = x_2 \& y_1 = -y_2 \\ (x_3, y_3) \text{ бошқа ҳолларда} \end{cases}$$

бу ерда,

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

ва

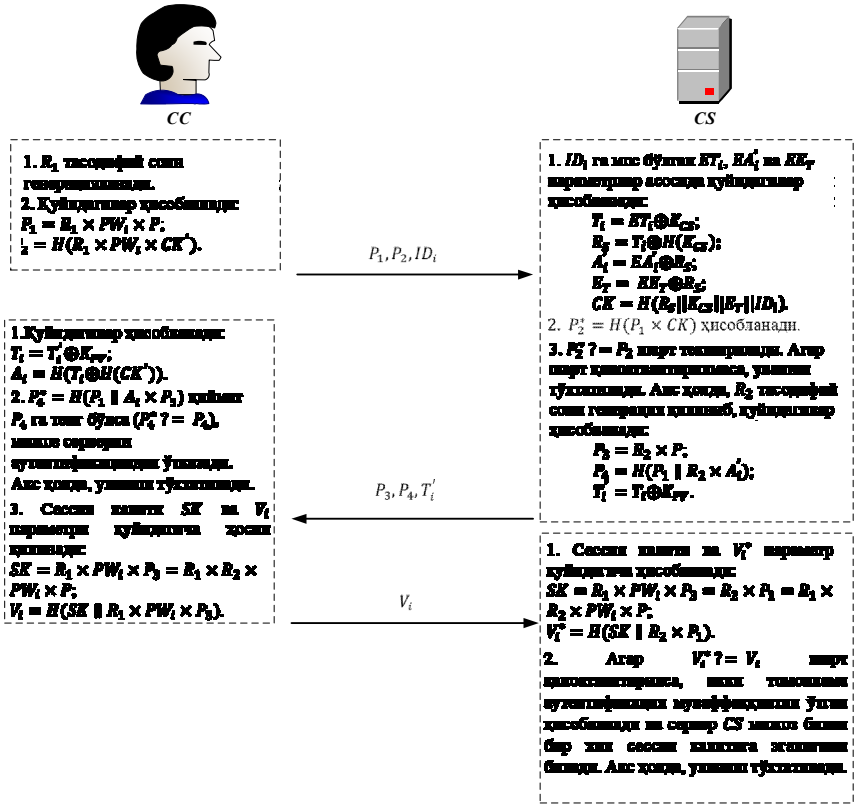
$$\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} \text{ агар } P_1 = P_2 \\ \dfrac{y_2 - y_1}{x_2 - x_1} \text{ бошқа ҳолларда} \end{cases}$$

Таъриф. *Эллиптик эгри чизиқда дискрет логарифм муаммоси ((ECDLP: Elliptic Curve Discrete Logarithm Problem):* берилган $P, Q \in E_g$ нуқталар учун $Q = m \times P$ тенгликдан $m \in [1, n-1]$ бутун сонни топиш мураккаб.

Юқоридаги таърифдан, $Q = m \times P$ тенгликдан Q, P берилган ҳолда m ни топиш мураккаб ҳисоблашларни талаб қилиши, яъни исботланган бардошликка эгалигини кўриш мумкин.

ECC асосида аутентификациялаш усуллари, калит узунлигининг кичикларида ҳам юқори бардошликни таъминлаши сабабли, булутли ҳисоблаш тизимларидаги турли ҳисоблаш имкониятига эга воситалар учун ҳам мос ҳисобланади. Бошқа аутентификация протоколлари каби ECCга асосланган протоколларни баҳолашда қатор омилларни инобатга олиш талаб этилади. Хусусан, протокол турли хавфсизлик талабларига жавоб бериши ҳисоблашлардаги, тармоқдаги юклама, сақлашдаги юкламалар ва ҳисоблаш вақти каби омиллар асосида баҳоланди. Бундан ташқари, хавфсизликни расмий таҳлилашнинг автоматлаштирилган воситаларидан (масалан, AVISPA, Scyther) кенг фойдаланилди.

Таклиф этилган ECCга асосланган аутентификация протоколи рўйхатдан ўтиш, аутентификациядан ўтиш ва паролни алмаштириш босқичларидан иборат. 2-расмда протоколнинг аутентификациядан ўтиш босқичи келтирилган.



2-расм. Протоколнинг аутентификациядан ўтиш босқичи

Бу ерда, CC_i –булутли ҳисоблаш тизими мижози (Cloud Client), CS – булутли ҳисоблаш тизими сервери (Cloud Server), ID_i – мижоз идентификатори, PW_i – фойдаланувчи пароли, PV_i- парол тасдиғи (password verifier), P – эллиптик эгри чизиқдаги нуқта.

Таклиф этилган протокол хавфсизлигининг формал таҳлили AVISPA (Automated Validation of Internet Security Protocols and Applications) воситаси асосида амалга оширилди. Протокол AVISPA нинг хавфсизлик протоколи аниматори (Security Protocol Animator for AVISPA, SPAN) ёрдамида OFMC ва CL-AtSe режимида таҳлилланди. Таҳлил натижаси ишлаб чиқилган протоколнинг турли хавфсизлик таҳдидларига, хусусан, такрорлаш ва ўртада турган одам ҳужумига, бардошли эканлигин кўрсатди.

Ишлаб чиқилган протокол хавфсизлигининг ноформал таҳлили амалга оширилди ва мавжудлари билан таққосланди. Ноформал таҳлил, (T1) икки томонлама аутентификациялаш имконияти, (T2) такрорлаш ҳужуми, (T3) паролга фараз бўйича ҳужум, (T4) ўртада турган одам ҳужуми, (T5) обрўсизлантириш ҳужумлари, (T6) сеанс калитини тақсимлаш имконияти ва (T7) тўла тўкис хавфсизлик талаби омиллари асосида амалга оширилди (3-жадвал).

3-жадвал

Протоколларнинг қиёсий таҳлили (“+” – талабни қаноатлантиради, “-” – талабни қаноатлантирмайди, “NA” – талаб инобатга олинмаган)

№	Протокол	T1	T2	T3	T4	T5	T6	T7
1.	С.К.Ҳафизул ва бошқалар.	+	+	NA	+	+	+	+
2.	Ю.П.Лиао ва бошқалар.	-	+	NA	-	-	+	+
3.	С.Калра ва бошқалар.	-	+	-	-	-	-	-
4.	С.Чанг ва бошқалар.	+	+	-	+	-	+	+
5.	K.Wang ва бошқалар.	+	+	-	+	-	+	+
6.	С.Кумари ва бошқалар.	+	+	+	+	-	+	+
7.	С.Бҳубанешвари ва бошқлар.	-	+	+	-	-	-	-
8.	Таклиф этилган протокол	+	+	+	+	+	+	+

Бундан ташқари, таклиф этилган протоколни амалга ошириш омиллари бўйича мавжудлари билан қиёсий таҳлили амалга оширилган. Ушбу омиллар қуйидагилар:

- протоколдаги ҳисоблашлар сони;
- протоколда узатилаётган маълумотлар ҳажми;
- протокол иштирокчиларида сақланадиган маълумот ҳажми.

Рўйхатга олиш ва аутентификация босқичлари учун хисоблашлар сони бўйича таҳлил натижалари 4-жадвалда келтирилган. Бу ерда, $N_{\text{х}}$ – хешлаш, $N_{\text{н.қ.}}$ – эллиптик эгри чизиқда нуқталарни қўшиш ва $N_{\text{н.к}}$ – эллиптик эгри чизиқда нуқтани скалярга кўпайтириш амаллари сони. Олинган натижалар таклиф этилган протоколни мавжуд протоколларга нисбатан ҳисоблашлар сони бўйича юқори самарадорликка эгалигини кўрсатди.

Протоколда узатилаётган маълумотлар ҳажми муҳим, уни ҳисоблашда аутентификация жараёнларида узатилаётган хабарларнинг сони ва уларнинг узунлигини билиш талаб этилади. Таклиф этилган ва танланган мавжуд протоколлар криптографик хэш функция ва эллиптик эгри чизиқларга асосланган боис, ҳисоблашлар учун 256 бит хэш қийматни генерация қилувчи ихтиёрий хэш функция ва 160 бит ўлчамга эга эллиптик эгри чизиқ параметрлари олинган. Бундан ташқари, тасодифий танланган қийматлар ва идентификатор қиймати ҳам 160 бит бўлган тақдирда, протоколда узатилаётган маълумотларнинг умумий ҳажми 1952 битга тенг бўлади.

4-жадвал

Протоколларнинг ҳисоблашлар сони бўйича таҳлили

№	Протокол	Булутли фойдаланувчи	Булутли сервер	Умумий
1.	С.К.Ҳафизул ва бошқалар.	$3N_{\text{х}} + 2N_{\text{н.қ.}} + 3N_{\text{н.ск}}$	$4N_{\text{х}} + 2N_{\text{н.қ.}} + 5N_{\text{н.ск}}$	$7N_{\text{х}} + 4N_{\text{н.қ.}} + 8N_{\text{н.ск}}$
2.	Ю.П.Лиао ва бошқалар.	$3N_{\text{н.қ.}} + 5N_{\text{н.ск}}$	$3N_{\text{н.қ.}} + 3N_{\text{н.ск}}$	$6N_{\text{н.қ.}} + 8N_{\text{н.ск}}$
3.	С.Калра ва бошқалар.	$4N_{\text{х}} + 3N_{\text{н.ск}}$	$8N_{\text{х}} + 5N_{\text{н.ск}}$	$12N_{\text{х}} + 8N_{\text{н.ск}}$
4.	С.Чанг ва бошқалар.	$5N_{\text{х}} + 4N_{\text{н.ск}}$	$9N_{\text{х}} + 6N_{\text{н.ск}}$	$14N_{\text{х}} + 10N_{\text{н.ск}}$
5.	K.Wang ва бошқалар.	$5N_{\text{х}} + 4N_{\text{н.ск}}$	$7N_{\text{х}} + 5N_{\text{н.ск}}$	$13N_{\text{х}} + 9N_{\text{н.ск}}$
6.	С.Кумари ва бошқалар.	$4N_{\text{х}} + 5N_{\text{н.ск}}$	$8N_{\text{х}} + 6N_{\text{н.ск}}$	$12N_{\text{х}} + 11N_{\text{н.ск}}$
7.	С.Бҳубанешвари ва бошқлар.	$5N_{\text{х}} + 5N_{\text{н.ск}}$	$6N_{\text{х}} + 5N_{\text{н.ск}}$	$11N_{\text{х}} + 10N_{\text{н.ск}}$
8.	Таклиф этилган протокол	$5N_{\text{х}} + 4N_{\text{н.ск}}$	$9N_{\text{х}} + 5N_{\text{н.ск}}$	$14N_{\text{х}} + 9N_{\text{н.ск}}$

Протоколлар яратиш жараёни иштирокчиларида сақланадиган маълумотларнинг ҳажми ҳам муҳим ҳисобланади. Таклиф этилган протоколда фойдаланувчининг рўйхатдан ўтиш жараёнида куки маълумоти CK' ни махфий сақлаш талаб этилади. Мазкур параметр эллиптик эгри чизиқ нуқтаси бўлгани ва унинг ўлчами сифатида 160 бит танлаб олингани боис, фойдаланувчи маълумотларни сақлаш учун 320 бит хотира талаб қилинади.

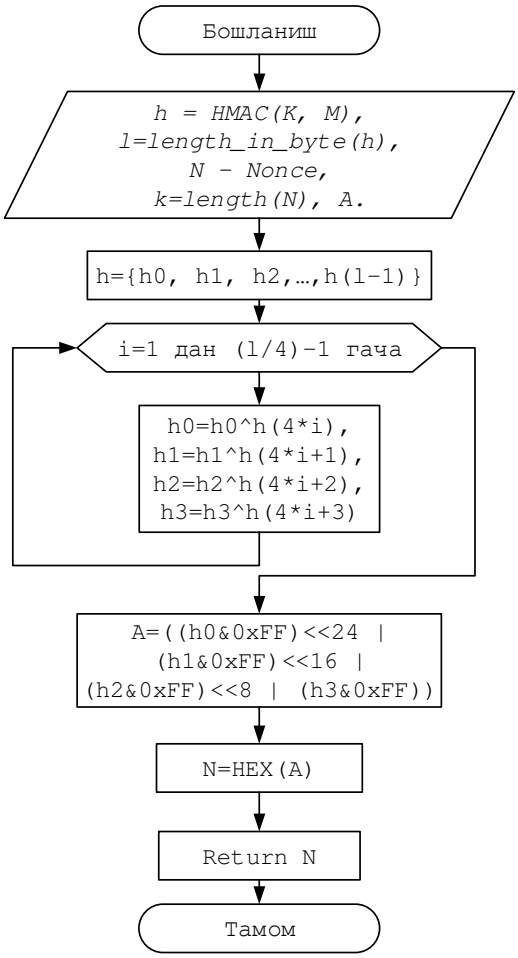
Диссертациянинг «**Мобил булутли ҳисоблаш тизимларида фойдаланувчиларни аутентификациялаш»** номли тўртинчи боби мобил булутли тизимлар учун мос аутентификация усулини ишлаб чиқиш ва таҳлиллаш масаласига бағишланган.

Мобил булутли ҳисоблаш тизимларида аутентификация усуллари одатий булутли ҳисоблаш тизимларидаги усуллардан бир неча фарқли томонларга эга. Хусусан, ресурс чекланганлиги, мобил қурилма сенсорлари, юқори мобиллик ва тармоқнинг хилма – хиллиги уларнинг асосийлари ҳисобланади. Келтирилган ресурс чекланганлигини инобатга олган ҳолда, мобил булутли тизимлар учун аутентификация усулини ишлаб чиқишда мос

сенсорларни танлаш ва амалга оширишда самарадорликка эътибор бериш шарт. Шу боис, ушбу бобда QR (Quick Response) технологияси асосида “савол-жавоб” (challenge-response) механизмидаги аутентификация протоколи таклиф этилган.

Одатда, ноёб саволга ноёб жавобни олиш учун криптографик хеш функциялардан фойдаланилади. Криптографик хеш функцияларга нисбатан қўйилган талабдан (агар $x \neq y$ бўлса, $h(x) \neq h(y)$ тенглик бажарилиши шарт) фойдаланиб, ноёб кириш учун ноёб чиқиш қийматини олиш мумкин. Одатдаги хеш функциялар маълумотни фақат кирувчи қиймат сифатида талаб қилади. “Савол-жавоб” механизмида эса берилган саволга махфий сирни бириктириш талаб этилади. Бошқача айтганда, томонлар орасида тақсимланган калит ва параметрларни савол билан бириктиришдан олинган хэш қиймат талаб этилади. Бу масалани ечишда маълумотларни аутентификациялаш кодлари (Message authentication code, MAC) деб номланувчи криптографик тизимлардан фойдаланилади. MAC тизимига яққол мисол сифатида HMAC (Hashed-MAC) алгоритмини келтириш мумкин.

Таклиф этилган протоколда ҳам берилган саволга жавоб топишда HMAC алгоритмидан фойдаланилган, бунда ҳосил бўлган хэш қийматни қисқартириш (мазкур ҳолда 32 бит) муҳим жиҳат ҳисобланади. Шу боис, 32 битга каррали узунликдаги хэш қийматни 32 битга зичлаш учун 3-расмда келтирилган алгоритмдан фойдаланилди.



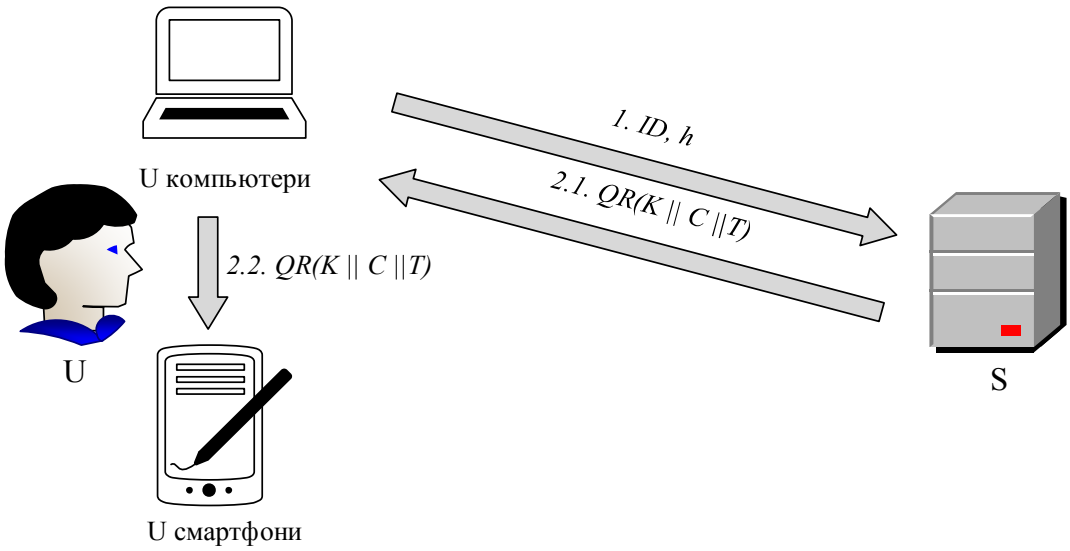
3-расм. Зичлаш

Хабарни аутентификациялашда маълумот ва калит маълум қоида асосида бириктирилади. Таклиф этилаётган аутентификация усулида HMAC усулидан фойдаланилди.

Умумий ҳолда таклиф қилинаётган аутентификация протоколи учун қуйидаги белгилашлар ўринли: ID – фойдаланувчи идентификатори, мажбурий параметр; U – фойдаланувчи, аутентификациядан ўтувчи; S – сервер, текширувчи; SQ – савол, мажбурий параметр, сервер томонидан генерацияланади ва фойдаланувчига юборилади; UQ – савол, мажбурий параметр, фойдаланувчи томонидан генерацияланади ва серверга юборилади; C – сон танлови, танловга кўра фойдаланилувчи параметр, ҳар иккала томонда ҳам синхрон бўлиши талаб этилади; K – фойдаланувчи ва сервер орасида тақсимланган калит, махфий сақланиши шарт; T – вақт

алгоритмининг блок схемаси созланмалари, танловга кўра фойдаланилувчи параметр, ҳар иккала томонда ҳам синхрон бўлиши талаб этилади; P – парол ёки ПИН код, танловга кўра, аутентификация усулидан алоҳида фойдаланилганида ишлатилади; $QR(M)$ – бирор M маълумотнинг QR код шакли; $F(K,M)$ – бирор M ва калит K асосида жавобни ҳосил қилувчи функция ва $F(K,M) = F_{Trunc}(HMAC(K,M))$ га тенг; $\Longrightarrow$ - томонлар орасида хавфсиз боғланиш мавжуд канал; $\rightarrow$ - одатий канал.

Ушбу аутентификация усулида бир томонлама ва икки томонлама аутентификациялаш режимлари мавжуд. Бир томонлама аутентификация усули фойдаланувчини сервер томонидан ҳақиқийлигини текширишда ишлатилади. Икки томонлама аутентификация усулига биноан фойдаланувчини сервер томонидан ва серверни фойдаланувчи томонидан ҳақиқийлиги текширилади. Ҳар иккала режим ҳам икки босқичдан: фойдаланувчини рўйхатдан ўтказиш ва аутентификация босқичларидан иборат. Рўйхатдан ўтиш босқичи ҳар иккала режим учун бир хил (4 – расм).

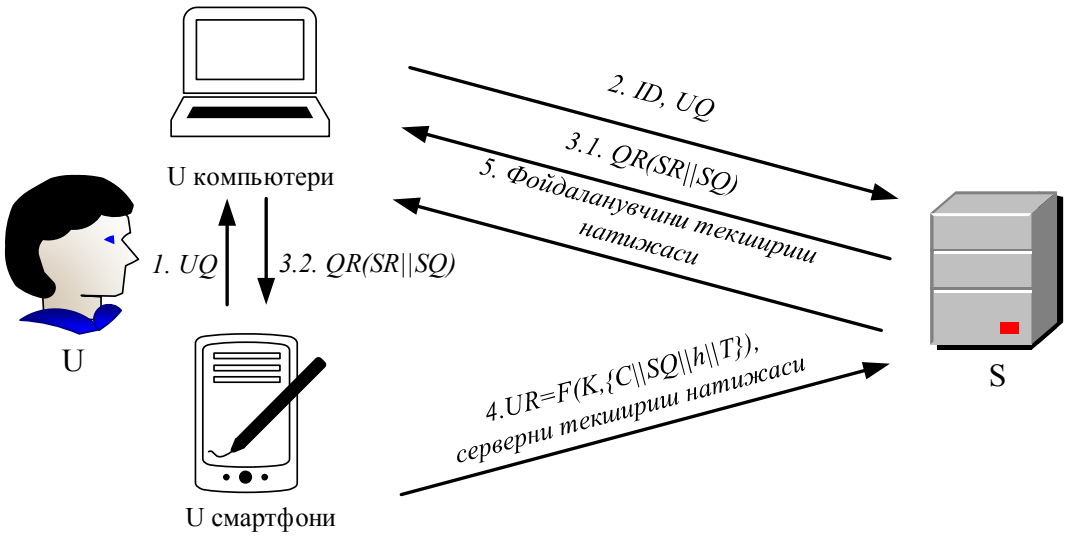


4-расм. “Савол-жавобга” асосланган аутентификациянинг рўйхатдан ўтиш босқичи

Икки томонлама “савол-жавобга” асосланган аутентификация усулига биноан аутентификациядан ўтиш босқичида фойдаланувчи ва сервер орасида h, K, C ва T параметрлар бир хил бўлиши талаб қилинади (5-расм). Хэш функция, H() сифатида ихтиёрий бардошли криптографик хеш алгоритмлардан фойдаланиш мумкин. Буларга мисол сифатида, SHA256, SHA512, Blake2, Blake3, Ripedm, GOST R 34.11-2012, O‘z DSt 1106:2009 алгоритмларини келтириш мумкин. Таклиф этилган протоколнинг дастурий таъминотини ишлаб чиқиш ва таҳлил қилиш мақсадида SHA256 алгоритми танлаб олинди.

Мобил булутли тизимлар учун ишлаб чиқилган аутентификация протоколининг хавфсизлик ва самарадорлик нуқтаи назаридан таҳлиллаш

муҳим ҳисобланади. Шу боис, протокол хавфсизлигининг формал тасдиғи Интернет протоколлари ва иловаларининг автоматлашган тасдиғи AVISPA воситаси ёрдамида амалга оширилди.



5-расм. Икки томонлама “савол-жавобга” асосланган аутентификация босқичи

Ишлаб чиқилган мобил булутли тизимларда фойдаланилувчи аутентификация протоколи AVISPA хавфсизлик протоколи аниматори (Security Protocol Animator for AVISPA, SPAN) ёрдамида OFMC ва CL-AtSe режимида таҳлилланди. Таҳлил натижалари таклиф этилган протоколнинг ҳар иккала режими (бир томонлама ва икки томонлама аутентификациялаш) турли хавфсизлик таҳдидларига, хусусан, такрорлаш ва ўртада турган одам ҳужумларига бардошли эканлигини кўрсатди.

Бундан ташқари, ишлаб чиқилган булутли ҳисоблаш тизимларида аутентификациялаш протоколлар хавфсизлигининг ноформал тасдиғи икки томонлама аутентификациялаш имконияти, такрорлаш ҳужуми, паролга фараз бўйича ҳужум ва ўртага турган одам ҳужуми, омиллари бўйича CHAP (Challenge Handshake Authentication Protocol), CRAM (Challenge-Response Authentication Mechanism), SCRAM (Salted Challenge Response Authentication Mechanism) протоколларига нисбатан юқори хавфсизликка эгалигини кўрсатди.

Протоколдаги ҳисоблашлар (ҳисоблашлар сони сифатида N_x – хешлашлар сони танлаб олинди) сони бўйича таклиф этилган протокол SCRAM протоколидан 2,5 марта кам, фақат бир томонлама аутентификацияни таъминловчи CHAP ва CRAM протоколларидан 2 марта кўп ҳамда OCRA (OATH Challenge-Response Algorithm) протоколи билан бир хил натижани қайд этганлигини кўрсатди.

Протоколда узатилаётган маълумот ҳажмига кўра амалга оширилган таҳлил натижаси таклиф этилган протоколнинг OCRA, CRAM протоколлари билан бир хил натижа қайд этганлиги ва SCRAM протоколидан 160 бит кам ахборот юборганлигини кўриш мумкин. Шунингдек, протокол иштирокчиларида сақланадиган маълумот ҳажми ва уни сақлаш тартибига

нисбатан олиб борилган таҳлил натижаси, CHAP, CRAM, SCRAM протоколларида фойдаланувчи паролни хотирасида сақлаши талаб этишини кўрсатган бўлса, OCRA ва таклиф этилган протокол учун криптографик калитдан фойдаланилишини кўрсатди. Шунинг учун, ушбу икки протокол паролга қаратилган фараз бўйича ҳужумларга бардошли ҳисобланади. Бошқа томондан, криптографик калит сифатида мураккаб паролдан фойдаланиш ёки калитни хавфсиз сақлаш талаби қўйилади. Шу сабабли, таклиф этилган протоколда криптографик калитни мобил иловада махсус дастурий воситада сақлаш амалга оширилган.

ХУЛОСА

«Булутли ҳисоблаш тизимларида фойдаланувчиларни аутентификациялаш усуллари ва алгоритмлари» мавзусидаги диссертация иши бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Булутли ҳисоблаш тизимларида мавжуд таҳдидлар STRIDE методологияси ва ҳужумлар OWASP ташкилоти томонидан келтирилган омиллар бўйича таҳлилланди. Таҳлил натижасида булутли ҳисоблаш тизимларида мавжуд муаммоларни олдини олишда фойдаланувчиларнинг ҳақиқийлигини текширишнинг самарали ва хавфсиз ечимини яратишнинг мақсадга мувофиқлиги асосланган.
2. Таҳлил натижасида танланган OpenID Connect протоколида мавжуд шахсий маълумотларни хавфсиз узатиш билан боғлик муаммоларни шифрлашга асосланган ҳолда бартараф этиш схемаси яратилди. Натижада фойдаланувчининг шахсий маълумотларини очиқ калитли криптографик алгоритмлари ёрдамида шифрлаш имконияти яратилди.
3. Булутли ҳисоблаш тизимлари учун фойдаланувчиларнинг ҳақиқийлигини текширишнинг эллиптик эгри чизиққа асосланган усули ишлаб чиқилган. Ишлаб чиқилган усул хавфсизлигининг формал ва ноформал таҳлили унинг такрорлаш, паролга фараз бўйича, ўртага турган одам ва обрўсизлантириш ҳужумларига бардошлигини ҳамда мавжуд усулларга нисбатан 1,16 марта кам вақт сарфини қайд этди.
4. Мобил булутли ҳисоблаш тизимларида фойдаланувчиларнинг ҳақиқийлигини текширишнинг “савол-жавоб” механизмига асосланган усули ишлаб чиқилди. Ишлаб чиқилган икки томонлама аутентификациялаш протоколи ҳисоблашлар сони бўйича SCRAM протоколига нисбатан 2,5 марта юқори самарадорлик қайд этди.
5. Ишлаб чиқилган эллиптик эгри чизиққа асосланган икки томонлама аутентификациялаш усуллари ёрдамида OpenID Connect протоколи такомиллаштирилди. Натижада OpenID Connect биргина фойдаланишли аутентификация тизими кўп сонли қайд ёзувларини ягона махфий параметр билан бошқариш ва паролни эсда сақлаш билан боғлиқ муаммоларни камайтириш имконини берди.

**НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.T.07.01
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ЗОКИРОВ ОДИЛЖОН ЁКУБЖОН УГЛИ

МЕТОДЫ И АЛГОРИТМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМАХ ОБЛАЧНОГО ВЫЧИСЛЕНИЯ

05.01.05 – Методы и системы защиты информации. Информационная безопасность.

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ
ДОКТОРА ФИЛОСОФИИ (PhD) ПО ТЕХНИЧЕСКИМ НАУКАМ**

Ташкент-2020

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2020.3.PhD/T1892.

Диссертация выполнена в Ташкентском университете информационных технологий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице научного совета (www.tuit.uz) и на Информационно-образовательном портале «ZiyoNet» (www.ziyonet.uz).

Научный руководитель:	**Ганиев Салим Каримович** доктор технических наук, профессор
Официальные оппоненты:	**Каримов Маджит Маликович** доктор технических наук, профессор
	Норматов Шербек Бахтиярович доктор философии технических наукам (PhD)
Ведущая организация:	**«UNICON.UZ» – центр научно-технических и маркетинговых исследований**

Защита диссертации состоится «__» _____2020 года в __ часов на заседании Научного совета DSc.13/30.12.2019.T.07.01 при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №___). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «___» _____ 2020 года.
(протокол рассылки №__ от «___» _____ 2020 года.)

Р.Х. Хамдамов
Председатель научного совета по присуждению ученых степеней, д.т.н., профессор

Ф.М. Нуралиев
Ученый секретарь научного совета по присуждению ученых степеней, д.т.н., доцент

Б.Ф.Абдурахимов

Заместитель председатель научного семинара при научном
совете по присуждению ученых степеней,
д.ф.-м.н. профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации. В результате быстрого роста потребности использования систем облачных вычислений в мире на передний план выдвигаются проблемы, связанные с безопасностью систем облачных вычислений. Уязвимость этих облачных систем объясняется раскрытием персональных данных пользователей, но и корпоративных секретов, а также информации, связанной с собственностью. В частности, по данным компании Statista «В 2019-2020 годах проблема безопасности возглавила список проблем в системе облачных вычислений организаций с показателем 85%»[3]. В облачных системах важную роль при предотвращения несанкционированного использования данных и ресурсов имеют методы аутентификации. В развитых странах, таких как США, Япония, Германия, Южная Корея, Индия и др. уделяется большое внимание сфере разработки методов внедрения облачных систем, методов защиты данных в облачных системах, методов гарантированной аутентификации пользователей.

Во всем мире ведутся исследования по созданию методов и алгоритмов направленных на решение проблем, возникающих при сохранении, обработке и передече, а также при достоверном использовании ресурсов систем облачных вычилений. При этом необходимо уделить особое внимание научным и практическим исследованиям по разработке криптографических алгоритмов, методов, и средств многофакторной аутентификации, что гарантирует легальное использование ресурсов облачных вычислений пользователями.

В нашей республике предпринимаются масштабные меры по обеспечению информационной безопасности, так как в государственных учреждениях, улицах и в общественных местах устанавливаются камеры наблюдения, которые весьма актуальны сегодня. В Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 гг. отмечены задачи, в том числе «...совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[4]. Одной из важных задач при выполнении исследовательских работ является разработка эффективных, безопасных и основанных на паролях методов, и инструментов для проверки подлинности пользователей.

Данное диссертационное исследование, в определенной степени вносит вклад в выполнение задач, предусмотренных Указами Президента Республики

[3] https://www.statista.com/statistics/511283/worldwide-survey-cloud-computing-risks/

[4] Указ Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан»

Узбекистан №УП-4947 от 7 февраля 2017 года «О Стратегии действий по дальнейшему развитию Республики Узбекистан», №УП-5379 от 14 марта 2018 года «О мерах по совершенствованию системы государственной безопасности Республики Узбекистан», №УП-5349 от 19 февраля 2018 года «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций» и Постановлением Кабинета Министров Республики Узбекистан №ПКМ-707 от 05 сентября 2018 года «О мерах по совершенствованию информационной безопасности во всемирной информационной сети интернет» и другими нормативно-правовыми документами, принятыми в данной сфере.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данное исследование выполнено в соответствие с приоритетным направлением развития науки и технологий Республики IV. «Информатизация и развитие информационно-коммуникационных технологий».

Степень изученности проблемы. Многие ученые проводят исследования в области криптографических алгоритмов и разработки методов и инструментов многофакторной аутентификации, обеспечивающих гарантированное использование ресурсов системы облачных вычислений.

В мире большое количество ученых ведут свои научно-исследовательские работы по классификациям методов аутентификации в системах облачных вычислений М.Ализадех, Х.Фарук, С.Дежамфар, С.Лим, по разработке методов аутентификации пользователей, основанных на эллиптических крывых С.Хафизул, Ю.Лиао, С.Калра, С.Чанг, С.Кумари, по разработке методов аутентификации для мобильных систем облачных вычислений Й.Чон, С.Дей, Ф.Омри, К.Бензекки, Д.Шваб, С.Жегадесан, по разработке средств контроля доступа и аутентификации для систем облачных вычислений компании Auth0, AMD Telecom, OpenID, IBM, iSM, WatchGuard.

В Узбекистане со стороны научных групп под руководством П.Ф.Хасанова, М.Арипова, С.К.Ганиева, М.М.Каримова, Д.Е.Акбарова, З.Т.Худойкулова изучены вопросы по анализу защищенности информационных систем, разработке средств аутентификации, совершенствования методов аутентификации и методов безопасной передачи паролей.

Вместе с тем, недостаточно внимания уделяется вопросам верификации пользователей в системах облачных вычислений с применением возможностей мобильных устройств и методов аутентификации, основанных на эллиптических крывых.

Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация. Диссертационное исследование выполнено в рамках научного проекта согласно плану научно-исследовательских работ Ташкентского университета информационных технологий №БФ-Ф4-023 - «Исследование проблем управления инцидентами и

противодействия кибератакам в распределенных информационно-коммуникационных системах» (2017-2020).

Целью исследования является разработка методов и алгоритмов аутентификации пользователей, которые основаны на двухфакторных и криптографических алгоритмах в системах облачных вычислений.

Задачи исследования:

усовершенствование протокола одноразовой аутентификации для систем облачных вычислений;

разработка протокола двусторонней аутентификации на основе эллиптических кривых для систем облачных вычислений;

разработка протокола безопасной аутентификации пользователей для мобильных систем облачных вычислений;

построение одноразовой системы аутентификации на основе разработанных протоколов аутентификации.

Объектом исследования является процесс проверки удостоверения подлинности пользователей в системах облачных вычислений.

Предмет исследования составляет методы и алгоритмы двухфакторной аутентификации, основанные на эллиптических кривых в системах облачных вычислений.

Методы исследования. В процессе исследования использованы алгоритмизация, теория чисел, сравнительный анализ, анализ на безопасность и методы объектно-ориентированного программирования.

Научная новизна исследования заключается в следующем:

усовершенствован протокол одноразовой аутентификации на основе шифрования личных данных и надежных методов аутентификации;

в системах облачных вычислений был разработан протокол двусторонней аутентификации пользователей с учетом преимуществ эллиптических кривых;

разработан протокол двусторонней аутентификации на основе механизма «вопрос-ответ» для мобильных систем облачных вычислений;

усовершенствована одноразовая система аутентификации на основе разработанных протоколов.

Практические результаты исследования заключаются в следующем:

разработаны меры безопасности для предотвращения проблем безопасности в протоколе OpenID Connect;

разработана безопасная структура проверки подлинности пользователей используя преимущества эллиптических кривых в системах облачных вычислений;

разработана система двусторонней аутентификации на основе механизма «вопрос-ответ» в мобильных облачных вычислительных системах;

усовершенствована OpenID Connect система контроля единичного доступа на основе применения разработанных методов аутентификации.

Достоверность результатов исследования. Достоверность результатов исследования подтверждается реальным и экспериментальным анализом, полученным из разработанных методов и алгоритмов для системы аутентификации единичного пользования, базирующейся на эллиптические кривые и возможности мобильных устройств в системах облачного вычисления.

Научная и практическая значимость результатов исследования. Научная значимость полученных результатов исследований объясняется разработкой и совершенствованием методов и алгоритмов для систем аутентификации единичного пользования в системах облачных вычислений, основанных на эллиптических кривых и возможностях мобильных устройств.

Практическая значимость полученных результатов исследования объясняется возможностью снижения угроз для аутентификации пользователей в системах облачных вычислений и выполнения процесса аутентификации по одному паролю для большого количества учетных записей.

Внедрение результатов исследования. На основании полученных научных результатов по разработке методов, алгоритмов и программных средств удостоверения подлинности пользователей в системах облачных вычислений:

программное средство протокола аутентификации пользователей, основанное на эллиптические кривые внедрено в практическую деятельность Государственного унитарного предприятия «UNICON.UZ» - Центр научно-технических и маркетинговых исследований. (справка Министерства по развитию информационных технологий и коммуникаций от 01 декабря 2020 года, №33-8/7322). Предложенный протокол аутентификации показал эффективность в 1,16 раза выше, чем существующие, с точки зрения вычислительного времени в обеих сторон;

усовершенствованная система аутентификации OpenID Connect с единичным пользованием на основе разработанных методов аутентификации была внедрена в ООО «COSCOM» (справка Министерства по развитию информационных технологий и коммуникаций от 01 декабря 2020 года, №33-8/7322). В результате научных исследований система аутентификации OpenID Connect с единичным пользованием позволила управлять многопарольной системой на основе одного секретного параметра и в 4 раза уменьшить проблемы хранения паролей;

программное средство, разработанная на основе методов аутентификации с применением возможностей мобильных устройств, было внедрено в практическую деятельность Агентства государственных услуг (справка Министерства по развитию информационных технологий и коммуникаций от 01 декабря 2020 года, №33-8/7322). Разработанный протокол аутентификации показал в 2,5 раза более высокую эффективность по количеству вычислений, чем протокол SCRAM.

Апробация результатов исследования. Результаты данного исследования были обсуждены на 1 международных и 6 республиканских научно-практических конференциях.

Публикация результатов исследования. По теме исследования опубликовано: 18 научных работ, из них 8 статей в журнальных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе 6 - в иностранных и 2 - в республиканских журналах, а также получены 3 свидетельства о регистрации программных продуктов для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложения. Объем диссертации составляет 107 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснованы актуальность и востребованность темы диссертации, показано соответствие с приоритетными направлениями развития науки и технологий Республики Узбекистан, формулируются цель и задачи, также объект и предмет исследования, изложены научная новизна и практические результаты исследования, обоснована достоверность полученных результатов, раскрыта их теоретическая и практическая значимость, приведен перечень внедрений в практику результатов исследования, сведения об опубликованных работах и структура диссертации.

Первая глава диссертации, озаглавленная как **«Проблемы безопасности в системах облачных вычислений»,** посвящена исследованию таких вопросов, как системы облачных вычислений, их возможности, существующие в них проблемы безопасности, в частности, анализу методов аутентификации пользователей.

В результате быстрого роста технологий хранения данных и развития Интернета компьютерные ресурсы стали дешевле и мощнее, чем раньше, а также появилась возможность использовать их в удобном для пользователей месте. Эта тенденция привела к появлению новой темы под названием облачные вычисления (Cloud Computing). В облачных вычислениях ресурсы (например, процессор и память) могут использоваться в качестве инструмента общества с учетом требований пользователей и Интернета.

Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) перечисляет ключевые особенности технологии облачных вычислений, такие как самообслуживание по запросу, использование сети, агрегирование ресурсов, быстрая гибкость и многомерное обслуживание. Поставщики облачных вычислений предоставляют пользователям ряд услуг и основаны на моделях обслуживания приложений (программное обеспечение как услуга, SaaS), платформенных услуг (платформа как услуга, PaaS) и инфраструктурных услуг (инфраструктура как услуга, IaaS).

В то время как системы облачных вычислений имеют такие преимущества, как снижение затрат, покрытие/гибкость, надежность, удобство использования с мобильных устройств, проблемы конфиденциальности, недостатки в стандартах и проблемы в непрерывном развитии и адаптации являются аспектами, требующими научных исследований.

Результаты анализа угроз в системах облачных вычислений с использованием методологии STRIDE показали, что они в основном сосредоточены на характере раскрытия информации, повышенных привилегиях и изменении. Кроме того, анализ показал, что существующие атаки на облачные системы в основном направлены на нарушение системы аутентификации, системы контроля доступа и раскрытие конфиденциальной информации. Исследования показали необходимость надежного и эффективного контроля доступа, аутентификации пользователей и защиты личной информации для предотвращения этих угроз и атак.

Анализ существующих методов аутентификации, используемых в системах облачных вычислений, выявил необходимость разработки нового метода аутентификации, который будет более надежным и эффективным, чем методы аутентификации на основе пароля. Кроме того, было обнаружено, что существующие методы аутентификации, разработанные для мобильных облачных систем, имеют очевидные проблемы с реализацией, безопасностью и эффективностью. Это подчеркнуло необходимость разработки нового метода аутентификации, который будет эффективным и надежным для мобильных систем облачных вычислений.

Во второй главе диссертации под названием «**Методы контроля доступа в системах облачных вычислений»,** проанализирована безопасность протоколов, основанных на единичном доступе, с целью предотвращения существующих проблем выбран протокол OpenID Connect, определены задачи усовершенствования выбранного протокола.

В настоящее время в системах облачных вычислений и корпоративных организациях аутентификация и авторизация пользователей осуществляется на основе единого использования (Single Sign-On, SSO). Эта технология позволяет пользователям использовать одну учетную запись для доступа к нескольким службам или системам. В настоящее время широко используемые протоколы SSO включают OAuth2, OpenID Connect, SAML, LDAP, CAS, CoSign и другие (Таблица 1).

Таблица 1

Анализ протоколов, реализующих технологию SSO

	Аутентификация	**Авторизация**	**Формат токена**	**Согласие пользователя**	**Срок токена**
OAuth2	Нет*	Есть	XML или JSON	Есть	По выбору
OpenID Connect	Есть	Есть	JSON	Есть	Есть

SAML 2.0	Есть	Есть	XML	Нет	Есть
LDAP	Есть	Есть	?	Нет	Нет
CAS	Есть	Нет	XML	Нет	?
CoSign 3	Есть	Нет	XML	Нет	?

***Примечание**: в таблице знак "?" - если информация неизвестна, знак "*" означает, что для авторизации требуется аутентификация, т.е. отдельной процедуры аутентификации нет.*

Результаты анализа показывают, что в протоколах OAuth2, CAS и CoSign отсутствуют процедуры авторизации или аутентификации. Хотя протокол LDAP используется для создания службы единого входа в локальной сети, это менее интересная область, поскольку не используется в веб-приложениях. Поскольку сам протокол SAML 2.0 предоставляет токен в формате XML, это неудобно для вычислительной среды. Поэтому был выбран протокол OpenID Connect, который предоставляет возможность выполнять аутентификацию, авторизацию в системах облачных вычислений в различных средах.

Протокол OpenID Connect основан на протоколе OAuth2 и отличается от него возможностью аутентификации и обмена личной информацией. Протокол OpenID Connect состоит из трех субпротоколов (называемых «flow» в описании протокола): основного протокола (Authorization Code Flow), протокола скрытой части (Implicit Flow) и протокола гибридной части (Hybrid Flow).

Анализ протокола OpenID Connect проводился по нескольким состояниям со стороны отраслевых исследователей. Описание протокола OpenID Connect обычно основывается на подходе «знания чего-либо» как метод аутентификации. Однако этот метод аутентификации относится ко второму уровню в четырехуровневой системе, указанной в стандарте ISO / IEC 29115. По результатам анализа используемый метод должен относиться к третьему или четвертому уровню. Главы 3 и 4 диссертации посвящены разработке протоколов аутентификации специально для протокола OpenID Connect. Кроме того, личная информация пользователей (имя, фамилия, информация профиля, изображение, номер кредитной карты и т.д.) не была надежно передана провайдеру IdP. Шифрование личной информации пользователя необходимо для предотвращения этой проблемы безопасности. Процедура шифрования личных данных в секретной части протокола OpenID Connect, реализующей это требование, показана на рисунке 1. Здесь RP (Relying Party) - провайдер услуг, EU (End User) – пользователь (услуги), IdP (Identity Provider) - поставщик идентификации, AS (Authorization Server) - сервер авторизации, TE (Token Endpoint) - модуль генерации токена, UE (UserInfo Endpoint) - модуль, предоставляющий информацию о пользователе.

Предлагаемые подходы и рекомендации по предотвращению угроз, наблюдаемых при документировании и реализации протокола OpenID Connect, классифицированы по факторам, перечисленным в таблице 2.

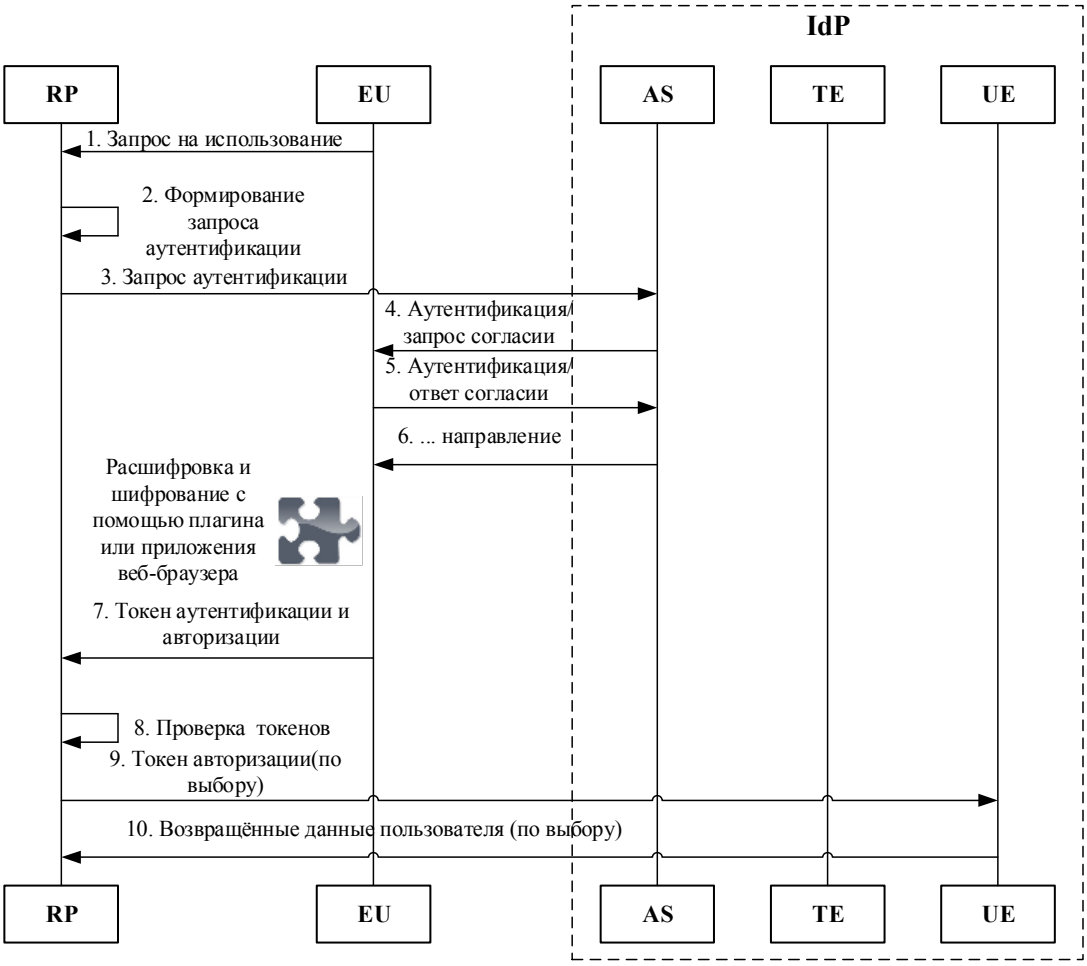


Рис.1. Шифрование персональной информации в скрытом подпротоколе

Таблица 2

Сравнительный анализ предложенного подхода с существующими

№	Источники	Протокол	Анализ безопасности	Анализ персональности	Токен	Криптография	Протоколы	Совершенст-вование	Политика, рекомендации
1	2	3	4	5	6	7	8	9	10
1.	Ху и другие	OAuth	+						
2.	Янг и Манохаран	OAuth	+						
3.	Бансал и дргуие	OAuth	+						
4.	Чари и другие	OAuth	+						
5.	Фетт и другие	OAuth	+						
6.	Янг и другие	OAuth	+		+			+	
7.	Биррел и Шнеидер	Много		+					
8.	Маинка и другие	OIDC	+		+			+	
9.	Маинка и Счвенк	OIDC	+						
10.	Вернер и Вестхалл	OIDC				+			+
11.	Фетт и другие	OIDC	+		+		+	+	
12.	Халпин Х.	OIDC				+	+		
13.	Вайнгертнер и Вестфалл	OIDC		+		+	+		

1	2	3	4	5	6	7	8	9	10
14.	Ли и другие	Много	+					+	
15.	Ли и другие	OIDC	+	+					+
16.	Навас Й., Бельтран М.	OIDC	+	+	+	+	+	+	+
17.	Предлагаемый подход	OIDC	+	+	+	+	+	+	+

Результаты сравнительного анализа показали, что предлагаемый подход имеет практические и теоретические защитные меры.

Третья глава диссертации под названием **«Методы и алгоритмы аутентификации пользователей в системах облачных вычислений»** посвящена разработке методов аутентификации, основанных на эллиптических кривых, которые соответствуют стандарту ISO/IEC 29115:2013 и оценке их безопасности.

Криптографические алгоритмы с открытым ключом используются на практике для аутентификации пользователей, обеспечения целостности сообщений и защиты от DDoS-атак. Среди криптографических алгоритмов с открытым ключом алгоритмы, основанные на эллиптических кривых (Elliptic curve cryptography, ECC), отличаются высокой вычислительной эффективностью без потери устойчивости. В конечном поле Z_q $(q > 2^{160})$ уравнение эллиптической кривой $E_q(a,b)$ представляется как $y^2 mod q = x^3 + ax + b(mod q)$, где q - большое простое число, а a и b являются двумя инвариантами $(a, b \in Z_q)$ и должны удовлетворять условию $4a^3 + 27b^2 \neq 0$. Если P - базовая точка эллиптической кривой с порядком n $(n > 2^{160})$, а $\emptyset$ - точка бесконечности, то условие $n \times P = \emptyset$ выполняется. Здесь P - точка в ECC характеризуется значениями координат (x, y). $\times$ - это операция умножения точки на скаляр.

Теорема. Предположим, что точки $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ лежат на эллиптической кривой $E_q(a,b)$. В этом случае точка $P_3 = P_1 + P_2 = (x_3, y_3)$ лежащая на эллиптической кривой $E_q(a,b)$, рассчитывается следующим образом:

$$P_1 + P_2 = \begin{cases} O_\infty \text{ если } x_1 = x_2 \& y_1 = -y_2 \\ (x_3, y_3) \text{ в иных случаях} \end{cases}$$

здесь,

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

и

$$\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} \text{ если } P_1 = P_2 \\ \dfrac{y_2 - y_1}{x_2 - x_1} \text{ в иных случаях} \end{cases}$$

Определение. *Задача дискретного логарифмирования на эллиптической кривой ((ECDLP: проблема дискретного логарифма эллиптической кривой): Трудно найти целое число* $m \in [1, n-1]$ *из уравнения* $Q = m \times P$ *для заданных точек* $P, Q \in E_g$.

Из приведенного выше определения видно что уравнения $Q = m \times P$ нахождение m при заданном Q, P требует сложных вычислений, то есть имеет подтвержденный стойкость.

Методы аутентификации на основе ECC также подходят для инструментов с различными вычислительными возможностями в системах облачных вычислений, поскольку они обеспечивают высокую стойкость даже при небольшой длине ключа. Как и в случае с другими протоколами аутентификации, при оценке протоколов на основе ECC необходимо учитывать ряд факторов. В частности, соответствие протокола различным требованиям безопасности оценивалось на основе таких факторов, как вычисления, загрузка сети, загрузка хранилища и время вычислений. Кроме того, широко используются автоматизированные инструменты для формального анализа безопасности (например, AVISPA, Scyther).

Предлагаемый протокол аутентификации на основе ECC состоит из шагов регистрации, аутентификации и смены пароля. На рисунке 2 показан этап аутентификации протокола.

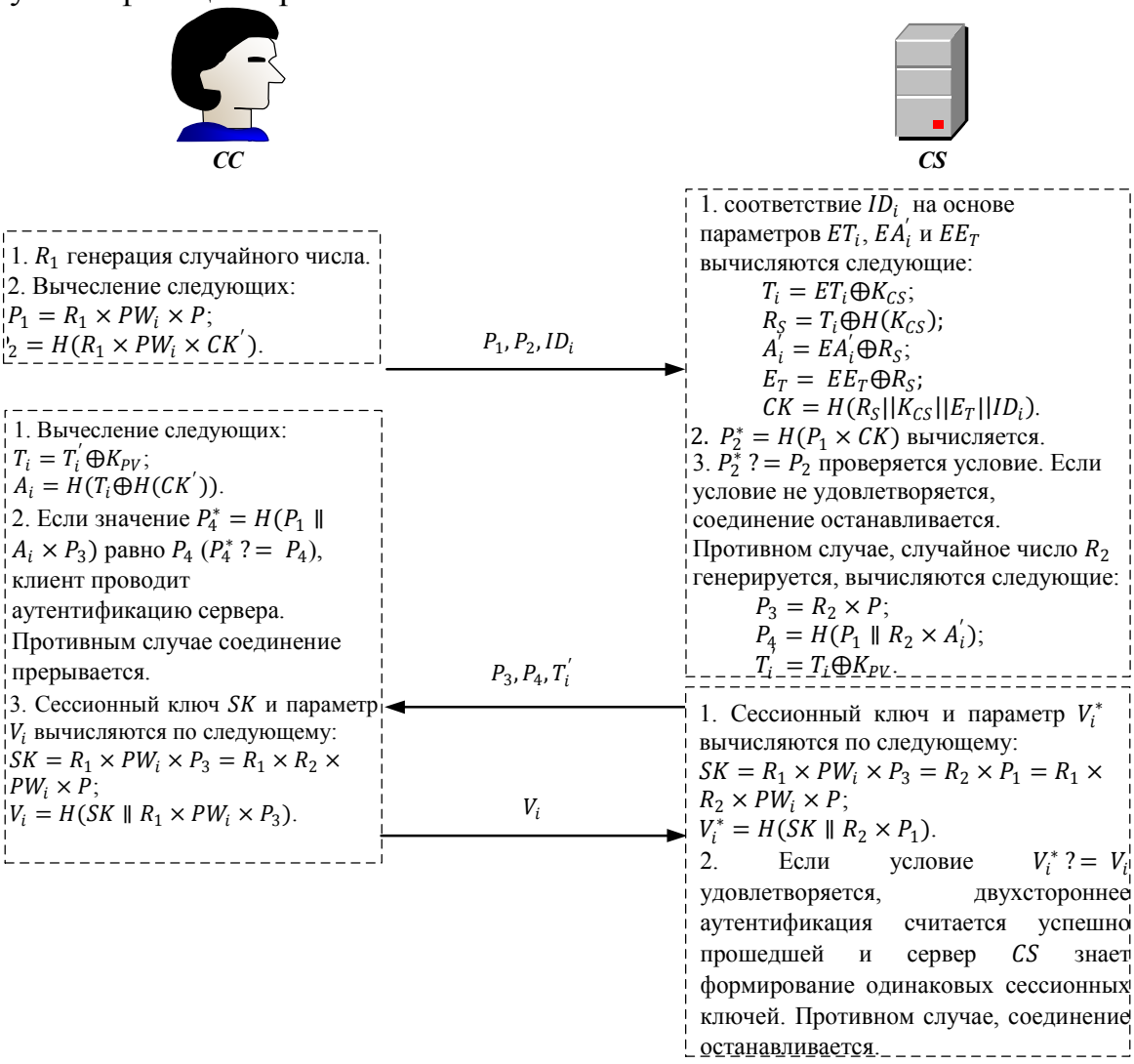


Рис.2. Этапы проведения протокола аутентификации

Здесь CC_i - это облачный клиент (Cloud Client), CS - облачный сервер (Cloud Server), ID_i - это идентификатор клиента, PW_i - пароль пользователя, PV_i – пароль-подтверждение (password verifier), P - точка на эллиптической кривой.

Формальный анализ безопасности предлагаемого протокола был выполнен на основе инструмента AVISPA (Automated Validation of Internet Security Protocols and Applications). Протокол был проанализирован в режимах OFMC и CL-AtSe с использованием AVISPA (Security Protocol Animator for AVISPA, SPAN). Результаты анализа показали, что разработанный протокол устойчив к различным угрозам безопасности, в частности, к атаке повторения и атаке человека посередине.

Проведен неформальный анализ безопасности разработанного протокола и проведено сравнение с существующими. Неформальный анализ выполнен с учетом (T1) возможностей двусторонней аутентификации, (T2) атак повторения, (T3) атак с использованием предположения пароля, (T4) промежуточных атак со стороны человека, (T5) атак компрометации, (T6) возможностей распределения сеансового ключа и (T7) полных коэффициентов требований безопасности (Таблица 3).

Таблица 3

Сравнительный анализ протокола (“+” – удовлетворяет, “-” – неудовлетворяет, “NA” – не учитывается)

№	Протокол	T1	T2	T3	T4	T5	T6	T7
1.	С.К.Хафизул и другие	+	+	NA	+	+	+	+
2.	Ю.П.Лиао и другие	-	+	NA	-	-	+	+
3.	С.Калра и другие	-	+	-	-	-	-	-
4.	С.Чанг и другие	+	+	-	+	-	+	+
5.	K.Wang и другие	+	+	-	+	-	+	+
6.	С.Кумари и другие	+	+	+	+	-	+	+
7.	С.Бхубанешвари и другие	-	+	+	-	-	-	-
8.	Предложенный протокол	+	+	+	+	+	+	+

Кроме того, был проведен сравнительный анализ предложенного протокола с существующими по факторам реализации. Эти факторы включают:

- количество расчетов в протоколе;
- количество данных, передаваемых в протоколе;
- количество информации, хранящейся в участниках протокола.

Результаты анализа количества вычислений для шагов регистрации и аутентификации представлены в таблице 4. Здесь $N_{\text{х}}$ – это процесс хеширования, $N_{\text{н.к.}}$ - количество операций для добавления точек на эллиптической кривой, а $N_{\text{н.к}}$ - количество операций для умножения на скаляр точки на эллиптической кривой. Полученные результаты показали, что предложенный протокол оказался более эффективным по количеству вычислений, чем существующие протоколы.

Объем данных, передаваемых в протоколе, важен, его расчет требует знания количества сообщений, переданных в процессе аутентификации, и их

длины. Поскольку предложенные и выбранные доступные протоколы основаны на криптографической хэш-функции и эллиптических кривых, для расчетов была получена произвольная хэш-функция, генерирующая 256-битные хэш-значения и 160-битные параметры эллиптической кривой. Кроме того, если и случайно выбранные значения, и значение идентификатора составляют 160 бит, общий объем данных, передаваемых в протоколе, будет 1952 бит.

Таблица 4

Анализ протокола по количеству вычислений

№	Протокол	Облачный пользователь	Облачный сервер	Общий
1.	С.К.Хафизул и другие	$3N_{\text{х}} + 2N_{\text{н.к.}} + 3N_{\text{н.ск}}$	$4N_{\text{х}} + 2N_{\text{н.к.}} + 5N_{\text{н.ск}}$	$7N_{\text{х}} + 4N_{\text{н.к.}} + 8N_{\text{н.ск}}$
2.	Ю.П.Лиао и другие	$3N_{\text{н.к.}} + 5N_{\text{н.ск}}$	$3N_{\text{н.к.}} + 3N_{\text{н.ск}}$	$6N_{\text{н.к.}} + 8N_{\text{н.ск}}$
3.	С.Калра и другие	$4N_{\text{х}} + 3N_{\text{н.ск}}$	$8N_{\text{х}} + 5N_{\text{н.ск}}$	$12N_{\text{х}} + 8N_{\text{н.ск}}$
4.	С.Чанг и другие	$5N_{\text{х}} + 4N_{\text{н.ск}}$	$9N_{\text{х}} + 6N_{\text{н.ск}}$	$14N_{\text{х}} + 10N_{\text{н.ск}}$
5.	K.Wang и другие	$5N_{\text{х}} + 4N_{\text{н.ск}}$	$7N_{\text{х}} + 5N_{\text{н.ск}}$	$13N_{\text{х}} + 9N_{\text{н.ск}}$
6.	С.Кумари и другие	$4N_{\text{х}} + 5N_{\text{н.ск}}$	$8N_{\text{х}} + 6N_{\text{н.ск}}$	$12N_{\text{х}} + 11N_{\text{н.ск}}$
7.	С.Бҳубанешвари и другие	$5N_{\text{х}} + 5N_{\text{н.ск}}$	$6N_{\text{х}} + 5N_{\text{н.ск}}$	$11N_{\text{х}} + 10N_{\text{н.ск}}$
8.	Предложенный протокол	$5N_{\text{х}} + 4N_{\text{н.ск}}$	$9N_{\text{х}} + 5N_{\text{н.ск}}$	$14N_{\text{х}} + 9N_{\text{н.ск}}$

Объем хранимых данных важен в процессе создания протокола в участниках. Предлагаемый протокол требует, чтобы пользователь сохранял конфиденциальность информации о файлах куки CK' во время процесса регистрации. Поскольку этот параметр представляет собой точку эллиптической кривой и в качестве его размера выбрано 160 бит, для хранения пользовательских данных требуется 320 бит памяти.

Четвертая глава диссертации под названием «**Аутентификация пользователей в мобильных системах облачных вычислений**», посвящена вопросам разработки и анализа соответствующего метода аутентификации для мобильных систем облачных вычислений.

Методы аутентификации в мобильных системах облачных вычислений имеют несколько аспектов, отличных от методов в традиционных системах облачных вычислений. В частности, основными факторами являются нехватка ресурсов, сенсоры мобильных устройств, высокая мобильность и разнородность сетей. Учитывая ограниченность указанных ресурсов, при разработке метода аутентификации для мобильных облачных систем следует уделять внимание эффективности выбора и внедрения соответствующих датчиков. Поэтому в этой главе предлагается протокол аутентификации в механизме «вопрос-ответ», основанный на технологии QR (Quick Response).

Обычно криптографические хэш-функции используются для получения уникального ответа на уникальный вопрос. Используя требование

криптографических хэш-функций (если $x \neq y$, должно выполняться уравнение $h(x) \neq h(y)$), можно получить уникальное выходное значение для уникального входа. Типичным хэш-функциям требуется информация только как нежелательное значение. В механизме «вопрос-ответ» к вопросу необходимо прикрепить секрет. Другими словами, требуется хэш-значение, полученное путем присоединения ключа и параметров, распределенных между рассматриваемыми сторонами. Для решения этой проблемы используются криптографические системы, называемые кодом аутентификации сообщения (Message authentication code, MAC). Очевидным примером системы MAC является алгоритм HMAC (Hashed-MAC).

Предложенный протокол также использует алгоритм HMAC для ответа на вопрос, при этом важным аспектом является уменьшение результирующего значения хеш-функции (в данном случае 32 бита). Поэтому алгоритм, показанный на рисунке 3, использовался для сжатия хэш-значения кратной длины по 32 бита в 32 бита.

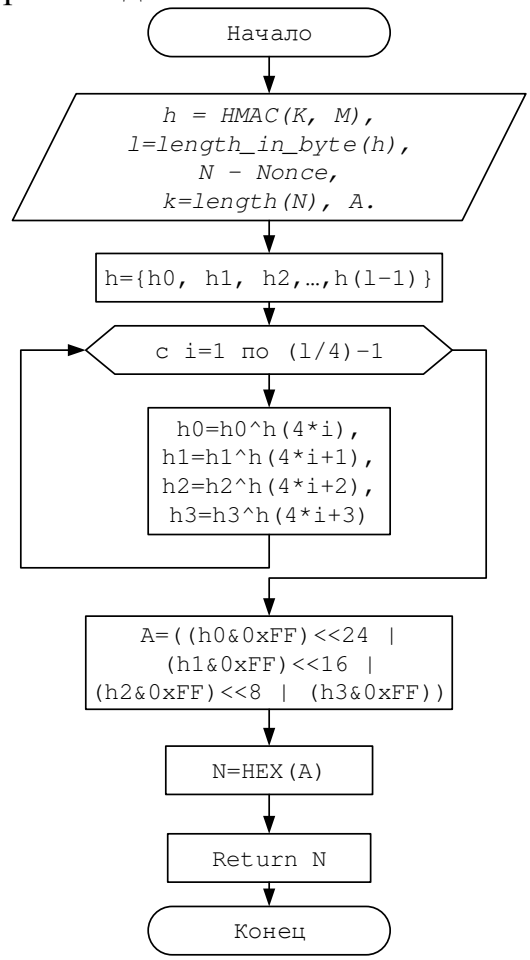


Рис.3. Блок схема алгоритма сжатия

При аутентификации сообщения информация и ключ прикрепляются согласно определенному правилу. Предлагаемый метод аутентификации использует метод HMAC.

В целом предлагаемому протоколу аутентификации подходят следующие определения: ID - идентификатор пользователя, обязательный параметр; U - пользователь, аутентифицированный; S - сервер, контроллер; SQ - вопрос, обязательный параметр, генерируемый сервером и отправляемый пользователю; UQ - вопрос, обязательный параметр, генерируемый пользователем и отправляемый на сервер; C - выбор номера, параметр, используемый в соответствии с выбором, должен быть синхронным с обеих сторон; K - ключ, распределяемый между пользователем и сервером, должен храниться в секрете; T - установка времени, опционально используемая опция, должна быть синхронной с обеих сторон; P - пароль или PIN-код, используется опционально, если метод аутентификации используется отдельно; $QR(M)$ - это форма QR-кода для M данных; $F(K, M)$ -

функция, которая генерирует ответ на основе M и ключа K и равна $F(K,M) = F_{Trunc}(HMAC(K,M))$; $\Longrightarrow$ - канал с защищенным соединением между сторонами; $\rightarrow$ - канал по умолчанию.

Этот метод аутентификации имеет односторонний и двусторонний режимы аутентификации. Односторонний метод аутентификации используется для проверки подлинности пользователя сервером. В соответствии с методом двусторонней аутентификации проверяется аутентификация пользователя сервером и сервером пользователя. Оба режима состоят из двух этапов: регистрации пользователя и аутентификации. Фаза регистрации одинакова для обоих режимов (рисунок 4).

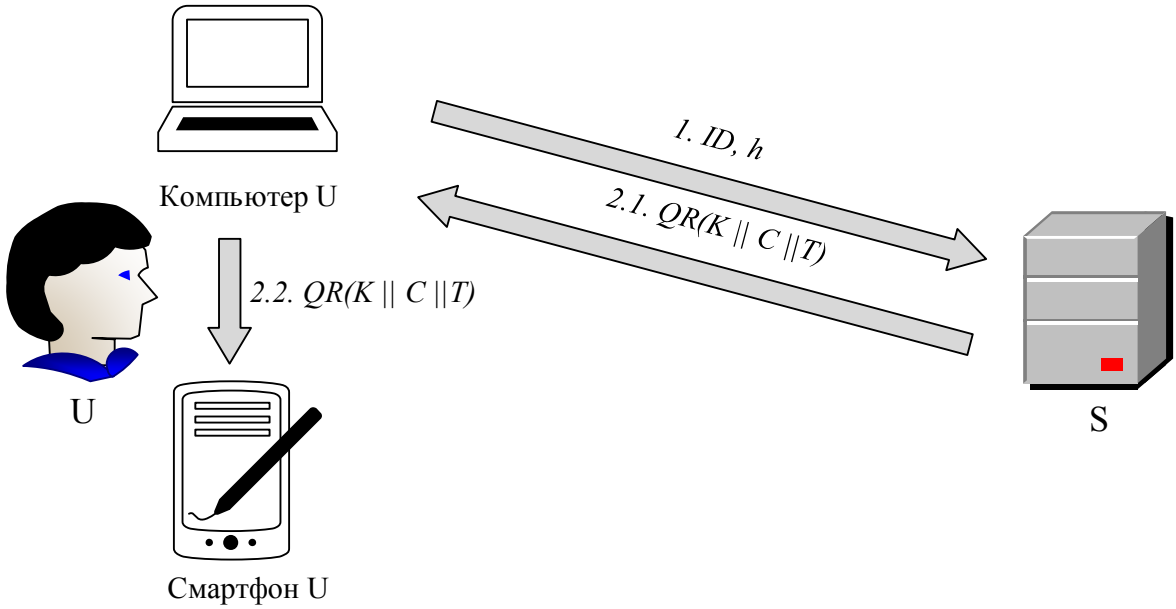


Рис.4. Эпат регистрации в аутентификации основанный на “вопрос-ответ”

В соответствии с методом двусторонней аутентификации «вопрос-ответ» параметры h, K, C и T должны быть одинаковыми для пользователя и сервера во время процесса аутентификации (рисунок 5). Хеш-функция может использовать произвольные надежные криптографические хеш-алгоритмы как H(). Примерами являются алгоритмы SHA256, SHA512, Blake2, Blake3, Ripedm, ГОСТ Р 34.11-2012, O‘z DSt 1106: 2009. Для разработки программного обеспечения и анализа предлагаемого протокола был выбран алгоритм SHA256.

Анализ протокола аутентификации, разработанного для мобильных облачных систем, важен с точки зрения безопасности и эффективности. Таким образом, формальное подтверждение безопасности протокола. Автоматическая проверка интернет-протоколов и приложений была выполнена с помощью инструмента AVISPA.

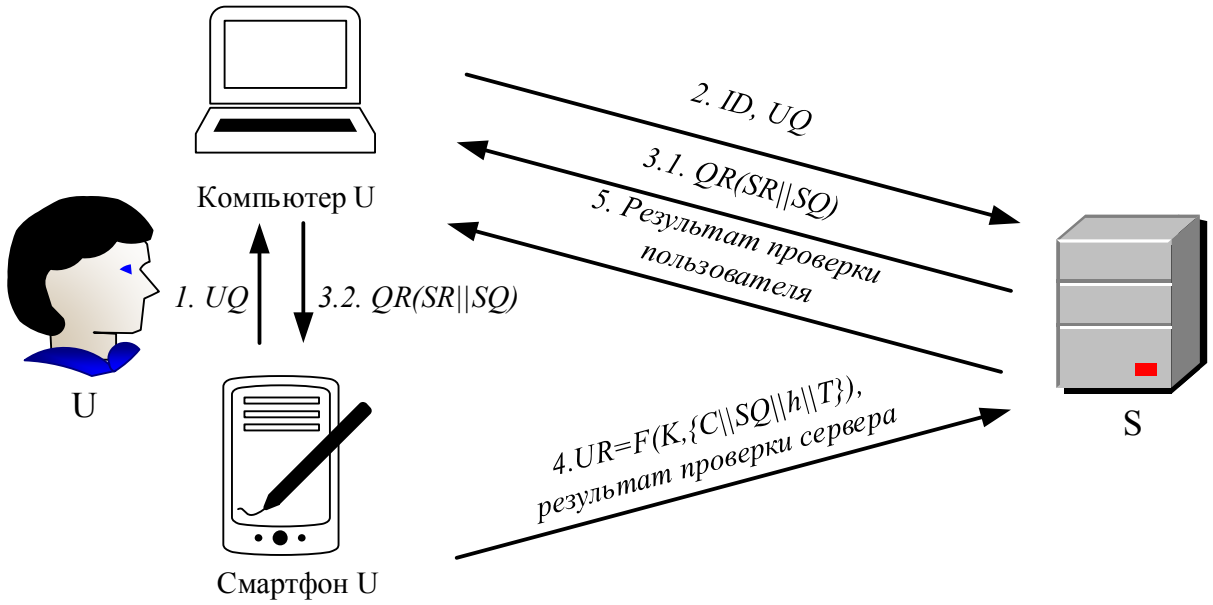


Рис.5. Этап аутентификации основанный на двухстороннем “вопрос-ответ”е

Протокол аутентификации, используемый в разработанных мобильных облачных системах, был проанализирован в режиме OFMC и CL-AtSe с помощью AVISPA (Security Protocol Animator for AVISPA, SPAN). Результаты анализа показали, что оба режима предложенного протокола (односторонняя и двусторонняя аутентификация) устойчивы к различным угрозам безопасности, в частности, дублированию и атакам человека посередине.

Кроме того, неформальным подтверждением безопасности протоколов аутентификации в системах облачных вычислений является возможность двусторонней аутентификации, повторной атаки, атаки гипотезы пароля и промежуточной атаки человека по факторам CHAP (Challenge Handshake Authentication Protocol), CRAM (Challenge-Response Authentication Mechanism), высокая безопастност по сравнению с протоколом SCRAM (Salted Challenge Response Authentication Mechanism).

По количеству вычислений в протоколе (N_x - количество хэширований было выбрано в качестве количества вычислений) предлагаемый протокол по объёму в 2,5 раза меньше протокола SCRAM, в 2 раза больше, чем протоколы CHAP и CRAM, обеспечивающие только одностороннюю аутентификацию и один с OCRA (OATH Challenge-Response Algorithm) показал тот же результат.

Анализ, проведенный по количеству данных, переданных в протоколе, показывает, что предложенный протокол записал тот же результат, что и протоколы OCRA, CRAM, и отправил на 160 бит меньше информации, чем протокол SCRAM. Также анализ количества хранимых в участниках протокола данных и порядка их хранения показал, что в протоколах CHAP, CRAM, SCRAM от пользователя требуется хранить пароль, тогда как OCRA и предлагаемый протокол используют криптографический ключ.

Следовательно, эти два протокола считаются защищенными от атак на пароли. С другой стороны, существует требование использовать сложный пароль в качестве криптографического ключа или обеспечивать безопасность ключа. Поэтому в предлагаемом протоколе криптографический ключ хранится в специальном программном средстве мобильного приложения.

ЗАКЛЮЧЕНИЕ

В результате исследовательской работы над диссертацией «Методы и алгоритмы аутентификации пользователей в системах облачных вычислений» были сделаны следующие выводы:

1. Существующие угрозы в системах облачных вычислений были проанализированы с использованием методологии STRIDE и факторов, указанных организацией OWASP. Анализ основан на целесообразности создания эффективного и безопасного решения для проверки подлинности пользователей при предотвращении существующих проблем в системах облачных вычислений.
2. В результате анализа было создано решение на основе шифрования проблем, связанных с безопасной передачей персональных данных в выбранном протоколе OpenID Connect. В результате можно зашифровать персональные данные пользователя с помощью криптографических алгоритмов с открытым ключом.
3. Для систем облачных вычислений был разработан метод аутентификации пользователя на основе эллиптической кривой. Формальный и неформальный анализ безопасности разработанного метода показал, что он устойчив к повторению, подбору пароля, атакам со стороны человека и компрометации, и тратит в 1,16 раза меньше времени, чем существующие методы.
4. Разработан метод, основанный на механизме «вопрос-ответ» для проверки подлинности пользователей в мобильных системах облачных вычислений. Разработанный протокол двусторонней аутентификации показал в 2,5 раза более высокую эффективность, чем протокол SCRAM по количеству вычислений.
5. Протокол OpenID Connect был улучшен с использованием методов двусторонней аутентификации на основе разработанной эллиптической кривой. В результате одноразовая система аутентификации OpenID Connect позволила управлять несколькими учетными записями с помощью одного секретного параметра и уменьшить проблемы с памятью паролей.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.13/30.12.2019.T.07.01 AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

ZOKIROV ODILJON YOQUBJON O‘G‘LI

METHODS AND ALGORITHMS FOR USER AUTHENTICATION IN CLOUD COMPUTING SYSTEMS

05.01.05 – Methods and systems of information protection. Information Security

DISSERTATION ABSTRACT OF THE DOCTOR OF PHILOSOPHY (PhD) ON TECHNICAL SCIENCES

Tashkent-2020

The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2020.3.PhD/T1892.

The dissertation has been prepared at Tashkent University of Information Techologies.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website www.tuit.uz and on the website of «ZiyoNet» Information and educational portal www.ziyonet.uz.

Scientific adviser:	**Ganiev Salim Karimovich** doctor of technical sciences, professor
Official opponents	**Karimov Madjit Malikovich** doctor of technical sciences, professor
	Normatov Sherbek Bakhtiyarovich doctor of philosophy on technical sciences
Leading organization:	**Scientific-Engineering and Marketing researches Center «UNICON.UZ»**

The defense will take place «____» _____ 2020 at _____ the meeting of Scientific council No. DSc.13/30.12.2019.T.07.01 at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No.___). (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on «____» _____ 2020 y.
(mailing report No. ___ on «____» _____ 2020 y.).

R.Kh. Khamdamov
Chairman of the scientific council
awarding scientific degrees,
Doctor of Technical Sciences, Professor

F.M. Nuraliev
Scientific secretary of scientific council
awarding scientific degrees,
Doctor of Technical Sciences, Docent

B.F. Abdurakhimov
Vise Chairman of the academic seminar under the
scientific council awarding scientific degrees,
Doctor of Physical-Mathematical Sciences, Professor

INTRODUCTION (abstract of PhD dissertation)

The aim of the research work is to develop methods and algorithms for user authentication based on two-factor and cryptographic algorithms in cloud computing systems.

The object of the research work is the process of checking the authenticity of users in cloud computing systems.

The scientific novelty of the research work is as follows:

single-use authentication protocol based on personal data encryption and robust authentication methods is improved;

considering into account the advantages of elliptical curves a two-way user authentication protocol in cloud computing systems is worked out;

a two-way authentication protocol based on the "question-answer" mechanism for mobile cloud computing systems is developed;

on the basis developed protocols the single-use authentication system is improved.

Implementation of the research results. On the basis results obtained on the methods, algorithms and software tools for checking the authenticity of users in the developed cloud computing systems:

the software tool for user authentication protocols based on elliptical curves was implemented into the practical activities of State Unitary Enterprise (SUE) “UNICON.UZ” - Center for scientific, technical and marketing research (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan dated December 01, 2020 No. 33-8/7322). The proposed authentication protocol in terms of computational time on both sides noted an efficiency of 1.16 times higher than the existing ones;

improved OpenID Connect single-use authentication based on the developed authentication methods was implemented into the practical activities of “COSCOM” LLC (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan dated December 01, 2020 No. 33-8/7322). As a result of scientific research OpenID Connect single-use authentication system allowed to manage a multi-password system which is conducted by employees of the organization based on a single secret parameter and to reduce problems with remembering a password by 4 times;

the software tool for authentication method based on the capabilities of mobile devices was implemented into the practical activities of the Agency for Public Services (certificate of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan dated December 01, 2020 No. 33-8/7322). The developed authentication protocol recorded 2.5 times higher efficiency than the SCRAM protocol in terms of the number of calculations.

Structure and volume of the dissertation. The structure of the dissertation consists of an introduction, four chapters, conclusion, references and appendix. The volume of the thesis is 107 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (Часть I; Part I)

1. Tashev K.A., Islomov Sh.Z., Zokirov O.Y., Analyze Threats in Cloud Computing // Journal of Electrical and Electronics Engineering, - India, 2016, Volume 4, Issue 6, – P.145-149 (05.00.00; №29).
2. Nasrullaev N.B., Islomov Sh.Z, Murtozoev Sh.A., Zokirov O.Y., Protection Cloud Computing Systems from threats // International Journal on Recent and Innovation Trends in Computing and Communication, -India, 2016, Volume 4, Issue 11, – P. 108 – 112 (05.00.00; №35).
3. Ganiev S.K., Islomov Sh.Z., Zokirov O.Y., Rustamov U.A., New authentication scheme for cloud computing // International Journal of Engineering & Technology, - United Arab Emirates, 2018, -P. 1-3 (05.00.00; №3).
4. Yusupov B.K., Nasrullayev N.B., Zokirov O.Y., Methods for Applying of Scheme of Packet Filtering Rules // International Journal of Innovative Technology and Exploring Engineering, India, 2019, Volume 8, Issue 11, – P 1014-1019 (05.00.00; №3).
5. Gulomov Sh.R., Abdullev A.G., Nasrullaev N.B., Zokirov O.Y., Method for determination of the probabilities of functioning states of information of protection on cloud computing // International Journal of Mechanical Engineering and Technology (IJMET), India, 2019, Volume 10, Issue 4, -P. 750-759 (05.00.00; №3).
6. Gulomov Sh.R., Rustamov U.A., Zokirov O.Y., Osculation Wireless Network Issues // International Journal of Advanced Research in Science, Engineering and Technology, India, 2019, Volume 6, Issue 1, -P. 7952-7956 (05.00.00; №35).
7. Назаров А.И., Кадиров Р.Х., Соатов Б.Э., Зокиров О.Ё., Моделирование природных процессов на основе гравитационных сил // Тошкент ахборот технологиялари университетининг илмий-техника ва ахборот-таҳлилий журнали, - Тошкент, 2014, №1(29) -P. 83-89 (05.00.00; №31).
8. Ганиев С.К., Зокиров О.Ё., Рустамов У.А., Булутли ҳисоблаш хизматларига таҳдидлар // “Муҳаммад ал-Хоразмий авлодлари” илмий-амалий ва ахборот-таҳлилий журнали, Тошкент, 2020, № 1(11), – Б. 8-10 (05.00.00; №31).

II бўлим (Часть II; Part II)

9. Islomov Sh.Z., Mardiev U.R., Zokirov O.Y., Salimov S.B., Comparing and implementation of public key cryptography algorithms on smart card // iScience. “АКТУАЛЬНЫЕ ВЫЗОВЫ СОВРЕМЕННОЙ НАУКИ”. СБОРНИК НАУЧНЫХ ТРУДОВ. X Международной научной конференции. – 2016, ВЫПУСК 7.Часть 1, - P. 40-43.

10. GanievA.A., Gulomov Sh.R., Zokirov O.Y., Creating approach protection e-mail from spam massages based on method of bayes // Perspectives for the development of information technologies ITPA-2015. -2015. - P. 78-83.

11. Юсупов Б.К., Зокиров О.Ё., Компьютер вирусларининг таркиби ва уларнинг таҳлили // “Ахборот ва телекомуникация технологиялари муаммолари” Республика илмий-техник конференциясининг маърузалар тўплами. -2016, 4-қисм. – Б. 109 – 110.

12. Ганиев С.К., Зокиров О.Ё., Булутли ҳисоблаш тизимларида open ID connect протоколи ёрдамида SSO технологиясини амалга ошириш учун ёндашувлар // “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги муаммолари” Республика илмий-техник семинари материаллари тўплами. -2020, – Б. 83-86.

13. Худойқулов З.Т., Зокиров О.Ё., Булутли ҳисоблаш тизимларида фойдаланувчиларни аутентификациялаш усуллари // “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги муаммолари” Республика илмий-техник семинари материаллари тўплами. -2020, – Б. 72-74.

14. Ғуломов Ш.Р., Зокиров О.Ё., Мобил қурилмаларда аутентификация масаласи // “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги муаммолари” Республика илмий-техник семинари материаллари тўплами. -2020, – Б. 31-32.

15. Абдурахмонов А.А., Зокиров О.Ё., Эллиптик эгри чизиқлар ва уларни аутентификацияда қўлланиши // “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги муаммолари” Республика илмий-техник семинари материаллари тўплами. -2020, – Б. 18-20.

16. Ганиев С.К., Худойқулов З.Т., Ғуломов Ш.Р., Насруллаев Н.Б., Абдурахманов А.А., Зокиров О.Ё., “CC Authentication дастурий воситаси” // Дастурга гувоҳнома № DGU 09196, 19.10.2020.

17. Ғуломов Ш.Р., Файзиева Д.С., Насруллаев Н.Б., Зокиров О.Ё., Шакаров М.А., “Security of distance learning system” // Дастурга гувоҳнома № DGU 09280, 29.10.2020.

18. Ганиев С.К., Худойқулов З.Т., Зокиров О.Ё., Абдурахмонов А.А., Холимтоева И.У., Корабаев Э.А., Шакаров М.А., “Mobile CC Authentication” // Дастурга гувоҳнома № DGU 09367, 11.11.2020.

Автореферат «Муҳаммад ал-Хоразмий авлодлари» илмий журнали таҳририятида таҳрирдан ўтказилди ва ўзбек, рус ва инглиз тилларидаги матнларини мослиги текширилди.