

Ishonchli hisoblash texnologiyasi va simsiz tarmoq asosida o'rnatilgan havfsiz terminal va multimedia ma'lumotlar bazasini yaratish.

Majidov Jahongir Mahmudovich.

Jizzax davlat pedagogika instituti katta o'qituvchisi.

Ergashev Ulug'bek Erkinovich.

Jizzax davlat pedagogika instituti katta o'qituvchisi.

Annotatsiya: Ushbu maqolada ishlab chiqilgan simsiz tarmoq o'rnatilgan xavfsizlik terminali mijoz terminali identifikatori autentifikatsiyasini, tegishli media kontentini himoya qilish va saqlashni hamda real vaqt rejimida translyatsiya kontentini kuzatishni o'z ichiga oladi. Taklif etilgan dizayn sxemasi asosida tajriba o'tkaziladi. Eksperimental natijalar shuni ko'rsatadiki, taklif etilgan va o'rnatilgan xavfsizlik terminali ishlashining afzalliklari, uning to'g'riligi va mavjudligi amalda o'z tasdig'ini topgan.

Аннотация: Интернет-технологии, как продукт развития сетевой эры, соединяют большое количество аппаратных устройств, но соединение многих устройств требует серьезной проверки соответствующей безопасности. Технология сетевой безопасности и соответствующая технология безопасности компьютерного оборудования стали центром внимания людей. В то же время создание мультимедийной базы данных на основе этой родственной технологии стало тенденцией развития исследований и внимания людей. Большая часть обычных технологий компьютерной безопасности сосредоточена на построении безопасности операционной системы, которая обладает определенной открытостью, поэтому ее соответствующая надежность очень низка, но также неконтролируема. Исходя из этого, в данной статье предлагается схема проектирования архитектуры общественной безопасности на встроенном терминале и реализуется проектирование системы управления мультимедийной безопасностью вещания на основе этой схемы, а также реализуется воспроизведение и хранение мультимедийных файлов, а также взаимодействие между соответствующими медиасерверами.

Annotation: Internet technology, as a product of the development of the network era, connects a large number of hardware devices, but the connection of many devices makes its corresponding security be greatly tested. The network security technology and the corresponding computer hardware security technology have become the focus of people's attention. At the same time, the construction of multimedia database based on this related technology has become the development trend of people's research and attention. Most of the conventional computer security technology focuses on the security construction of the operating system, which has certain openness, so its corresponding reliability is very low, but also uncontrollable.

Based on this, this paper proposes a design scheme of the public security architecture on the embedded terminal, and realizes the design of the multimedia security broadcast control system based on this scheme, and realizes the play and storage of multimedia files, as well as the interaction between the corresponding media servers.

Kalit so'zlar: ishonchli hisoblash texnologiyasi; simsiz tarmoq; o'rnatilgan xavfsizlik terminali; multimedia ma'lumotlar bazasi; jamoat xavfsizligi arxitekturasini; mijoz terminali identifikatori autentifikatsiyasi; media kontentini himoya qilish.

Ключевые слова: надежные вычислительные технологии; Встроенный терминал безопасности беспроводной сети; Мультимедийная база данных; Архитектура общественной безопасности; Аутентификация личности клиентского терминала; Защита медиаконтента.

Keywords: trusted computing technology; Wireless network embedded security terminal; Multimedia database; Public security architecture; Client terminal identity authentication; Media content protection.

1.Kirish.

Internet texnologiyasi axborot asrida eng mashhur texnologiya sifatida inson hayotiga va ishlab chiqarishga katta ta'sir ko'rsatadi. Internet juda ko'p sonli kompyuterlar, serverlar, noutbuklar va turli xil mobil qurilmalar, palmtoplar va hatto bir-biriga ulangan o'rnatilgan qurilmalarni yaratadi. Bu hodisa shuni anglatadiki, ko'p sonli kompyuterlar va mos keladigan mobil qurilmalar ham katta miqdordagi zararli hujum xavfini keltirib chiqaradi. An'anaviy tarmoq xavfsizligi muammolari faqat operatsion tizimning xavfsizlik komponentlariga qaratilgan bo'ladi. Ko'pincha operatsion tizim ochiq deb ta'riflanadi ammo tegishli dasturiy ta'minot tizimi juda murakkab, shuning uchun faqat operatsion tizim xavfsizligiga tayanish juda ishonchsizdir. Kompyuter texnologiyalari xavfsizligi muammosini hal qilishning yana bir yo'li - bu asosan apparat sxemasi bilan hal qilinadigan xavfsizlik modulini loyihalashdir. Asosiy yechim protsessorga tegishli xavfsizlik algoritmini qo'shishdir, ammo bu sxema etarli darajada moslashuvchan emasligi aniq. U real vaqtda yangi xavfsizlik funksiyasini sozlay olmaydi va shu bilan birga mos keladigan dizayn narxini oshiradi. Shuning uchun yuqoridagi tahlilga asoslanib, ishonchli kompyuter texnologiyasiga asoslangan o'rnatilgan xavfsizlik sxemasini ko'rib o'tamiz.

Ishonchli hisoblash texnologiyalari, tarmoq xavfsizligi texnologiyalari va boshqa sohalarda ko'plab tadqiqotchilar va tegishli ilmiy muassasalar bu borada tadqiqot va tahlillarni amalga oshirdilar. Bir vaqtlar Microsoft kompyuterning ishonchli hisoblash tizimini aniqladi, u asosan bir nechta xususiyatlarni o'z ichiga oladi: xavfsizlik, maxfiylik, ishonchlilik va yaxlitligi. Uning tegishli ta'rifi butun hisoblash ekotizimini qamrab oluvchi kompyuter xavfsizligidan ancha oshib ketadi,

ammo Microsoftning bu ta'riflari haligacha kontseptual muhokamalardir. Ishonchli mobil platforma tushunchasi AQShning tegishli universitetlari tomonidan ilgari surilgan. Ular ishonchli mobil platforma quyidagi uchta qismni o'z ichiga olishi kerak deb o'ylashadi: ishonchli apparat arxitekturasini spetsifikatsiyasi, ishonchli dasturiy ta'minot arxitekturasini spetsifikatsiyasi va protokol stekining spetsifikatsiyasi. Tizim kompyuterning ishonchli texnologiyasining tegishli apparat ta'rifini belgilaydi, shuningdek, mos keladigan qo'llab-quvvatlovchi apparat arxitektura platformasini ko'rsatadi. Kompyuter texnologiyasida Protokol va tegishli standartlar nuqtai nazaridan AQSh Mudofaa vazirligi birinchi navbatda hisoblash tizimini aniq belgilab beruvchi ishonchli kompyuter tizimini baholash standartini taklif qildi. Ishonchli hisoblash texnologiyasini yaratish uchun tegishli tadqiqot institutlar juda ko'p tadqiqotlar o'tkazdi, uning asosiy xavfsizlik texnologiyasi SSL, IPSec va boshqa kirishni boshqarish mexanizmlarini o'z ichiga oladi, uning asosiy texnik atributlari uchta darajani o'z ichiga oladi: autentifikatsiya texnologiyasi, yaxlitlik va maxfiylik, lekin ishonchli dasturiy ta'minotning bunday turi kompyuter tizimining xavfsizlik muammolarini oshiradi va shu bilan birga ishonchlilikning sezilarli darajada pasayishiga olib keladi. Ishonchli texnologiyani hisoblashda tadqiq qilish nuqtai nazaridan asosiy tadqiqot tegishli mobil qurilmalarni, jumladan saqlash boshqaruvchisi, uzilish nazoratchisi, DMA kontrolleri va turli xil mos mantiqiy sxemalarni tadqiq qilish bilan chegaralanadi, ammo bu sxema ma'lum darajada moslashuvchan emas va quvvat iste'moli bilan bog'liq ko'plab muammolar mavjud. Ishonchli hisoblash texnologiyasi apparat tadqiqini davom ettirish uchun asosiy yechim protsessorga tegishli xavfsizlik algoritmini qo'shishdir. Biroq, bu yechim yetarlicha moslashuvchan emas va u real vaqtda yangi xavfsizlik funksiyasini sozlay olmaydi. Shu bilan birga, bu mos keladigan dizayn narxini oshiradi, bu tizimning quvvat sarfiga juda zararli. Shuning uchun ishonchli hisoblash texnologiyasi bo'yicha olib borilayotgan tadqiqotlar asosan texnik va dasturiy ta'minotga qaratilgan bo'lib bir qator kamchiliklar mavjud.

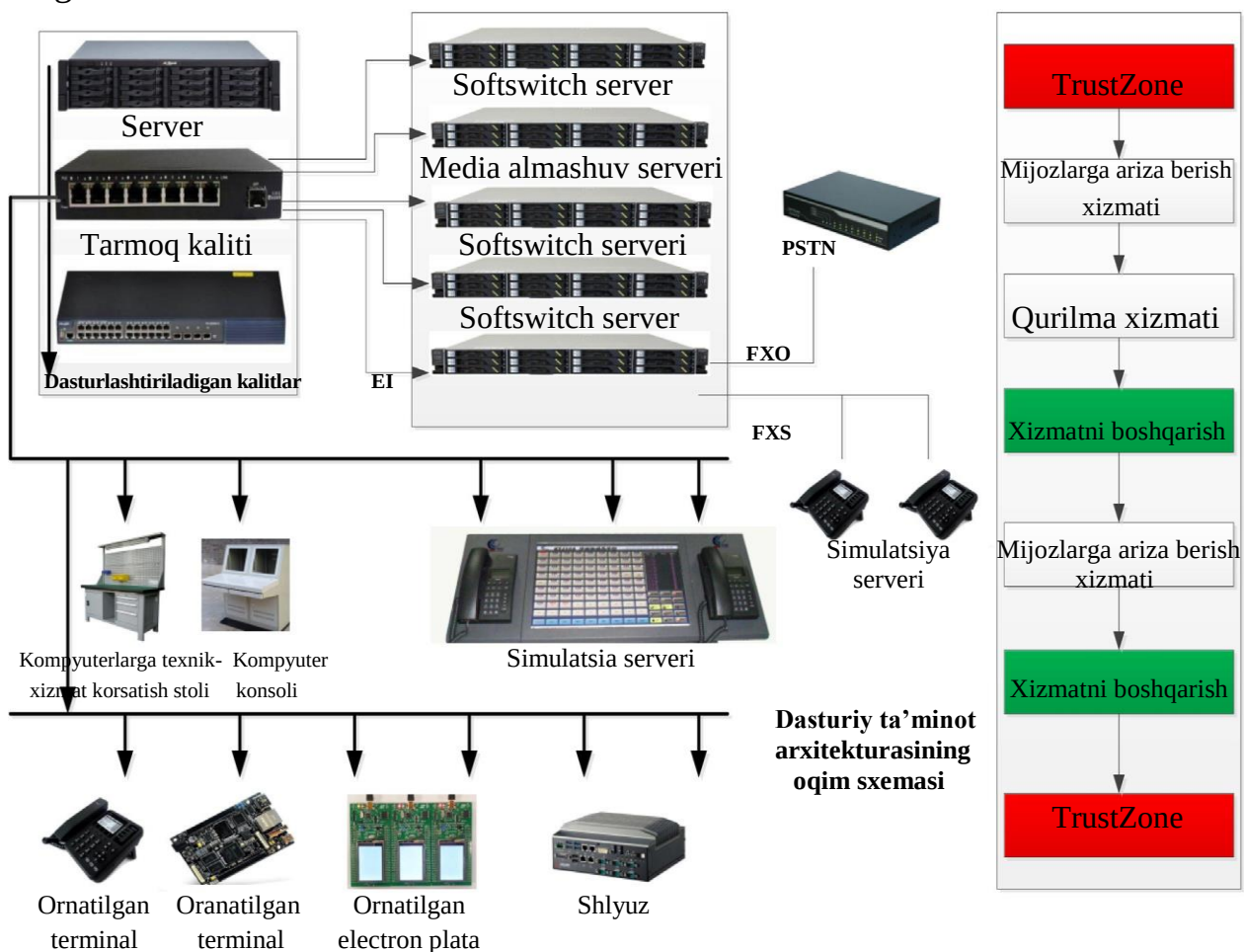
Yuqoridagi tahlillarga asoslanib, ushbu maqolada ishonchli hisoblash texnologiyasining hozirgi tadqiqot holatiga e'tibor qaratiladi va tegishli texnik va dasturiy ta'minot texnologiyasini tasniflanadi. Ushbu tahlilga asoslanib o'rnatilgan terminalda jamoat xavfsizligi arxitekturasining dizayn sxemasini taklif qilinadi. Shu bilan birga, ushbu sxema asosida multimedia xavfsizligini boshqarish tizimini loyihalash amalga oshiriladi va multimedia fayllarini o'ynash va saqlash hamda tegishli media-serverlar o'rtasidagi o'zaro ta'sir amalga oshiriladi. Ushbu maqolada ishlab chiqilgan simsiz tarmoq o'rnatilgan xavfsizlik terminali mijoz terminali identifikatori autentifikatsiyasini, tegishli media kontentini himoya qilish va saqlashni hamda real vaqtda translyatsiya kontentini kuzatishni o'z ichiga oladi. Nihoyat, taklif qilingan dizayn sxemasi asosida tajriba o'tkaziladi. Eksperimental

natijalar shuni ko'rsatadiki, taklif qilingan o'rnatilgan xavfsizlik terminali ishlashning afzalliklari va uning to'g'riligi va mavjudligi amalda tasdiqlangan.

Ushbu maqolaning tuzilishi quyidagicha tartibga solingan: Ishonchli hisoblash texnologiyasiga asoslangan simsiz tarmoq o'rnatilgan xavfsizlik terminalining dizayn sxemasi taklif etiladi va uning tegishli printsiplari tahlil qilinadi; taklif qilingan loyihalash sxemasi asosida tarmoq multimediasining ma'lumotlar bazasini qurish amalga oshiriladi va uning tahlili va tadqiqoti amalga oshiriladi; nihoyat ushbu maqolaning qisqacha mazmuni tuziladi.

2. Ishonchli hisoblash texnologiyasiga asoslangan simsiz tarmoq o'rnatilgan xavfsizlik terminalining dizayn sxemasi.

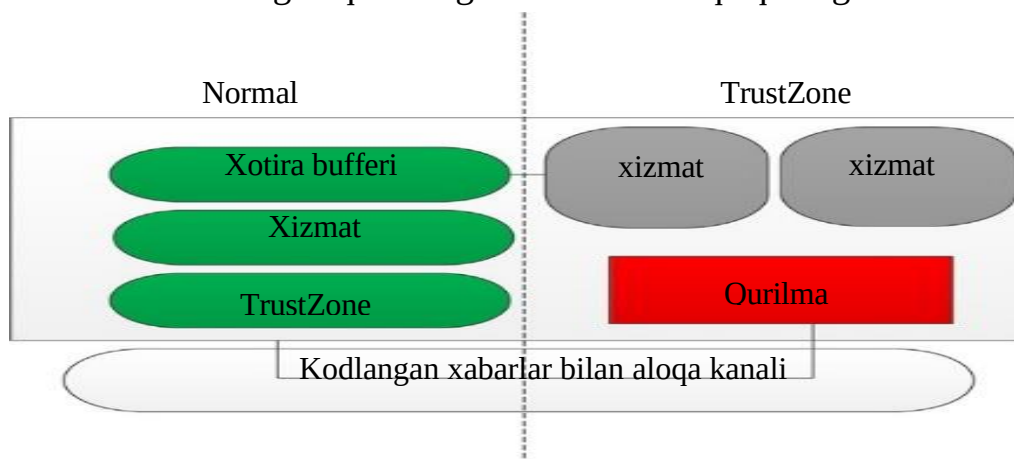
Ushbu maqolada ishlab chiqilgan ishonchli hisoblash vositalari asosan ikki darajaga bo'lingan: texnik tuzilmasi darajasi va dasturiy ta'minot tuzilmasi darajasi. Tegishli umumiy dizayn sxemasining tafsilotlari 1-rasmda ko'rsatilgan. Rasmda biz mos keladigan texnik qismini va mos keladigan dasturiy qismning mos ramka diagrammasini ko'rishimiz mumkin.



1-rasm. Ishonchli hisoblash texnologiyasi asosida simsiz tarmoq o'rnatilgan terminalining dasturiy va apparat dizayni.

Tegishli o'rnatilgan terminalning jamoat xavfsizligi arxitekturasining dizayni 2-rasmda ko'rsatilgan. Rasmdan ko'rinib turibdiki, butun xavfsizlik arxitekturasini

xavfsizlik va qo'riqlanmagan qismga bo'lingan. Tegishli xavfsizlik qismi asosan shifrlash va shifrni hal qilish, xavfsizlik ma'lumotlarini saqlash, identifikatsiyani autentifikatsiya qilish, yaxlitlikni tekshirish va boshqalar kabi modullarni o'z ichiga oladi. Xavfsizlik bo'lmagan qismi tegishli xizmat aloqa qismiga mos keladi.



2-rasm. Ishonchli hisoblash texnologiyasiga asoslangan simsiz tarmoq o'rnatilgan terminalining jamoat xavfsizligi arxitekturasini dizayni.

Asosiy texnik platforma arxitekturasini protsessor, flesh, saqlash boshqaruvchisi, DMA kontrolleri, uzilish boshqaruvchisi va turli simsiz tarmoq aloqa protokollarining tegishli interfeyslarini, turli xil mantiqiy sxemalarni o'z ichiga oladi. Ular orasida tegishli protsessor apparatini boshqarish platformasi mavjud bo'lib asosan operatsion tizim va tegishli turli protokollarni ishga tushirish uchun ishlatiladi. Tegishli apparat strukturasi texnologiyasi TrustZone texnologiyasini qabul qiladi, bu an'anaviy apparat tuzilmasi bilan solishtirganda quyidagi uchta xususiyatga ega:

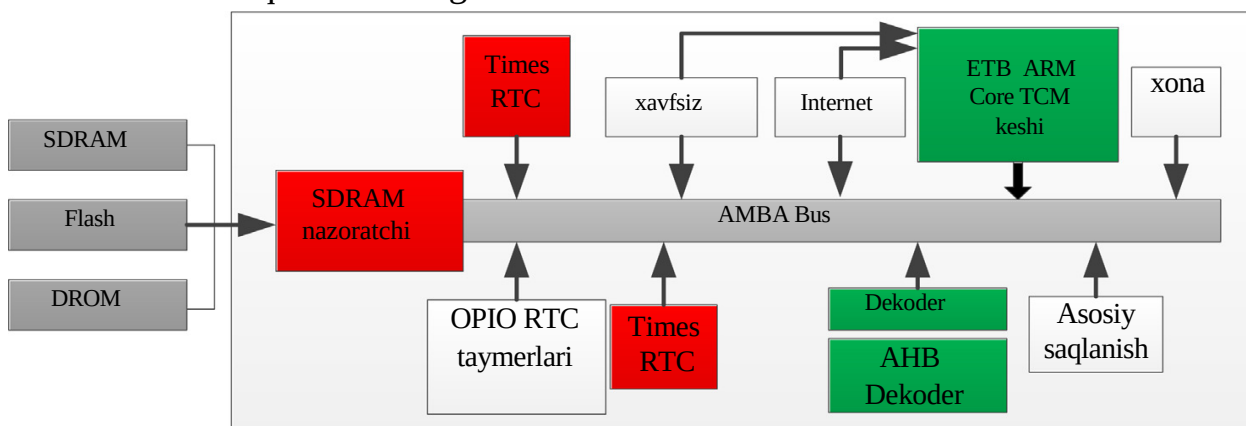
(A) Tizim xavfsiz holatda yoki xavfli holatda ekanligini aniqlaydigan indikator biti qo'shiladi. Butun tizim xavfli holatda bo'lsa, uning mos keladigan joylashuvi identifikatsiyasini o'zgartirib bo'lmaydi va tizim qayta o'rnatilgandan so'ng avtomatik ravishda xavfsiz holatda bo'ladi.

(B) Apparatning reestri kengaytirilgan. Butun apparat tizimining tegishli holati xavfsiz holatga o'tkazilganda, holatni almashtirish va tegishli ma'lumotlar registrda saqlanadi.

(C) Ko'p sonli xotira va tegishli kesh apparati qo'shiladi. Tizim xavfsiz bo'lmagan holatda bo'lsa, xavfsizlik biti kirish kerak bo'lgan sahifa jadvalida belgilanadi. Butun apparat tizimida xavfsizlik bilan bog'liq muammolar mavjud bo'lsa, mos keladigan tizim g'ayritabiiy uzilish so'rovini yaratadi.

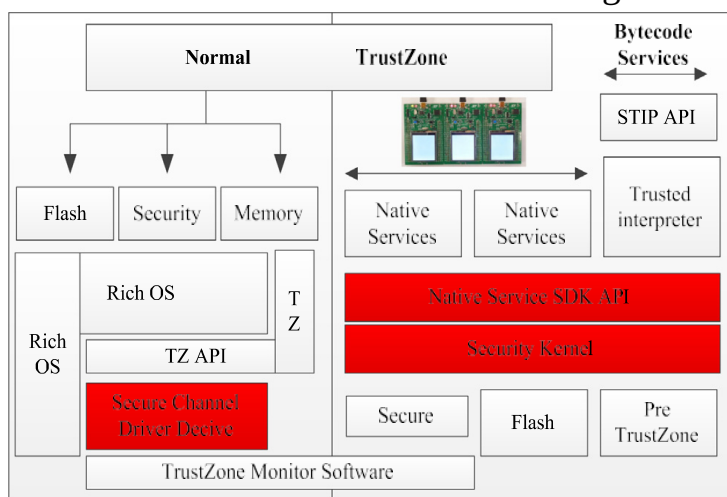
Tegishli apparat tizimining arxitektura tafsilotlari 3-rasmda ko'rsatilgan. Rasmdan ko'rinib turibdiki, tizim butun apparat tizimidagi saqlash qurilmalari va umumiy periferik qurilmalar uchun xavfsizlikni ta'minlaydi. O'rnatilgan tizim chip va tashqi xotiraning bir qismiga asoslangan butun tizimga kengaytirish uchun mos keladigan TrustZone texnologiyasidan foydalanishi mumkin. RAM, ROM va mos

keladigan flesh kabi xotiraning tegishli texnik qismi S-bitga o'rnatiladi. Himoya uchun periferiyadan foydalanilganda, tegishli atrof-muhit birligining drayveri harakatlanuvchi qismlarni o'zgartirishi mumkin.



3-rasm. Ishonchli hisoblash texnologiyasi simsiz tarmoq o'rnatilgan terminalining apparat detallari.

Tegishli dasturiy ta'minot darajasida ishlatiladigan asosiy dasturiy ta'minot texnologiyasi TrustZone dasturiy ta'minot texnologiyasidir. Uning asosiy xususiyatlari quyidagilardan iborat: texnologiya juda moslashuvchan va mos keladigan portativligi kuchli; tegishli autentifikatsiya qobiliyati va xavfsizligi kuchli; mos keladigan rivojlanish xavfini kamaytirishi, rivojlanish siklini qisqartirishi mumkin va uning mos keladigan rivojlanish narxi nisbatan past; texnologiyaning dasturiy ta'minot muvofiqligi kuchli. Butun ishonchli hisoblash texnologiyasiga mos keladigan simsiz tarmoq o'rnatilgan terminalining dasturiy ta'minot arxitekturasini 4-rasmda ko'rsatilgan.



4-rasm. Ishonchli hisoblash texnologiyasining simsiz tarmoq o'rnatilgan terminal dasturiy ta'minotining tafsilotlari.

Rasmdan ko'rinib turibdiki, butun dasturiy ta'minot arxitekturasini asosan TrustZone, xavfsizlik yadrosi xavfsizligi va shunga o'xshash dasturiy paketlardan iborat. Ishonchli hisoblash texnologiyasining simsiz tarmoqqa o'rnatilgan terminal dasturiy ta'minot tizimi butun tizim uchun xavfsiz va ishonchli ish muhitini ta'minlaydi. Tizimning amaliy dasturida u istalgan vaqtda TrustZone-ning tegishli

dasturiy modullari tomonidan taqdim etilgan xizmatlarga va tegishli asosiy apparat ta'sir o'tkazish funksiyalariga qo'ng'iroq qilib, xavfsizlikni himoya qilishi mumkin.

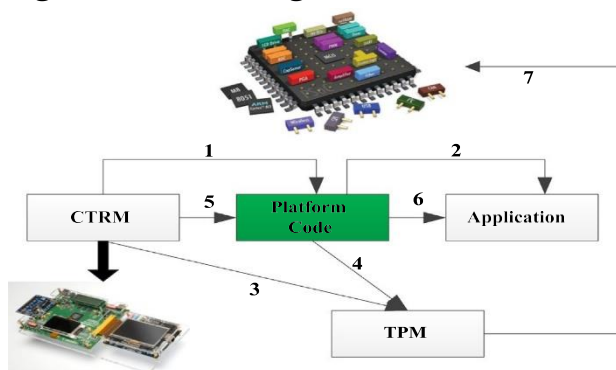
Yuqoridagi dasturiy ta'minot va apparat strukturasi umumiy dizayniga asoslanib, umumiy sxemada tegishli ilovalarning batafsil texnik tafsilotlari quyidagicha:

(A) Mijozlarga ilovalar xizmati: u boshqa ilovalar uchun xavfsizlik xizmatlarini taqdim etish maqsadida alohida dastur va kutubxona funksiyasi sifatida ishlatilishi mumkin.

(B) Qurilma xizmati: u asosan har xil turdagi texnikadan iborat. Tegishli qurilmalar tegishli eksklyuziv resurslarga va tegishli operatsiyalarga ega. Barcha tegishli xavfsizlik dasturlari bitta qurilmaga tegishli. Tegishli qurilma xizmati ilovasi xavfsizlik xizmatiga kirishini va mos keladigan interfeys orqali qurilmaga ulanishi mumkin.

(C) Xizmatlarni boshqarish: Xizmatlarni boshqarish moduli joriy xizmat holatini ko'rish va ularning xususiyatlarini qaytarish uchun tegishli interfeysni taqdim etadi. Tegishli xizmat boshqaruvi faqat o'qish ruxsatiga ega, u tegishli xizmatni yuklab olmaydi yoki o'chira olmaydi.

Yuqorida aytib o'tilgan ishonchli hisoblash tizimi arxitekturasida mos keladigan ishonchli zanjirni uzatish jarayoni 5-rasmda ko'rsatilgan va uni amalga oshirishning asosiy jarayoni quyidagicha: birinchidan, ishonchni o'lchash yadrosi mos keladigan platforma kodini o'lchaydi va bir vaqtning o'zida o'lchov qiymatini taqqoslash uchun CPU chipiga o'lchov qiymatini beradi, so'ngra platforma dasturi mos keladigan o'lchov qiymatini o'lchaydi va bir vaqtning o'zida tegishli boshqaruv huquqini tegishli dasturga o'tkazadi, so'ngra platforma tegishli ko'rsatkichlarni PCRga topshiradi. Agar tegishli dastur ko'rsatkichlari to'g'ri bo'lsa, tegishli platforma ilovani ishga tushirish va tegishli ma'lumotlarni o'qish imkonini beradi.



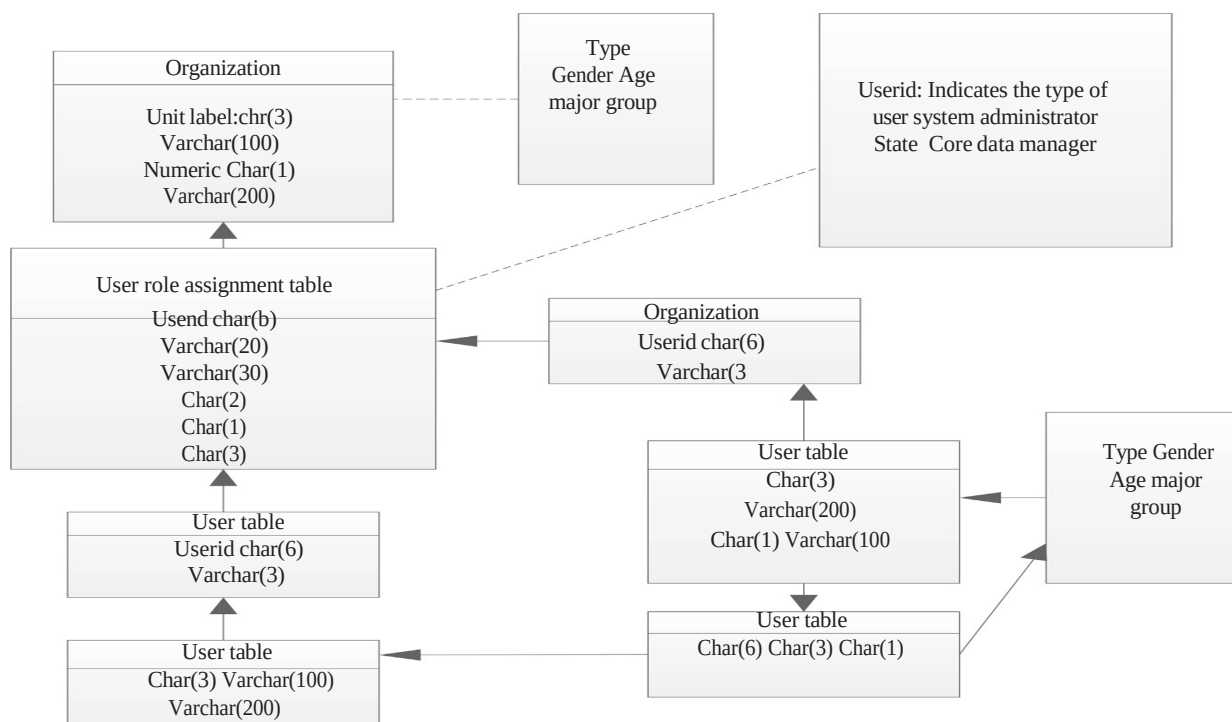
5-rasm. Ishonchli hisoblash texnologiyasiga asoslangan simsiz tarmoq o'rnatilgan terminalining ishonchli zanjir uzatish diagrammasi.

3. Tarmoq multimedia ma'lumotlar bazasini qurish va ma'lumotlarni tahlil qilish.

Simsiz tarmoq o'rnatilgan terminalining yuqoridagi ishonchli hisoblash texnologiyasiga asoslanib tarmoq multimedia ma'lumotlarini qurishda qo'llaydi.

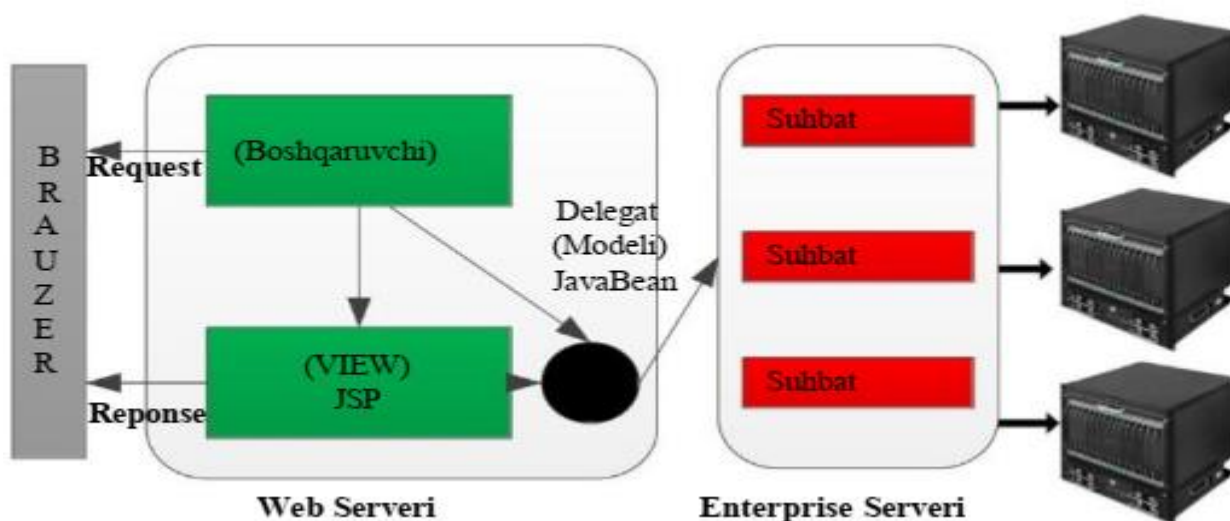
Butun multimedia ma'lumotlar bazasini qurishning mos keladigan oqim sxemasi 6-rasmda ko'rsatilgan.

6-rasm. Tarmoq multimedia ma'lumotlar bazasini qurish sxemasi.



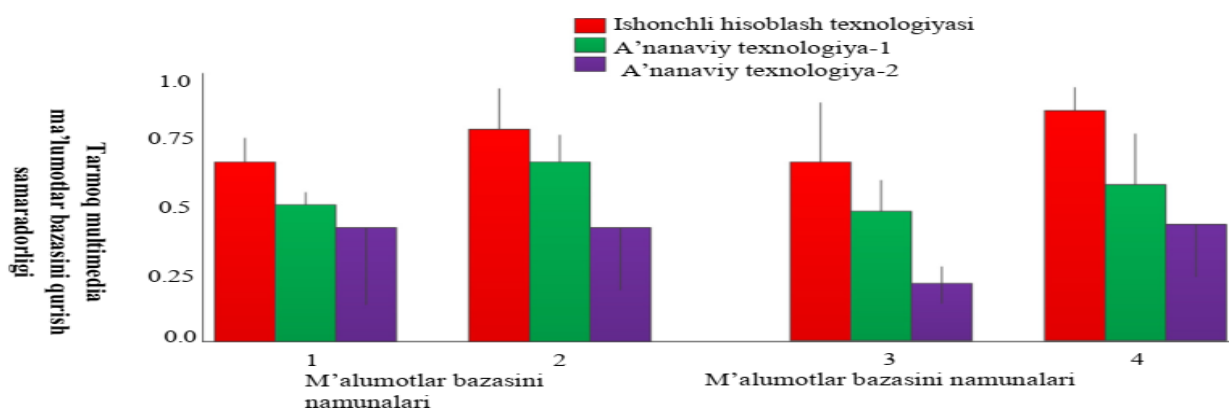
7-rasm Tarmoq multimedia ma'lumotlar bazasi foydalanuvchilarni boshqarish modulini loyihalash.

Butun multimedia ma'lumotlar konstruktsiyasining tegishli veb-qatlamini loyihalashda asosan o'zaro mustaqil va hamkorlikda bo'lgan uchta modul qo'llaniladi. Tegishli modullar quyidagilardir: so'rovlarni yuboruvchi va trafikni boshqaruvchi, ma'lumotlarni ko'rsatish va foydalanuvchi kiritishini ta'minlovchi ko'rinish va biznes agent moduli. Tegishli batafsil blok diagrammasi 8-rasmda ko'rsatilgan. Dasturga bog'liq so'rovlarni qayta ishlash va mos keladigan ko'rinishni tanlash bitta komponentda markazlashtirilgan bo'lib, mijozlar uchun oddiy interfeysni ta'minlaydi. Komponentlar va ichki munosabatlar o'rtasidagi o'zaro ta'sirni yashirish orqali va mijozlar oldida tranzaksiya ob'ektini qayta ishlashni kamaytiradi.



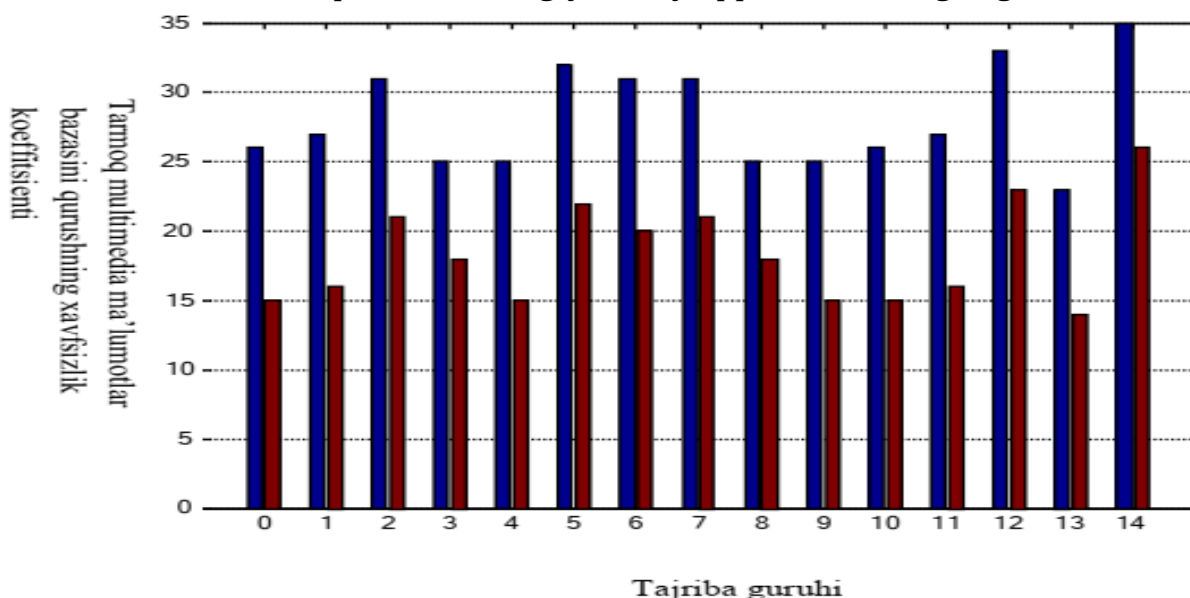
8-rasm Tarmoq multimedia ma'lumotlar bazasining veb-qatlami tuzilishi.

Yuqorida aytib o'tilgan ishonchli hisoblash texnologiyasiga asoslanib, simsiz tarmoq o'rnatilgan terminali tarmoq multimedia ma'lumotlar bazasini qurishda qo'llaniladi. Tegishli eksperimental ob'ekt - universitetning multimedia o'quv resurslari ma'lumotlar bazasi tizimi. 9-rasmda ko'rsatilganidek, tegishli tarmoq multimedia ma'lumotlar bazasini qurishda ishonchli hisoblash texnologiyasining simsiz tarmoq o'rnatilgan terminali samaradorligi sezilarli darajada yuqori.



9-rasm Tarmoq multimedia ma'lumotlar bazasini qurish samaradorligi egri chizig'i.

10-rasmda ikki turdagi multimedia ma'lumotlar bazasini qurish texnologiyalari ostida ma'lumotlar bazasi xavfsizlik koeffitsientining egri diagrammasi ko'rsatilgan. Ushbu maqolada butun tizimda taqdim etilgan ishonchli hisoblash texnologiyasining simsiz tarmoq o'rnatilgan terminali xavfsizlik koeffitsientida tarmoq multimedia ma'lumotlar bazasini qurish texnologiyasida yaqqol afzalliklarga ega.



10-rasm Tarmoq multimedia ma'lumotlar bazasini qurishning xavfsizlik koeffitsienti egri chizig'i.

4. Xulosa

Ushbu maqola asosan simsiz tarmoq o'rnatilgan xavfsizlik terminalida joriy tarmoq xavfsizligida ishonchli hisoblash texnologiyasini qo'llashni tahlil qiladi, shu bilan birga u tegishli ishonchli hisoblash texnologiyasining joriy tadqiqot holatini aniq tahlil qiladi va afzalliklarini taqqoslaydi. Unga mos keladigan algoritm texnologiyasining kamchiliklari va afzalliklari to'risida quyidagi xulosalar chiqaradi: Ushbu texnologiya asosida multimedia ma'lumotlar bazasini qurish rivojlanish tendentsiyasiga aylandi. An'anaviy kompyuter xavfsizligi texnologiyalarining aksariyati ma'lum bir ochiqlikka ega bo'lgan operatsion tizimning xavfsizligini ta'minlashga qaratilgan, shuning uchun uning ishonchliligi juda past. Shunga asoslanib, ushbu hujjat o'rnatilgan terminalda jamoat xavfsizligi arxitekturasining dizayn sxemasini taklif qiladi va ushbu sxema asosida multimedia xavfsizligini boshqarish tizimini loyihalashni amalga oshiradi va multimedia fayllarini o'ynash va saqlashni amalga oshiradi. Maqolada ishlab chiqilgan simsiz tarmoq o'rnatilgan xavfsizlik terminali mijoz terminali identifikatori autentifikatsiyasini, mos keladigan media kontentini himoya qilish va saqlashni va real vaqtda translyatsiya kontentini kuzatishni o'z ichiga oladi.

Adabiyotlar:

1. F. Vang, Axborot texnologiyalariga asoslangan ekologik iqtisod kursi uchun multimedia o'quv platformasini qurish, *Int. J. Emerg. Technol. O'rganing*. 12 (9) (2017) 73–82.
2. G.J.F. Jons, Til va multimedia texnologiyalari tadqiqotlari uchun kraudsorsingga kirish, *Lekt. Eslatmalarni hisoblash. Sci.* 7757 (4) (2013) 132–154.
3. W. Go, K. Li, J. Kwak, Barmoq izi ma'lumotlari va paroldan foydalangan holda xavfsiz ikki faktorli foydalanuvchi autentifikatsiya tizimini qurish, *J. Intell. Ishlab chiqaruvchi*. 25 (2) (2014) 56–65.
4. D. Xe, S. Chan, M. Guizani, Simsiz ulanish tarmoqlari uchun hisob beruvchi, maxfiylikni saqlaydigan va samarali autentifikatsiya tizimi, *IEEE Trans. Veh. Technol.* 65 (3) (2016) 1605–1614.
5. S. Kumari, M.K. Khan, X. Li, smart-kartaga asoslangan yanada xavfsiz raqamli huquqlarni boshqarish autentifikatsiya sxemasi, *Multimedia Tools Appl.* 75 (2) (2014) 1–24.
6. H. Yin, D. Guo, K. Vang, Hyperconnected tarmoq: markazlashtirilmagan ishonchli hisoblash va tarmoq paradigmasi, *IEEE Network* 32 (1) (2018) 112–117.
7. P. Vijayakumar, M. Azees, A. Kannan, Dual autentifikatsiya va avtomobil Ad Hoc tarmoqlarida xavfsiz ma'lumotlarni uzatish uchun kalitlarni boshqarish usullari, *IEEE Trans. Intell. Transp. Sist.* 17 (4) (2015) 1–14.
8. Y. Chju, X.u. Rui, T. Takagi, kalit almashishsiz shifrlangan bulutli ma'lumotlar bazasida xavfsiz k-NN so'rovi, *Int. J. Elektron. Xavfsiz. Raqam. Sud ekspertizasi* 5 (3/4) (2013) 201–217.