RFID TEXNOLOGIYASI UCHUN MA’LUMOTLARNI ELEKTRON IDENTIFIKATSIYA QILISH VOSITALARINING TASNIFI

M.A.Fayzullaeva
(Axborot xafvsizligi kafedrasi assistenti)
B.M.Shanazarov
(Axborot xafvsizligi kafedrasi assistenti)

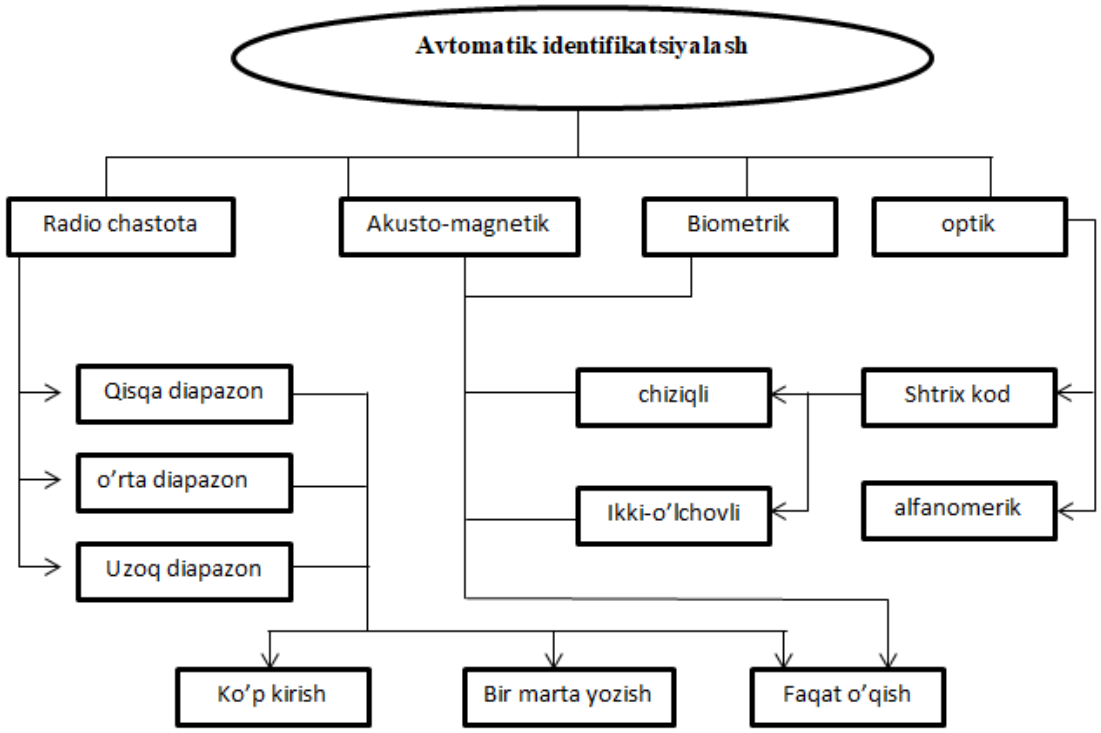
Annotatsya: *Radiochastota teglari (RFID teglari) ob'ektlarni aniqlash va autentifikatsiya qilish uchun keng qo'llanib kelmoqda. Identifikatsiya xususiyatlari va RFID teglarini xotira resurslari va hisoblash quvvati tavsiflanadi, bu esa o'z navbatida ishlatiladigan kriptografik mexanizmlarga ta'sir qiladi. Asosiy e'tibor axborotni himoya qilishning mexanizmlarini qiyosiy tahlil qilishga, ulardan radiochastota teglariga ma’lumotlarni identifikatsiyalash vositalaridan foydalanishning o'ziga xos xususiyatlarini hisobga olishga qaratilgan.*

Kalit so'zlar: *identifikatsiya, autentifikatsiya, teg, radiochastota.*

Fan va texnika yutuqlari avtomatik identifikatsiyalash vositalarini ishlab chiqish, tanib olish funksiyalarini avtomatlashtirishga urinishlardan boshlab qo'lda bajarilgan, keyinchalik eng so'nggi foydalanishga asoslangan. Sensordan olingan ma'lumotlarni olish yoki hisoblash uchun signal yaxshi aniqlangan RFID xususiyatining o'qish va javob berish qobiliyatidir. Bir qator tadqiqotlar mavjud RFID sensorlari bemorning klinik holatini baholashda yordam berishi mumkinligini ko'rsatdi [4]. RFID texnologiyasidan foydalangan holda sog'liqni saqlash ilovalari yordamida uskunalarni masofadan boshqarish imkonini beradi.

Avtomatik identifikatsiya hozirgi vaqtda quyidagi usullardan foydalanish mumkin (1-sxema) [1, 2]:

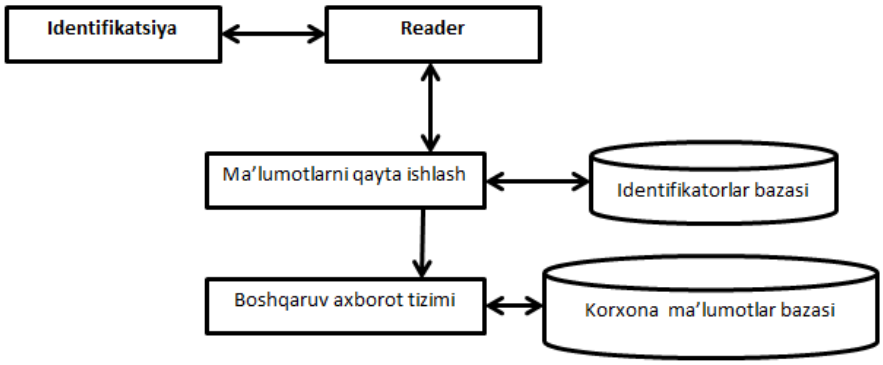
- Akusto-magnit magnitlangan elementli plastinkadan foydalanish ma'lumotlarning o'qilishi asoslanadi (magnit karta), shunchaki lentadagi kabi kerakli ma'lumotlar qayd etiladi. Bu usul asosan muayyan xizmatlarni ko'rsatishga kirish uchun keng tarqaldi (debet kartalari, kirish kartalari va boshqalar).
- Radiochastotani identifikatsiyalash (RFID texnologiyasi) kam quvvatli radio uzatgichni joylashtirish orqali amalga oshiriladi (transponder) identifikatsiya qilinadigan ob'ekt ustida, ustiga ma'lumotni uzatuvchi o'quvchining qo'ng'iroq signali xotirada qayd etilgan hisoblanadi.
- O'rnatilgan maxsus belgilarni optik aniqlash, odatda shtrix-kod ko'rinishida bo’lib, yorliqning tan olinishi transport yorliqlari alfanumerik bosqichda ham past ishonchliligi tufayli juda kam uchraydi o'qish va tan olish bosqichida belgilar hisoblanadi.



1-sxema. Avtomatik identifikatsiya qilish usullari.

- Biometrik identifikatsiya sub'ektlarining o'ziga xos jismoniy xususiyatlaridan o'lchovga asoslanadi tizimi va yuqori darajasi bilan ajralib turadi identifikatsiyaning ishonchliligi, biometrikning ajralmasligi mavzudan xususiyatlar va ularning yuqori murakkabligi soxtalashtirish. Hozirgi vaqtda foydalanish texnologiyalarida quyidagi biometrik xususiyatlar ishlab chiqilgan: barmoq izlari (44%), yuz shakli va hajmi (14%), geometrik shakli kaft (13%), ovoz xususiyatlari (10%). 1-sxemadan ko'rinib turibdiki, faqat RFID identifikator usullari ma'lumotlari o'zgartirilishi kerak. Yuk yoki yo'lovchini etkazib berish jarayoni ishtirokchilari transportni hisobga olish uchun bu afzalliklarni belgilaydi.

Avtomatik identifikatsiyaning sxematik diagrammasi tizimning ishlashi 2-sxemada ko'rsatilgan. Identifikatorning ma'lumotlari tomonidan tan olingan identifikatsiya ob'ektiga o'rnatilgan o'quvchi va qayta ishlash uchun uzatiladi. Jarayonida identifikator ma'lumotlar bazasidan foydalangan holda identifikator ma'lumotlarini qayta ishlash, autentifikatsiya va avtorizatsiya jarayonlari amalga oshiriladi[5]. Bu identifikator ma'lumotlar bazasi a bo'lishi mumkinligini yodda tutish kerak amalga oshiruvchi tashkilotning jismoniy resursi ob'ektning identifikatsiyasi yoki mustaqilga tegishli identifikatsiya tizimining operatori. Ikkinchi holda, shunday identifikatorlar bazasiga kirishni tashkil qilish uchun zarur global kompyuter tarmog'i orqali yoki to'g'ridan-to'g'ri modem yordamida ulanish.



2-sxema. Avtomatik identifikatsiya tizimining sxematik diagrammasi

Avtorizatsiya natijalariga ko'ra identifikator ma'lumotlari hisoblanadi, tashkilotning muayyan boshqaruv axborot harakatlarni bajarish tizimida foydalaniladi. Ma'lumotlar tegda saqlanadi, ya'ni shaxsiy yoki shaxsiy ma'lumotlarga ko'rsatgich vazifasini bajaradigan ma'lumotlar maqsad oxirida yo'q qilinishi kerak, agar ma’lumot o'zgartirilmoqchi bo’lsa tegdagi ma'lumotlarni yangi maqsadda saqlashga rozilik yoziladi[3].

RFID teglari o'rnatilgan quvvat manbasiga ko'ra uchtaga bo'linadi toifalar: faol teglar, yarim passiv teglar va passiv teglar.

Faol teglarda radio signal uzatgich quvvat manbai bilan birga o'rnatilgan, odatda uni quvvatlantirish uchun kichik batareya shaklida. Bort batareyasi tufayli faol RFID teglari aloqani boshlashi va o'zini faollashtirishi mumkin ularning yaqinida o'quvchi borligidan qat'i nazar. Biroq, odatda faol teglar yuborilayotgan RF maydoni mavjudligini aniqlamaguncha past quvvat holatida qoladilar batareyani tejash uchun o'quvchi tomonidan. Teg yaqin atrofni tark etganda o'quvchi, u yana kam quvvat holatiga qaytadi. Jihozlangan batareya tufayli faol teglar bilan solishtirganda uzoqroq masofani qamrab olishi mumkin boshqa turdagi teglar. Shuning uchun, bu teglar mavjud bo'lganda o'quvchi tomonidan o'qilishi mumkin ancha uzoqroqda. Biroq, ularning umri ularning imkoniyatlari bilan cheklangan batareya. Garchi ularning ba'zilari bir necha yil umr ko'rish uchun qurilgan bo'lsa ham, ular hali ham cheklangan umrga ega. Ushbu xususiyatlar tufayli faol teglar odatda namlik kabi atrof-muhit parametrlarini o'lchash uchun real vaqt tizimlarida foydalaniladi, harorat va bosim. Boshqa turdagi teglar bilan solishtirganda, faol teglar ko'proq qimmat va batareyaning mavjudligi sababli ko'proq cheklovlarga ega.

Yarim passiv teglar integratsiyani qo'llab-quvvatlaydigan o'z quvvat manbaiga ega faqat mikrochip. Batareya zaryadsizlanganda, bu teglar signallarni uzata olmaydi yana. Faol teglardan farqli o'laroq, yarim passiv teglarda faol transmitter yo'q o'quvchi bilan muloqot qilish, ular orqaga tarqalish texnikasidan foydalanadilar, bu texnikada o'quvchidan uzatiladigan radiochastota energiyasi yig'iladi va o'quvchi aniqlay oladigan tarzda ma'lumotlarni uzatish uchun o'zgartirildi. Shuning uchun ular qila olmaydi muloqotni boshlash.

Passiv teglar ichki quvvat manbaiga ega emas. Ular o'z kuchlarini undan olishadi RFID o'quvchi tomonidan yaratilgan elektromagnit maydon. Ularda ham bor faol

transmitter yo'q va faqat o'quvchi signalidan keladigan quvvatga tayanadi. Passiv teglar, agar o'quvchi ularni faollashtirmasa, faol emas. Boshqa turlar bilan solishtirganda teglar, passiv teglar arzonroq va kichikroq, qoplangan diapazon esa qisqaroq. Passiv teglar hisob-kitoblarni qo'llab-quvvatlash uchun batareyaga ega bo'lishni talab qilmaydi va aloqa, ular juda uzoq vaqt davomida foydalanishda qolishi mumkin. Shular tufayli Ularni keng ko'lamli ilovalar uchun moslashtiradigan xususiyatlar, passiv teglar bozorda eng keng tarqalgan teglar turi. Bundan tashqari, passiv teglar ham mumkin atrof-muhit sharoitlariga toqat qiling, bu sharoitlar teglardan foydalanishni cheklaydi bort batareyalari. Biroq, passiv teglarda, hisoblash uchun zarur bo'lgan quvvat va aloqa maydondan olingan quvvat bilan cheklangan. Ba'zi echimlar teglarda olingan quvvatni oshirish uchun berilgan. Bunday yechimlardan biri teglarning antenna daromadini oshirish, bu esa ko'proq energiya yig'ishga yordam beradi maydon. Teg o'lchamida cheklov borligi sababli, bu yechim amaliy bo'lmagan. Maydonning kuchini oshirish boshqa yechimdir. Biroq, o'quvchilar tomonidan yuborilgan signallarning maksimal kuchi qonun bilan cheklangan. Tabiat tufayli RFID teglaridan foydalangan holda dizaynerlar ko'plab texnik cheklovlarga duch kelishadi, masalan:

- Cheklangan quvvat sarfi
- Cheklangan hudud
- Cheklangan ijro vaqti
- Cheklangan orqaga kanal
- Xotiraga kirish cheklangan

Passiv RFID teglari ishlashiga misol sifatida, passiv teg va o'quvchi o'rtasidagi aloqa orqali amalga oshiriladi energiya va ma'lumotlarni uzatishlarni aytib o’tsak bo’ladi. O'quvchi tomonidan taqdim etilgan energiya ga o'tkaziladi elektromagnit maydonlar orqali ulash yordamida teg. Energiyani olish uchun RFID teglari mumkin elektr maydonini ham, magnit maydonini ham yoki ulardan birini ishlating. Passiv RFID teglari bu maydonlardan biriga kirgunga qadar aloqa uchun hech qanday energiya yo'q. Sifatida teglar maydondan o'tishi bilan ular etarli quvvatni tortib olishlari mumkin maydon faollashtiriladi.

Taqdim etilgan maydonga asoslanib, ma'lumotlarni uzatishning turli usullari mavjud tegdan o'quvchiga. Zamonaviy usullardan biri bu orqaga o'tishdir qaysi oldin tasvirlangan edi. Bu usulda o'quvchi uzluksiz to'lqinni uzatadi radiochastota signalining atrof-muhitga tarqalishi. Bu sohaga teg kirsa, u o'quvchi signalini qabul qiladi va uni demodulyatsiya qiladi. O'tkazilgan to'lqin quyidagilardan iborat tegga qanday amallarni bajarish kerakligini bildiruvchi buyruqlar. Bunga javoban teg modulyatsiyalanadi uning javobi va uni o'quvchiga qaytarib yuboradi. Induktiv ulanish energiyani passivga o'tkazishning yana bir keng tarqalgan usuli hisoblanadi teglar. Bu usul dirijyorning paydo bo'lishiga asoslanadi magnit maydon, magnit maydon o'tkazgichda oqim oqimini hosil qiladi [4]. Ushbu usulda o'quvchining antennasi magnit maydon va tegni ta'minlaydi dirijyor sifatida o'ynaydi. Teg magnit maydonga

kirganda, uning antennasi hosil bo'ladi uni quvvatlantirish uchun tegga oqim. Magnit maydonlar past chastotada qo'llaniladi (LF) va yuqori chastotali (HF) RFID teglari teg va teg orasidagi masofa o'quvchi qisqa. Elektromagnit ulanish usuli induktiv ulash usuliga o'xshaydi farqi bilan magnit maydonni ishlatish o'rniga elektromagnit maydon energiyani teglarga o'tkazish uchun uzoqroq masofani bosib o'tadigan ishlatiladi.

RFID xavfsizlik hujumlarini ikkita asosiy toifaga bo'lish mumkin: maxfiylikni buzish va xavfsizlikni buzish. Maxfiylik buzilishida tajovuzkor hosilni yig'ishga harakat qiladi o'rtasidagi aloqalarni tinglash orqali ob'ektlardan ma'lumot olish ob'ekt va o'quvchi yoki ularni kuzatish orqali. Xavfsizlik buzilishida raqib nomaqbul aloqalarni amalga oshirish uchun teg yoki o'quvchining xatti-harakatlarini qalbakilashtiradi. Bunday xavfsizlik hujumlari jismoniy teg, aloqani nishonga olishi mumkin teg va o'quvchi yoki dastur yoki tizim o'rtasidagi kanal RFID texnologiyasidan foydalanadi. Ko'proq ta'sir qiladigan ko'p qatlamli hujumlar ham mavjud bir qatlam [7]. Quyida biz mavjud xavfsizlik xatarlari va tahdidlarini tasniflaymiz maqsadiga ko'ra jismoniy tahdidlar, kanal tahdidlari va tizim tahdidlari. Albatta, bugungi kunda RFID tizimlari duch keladigan tahdidlar sanab o'tilganlar bilan cheklanmaydi quyida. Axborot xavfsizligini tadqiq qilishning xususiyatlari shundaki, siz hech qachon bilmaysiz hujumchi keyingi qanday hujum qadamlarini qo'yadi. RFIDning mashhurligi bilan tizimlari, RFID tizimlariga qaratilgan hujumlar kuchayadi va murakkablashadi.

Har qanday kriptotizimning kuchini faqat ma'lum bir raqib modeli doirasida baholash mumkin va ular uchta komponentdan iborat:

1. **Hujum turi:** dushmanning tizim bilan o'zaro ta'sir qilish qobiliyati;
2. **Tahdid modeli:** dushmanning xavfsizlik xususiyatini buzish vazifasi;
3. **Dushman resurslarini taxmin qilish:** ham hisoblash, ham axborot.

Quyida sanab o'tilgan fikrlarning har birini batafsil ko'rib chiqamiz.

Hujum turi: Tizimning chidamliligini tahlil qilganda, raqib uning ishiga qanday xalaqit berishi mumkinligini aniqlash kerak. Dushmanning kriptotizim bilan o'zaro ta'sir qilishning sifatli imkoniyatlari hujum turiga qarab belgilanadi. Amaliyot darajasiga ko'ra, barcha turdagi hujumlarni ikki sinfga bo'lish mumkin:

1. protokol qatlami hujumlari;
2. jismoniy qatlam hujumlari: tizim komponentlariga jismoniy ta'sir.

Komponentlaridan biri RFID teglari bo'lgan narsalar Interneti (IoT qurilmalari) texnologiyasini ko'rib chiqishga bag'ishlangan ishlarda qo'shimcha ma'lumotlarni olish mumkin.

Protokoli qatlami hujumlarini jismoniy qatlam hujumlari doirasida raqiblarni quyidagi imkoniyatlarga ega deb hisoblash mumkin:

• ruxsatsiz jismoniy ta'sir qilish orqali RFID teg xotirasi hududidan ma'lumotlarni o'qish, nusxalash va o'zgartirish;

• tegning yaroqsizligi (jismoniy ochilish yoki kuchli elektromagnit maydon ta'siridan keyin);

• yon kanallardan kalitlar va qayta ishlangan ma'lumotlar haqida ma'lumot olish (masalan, maxfiy ma'lumotlarni qayta tiklash uchun tegning javob berish vaqti va quvvat sarfini o'lchash yo'li bilan);

• teg va reader o'rtasidagi aloqa kanalini blokirovka qilish (masalan, interferensiya kiritish orqali).

Jismoniy qatlam hujumlarini faqat qisman kriptografik usullar bilan oldini olish mumkin (masalan, RFC 8645 dan tashqi yoki ichki kalitlarni qayta yozish mexanizmlari yon kanal hujumlaridan himoya qilish uchun ishlatilishi mumkin).

RFID tizimlari uchun raqib modelini shakllantirishda qo'shimcha tashkiliy choralar hisobga olinishi va raqibning jismoniy darajadagi hujumlarni amalga oshirish qobiliyatini cheklash uchun qo'llanilishi mumkin (masalan, RFID teglarini xavfsiz saqlash uchun maxsus talablarni belgilash).

Yuqorida aytib o'tilgan turli xil xavfsizlik tahdidlarini bartaraf etish uchun RFID qurilmalaridan foydalanish kerak edi turli xil tahdidlarga qarshi kurashish uchun mo'ljallangan turli xil xavfsizlik choralari. Buning sababi kuchliroq Ko'proq resurslarga ega RFIDlar xavfsizlikni yanada oshirish uchun kriptografiyadan foydalanishi mumkin tizimning. RFID teglari beri alohida elementlarga shtrix kodlarni almashtiring, ular narxiga sezilarli hissa qo'shadi agar teg narxi yuqori bo'lsa, ushbu elementlar. Biz bunday texnikalarni maxfiylik muammolari va xavfsizlik bilan bog'liq muammolar bilan bog’liq bo’lgan murojaat qiladiganlarga tasniflaymiz.

FOYDALANILGAN ADABIYOTLAR:

1. Григорьева Анастасия. Rfid в 2015 и в 2020 году // Компоненты и технологии. –– 2021. –– Vol. 3.

2. Scharfeld Tom Ahlkvist. An analysis of the fundamental constraints on low cost passive radiofrequency identification system design : Ph.D. thesis / Tom Ahlkvist Scharfeld ; Massachusetts Institute of Technology. –– 2001.

3. A. E. GOREV «Informatsionniye texnologii na transporte. elektronnaya dentifikatsiya avtotransportnix sredstv i transportnogo oborudovaniya» Sankt-Peterburg. 2010 g. -s. 7

4. Alvarez Lopez va boshqalar, 2018; Jebali va Kouki, 2018; Tu va boshq., 2019

5. Babadjanov.E.S RFID kontaktsiz radiochastatali identifikatsiyalash tizimlarining ahamiyati // Respublika ilmiy-amaliy konferensiyasi maqolalar to‘plami. QDU 9-noyabr, 2021-yıl. 230-236 b

6. Babadjanov E.S., M.A.Fayzullaeva. Ishlab chiqarishdagi RFID standartlar tahlili // “O‘zbekistonda Fanlararo Innovatsiyalar va Ilmiy Tadqiqotlar” jurnali. «Best Publication». O‘zbekiston 2021. 3-son. 158-164 б.

7. Mol Petros, Tessaro Stefano. SecretKey Authentication Beyond the ChallengeResponse Paradigm: Definitional Issues and New Protocols // Manuscript, December. –– 2012.