Қазақстан Республикасының Білім және Ғылым Министірлігі

Л. Н. Гумилев атындағы Еуразия ұлттық университеті

Нығметов Алмас Асхатұлы

Байланыссыз төлем жүйесін әзірлеу

ДИПЛОМДЫҚ ЖҰМЫС

5В070400 – «Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы

Нұр-Сұлтан 2022

Қазақстан Республикасының Білім және Ғылым Министрлігі

Л.Н.Гумилев атындағы Еуразия ұлттық университеті

«Қорғауға жіберілді»
Компьютерлік және
программалық инженерия
кафедрасының меңгерушісі
т.ғ.к., доцент м.а.
Дюсекеев К.А. _____
«____» _____20___ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы: «Байланыссыз төлем жүйесін әзірлеу»

5В070400 – «Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы бойынша

Орындады: Нығметов А.А.

Ғылыми жетекшісі: Жартыбаева М.Г.

Нұр-Сұлтан 2022

Л. Н. Гумилев атындағы Еуразия ұлттық университеті

Ақпараттық технологиялар факультеті
5В070400 – «Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы
«Компьютерлік және программалық инженерия» кафедрасы

Бекітемін
Кафедра меңгерушісі
т.ғ.к. Дюсекеев К.А.
_____
« ___ » _____ 20___ ж.

Диплом жұмысын орындауға
ТАПСЫРМА

Студент Нығметов Алмас Асхатұлы, 4 курс, В4-70400-09/1 тобы, 5В070400 – «Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы, күндізгі бөлім.

1. Дипломдық жұмыс тақырыбы: «Байланыссыз төлем жүйесін әзірлеу» № 47-п ректорының бұйрығымен бекітілген 14 қаңтар 2022ж.
2. Білім алушының аяқталған жұмысты тапсыру мерзімі: 2 маусым 2022 ж
3. Жұмысқа қажетті бастапқы деректер (заңдар, әдебиет көздері, зертханалық және өндірістік мәліметтер):
   - Байланыссыз төлем технологияларын зерттеу;
   - Python бағдарламалау тілін және Qt ортасын зерттеп тану;
   - Arduino ортасының сипаттамасы ;
   - Деректер базасын құру сипаттамасы
4. Дипломдық жұмыста қарастырылатын сұрақтар тізімі:
   - Кіріспе;
   - Байланыссыз төлем технологияларының ерекшеліктері;
   - Байланыссыз төлемдерді жүзеге асыратын жүйелер және құралдар;
   - Алгоритмдер мен технологияларды негіздеу;
   - Байланыссыз төлем жүйесінің қосымшасын жүзеге асыру;
   - Қорытынды.
5. Графикалық құжаттар тізімі (сызбалар, кестелер, диаграммалар

және т.б.):

- Байланыссыз төлем технологияларының әрекет сызбалары;
- Деректер ағынының схемасы;
- Жүйенің архитектурасы;
- қосымша моделі;

6. Ұсынылатын негізгі әдебиеттер тізімі:

- Laurence Moroney. The Firebase Realtime Database(The Definitive Guide to Firebase.) pp 51–71
- Explaining an Adoption and Continuance Intention to Use Contactless Payment Technologies: During the COVID-19 Pandemic(Wilert Puriwat, Suchart Tripopsakul)
- Hussein al ofeishat (2012). IJCSNS International Journal of Computer Science and Network Security, VOL.12, pp 93-99
- Learning OpenCV: Computer Vision with the OpenCV Library (Gary Bradski, Adrian Kaehler) 2011. 901p.
- Throughput Analysis of an Amazon Go Retail under the COVID-19-related Capacity Constraints// Procedia Computer Science, 2022, Vol.198,pp 602-607.

7. Жұмыс бойынша кеңестер (оларға қатысты жұмыс бөлімдерін көрсете отырып)

Номер, бөлімнің, тараудың атауы	Ғылыми жетекші, консультант	Тапсырма алу мерзімі	Тапсырманы берді (қолы)	Тапсырманы қабылдады (қолы)
Мазмұны	Жартыбаева М.Г.	22.12.2021-10.01.2022		
Кіріспе	Жартыбаева М.Г.	22.12.2021-10.01.2022		
Әдебиеттер тізімі	Жартыбаева М.Г.	22.12.2021-10.01.2022		
1 тарау	Жартыбаева М.Г.	11.01.2022-04.02.2022		
2 тарау	Жартыбаева М.Г.	04.02.2022-05.03.2022		
3 тарау	Жартыбаева М.Г.	05.03.2022-08.04.2022		
Қорытынды	Жартыбаева М.Г.	24.04.2022-03.05.2022		

8. Дипломдық жұмысты орындау кестесі

№	Жұмыс кезеңдері	Жұмыстың кезеңдерінің орындалу мерзімі	Ескерту
1	Дипломдық жұмыстың тақырыбын бекіту	22.12.2021	№47-п бұйрық
2	Дипломдық жұмысты даярлау үшін материал жинау	14.12.2021	Практика алдында
3	Дипломдық жұмыстың аналитикалық бөлімін дайындау (1 тарау)	17.12.2021	Практика алдында
4	Дипломдық жұмыстың жобалық бөлімін дайындау (2 тарау)	20.01.2021	Практика кезінде
5	Дипломдық жұмыстың экономикалық бөлімін дайындау (3 тарау)	31.01.2021	Практика кезінде
7	Дипломдық жұмыстың толық мәтінінің алдынғы нұсқасын аяқтау	16.03.2022	Практикадан кейінгі бірінші аптада
8	Дипломдық жұмысты алдын-ала қорғауға тапсыру	17.04.2022	Диплом алдындағы практика
9	Дипломдық жұмысты пікірлеме алуға тапсыру	16.05.2022	
10	Дипломдық жұмыстың соңғы нұсқасын ғылыми жетекшінің пікірімен тапсыру	25.05.2022	
11	Дипломдық жұмысты қорғау	02.06.2022	

Тапсырманың берілген күні «17» қаңтар 2022

Ғылыми жетекшісі
PhD, доцент м.а _____ Жартыбаева М.Г.

Тапсырманы қабылдады студент _____ Нығметов А.А.

Мазмұны

Кіріспе

Бүгінгі таңда бизнес технологияларының енгізу жылдамдығы корпорациялармен тұтынушыларға байланысты, бірақта тұтынушылар арасында шыққан инновациялар әлдеқайда жылдам қабылданады. Қазіргі уақытта сондай инновациялардың бірі бұл – байланыссыз төлем жүйесі болып табылады.

Әрине байланыссыз төлем жүйесі өзінің мөлшер шектеулері бойынша кез келген төлемдерді іске асыра алмайды, бірақта шағын операцияларға келгенде өте ыңғайлы болып табылады. Мысалға айтарға қала ішінде автобуста және метрода мобильді байланыссыз төлем жасаған, ескірген жолаушы картасымен(AstraBus,Onay) төлем жасағаннан әлдеқайдам ыңғайлы болып келеді. Және де тек транспорт саласында емес, бүткіл шағын бизнесте байланыссыз төлем жүйесі PIN және қарапайым банк карталарын озып түсіп, Қазақстандағы ең танымал төлем жүйесіне айналғаны факт болып табылады.

Бұл жаңа тенденцияның ең басты қауіпі – бұл байланыссыз төлемдердің мемлекет деңгейінде есепке алынуың және салық салу мәселесінің қиындауы. Бірақта қазір ол мәселе шешілуде және де кейбір дүкендер әлі күнге чек беруді тоқтатпады.

Мобильді технологиялардың дамуы байланыссыз төлем жүйесінің дамуына тікелей әсерін тигізеді. Мобильді электронды әмияндарды қолдану қазіргі уақытта ең үлкен өзгерістердің бірі болып табылады. Мобильді құрылғылар жай ғана төлем және аударма операциялары туралы информацияны таратып қоймай, сол операцияларды іске асыру құралы ретінде үлкен потенциалын көрсетуде. Электронды мобильді әмияндар уақыт өте көптеген тұтынушылардың арасында кең тарауда. Соған байланысты банктер және де басқа финанс компаниялары осы технологияға аса көп назар аударуда. Америка Банкінің коммерциялық карталар бөлімшесінің басқармасы David Voss-тың айтуы бойынша – “Мобильді құрылғылар болашақта физикалық төлем карталарын алмастыруы әбден мүмкін”

Мобильді әмияндар ұсынатын байланыссыз төлем жүйесі қолма қол ақша қолданбайтын болғандықтан экологиялық жағдайдан, және Covid-19 жағдайында өзін жақсы көрсетеді. Бұлда технологияның тез дамып, ортаға тез сіңіп кетуінің бірден бір себебі болып табылады.

Физикалық картаның қажет етпеу ыңғайлығынан басқа, жаңа аутентификация мүмкіндіктері мен токенизация технологиясының арқасында мобильді әмиян арқылы төлемдер бұрынғыдан бетер қауіпсіз болып саналады. Саусақ іздері немесе бетті тану сияқты биометриялық деректерді қолдана отырып, төлемдер біріктіріліп, электрондық коммерция ортасында қауіпсіздіктің жоғары деңгейін қамтамасыз ете алады. Сонымен қатар, мобильді әмиянды пайдаланатын транзакциялар байланыссыз лимитке ие емес және таңбаланған шот нөмірін пайдалану арқылы дәстүрлі карточкалық төлемдермен салыстырғанда қауіпсіздігі жоғары болып келеді. Бұл шоттың

нақты нөмірі ешқашан мобильді құрылғыда сақталмайды және транзакцияны аяқтау үшін сатушыға берілмейді дегенді білдіреді.

Қазіргі уақытта әлем бойынша мобильді әмияндар тез танымалдыққа ие болуда, әсіресе азия елдерінде, мысалы Қытай тұтынушыларының 70% мобильді әмияндарды пайдаланады. Сонымен қатар тек Қытай да емес Қазақстанда да мобильді әмиянды қолданушылар саны тез артуда. Бұның басты себебі Kaspi банкі және оның мобильді қосымшасы болып табылады. Комиссиясыз төлемдер, жылдам кредиттер, басқа тұтынушылармен тез ақша алмасу, және де бөліп төлеу мен тауарды үйге жеткізу қызметтері қосымшаны басқа банктардың арасында фаворит қылдырды. Статистикаға сүйенсек қазақстандықтардың 58% қосымшаны орнатып, күн сайын қолданады екен, бұл дегеніміз 11 миллион адам.

Жаңа технологиялардың дамуы сауда жүргізу процессін күрт өзгертті, дүкендерде тұтынушылар санына шектеу қойылып, ара қашықтық сақтау заңдары шықты. Осы қойылған шектеулер шағын бизнес иелеріне қиындық тудыртты. Азық-түлік, ұсақ тауарлардың өзін жеткізу қызметі арқылы алдыртатын болды. Қазір жағдай жақсарып, өз қалпына келуде, алайда осындай жағдайларды алдын алу жолдары қарастырылып жатыр. Осы мәселе бойынша байланыссыз төлем әдістері өте қолайлы болып табылады. Қазіргі технологиялар тікелей жанауды немесе дүкен саудагерімен байланысқа түспей ақ тұтынушы өз тауарларын кассадан өткізіп, төлем жасау жүйесін құрастыру мүмкіндігін береді.

Дипломдық жұмыстың мақсаты байланыссыз төлем жүйесін қолданып Covid-19 жағдайын ескеріп, тікелей жанаусыз, сауда жүргізуге арналған қосымшаның моделін құрастыру.

Мақсатқа сәйкес келесі міндеттер орындалады:

1. Arduino микропроцессор программалау ортасын және байланыссыз түрде деректер алмасу әдістерін зерттеу;
2. Байланыссыз төлем жүйесін толық қамтамасыз ететін қосымшаны әзірлеу;
3. Қосымшаның программалық бөлігін әзірлеу
4. Қосымшаның техникалық бөлігін әзірлеу

Дипломдық жоба келесі құрылымға ие:

1. Бірінші бөлімде байланыссыз төлем жүйесіне шолу жасалып оның қазіргі қолдану орталары зерттеледі. Қазіргі таңда іске асырылған жүйелер зерттеліп, олардың айырмашылығы анықталады. Технологияның даму тарихы мен мүмкіндіктері қарастырылып, жұмыс істеу принципі барынша зерттеліп, сараланды;
2. Екінші бөлімде байланыссыз төлем жүйесінің технологияларының артықшылықтары мен кемшіліктерін зерттеп, қосымшаны құрудағы ең тиімдісі таңдалады. Қосымшаны құру ортасын және программалау орталары таңдалады;
3. Үшінші бөлімде дипломдық жұмыстың мақсатына сәйкес моделді практика жүзінде Python программа тілімен Arduino программалау ортасында әзірлеу үрдісі көрсетілген. Зерттеу жұмысы кезінде жиналған мәліметтерді

қолдана отырып, құрастырылған моделдің жұмысы сипатталған. Қандай құралдар қолданғаны, қандай программалау кодтары арқылы жұмыс істейтіні туралы барлығы баяндалып, сипатталынады;

4. Қортынды бөлімде жұмыстың міндеттерінің орындалу дәрежесі мен зерттеу нәтижелері қарастырылып, тақырып бойынша толық қортынды жасалған.

1 Байланыссыз төлем жүйесінің ерекшеліктері

1.1 Байланыссыз төлем жүйесі түсінігі

Байланыссыз төлем бұл дебеттік, несиелік, смарт-карта, смартфондар немесе радиожиілікті сәйкестендіруді (RFID) және жақын өрісті байланыс технологиясын (NFC) пайдаланатын басқа төлем құрылғысы арқылы тұтынушылардың тауарларды немесе қызметтерді сатып алуының қауіпсіз әдісі. Бұл төлем әдісі төлем картасын немесе басқа құрылғыны байланыссыз төлем терминалына тигізу арқылы жүзеге асырылады. Кейбір банктер мен кәсіпорындар байланыссыз төлемдерді tap-and-go немесе tap деп атайды.

Байланыссыз төлемді кеңінен қолдану тарихындағы алғашқы оқиға 1995 жылы Оңтүстік Кореяда болды, онда Сеулдің автобус көлік қауымдастығы жолаушыларға UPass картасын шығарды. Ол жолақысын байланыссыз төлеуге мүмкіндік берді. Mobil компаниясында байланыссыз төлем технологиясы 1997 жылы пайда болды: жанармай құю бекеттеріндегі автокөлік иелері отынды кезексіз төлей отырып, уақытты үнемдеуге мүмкіндік алды (сурет 1.1).

Сурет 1.1 Алғашқы қолданыста болған UPass және Mobil компанияларының байланыссыз төлем карталары.

Банк карталарымен байланыссыз төлем жүргізуге арналған бірінші халықаралық стандартты 1996 жылы Europay, Visa және Mastercard компаниялары бірлесіп әзірледі. Стандарттың кең қолданысқа енгенге дейін көптеген жылдар өтеді, алайда дәл осы қадам сатушылардың NFC байланыссыз технологиясы бар төлем терминалдарына ауқымды көшуіне себеп болады.

Жылдар өте, 2004 жылы Sony, Nokia және NXP Semiconductors компаниясы NFC Forum коммерциялық емес қауымдастығын құрды, ол технологияны тұрмыстық электроникаға, мобильді құрылғыларға және компьютерлерге тарату міндетін алды. Сол жылы АҚШ-та байланыссыз Банктік карталар пайда болды, ал төрт жылдан кейін Mastercard, Visa және American Express дебеттік карталарды ғана емес, сонымен бірге несиелік

байланыссыз карталарын да жасай бастады.

Екі жылдан кейін NFC функциясы бар тарихтағы алғашқы мобильді құрылғы-Nokia 6131 (сурет 1.2) телефоны сатылымға шықты. Қазақстанға бұл технология тек 2016 жылдан бастап енгізіле бастады. NFC технологиясын алғаш Visa көмегімен Казкоммерцбанкі орнатқан болатын. Бірақта технология халық арасында кең тарай қоймады. Оған себеп технологияның өз уақытынан озық болғаны, және де сол кезде NFC технологиясы орнатылған телефондардың да саны көп болмады.

Сурет 1.2 Маркерге негізделген толықтырылған шынайылық.

NFC технологиясының дамуына ең үлкен үлес қосқан Google, Android секілді технологиялық алыптар болып табылады. Олар тұтынушы әмиянын үйде ұмытып кетсе де, телефонын әрқашан өзімен алып жүреді деген ойда болды. Егерде тұтынушы картамен емес, тек телефонымен төлем жүргізсе деген оймен Google компаниясы 2011 жылы Google Wallet қосымшасын іске қосты. Төрт жылдан кейін оған Android Pay функциясы қосылды, ал 2018 жылы аты өзімізге таныс Google Pay (сурет 1.3) ауысты.

Сурет 1.3 Google Pay қосымшасы.

Google компаниясына жауап ретінде 2014 жылы Apple компаниясы өзінің Apple Pay қосымшасын жасап шығарды. Бір жылдан соң Samsung өзінің аналогын шығарды. Samsung Pay қосымшасының басқаларынан айырмашылығы ол NFC төлемдерін ғана емес, сондай-ақ магниттік жолағы бар

карталарға арналған терминалдар бойынша төлемдерді де қолдады.

Ақырында, 2015 жылы чип орнатылған банк карталары бойынша операцияларға арналған халықаралық стандарт - EMV (Europay + Mastercard + Visa) технологиясы құрастырылды. Жаңа стандарт транзакциялардың қауіпсіздігін едәуір арттыруға арналған. Мұндай технологияның пайда болуы бүкіл әлем бойынша жүздеген мың компанияларды NFC-төлемі бар терминалдарға көшуге итермелейді. Сервисті оңай баптауға болады: карта нөмірі смартфонда да, төлем жүйелерінің серверлерінде де сақталмайды. Төлем кезінде телефонды немесе сағатты төлем терминалына жақындатса болғаны-ПИН-кодты енгізу қажет емес. EMV технологиясы енгізілгеннен кейін "әмиянымды ұмытып кетіппін, төлей алмаймын" деген жағдай жиі кездесетін болады, ал смартфондар мен ақылды сағаттар әмиянды мүлдем ауыстыруы мүмкін. Бір кемшілік: NFC қолдайтын сауда нүктелерінің саны аз. Бірақ бұл уақыт мәселесі. Соңғы жылдары банктер де, сауда желілері де байланыссыз төлемдер үшін инфрақұрылымды белсенді дамытуда.

1.2 Байланыссыз төлем жүйесінің негізгі технологиялары

1.2.1 NFC-жақын өріс байланысы

NFC-байланыссыз транзакциялар үшін сымсыз байланыс технологиясы. NFC ISO 18092 стандартында анықталған және ISO14443 смарт-карта стандартымен кері үйлесімді. Демек, NFC құрылғыларын смарт-карталар негізінде бұрыннан бар инфрақұрылымдарға оңай біріктіруге болады. NFC 10 сантиметрге дейінгі қашықтықта байланыссыз транзакцияларды жүргізуге мүмкіндік береді. Бұл билет кассалары мен POS терминалдарындағы транзакциялар үшін ақылға қонымды жұмыс ауқымы, ал логистика мен денсаулық сақтау саласында радиожиілікті Сәйкестендіру (RFID) технологиясы қолданылады. технология. NFC және RFID технологиялары бірдей физикалық технологияға негізделген: электромагниттік толқындар [1].

Магниттік толқындар. RFID байланыс үшін бірнеше түрлі жиілік диапазондарын қолданыста болса, NFC 13,56 МГц диапазонында жұмыс істейді. RFID негізінен тауарлар мен адамдарды қашықтықтан бақылау және анықтау үшін қолданылады. Екінші жағынан, NFC байланыссыз қол жеткізу немесе төлем сияқты күрделі және қауіпсіз транзакциялар үшін қолданылады. Қысқа жұмыс қашықтығының артықшылығы-транзакциялар әдетте тек арнайы түрде шақырылады [2].

NFC қосылған құрылғыда келесі жұмыс режимдері бар:

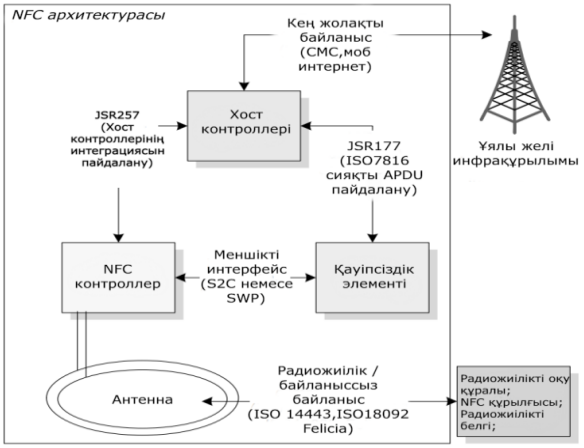
Оқу/жазу режимі (Proximity Coupling Device, PCD): осы режимде жұмыс істей отырып, NFC құрылғысы NFC үйлесімді пассивті (батареясыз) транспондерлерде сақталған деректерді оқи және өзгерте алады. Мұндай

белгілерді, мысалы, онлайн дүкендерде табуға болады, бұл пайдаланушыға NFC құрылғысын пайдаланып белгіні оқу арқылы қосымша ақпарат алуға мүмкіндік береді [3].

Карта эмуляциясы (Proximity Inductive Coupling Card, PICC): NFC құрылғысы карта эмуляция режиміне ауысқаннан кейін смарт-карта ретінде де жұмыс істей алады. Бұл жағдайда сыртқы оқырман смарт-картаны NFC құрылғысынан ажырата алмайды. Бұл режим, мысалы, билеттерді төлеу және сату қосымшалары үшін пайдалы. Peer-to-Peer (Near Field Communication, NFC):

NFC peer-to-peer режимі NFC қосылған екі құрылғыға контактілерді, Bluetooth жұптастыру ақпаратын немесе кез-келген басқа деректерді бөлісу үшін қос бағытты байланыс орнатуға мүмкіндік береді.

Хаттаманы өңдеу, сондай-ақ аналогтық сигналды сандық және керісінше түрлендіруді NFC контроллері жүзеге асырады. Осы интегралды Схемадан басқа, мобильді құрылғы - әдетте ұялы телефон - құпия деректерді сақтау үшін қосымша қорғалған чипті қамтиды. Бұл қорғалған чипті жүзеге асырудың әртүрлі тәсілдері бар: SIM картасын пайдалану, қосымша смарт-карта чипін қосу немесе деректерді қорғалған жад картасында сақтау [4]. Мұндай қауіпсіз деректер контейнеріндегі мәліметтер - қорғалған элемент (SE) деп те аталады- бір жағынан NFC интерфейсі арқылы қол жетімді болуы мүмкін (NFC контроллерінің чипі жапсырма эмуляциясы режимінде), ал екінші жағынан хост контроллері арқылы. Мысалы, ұялы желі арқылы алынған деректерді (мысалы, GSM) қорғалған элементте сақтауға болады, содан кейін NFC [3] интерфейсі арқылы сұрауға болады.Қорғалған элементтің өзі бұзылуға төзімді етіп жасалған. (сурет 1.4) NFC құрылғысының архитектурасы көрсетілген.



Сурет 1.4 NFC-техгнологиясын ұялы телефонға және байланыс ағындары/интерфейстеріне біріктіру.

NFC-тің басты артықшылығы-Bluetooth немесе WiFi-ге қарағанда жылдам байланыс уақыты (200 мс).

Bluetooth немесе WiFi-мен салыстырғанда. Әдетте NFC құрылғылары

арасында байланыс орнату үшін пайдаланушының араласуы немесе PIN-кодты енгізу қажет емес. Алайда, NFC қосылымындағы деректерді беру жылдамдығы (максимум 424 кбит/сек) осы технологияларға қарағанда әлдеқайда төмен. Өнеркәсіп пен ғылыми орта NFC технологиясын мобильді құрылғыларға біріктіруге мүдделі. Марк Вайзер атап өткендей, технологияның өзі жоғалып кетуі өте маңызды және тек қолданушымен өзара әрекеттесу пайдаланушыға көрінуі керек. NFC өзінің Touch and Go философиясының арқасында осы өлшемге сәйкес келуге жақсы мүмкіндігі бар. NFC қосылған телефондар пайдаланушыларға қоршаған ортамен бұрын-соңды болмаған қарым-қатынас жасауға мүмкіндік береді. Сонымен қатар, біріктірілген қауіпсіз элемент Сатянараянан ұсынғандай, пайдаланушы үшін сәйкестендіру ақпаратын қауіпсіз түрде сақтайды [5] [6] [7].

1.2.2 Мобильді төлемдер

Смартфондар мен ұялы телефондар сияқты сымсыз құрылғылар арқылы жасалатын төлемдер транзакция үшін төлемді азайтуға, онлайн төлемдердің қауіпсіздігі мен ыңғайлылығын арттыруға мүмкіндік береді. Бұл төлем әдісі кәсіпорындарға өз клиенттері туралы, сондай-ақ оларды сатып алу туралы пайдалы ақпарат жинауды жеңілдетті. Мобильді төлем жүйелері бүкіл әлемде басқа телекоммуникациялық инфрақұрылымдармен салыстырғанда мобильді құрылғылардың таңқаларлық өсуі мен кең таралуы нәтижесінде қолданылады. Мобильді төлемдерді онлайн сатып алу үшін де, оффлайндық микро төлемдер үшін де пайдалануға болатындығы анықталды. Ұялы телефондарда үлкен тұтынушылық база болғандықтан, онлайн-саудагерлер бұл төлем әдісі үшін тартымды болуы мүмкін. Мобильді төлем қызметтерін пайдалану транзакцияның жалпы құнын төмендетеді, сонымен қатар қауіпсіздікті жақсартады.Алайда, олардың халықаралық төлемдер мен құпиялылықты қамтамасыз ете алмауы айтарлықтай пайдаланушы базасын жаулап алудағы бірнеше проблемаларға әкелді[16].

Сымсыз төлемдер ұялы телефондар, смартфондар, жеке сандық көмекшілер (PDA) немесе ұялы терминалдар сияқты мобильді пайдаланушылардың құрылғыларындағы сату нүктелерінде және/немесе транзакцияларға қызмет көрсету нүктелерінде төлемдерді қолдау үшін мобильді коммерцияға арналған сымсыз электрондық төлемдер. Сымсыз төлем жүйесі дегеніміз не? Сымсыз төлем жүйесі - бұл мобильді сауда жүйесі сымсыз желілерде және сымсыз интернет инфрақұрылымдарында мобильді коммерциялық қосымшаларды қолдайтын электрондық сауда төлем операцияларын өңдейді. Жалпы, сымсыз төлем жүйелерін сымсыз сатушылар, мобильді контент сатушылар және сымсыз ақпараттық және коммерциялық провайдерлер пайдалана алады. мобильді контент провайдерлері және сымсыз коммерция қосымшалары жүзеге асыратын төлем операцияларын өңдеуге және

қолдауға арналған сымсыз Ақпарат және коммерциялық қызмет провайдерлері. Бұған сымсыз технологияларға негізделген сауда жүйелері, мобильді порталдар, сымсыз ақпараттық және коммерциялық сервистік қосымшалар кіреді.

Қолданыстағы сымсыз төлем жүйелерін үш түрге жіктеуге болады. Бірінші түрі белгілі шот-фактураға негізделген төлем жүйелері, онда әр клиент сенімді үшінші тарап жүргізетін белгілі бір шот-фактурамен байланысады, мысалы, банк (немесе телекоммуникациялық компания). Алдын ала төленген транзакцияларда бұл шот тұтынушының жинақ шотына тікелей байланысты болады. Тұтынушы алдын-ала төленген транзакцияны өңдеу кезінде есептен шығарылатын осы шоттағы оң балансты сақтайды. Егер төлемнен кейінгі операцияларға қолдау көрсетілсе, операция бойынша шығыстар тұтынушының шотына есептеледі. Содан кейін тұтынушыға мезгіл-мезгіл шот беріледі және ол банктегі шоттағы қалдықты төлейді. Қазіргі уақытта шот-фактураға негізделген сымсыз төлем жүйелерінің үш бөлімі бар:

а) тұтынушыларға ұялы телефондар арқылы тауарлар мен қызметтерді сатып алуға және төлеуге мүмкіндік беретін ұялы телефондарға негізделген төлем жүйелері;

б) смарт-картаны, жады бар микропроцессорды және жадты басқару үшін операциялық жүйемен бірге микропроцессорды пайдаланатын смарт-карталарға негізделген төлем жүйелері;

в) тұтынушыларға несие карталары арқылы мобильді құрылғыларда төлем жасауға мүмкіндік беретін несие карталарына негізделген мобильді төлем жүйелері.

Сымсыз төлем жүйелерінің екінші түріне мобильді POS-төлем жүйелері кіреді, олар тұтынушыларға ұялы телефондарын пайдаланып сауда автоматтарынан (немесе бөлшек сауда дүкендерінен) тауарлар сатып алуға мүмкіндік береді. Төлем жүйелерінің бұл түрі Ұялы телефон пайдаланушыларына телефондарын өздері таңдаған төлем құралдарына айналдыруға мүмкіндік беретін жүйенің қолданыстағы несиелік және дебеттік карта жүйелерін толықтыруға арналған. Қазіргі уақытта POS төлем жүйелерінің екі түрі бар. Бірінші түрі сату нүктелерінде автоматтандырылған төлемдер ретінде белгілі. Олар көбінесе сауда автоматтарында, тұрақ есептегіштерінде немесе ақылы машиналарда қолданылады, бұл мобильді пайдаланушыларға тауарларды сатып алуға мүмкіндік береді (мысалы, жеңіл тағамдар, тұрақ рұқсаттары және кино билеттері). Тағы бір түрі сату нүктелеріндегі төлемдер (дүкен сөрелері, такси) деп аталады, бұл мобильді пайдаланушыларға такси жүргізушісі немесе есептегіштегі сатушы сияқты қызмет көрсететін тараптың көмегімен мобильді құрылғылар арқылы төлемдер жасауға мүмкіндік береді.

Үшінші түрі Ұялы әмияндар ретінде белгілі, бұл сымсыз транзакциялар үшін мобильді төлемдердің ең танымал түрі. Электрондық әмияндар сияқты, олар қолданушыға мобильді құрылғыдан сатып алу кезінде бір рет басу арқылы еске түсіретін шот-фактуралар мен жеткізілім туралы ақпаратты сақтауға мүмкіндік береді [11]. SET технологиясын пайдаланатын серверлік мобильді

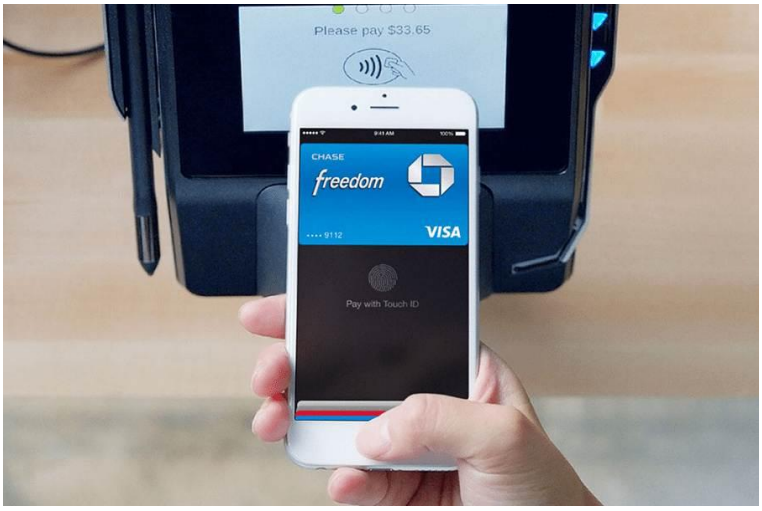
MasterCard электрондық әмияндары сатушылар мен карта ұстаушылар үшін қауіпсіз транзакциялық мүмкіндіктерді қамтамасыз ету үшін қолданылады. Бірқатар сымсыз төлем жүйелерін ірі ойыншылар ұсынғанына қарамастан, сымсыз төлем жүйелерін жобалау мен іске асыруға арналған техникалық басылымдар және егжей-тегжейлі төлем хаттамалары өте аз. Бұл мақалада біз Bluetooth технологиясын қолдана отырып, динамикалық мобильді ортада сымсыз төлем операцияларын жүргізу үшін мобильді пайдаланушыларға қолдау көрсету үшін сымсыз төлем жүйесін әзірлеу және енгізу туралы хабарлаймыз. Мобильді төлемдердің бұл түрін динамикалық мобильді ортада төлеуші мен төлем алушыға мобильді коммерция үшін сымсыз төлем операцияларын жүргізуге мүмкіндік беру үшін пайдалануға болады. Қолданудың типтік мысалдары:

Үшінші түрі Ұялы әмияндар ретінде белгілі, бұл сымсыз транзакциялар үшін мобильді төлемдердің ең танымал түрі. Электрондық әмияндар сияқты, олар қолданушыға мобильді құрылғыдан сатып алу кезінде бір рет басу арқылы еске түсіретін шот-фактуралар мен жеткізілім туралы ақпаратты сақтауға мүмкіндік береді [11]. SET технологиясын пайдаланатын серверлік мобильді MasterCard электрондық әмияндары сатушылар мен карта ұстаушылар үшін қауіпсіз транзакциялық мүмкіндіктерді қамтамасыз ету үшін қолданылады. Бірқатар сымсыз төлем жүйелерін ірі ойыншылар ұсынғанына қарамастан, сымсыз төлем жүйелерін жобалау мен іске асыруға арналған техникалық басылымдар және егжей-тегжейлі төлем хаттамалары өте аз. Бұл мақалада біз Bluetooth технологиясын қолдана отырып, динамикалық мобильді ортада сымсыз төлем операцияларын жүргізу үшін мобильді пайдаланушыларға қолдау көрсету үшін сымсыз төлем жүйесін әзірлеу және енгізу туралы хабарлаймыз. Мобильді төлемдердің бұл түрін динамикалық мобильді ортада төлеуші мен төлем алушыға мобильді коммерция үшін сымсыз төлем операцияларын жүргізуге мүмкіндік беру үшін пайдалануға болады. Қолданудың типтік мысалдары:

- TAXI жолаушысы мен жүргізушісінің арасындағы мобильді төлемдер
- Еркін нарықтағы саудагер мен тұтынушының арасындағы мобильді төлемдер.
- Тұрақ немесе метро үшін мобильді төлемдер

Мобильді төлем жүйесі үшін өте қызықты тәсілді Fujitsu Lab ' s [8] - те сымсыз әмиян деп атады. Ұсынылған құрылым онлайн төлем жүйесін әртүрлі клиринг әдістерімен және POS түрлерімен жүзеге асыруға мүмкіндік береді. Олар сондай-ақ сымсыз саудагерлермен транзакциялар жүргізу үшін WLAN пайдаланатын мобильді төлем құрылғысы үшін бірегей аппараттық әзірлемені ұсынды. Сонымен қатар, ұялы телефонға арналған J2ME нұсқасы іске асырылды. Бұл жағдайда мобильді желі ішкі серверлік жүйемен төлем операцияларын өңдеу үшін пайдаланылды. [9], [10] Гао және т.б. төлеуші мен алушыны онлайн-тексеру үшін сервермен жергілікті транзакция үшін Bluetooth негізіндегі сымсыз төлем жүйесін ұсынады. Жүйе POS төлемдерін, сондай-ақ тең-теңімен транзакцияларды қауіпсіз түрде жүзеге асыра алады. Екі жүйе де,

сымсыз әмиян және Bluetooth негізіндегі енгізу сервердің артқы жағында болуын талап етеді. Төлеушіге немесе алушыға төлем операциясына қатысатын даналардың төлнұсқалығын тексеру үшін онлайн-қосылу қажет. Онлайн-төлем жүйелеріне келетін болсақ. Мұндай жүйеде жеке ақпарат - әдетте ақша немесе билеттер-жоғары қорғалған қашықтағы құрылғыда/интеграцияланған схемада сақталады. Транзакциялар серверге онлайн қосылуды қажет етпейді және осылайша транзакция кезінде уақытты үнемдейді. Әмияндар мен терминалдар клиринг пен есеп айырысу үшін немесе әмиянды ақшамен толтыру үшін мезгіл-мезгіл синхрондалуы керек. Хольцманмен сипатталған. Жүйе контактілі смарт-картаға негізделген және микроплатеж операцияларын жүргізуге арналған. Смарт-картада ақшаны сақтауға арналған қорғалған әмиян бар. Бұл алдын-ала төленген әмиян қолданар алдында банкоматта толтырылады. POS сайтында смарт-карта терминалға салынып, тиесілі сома әмияннан алынады. Терминал пайдаланушыдан төлем операциясын жасау үшін PIN-кодты енгізуді талап етпейді. мәміле. Пайдаланушылардың көзқарасы бойынша, алдын-ала төленген жүйелер өте танымал емес, өйткені Дальберг және т.б.] атап өткендей, бұл қауіпсіз автономды төлем жүйесінің жалғыз техникалық шешімі. Акио және т.б. Japan Rail компаниясы жүзеге асырған қоғамдық көлік билеттерін төлеудің үлестірілген жүйесін егжей-тегжейлі сипаттайды. Әмиян Sony FeLiCa технологиясын қолданатын байланыссыз смарт-картада орналасқан. Бұл әмиян - QUICK сияқты-банкоматта қайта зарядтау керек. Akia және т. б. орталықтандырылған емес, әмиянға негізделген үлестірілген тәсілді таңдаудың келесі себептері аталады: жақсырақ масштабталу, енгізу және техникалық қызмет көрсету шығындары, сондай-ақ жүйенің қарапайым архитектурасы. сондай-ақ жүйенің қарапайым архитектурасы. NFC технологиясының мобильді құрылғыда қолдануы келесі (сурет 1.5) көрсетілген



Сурет 1.5 NFC технологиясы арқылы мобильді төлемді іске асыру процессі.

Төлем жасау үшін байланыссыз интерфейсті қолдана отырып, әмиянды

NFC құрылғысының қауіпсіз элементіне біріктіру идеясы айқын [14]. Бұл факт қауіпсіз элементтегі ақпаратты өзгерту мүмкіндігімен бірге билеттерді төлеу және сату сияқты жаңа қосымшалар үшін перспективалы тәсіл болып табылады. Сондай-ақ, Zmijewska [15] NFC ұялы төлемдер үшін перспективалы технология екенін атап өтті.

1.3 Байланыссыз төлем жүйелеренің covid-19 кезіндегі әсері

Коронавирустық Пандемия біздің өміріміздің барлық саласында тұтынушылардың мінез-құлқына әсер етуді жалғастыруда. Сатып алушылардың мінез-құлқындағы өзгерістермен қатар төлем әдістері де өзгереді: адамдар қолма-қол ақша немесе чипі және/немесе PIN-коды бар банк карталары сияқты дәстүрлі әдістерден бас тартады және карталар, телефон қосымшалары немесе тозатын құрылғылар арқылы байланыссыз төлемге көшеді.

Жылдам, жиі және аз мөлшерде транзакциялар үшін қолданылатын байланыссыз әдістер төлемдерді төлем терминалына немесе сауда нүктесінің терминалына (POS) апару немесе апару арқылы жүзеге асыруға мүмкіндік береді. Пандемия кезінде олар жаһандық және ұлттық денсаулық сақтау ұйымдары шығарған қауіпсіздік нұсқауларына сәйкес келетін тартымды нұсқа болып табылады. Байланыссыз әдістер адамдармен және құрылғылармен физикалық байланысты шектейді, әлеуметтік алыстауды жеңілдетеді және қолма-қол ақшамен, жалпы POS терминалдарымен немесе қаламдармен/стилустармен айналысудан аулақ болады.

Dynata журналының "байланыссыз төлемдердегі серпіліс"шағын есебінде[17] Жаңа қалыпты жағдайда тұтынушылық төлем әдістерінің үш негізгі аспектісі, соның ішінде:

1) Пандемия байланыссыз төлемдерді қолдануды жеделдетті:

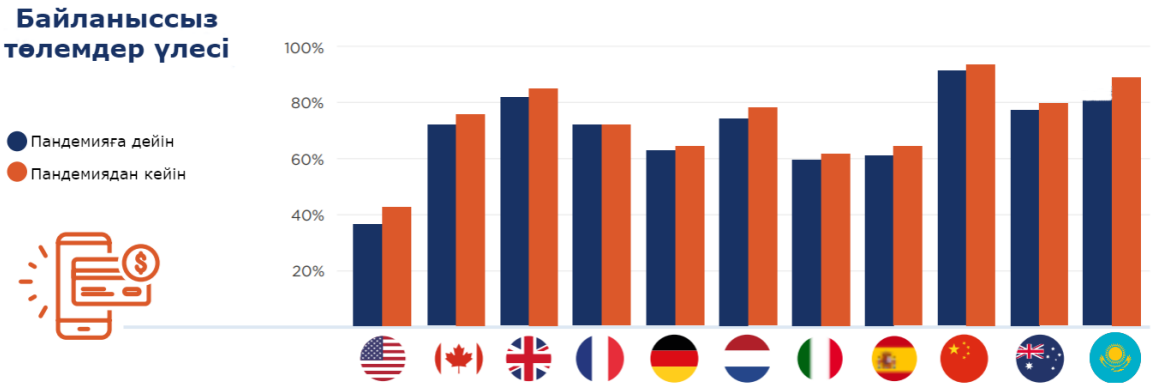
Зерттеу жүргізілген әр елде (және ұрпақта) байланыссыз төлем әдістерін қолданатын тұтынушылар санының өсуі байқалады, ал АҚШ - та пандемияға дейінгі деңгеймен салыстырғанда ең жоғары өсім 19% байқалды.

2) Тұтынушылар қосымша опцияларға байланыссыз төлем әдістерін қалайды

Жалпы алғанда, бүкіл әлемдегі тұтынушылардың 59%-ы қолма-қол ақшамен, чиппен/PIN-кодпен немесе магниттік жолақпен (38% бірге) байланыссыз төлем әдістерін қалайды.

3) Енгізу өсуді жалғастырады

Сауалнамаға қатысқан тұтынушылардың жартысынан көбі, ең болмағанда, карта немесе телефон қосымшасы болсын, жақын арада байланыссыз төлем әдісін қолдануға көшетіндерін айтты (оның ішінде 34% сенімді немесе өте сенімді). Тек 8% байланыссыз төлемдерге көшу "мүмкін емес"деп мәлімдеді.



Сурет 1.6 Әр елдердегі пандемияға дейінгі және кейінгі қолданыстағы байланыссыз төлемдердің үлесі.

Көрсетілген (сурет 1.6) -ке мән берсек пандемияға дейін біз тұтынушыларға қол жетімді карталар (байланыссыз, чипті және ПИН-кодты карталар және магниттік жолақ карталары) арқылы төлем нұсқаларының түрлерінде айқын айырмашылықтарды байқадық. Мысалы, не пайдалану керек деген сұраққа канадалықтардың 59%-ы Чип пен PIN-код бар картаға қол жеткізе алатындығын хабарлады; Канадада бұл көрсеткіш 14% - ға дейін төмендеді. карталар; Қытайда бұл көрсеткіш 14% - ға дейін төмендеді. Сол сияқты, АҚШ PIN-кодсыз магниттік жолақ карталары үшін ең жоғары деңгей туралы хабарлады (34%), ал Францияда ең төмен (9%). Бұдан басқа, бірнеше елдер халықтың кемінде 10% (немесе одан да көп) карталармен (байланыссыз қосымшаларды қоса алғанда) төлем жасаудың қандай да бір әдістеріне қол жеткізе алмайтынын, Италия (13%), Германия (11%) және АҚШ (10%) көш бастап тұрғанын хабарлады. Барлық нарықтарда пандемияға дейін байланыссыз төлемдерді иеленудің ең жоғары деңгейі Қытайда байқалды-90%, одан кейін Қазақстан (85%), халық байланыссыз картаның немесе телефон қосымшасының қандай да бір түріне ие, Ұлыбритания (81%) және Австралия (78%). АҚШ-та, керісінше, оннан төртеуі пандемияға дейін байланыссыз төлем әдістерін қолданды, бұл орташа әлемдік көрсеткіштен 68% - ға төмен. Пандемиядан бұрын танымал болған COVID-19 дағдарысы әр түрлі дәрежеде болса да, зерттелген барлық елдерде байланыссыз төлемдерді енгізудің өсуіне ықпал етті. Кейбір елдерде, мысалы, АҚШ - та, қол жетімділік деңгейі көтерілді-пандемияға дейін американдық тұтынушылардың 38% - ы байланыссыз карталарға немесе қосымшаларға қол жеткізді; қазір бұл сан 46%, айырмашылық 19%. Барлық басқа елдер меншік деңгейінің айтарлықтай өсуін көрсетті - қазіргі деңгеймен салыстырғанда COVID-19-ға дейін 5% немесе одан аз.

QR кодтары ақпаратты жылдам сәйкестендіру және транзакциялық әрекеттерді жүзеге асыру ретінде барлық салаларда кеңінен қолданылады, мұнда шифрланған URL оны смартфон камерасымен жылдам сканерлеуге

мүмкіндік береді. Цифрландыру денсаулық сақтаудың, кеңсе қызметкерлерінің, білім берудің онлайн-ортасына көшуге және аурулардың таралуы туралы көбірек мәліметтер алуға, ақпарат алмасуға және бұрмалаусыз зертханалық зерттеулердің нәтижелерін тез алуға ықпал етеді. Сайт ұсынылған шешім HL7 (Health Level 7 - "жетінші деңгей"), ASTM (American Society for Testing and Materials-HL7 (health Level 7 - "жетінші деңгей") халықаралық стандарттарына сәйкес зертханалық жабдықпен тікелей өзара іс-қимыл жасау арқылы шынайы нәтижелерге қол жеткізу үшін барлық жұмыс процестерін сақтай отырып, әртүрлі бейіндегі зертханаларды кешенді автоматтандыруды жүзеге асыратын SMARTLAB [18] Лис платформасының құрамдас бөлігі болып табылады. "Американдық материалдарды сынау қоғамы") және стандартты мәндерден ауытқуларды автоматты түрде анықтау [19]. 2019 жылы Алматы қ.тері-венерологиялық диспансері зертханасының базасында нәтижелерді верификациялауға пилоттық енгізу жүргізілді, оның нәтижелері ПТР (полимеразды тізбекті реакция), генетика, микробиология және клиникалық диагностика сияқты зертханалық диагностиканың басқа бейіндеріне QR-кодтарды енгізуге мүмкіндік берді. Енді пандемияға байланысты COVID-19 вирусының РНҚ-ны анықтауға арналған зертханалық зерттеулердің барлық нәтижелерінде жалған нәтижелерге жол бермеу үшін QR коды болуы керек.

2018 жылдан бастап 2022 жылға дейінгі кезеңде іске асырылатын "Цифрлық Қазақстан" мемлекеттік бағдарламасы цифрлық технологияларды пайдалану есебінен ел халқының өмір сүру деңгейін арттыруға бағытталған стратегиялық кешенді бағдарлама болып табылады [6]. Бағдарлама шеңберінде Қазақстан Республикасы халқының электрондық денсаулық паспортын ауқымды енгізуге ерекше көңіл бөлінеді, онда клиникалық-диагностикалық зертханаларды автоматтандыру маңызды рөл атқарады. "Цифрлық Қазақстан" бағдарламасы шеңберінде, әсіресе электрондық денсаулық паспортын зертханалық талдау бөлігінде, 2018 жылдан бастап зертханалық зерттеулер нәтижелерін QR-верификациялауды пайдалану басталды, онда зертханалық зерттеулер нәтижелерін қолдан жасаудан қорғауға ерекше назар аударылады. Шешім SmartLAB зертханалық ақпараттық жүйесінің платформасында іске асырылды, онда QR-кодтар автоматты режимде зертханалық зерттеулер нәтижелерінің бланкілеріне қолданылды. Нәтижелерді тексеру нәтижелерді тексерудің онлайн-сервисі арқылы жүзеге асырылды.

Қазіргі уақытта QR коды Азияда, Еуропада және Солтүстік Америкада кең таралған. Жапонияда мұндай кодтар өте танымал және барлық өнімдерге қолданылады. QR-кодтарды пайдалану банк секторында ерекше танымалдылыққа ие болды. Мысалы, Қытайда WeChat Pay (Tencent компаниясына тиесілі WeChat мессенджері арқылы төлем жасау үшін төлем жүйесі) және Alipay (Alibaba Group құрамына кіретін ең ірі төлем жүйелерінің бірі) QR-кодтарға негізделген ең көп таралған төлем схемасы болып табылады. 2016 жылы QR-код арқылы Қытайда 1,65 трлн доллар сомасына төлемдер мен аударымдар жасалды, бұл елдегі барлық мобильді төлемдердің үштен бірін құрайды. Қазақстанда QR-код Kaspi QR-сервисін іске қосқаннан кейін танымал

болды, ол мобильді қосымшада қауіпсіз қызмет көрсетті Kaspi.kz. Осы мақалада жарияланған зертханалық зерттеулер нәтижелерінің нысандары Дербес деректер туралы заңмен қорғалатын пациенттердің дербес деректерін жарияламау үшін пациенттердің дербес деректерінсіз иесіздендірілген және ұсынылған [7] [8] [9].

2.Байланыссыз төлем ортасының сипаты және оның қосымша құралдарын сипаттау

2.1.QR-технологиясы және мәліметтер алмасу мүмкіншіліктері

QR коды-шифрланған мәтінмен құрылған екі өлшемді пішіндегі матрицалық штрих-кодтың бір түрі (сурет 2.1) . QR кодын оқу үшін сканер ретінде камера қажет, ал кодты смартфондардан жасауға және экранда көрсетуге болады. QR кодын жасау және оқу процесі суретті сандық өңдеуді қамтиды және оны мәтіндер немесе суреттер түрінде сақтауға болады. QR кодын екі медиада қолдануға болады, мысалы, газеттер, плакаттар, баспа билеттері мен журналдар және сандық медиа, олар веб-сайттарды қолдана алады және иондық компьютерлерде немесе смартфондарда көрсетілуі мүмкін (Coleman, 2011). QR коды деректерді көрсету үшін арнайы медианы қажет етпейді (QR коды), өйткені кодты қалай көруге және оқуға болатындығы маңызды.

Сурет 2.1 QR кодының мысалы.

QR кодын осы нақты ақпаратты қажет ететін тарап оқиды. Мысалы, егер пайдаланушы ұялы телефон арқылы төлем жасағысы келсе, онда ол сауда нүктесіне тиесілі QR кодын сканерлеуі керек. Сондай-ақ, егер пайдаланушы журналдағы белгілі бір өнім туралы ақпаратты білгісі келсе, QR кодын сканерлеуі керек. Негізінен, QR коды деректерді алушы клиент болып табылатын біржақты алмасу үшін қолданылады. Тек шағын жағдайларда QR кодты клиент жеке деректерді беру үшін, мысалы авторизация үшін пайдалана алады.

Смартфондарда камера функциялары және экранның сапасы жеткілікті, сондықтан QR кодын оңай іске асыруға болады және ол NFC-ге қарағанда үнемді . Сонымен қатар, QR кодын пайдалану ешқандай мамандандырылған медианы қажет етпейді, сондықтан оны кез-келген медиада қолдануға болады. QR коды сонымен қатар қашықтықпен шектелмейді. Басқаша айтқанда, код

көрінгенге дейін оны санауға болады. Сонымен қатар, кейбір пайдаланушылар бірдей QR кодына қол жеткізе алады және қолдана алады, бірақ пайдаланушы кодқа белгілі бір уақытта ғана қол жеткізе алады. уақыты.

QR кодын қолданудың тағы бір артықшылығы-басып шығару үшін стандартты принтерлерді қолдануға болады және қағазды басып шығару үшін пайдалануға болады . Алайда, егер код сандық форматта қолданылса, оны басып шығарудың қажеті жоқ. Сонымен қатар, теру үшін пернетақта қажет емес. Сонымен қатар, QR коды NFC және RFID сияқты үлкен деректерді сақтай алады және қателерді түзету функциясы мен жоғары анықтау қабілетіне ие. Осылайша, егер ол сынған болса, оны әлі де оқуға болады. Шифрлау және сандық қолтаңбаны QR Code-де де қолдануға болады. Сонымен қатар, QR кодын аутентификация үшін пайдалануға болады, мысалы, сайтқа кіру, WiFi желісіне кіру және мессенджерлерге кіру (WhatsApp және Line messenger).

Қазіргі уақытта QR кодтарын сканерлеуге арналған көптеген қосымшалар бар, олар пайдаланушыларға QR кодтарын барынша оңай сканерлеуге мүмкіндік береді. Пайдаланушыға тек камераны ашып, оны QR кодына апару керек; ол оны дереу анықтайды және кейіннен push-хабарламаны ашады. Содан кейін пайдаланушы операцияны аяқтау үшін оны басу керек.

Сондай-ақ, кейбір төлем және банктік қосымшалары банктік аударымдар мен төлемдерді жүзеге асыру үшін QR кодтарын өңдей алады.Мысалы ретінде:

1)Смартфонның көмегімен алушының QR-кодын сканерлеу

Бұл процесте пайдаланушы QR кодын сканерлеу үшін телефон камерасын немесе тиісті қосымшаны ашуы керек. Осыдан кейін олар жеке өнімде, қағаз шотында немесе дүкен кассасында көрсетілген кодты сканерлеуі керек. Әр түрлі ұсыныстар мен адалдық ұпайлары, егер ол белгілі бір дүкенге арналған бағдарлама болса, қолданба арқылы да қолданыла алады.

2)Бөлшек сатушылар тұтынушының телефон экранындағы QR кодын POS терминал сканерлейді

QR-код арқылы төлеу процесінде пайдаланушы транзакцияның жалпы сомасы бөлшек сатушының POS-жүйесінде белгіленгеннен кейін төлем қосымшасын ашады. QR-коды бар төлем қосымшасы пайдаланушы картасының деректерімен сәйкестендірілетін QR-кодты көрсетеді. Содан кейін сатушы QR кодын сканермен сканерлейді, осылайша транзакцияны аяқтайды.

3) Қосымшалар арасындағы төлемдер

Бұл жағдайда жіберуші де, алушы да өз қосымшаларын ашады. Содан кейін жіберуші алушының қосымшасында жасалған бірегей QR кодын сканерлейді. Соңында жіберуші төлеуге тиісті соманы растайды және төлемді аяқтау үшін түймені басады.

QR код санаттарының екі түрі бар. Статикалық және динамикалық.

Статикалық QR коды.

QR кодының бұл түрінде тағайындалған сайттың URL мекен-жайы тікелей QR кодына орналастырылады. Бұл QR кодтарының мазмұны өңделмейді. Оларды байқауға болмайды; дегенмен, оларды URL қосу арқылы түзетуге болады.

Тұрақты QR кодтары жеткізу қызметі, үй қызметтері, дүкендердегі бөлшек сауда, такси жүргізушілері және көше сатушылары сияқты әртүрлі салаларда тез және қарапайым төлемдерді жеңілдету үшін қолданылады. Барлық осы жағдайларда пайдаланушыға ешқандай қиындықсыз төлем жасау үшін QR кодын сканерлеу жеткілікті.

Динамикалық QR коды

Динамикалық QR кодын өңдеуге болады. Сондай-ақ, қол жеткізуді басқару, құпия сөзді қорғау, сканерлеуді талдау және құрылғыларға негізделген қайта бағыттау сияқты қосымша мүмкіндіктер бар. Динамикалық QR кодының көмегімен сіз әртүрлі мәліметтерді біле аласыз.

Динамикалық QR кодтарын қазір сатушылар кеңінен қолданады, өйткені олар сатып алу сомасын да, сатушы туралы ақпаратты да жібереді. Осы функцияның нәтижесінде пайдаланушы тек өзінің қосымшасында транзакцияны қабылдай алады. Сипаттамасы (кесте 1) келтірілген.Сонымен қатар, бұл QR кодын жіберетін адамның төлем мөлшерін көбірек басқаратындығын білдіреді.

Статикалық QR коды жағдайында пайдаланушы сатып алу сомасын енгізуі керек еді, содан кейін саудагер оны мұқият тексеруі керек еді. Алайда, динамикалық QR коды пайдаланушылар үшін де, сатушылар үшін де осы факторлардың барлығын жою арқылы ең жақсы төлем тәжірибесін ұсынады.

Кесте 1

Динамикалық және Статикалық QR кодтарының салыстырмасы

Мүмкіншіліктері	Динамикалық QR-код	Статикалық QR - код
бақылау мүмкіндігі	бар	жоқ
өзгеру қабілеті	бар	жоқ
url сілтемесін қысқарту мүмкіндігі	бар	жоқ
қателерді түзету мүмкіндігі	бар	жоқ
динамикалық маркетингтік науқандарда жұмыс істеу мүмкіндігі	бар	жоқ
жаппай өндіріс мүмкіндігі	бар	бар

QR-кодтың барлық әлеуетті клиенттерді өз бизнесіңізге аударуға көмектесетін бірқатар артықшылықтары бар. Олардың кейбірін қарастырайық.

QR кодтарын қолданудың ең үлкен артықшылықтарының бірі-олар жедел төлемді жеңілдетеді. QR кодтары арқылы төлем Басқа төлем әдістерімен салыстырғанда өте тез жүреді. Пайдаланушыға тек QR кодтарын сканерлеуге, QR кодын сканерлеуге және төлемді растауға арналған қосымшаны ашу керек.

Бірнеше секунд ішінде төлем жасалады.

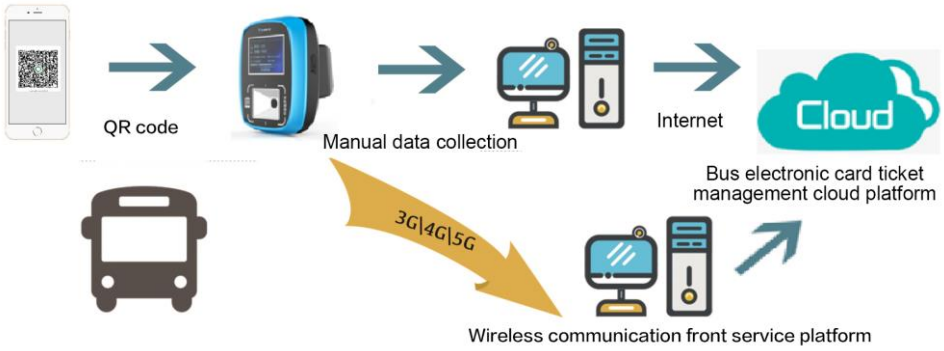
QR коды арқылы төлемдерді орнату өте қарапайым. Сізге арнайы инфрақұрылым қажет емес. Сізге тек камерасы бар смартфон және басылған немесе электронды түрде QR коды қажет. Төлемдер үшін QR-кодтарды пайдалану сауда нүктелеріндегі автоматтарға немесе төлемдер үшін пайдаланылатын кез келген басқа арнайы жабдыққа деген қажеттілікті жояды.

QR-кодтарды пайдаланатын төлемдер төлеудің сенімді әдісі болып табылады, өйткені олар кез келген қатенің ықтималдығын жоққа шығарады. Қара жәшіктердің суреті бірегей деректерден тұрады, бұл QR-кодтарды пайдалану арқылы төлемдердің сенімділігін арттырады.

QR кодтары арқылы төлемдерді жүзеге асыру өте қауіпсіз. Себебі, QR коды ақпарат алмасу үшін қолданылатын құрал ғана. QR кодтары арқылы берілетін кез келген деректер шифрланады, бұл төлемді сенімді қорғалған етеді.

QR үшін мобильді төлем жүйесін құру үшін сізге бірнеше нәрсе қажет.

Біріншісі-мобильді құрылғыдағы қосымша, онда пайдаланушы жеке деректерін енгізу арқылы тіркеліп, кіре алады.Екіншісі-сатып алушылар мен сатушылар туралы ақпарат сақталатын мәліметтер базасы. Әрі қарай, пайдаланушы өз жүйесіне кіріп, POS терминалы экранынан QR сканерлейді.



Сурет 2.2 Қолданушы мен сервер арасындағы QR арқылы мәлімет алмасу процесі.

Бұл QR кодында мәліметтер базасына жіберілетін динамикалық сілтеме бар. QR коды сақталған деректер-бұл транзакция үшін арнайы жасалған token, QR кодын сканерлеу арқылы пайдаланушы жүйеге өзінің авторизациялық деректерін білуге және транзакцияларды орындауға келісім береді.Мәлімет алмасу процессі (сурет 2.2) көрсетілген.

2.2 Мобильді байланыссыз төлемдердің қауіпсіздік жағдайы

Интернетті және ұялы байланысты пайдалану үшін тұтастық пен құпиялылықты қамтамасыз ету үшін қауіпсіздік қызметтері қажет. Ұялы байланыс-бұл географиялық орналасуына қарамастан кез-келген уақытта операция жасау мүмкіндігі мен мүмкіндігі. Барлық ұялы байланыс абоненттері осы ресурстардың барлығына қол жеткізу үшін мобильді құрылғыларды пайдаланады. Мобильдік төлемдер операциялары мобильдік құрылғылардың көмегімен жүзеге асырылады. Бұл құрылғылардың ортақ ерекшелігі-олар кішкентай және портативті. Әр кезеңде оларға қауіпсіздік қызметтері қажет. Ақпараттың толықтығын қамтамасыз ететін әртүрлі қауіпсіздік қызметтері бар. Мобильді транзакцияларға қойылатын жалпы талаптар-тұтастықты, құпиялылықты, көрсетілмеуді, аутентификацияны, авторизацияны қамтамасыз ету. Осы талаптарға қосымша, мобильді транзакциялар оларды жүзеге асыруда қосымша қауіпсіздік мәселелеріне тап болады. Мұндай проблемалар-дұшпандық, Ақпараттық қауіпсіздік және осалдық. Олар келесідей сипатталады:

- Аутентификация
- Авторландыру
- Құпиялылық
- Тұтастық
- Дұшпандық
- Ақпараттық қауіпсіздік
- Осалдық

Аутентификация

Федералды ақпаратты өңдеу стандарттарына сәйкес стандарттар, аутентификация "пайдаланушының, процестің немесе құрылғының жеке басын, көбінесе ақпараттық жүйеде ресурстарға қол жеткізуге рұқсат беру шарты ретінде"тексереді. Аутентификация-бұл қарапайым процесс пайдаланушы жүйеге тіркелгі деректерін енгізген кезде. Егер тіркелгі деректері жүйеде бар жиынмен сәйкес келсе, онда пайдаланушыға басқаша рұқсат беріледі - жоқ. Аутентификацияның мақсаты-ұсынылған ақпараттың белгілі бір жиынтығын тексеру бұл сұрау белгілі бір субъектіден шынайы екенін растайды. Бұл субъектіге берілген барлық құқықтар мен артықшылықтардың негізі болып табылатын субъектінің жеке басын тексеру үшін маңызды. Ұсынылған нысан-компьютерлік бағдарлама немесе пайдаланушы болсын, аутентификация процесі үшін маңызды емес процесс.

Аутентификация-бұл таратушы тұлға өзі беретін адам екендігінің кепілі. Жүйе пайдаланушының кез-келген электрондық операцияларды орындауға немесе жүйеге кіруге рұқсаты бар-жоғын анықтау үшін түпнұсқалығын тексереді.

Кез-келген электрондық әрекетті орындау үшін аутентификация процесі сұраудан басталады. Клиент аутентификацияны талап ететін қызметтерді

сұрайды. Қызмет провайдерлері пайдаланушыны аутентификациялау құралы ретінде қызмет ететін және оның жеке басын растайтын бірегей маркерді сұрайды. Бірегей таңбалауыш пайдаланушының жеке басын құпиямен байланыстырады және тіркеу кезінде пайдаланушыға беріледі. Пайдаланушы аутентификация кезінде өзінің бірегей таңбалауышын ұсынған кезде, аутентификация жағы пайдаланушының жеке басын тексереді, өйткені бірегей таңбалауыш барлығына ерекше.

Таңбалауышты келесідей жіктеуге болады:

- Сіз білетін нәрсе, яғни құпия сөздер.
- Сізде бар нәрсе, яғни аппараттық токендер.
- Сіз, яғни биометрия.

Бүгінгі таңда бұл әдістер аутентификацияның үш факторы деп аталады. ISC2 сонымен қатар сіздің орналасқан жеріңізге негізделген және әдетте GPS (Ғаламдық орналастыру жүйесі) қолданатын "сіз бір жерде" деп аталатын төртінші санатты қосады.

Бекітілген құпия сөздер сияқты аутентификация әлсіз аутентификация процесі болып саналады, ал сіз білетін нәрсеге негізделген бір факторлы аутентификация жоқ. Ол тыңдау, сөздік шабуыл және қайта ойнату шабуылы сияқты көптеген шабуылдарға ұшырайды. Күшті аутентификация схемалары бірнеше факторға сүйенеді, яғни сіз білетін нәрсені (құпия сөздерді) сізде бар нәрсемен (аппараттық құралдармен) біріктіреді. Аутентификация стратегияларын бір факторлы аутентификация және көп факторлы аутентификация деп бөлуге болады.

Бір факторлы аутентификация (SFA)

Бір факторлы аутентификация-бұл пайдаланушыға кіру алдында логин мен құпия сөзді енгізуді қажет ететін дәстүрлі қауіпсіздік процесі. SFA қауіпсіздігі қосымша сақтық шараларын қабылдауы керек пайдаланушының ынтасына байланысты - мысалы, күшті құпия сөз жасау және оған ешкім қол жеткізе алмайтындығына көз жеткізу. Қауіпсіздікті жақсартуды қажет ететін қосымшалар үшін көп факторлы аутентификация сияқты күрделі жүйелерді енгізу орынды болуы мүмкін.

Құпия сөздер

Көбінесе компьютерлерде құпия сөздер қолданылады, яғни негізгі аутентификация үшін "Сіз білетін нәрсе" факторы. Қауіпсіздікті қамтамасыз етудің ең көп таралған тәсілі-құпия сөздер мен пайдаланушы аттарын пайдалану. Бұл әлсіз аутентификация механизмі, оны желілік қосылымды тыңдау немесе пайдаланушыларға ұқыпсыз қарау арқылы жоюға болады. Интернетте көбірек қызметтер қол жетімді болғандықтан және бұл қызметтердің көпшілігі аутентификация тетіктерін қажет етеді. Пайдаланушы аты мен құпия сөз ретінде әрекет ететін әр түрлі кілт комбинацияларын басқару қиын.

Құпия сөздер-бұл қарапайым аутентификация моделі сондықтан құпия сөз модельдері өте кең таралған. Өкінішке орай, құпия сөз модельдері де аутентификацияның ең әлсіз моделі болып табылады өйткені құпия сөздер

салыстырмалы түрде оңай бұзылады немесе ұрланады. Сондай-ақ, ол кез-келген құпия сөз моделін осал етуі мүмкін. Егер құпия сөздер арнайы таңбаларды қосу арқылы қиындатылса да, бұл шаралар пайдаланушыларды құпия сөздың ұмытпау үшін оны бір жерде сақтап жазып қоюғаетуі мүмкін,бұл дегенімі құпиясөздің құндылығын түсіреді.

Құпия сөз бұзудың төрт түрі:

- Сөздік көмегімен бұзу: құпия сөздерді бұзу үшін әртүрлі сөздіктерді қарапайым пайдалану.

- Сөздер мен сандарды орындарын ауыстыру:

Сөздік файлдағы әр сөз үшін құпия сөзге ықтимал үміткерлерді құру үшін 0, 1, 2 және 3 сандарымен пермутация жасаңыз. Сондай-ақ, сандардың әдеттегі алмастырғыштарын қолданыңыз, мысалы, I үшін 1, S үшін 5 және т. б.

* Пайдаланушы туралы ақпаратты қолдана отырып бұзушылық жасау: құпия сөз файлдарынан жиналған пайдаланушы туралы ақпаратты пайдалану, мысалы, пайдаланушы идентификаторы, Толық аты, аты-жөні, құпия сөздерді бұзу үшін.

- Қатыгез бұзушылық: біз бұл бұзу тұрін ұзындығы небары 6 таңбадан тұратын кез-келген құпия сөзге жүргіздік.

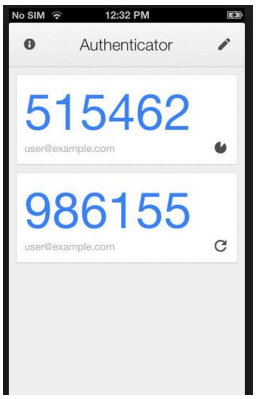
Аппараттық токендер

Кейбір аутентификация жүйелерінде әдетте таңбалауыштар қолданылады, яғни пайдаланушыны аутентификациялай алатын кез келген құрылғылар немесе Нысандар. Жалпы мысалдарға физикалық кілттер, байланыссыз карталар, несие карталары немесе банкомат карталары жатады. Токендер жақсы, өйткені олар қарапайым. Физикалық кілттер, мысалы, кеңінен қолданылады және өндіруге және пайдалануға арзан. Компьютерлік аутентификация кезінде криптографиялық кілттерді, әсіресе SSH (secure shell) сияқты қашықтағы протоколдарда пайдалануға болады. Қашықтағы протоколдарға арналған криптографиялық кілттердің артықшылығы-оларды пайдаланушының түпнұсқалығын растау үшін ғана емес, сонымен қатар хабарларды аутентификациялау және деректерді шифрлау үшін де пайдалануға болады. Алайда, таңбалауыштардың кемшіліктері бар. Токендер қарапайым және арзан болғандықтан, оларды көбейту оңай және арзан. Бұл оларды жалғандыққа осал етеді. Сонымен қатар, олар әдетте физикалық объект немесе құрылғы болғандықтан, құпия сөздерге қарағанда ұрлау оңайырақ. Осы себепті, таңбалауыштар басқа әдіспен бірге қолданылады, мысалы, PIN-код, ұрлық жағдайында олардың пайдалылығын азайту үшін.

Бағдарламалық токендер

Бағдарламалық жасақтама таңбалауыштары аппараттық таңбалауыштарға ұқсас. Бұл аппараттық таңбалауыштардың бағдарламалық жасақтамасы(сурет 2.3). Бағдарламалық жасақтама таңбалауыштары компьютерде немесе бөлек көп мақсатты құрылғыда жұмыс істейді, ал аппараттық таңбалауыштар компьютерден алыс жерде сыртқы құрылғыда сақталады. Бағдарламалық жасақтама таңбалауыштары екі тараптың аутентификациясын қолдайды және аутентификация үшін деректерді беру үшін пайдаланылатын байланыс арнасын

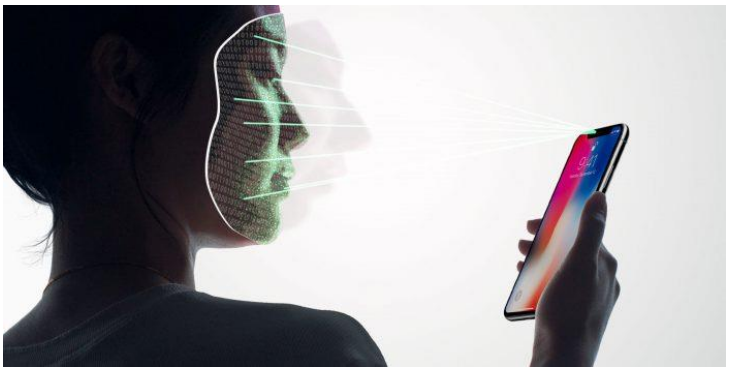
қорғайды. Бағдарламалық жасақтама таңбалауыштарының кемшілігі-оларды пайдаланушының білімінсіз оңай көшіруге болады.



Сурет 2.3 Google компаниясының Google authenticator токендар алмасу сервисі.

Биометрия

Биометрия-бұл белгілі бір биологиялық немесе мінез-құлық сипаттамаларына негізделген адамды анықтау үшін қолданылатын автоматты әдістер. Саусақ іздері, ДНҚ туралы ақпарат (дезоксирибонуклеин қышқылы) және т.б. сияқты көптеген биологиялық сипаттамалар және дауыс, қолтаңба сияқты мінез-құлық сипаттамалары әр адамға тән. Демек, Биометрия жеке басын куәландыратын құжатқа немесе құпия сөзге негізделген кез-келген басқа әдістерге қарағанда әр түрлі адамдарды ажыратуда анағұрлым қабілетті және сенімді.(сурет 2.4) Биометриялық жүйе-бұл жеке тұлғаны анықтауға мүмкіндік беретін үлгіні ану жүйесі. Биометриялық жүйелер әр түрлі болады және олардың әрқайсысы физикалық сипаттаманы өлшейді, ол белгілі бір адам үшін ақылға қонымды шектерде салыстырмалы түрде ерекше болады. Пайдаланушы биометриялық жүйеге тіркеліп, жүйемен өлшенетін физикалық сипаттаманың үлгісін ұсынады. Содан кейін жүйе үлгіні жасау үшін осы "аналогтық" сипаттаманы сандық түрге айналдырады.



Сурет 2.4 Iphone смарфтонындағы бет-әлпетті тану функциясы.

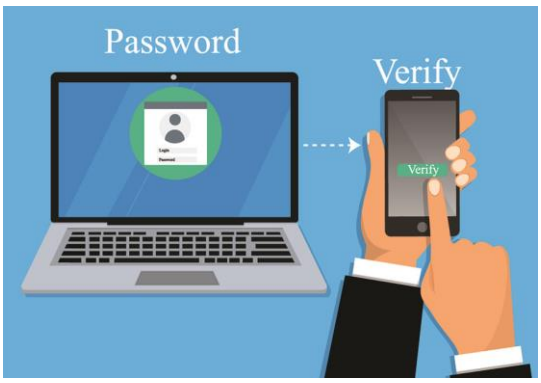
Содан кейін үлгі орталық аутентификация серверінде сақталады. Пайдаланушы жүйеде түпнұсқалық растама береді, содан кейін цифрландырылған жаңа үлгіні сақталған шаблонмен салыстырады. Егер екі цифрланған үлгі белгілі бір рұқсат шегінде ұқсас болса, пайдаланушы қабылданады. Биометриялық тәсілдер екі санатқа бөлінеді: физиологиялық және мінез-құлық. Физиологиялық биометрия саусақ іздері, иристі сканерлеу және бетті тану сияқты дене сипаттамаларына негізделген. Мінез-құлық биометриясы адамдардың белгілі бір әрекеттерді қалай жасайтынына негізделген, мысалы, пернелер динамикасы, тінтуірдің қозғалысы және сөйлеуді тану. Төменде биометриялық технологияның әртүрлі түрлері берілген:

- Бет-әлпетті тану-бұл адамдардың бет-әлпетін немесе бейнефотографиясын анықтайтын технология.
- Саусақ ізін сәйкестендіру-бұл саусақ ізін аутентификациялауға мүмкіндік беретін технология. Саусақ ізі-бұл саусақ ұшының бетіндегі жоталар мен ойықтардың үлгісі. Өрнектері бірдей екі адам жоқ, ал бір адамның өрнектері өмір бойы өзгеріссіз қалады.

Көп факторлы аутентификация (MFA)

Көп факторлы аутентификация-бұл бірнеше бір факторлы аутентификацияны біріктіретін пайдаланушыны анықтау әдісі. Ол жоғары тәуекелді клиенттер мен қаржылық операциялар туралы басым ақпарат алу үшін қолданылады. Аутентификация механизмінің күшін оның қанша факторға байланысты екенін анықтауға болады. Бір фактордың екі түрін қолдану көп факторлы аутентификация емес. Мысалы, құпия сөз мен жеке ақпарат-бұл сіз білетін нәрсе, сондықтан оларды бөлісу әлі де бір факторлы аутентификация болады. Аутентификация кілттерінің күші факторлардың бір санатында да өзгеруі мүмкін. Ананың қыздың тегі, төрт таңбалы код және кездейсоқ сегіз таңбалы әріптік-сандық құпия сөз-бұл сіз білетін нәрсеге негізделген аутентификация кілттерінің мысалдары, бірақ олардың әрқайсысы анықтау шабуылдарынан әр түрлі қорғауды қамтамасыз етеді. Сондықтан аутентификация процесінің қауіпсіздігіне нақты қолданылатын шешім әсер етеді. Алайда, көп факторлы аутентификация қауіпсіздікті арттырады деген пікір жалпы қабылданған. Көп факторлы аутентификация екі факторлы немесе үш факторлы.

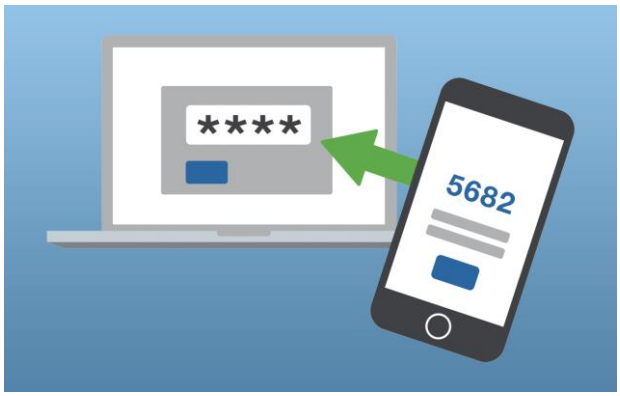
- Екі факторлы аутентификация:(сурет 2.5) аутентификацияның үш факторының екеуі қолданылады. Банкомат арқылы шотқа кіру екі аутентификация факторына негізделген: PIN (сіз білесіз) және банкомат картасы (сіз білесіз) және банкомат картасы (сізде бар).
- Үш факторлы аутентификация: аутентификацияның барлық үш факторы қолданылады. Мысалы, қорғалған сайтқа кіру үшін сіз өзіңіздің бетіңізді сақталған кескінмен тексеретін күзетшінің қасынан өтуіңіз керек (Сіз не екенсіз), кіру картасын (сізде бар) жүргізіп, төрт таңбалы кодты енгізуіңіз керек. не бар) және төрт таңбалы кодты енгізіңіз (сіз білесіз).



Сурет 2.5 Екі факторлы аутентификацияның өту процессі.

Бір реттік құпия сөз (БРҚС)

Бір реттік құпия сөздер(сурет 2.6)-бұл тек бір немесе бірнеше операция үшін жарамды құпия сөздер. Бұл көптеген операциялар үшін жарамды әдеттегі құпия сөздерден ерекшеленеді, өйткені пайдаланушылар құпия сөздерді өз еркімен жиі өзгерткісі келмейді. БРҚС тек шектеулі пайдалану үшін жарамды болғандықтан, шабуылдаушының мұндай құпия сөзмен қорғалған ресурстарға қол жеткізуге уақыты аз болады, өйткені бұрын ұрланған барлық құпия сөздер жарамсыз болып қалуы мүмкін. Әдетте, бір реттік құпия сөз аппараттық құралмен жасалады, оны аутентификациялағысы келетін адам көптеген физикалық шалғай аудандарда қолдануға ықпал етеді. Аппараттық құрал аутентификаторға белгілі бір жолмен құпия сөздер жасайтын алгоритмді қолданады. Пайдаланушы оны аутентификаторға енгізе алатындай етіп, аппараттық құрал құпия сөзді кішкентай экранда жиі көрсетеді. Осындай аппараттық тәсілмен, егер құпия сөздер шығаратын жабдық немесе компьютер ұрланса, ұры дисплейдегі сандарды оқу арқылы өзін-өзі растай алады. Осы себепті, бір реттік құпия сөздер көбінесе пайдаланушыны анықтау үшін екі немесе одан да көп тәуелсіз аутентификация факторларын қолданатын көп факторлы аутентификация жүйесінің бөлігі болып табылады.



Сурет 2.6 Бір реттік құпия сөзді мобильді құрылғы арқылы алу.

Уақытша құпия сөздерді құратын алгоритмдер уақытша немесе

математикалық болуы мүмкін. Уақытқа негізделген Алгоритмдер алгоритм (көбінесе аппараттық құрал) автоматты түрде жаңартылғанға дейін белгілі бір уақыт аралығында жарамды құпия сөздер жасайды. Техникалық тұрғыдан алғанда, бір реттік термин дұрыс емес, өйткені құпия сөз бір уақыт аралығында әрекет етсе, оны бірнеше рет қолдануға болады. Мұндай түрдегі аппараттық құрал әдетте әрқашан құпия сөзді көрсетеді және ол үнемі өзгеріп отырады. БРҚС әрекет ететін уақыт ұзақтығы мұндай схемалардағы маңызды қауіпсіздік параметрі болып табылады, өйткені бір құпия сөз мерзімі аяқталғанға дейін жарамды, содан кейін жаңартылады. Егер құпия сөз сирек жаңартылса, шабуылдаушыда пайдалану үшін ұзағырақ терезе пайда болады. Кезеңнің ұзақтығы ұлғайған сайын БРҚС қауіпсіздігі әдеттегі құпия сөздердің қауіпсіздігіне жақындайды. Мысалы, тыңдаушы құрылғы жаңа құрылған БРҚС -ді желі арқылы жылжыту кезінде ұстап алады. Ұсталғаннан кейін шабуылдаушыда рұқсатсыз кіру үшін құпия сөздің бүкіл мерзімі қалады. SecurID-бұл RSA Security компаниясының патенттелген коммерциялық жүйесі, әр отыз-алпыс секунд сайын өзгеретін құпия сөздерді құру үшін аппараттық құралдарды қолданады.

Авторландыру

Авторизация-бұл адамның белгілі бір әрекетті орындауға құқығы немесе рұқсаты бар-жоғын анықтайтын процесс. Бұл жүйе белгілі бір аутентификацияланған пайдаланушының жүйе басқаратын қорғалған ресурстарға қол жетімділіктің қандай деңгейіне ие болатындығын анықтайтын механизм. Авторизация туралы ақпарат, мысалы, кіруді бақылау тізім басқарады. Интернет қызметтері тез дамып келеді, сондықтан ықтимал әрекеттер жиынтығы және оларды сұрай алатын пайдаланушылар алдын-ала белгілі емес; бұл авторизация туралы ақпарат динамикалық және таратылған түрде жасалады, сақталады және басқарылады дегенді білдіреді. Көбінесе пайдаланушылар әрекетті авторизациялау үшін қажетті тіркелгі деректерін жинайды және оларды сұраумен бірге береді деп күтілуде. Бұл тіркелгі деректері әрдайым авторизация туралы шешім қабылдаған қызметтің бақылауында бола бермейтіндіктен, оларды өзгерту немесе ұрлау қаупі бар. Осылайша, ашық кілт қолтаңбасы авторизация жүйесінің бөлігі болуы керек. Дәстүрлі аутентификация мен қол жеткізуді басқаруда сәйкестендіру ұғымы маңызды рөл атқарады. Дәстүрлі жүйеде сәйкестендіру көбінесе қолданыстағы пайдаланушы тіркелгісін білдіреді. Пайдаланушылардың есептік жазбалары жүйеде кез келген сұрау берілгенге дейін жасалады. Бұрын PKI ұсыныстары жүйеде әр объектіге ерекше атау беретін, содан кейін әр ашық кілтті Ғаламдық бірегей "сәйкестендірумен" байланыстыратын ұқсас "пайдаланушы тіркелгілері"жүйесін құруға тырысты. Интернеттегі қосымшаларда сәйкестендіру ұғымы проблемалы болады. Сәйкестік термині бастапқыда біртектілікті немесе бірлікті білдіреді. Бұрын бейтаныс адамды алғаш кездестіргенде, біз оны ештеңемен анықтай алмаймыз. Уәкілетті және Сұрау салушы ешқандай алдын ала қарым-қатынасы жоқ сценарийде сұрау салушының атын немесе жеке басын білу уәкілетті адамға шешім қабылдауға

көмектеспеуі мүмкін. Сәйкестендіру үшін қажет нақты мүлік-бұл сұрау немесе өкілеттіктерді белгілі бір адам бергенін және белгілі бір адамды оның өкілеттіктерімен байланыстыруға болатындығын тексеруге болады.

Құпиялылық

Құпиялылық дегеніміз-ақпаратқа қол жеткізуге және оны ашуға рұқсат етілген шектеулерді сақтау. Ол жеке құпиялылық пен қызметтік ақпаратты қорғау құралдарын қамтиды. Құпиялылықты жоғалту-бұл ақпаратты рұқсатсыз ашу. Құпиялылық ақпараттың рұқсат етілмеген пайдаланушыларға қол жетімді болмауын немесе ашылмауын қамтамасыз ететін мүлік ретінде анықталады. Құпиялылық тетіктері оны алуға уәкілетті емес пайдаланушылар арасында ақпараттың таралуын болдырмауға арналған. Құпиялылық механизмі артықшылықтарға ие адамдардан басқа барлық адамдар үшін ақпаратқа қол жеткізуге, ақпаратты жасыруға немесе өзгертуге жол бермейді. Ақпараттың құпиялылығын оның әсер ету деңгейімен анықтауға болады, яғни төмен, орташа немесе жоғары. Ақпаратты берудің құпиялылығы оны беру алдында коммуникацияларды шифрлау немесе ақпаратты шифрлау арқылы қорғалуы мүмкін.

2.3 Мобильді төлемдердің электрондық төлем жүйесі ретіндегі болашағы

MEF-тің «Global Mobile Money»[20] атты үшінші жылдық есебіне сәйкес, электрондық коммерция және мобильді банкингтер үлесі өсуде, мобильді құрылғыларды пайдаланушылардың 69%-ы мобильді құрылғылар арқылы банкинг жүргізеді . Есеп бойынша әлемнің 15 түрлі еліндегі 15 000 мобильді құрылғы пайдаланушысын зерттеді. Есеп дүкен ішіндегі төлемді, операторлық есепшотты, онлайн төлемдерді, өзара төлемдерді және мобильді әмиян төлемдерін қоса алғанда, қызметтерге арналған «ұялы ақша» терминін анықтайды. Мобильді төлем әдістерін қолданудың өсуі дамыған нарықтарды дүкендерде мобильді транзакцияларды қолдау үшін құрылғылардың енуін және инфрақұрылымды орнатуға итермеледі. Сонымен қатар, контактісіз төлем әдістері әртүрлі жерлерде жылдам, оңай және қауіпсіз төлем әдісін ұсынатын киілетін технологияның (Sacco, 2015) арқасында танымал бола бастады. Мобильді төлем технологиясы ақылды сағаттарды, сақиналарды, білезіктерді және Android немесе iOS смартфондарының бірқатар қолданбаларын қамтиды. 2013 жылғы GSMA саланың жай-күйі есебінде мобильді төлемдердің болашағына жарық түсіретін кейбір статистика да берілген. Осы есепке сәйкес, «2013 жылдың ортасына қарай дүние жүзінде 203 миллионнан астам мобильді ақша шоты тіркелген, мобильді ақша бөлімшелері дүние жүзіндегі нарықтардың 80%-дан астамында банк филиалдарынан асып түсті»). Дүние жүзінде мобильді төлем транзакцияларының жылдамдығы айтарлықтай артып келеді және олардың құны 12,8 миллиард АҚШ долларынан 2017 жылға қарай 90 миллиард АҚШ долларына дейін өседі. Бұл статистика бізді смартфондар

мен планшеттер арқылы төлемдерді жүзеге асырудың қауіпсіз және ыңғайлы нұсқалары бар қолма-қол ақшасыз болашақ күтіп тұрғанын анық көрсетеді. Мобильді төлем жүйелері саудагерлер мен клиенттер үшін жаңа мүмкіндіктер ашты, бірақ сонымен бірге олар құпиялылық пен қауіпсіздік мәселелеріне байланысты жаңа тәуекелдерге ұшырайды. Мобильді төлем есебіне сәйкес, қауіпсіздікті болашақта онлайн төлем әдістерінің маңызды элементіне айналдыру үшін мұқият жоспарлау қажет. Мобильді төлемдер нарығы болашақта гүлденуі үшін ұялы телефон өндірушілері, телекоммуникация компаниялары және төлем индустриясы ең қауіпсіз онлайн төлем ортасын қамтамасыз ететін платформа құру үшін бірлесіп жұмыс істеуі керек. Дегенмен, мобильді төлем жүйелері саламен байланысты барлық негізгі қауіпсіздік пен құпиялылық мәселелерін шешуге мүмкіндігі бар деп саналады және ағымдағы оқиғалар инновациялардың қазірдің өзінде жүріп жатқанын көрсетеді. Редди [12] айтуынша, мобильді төлемдердің болашағын осы саланың алдында тұрған практикалық және аналитикалық қиындықтарды еңсеру үшін соңғы технологияларды пайдалану арқылы қамтамасыз етуге болады. Радио штрих-код технологиясы мобильді төлем жүйелеріне революциялық қосымша болып саналады. Бұл радио штрих-кодтар олар қолданылатын элементтерді анықтау үшін пайдаланылатын радио сигналдарын жібереді. Радио штрих-кодтарды қолдану арқылы мобильді төлемдер нарығы тұтынушыларға қауіпсіздік пен ыңғайлылықты қамтамасыз ететін перспективалы болашаққа ие болуы мүмкін. Радио штрих-код технологиясы саудагерлерге өтіп бара жатқанда тұтынушылардың несие картасының нөмірлері мен жарамдылық мерзімін оқуға мүмкіндік береді. Қауіпсіздік хаттамаларын жақсарту және радио штрих-кодтар сияқты соңғы технологияларды пайдалану арқылы мобильді төлем қызметтерін жеткізушілер үлкен деңгейлерде ғана емес, сонымен қатар тұтынушылар үшін ең қолайлы жүйе құра алады.

Смартфондар күнделікті өмірімізде оятқыш, сағат, музыка ойнатқышы және магнитофон сияқты бірнеше нәрсені ауыстырғандықтан, бұл тізімге қолма-қол ақша мен әмияндар да қосылды. Төлем әдістері қолма-қол ақшадан чектерге, дебеттік және несиелік карталарға, ал енді электронды коммерция мен мобильді банкингке дейін бірқатар эволюциялардан өтті. Бұл зерттеу көрсеткендей, сатып алушылар өздерінің тұрақты онлайн сатып алулары үшін, сондай-ақ сайттан сатып алу үшін мобильді төлем әдістерін көбірек пайдаланады. Мобильді транзакцияларды қолдайтын және оларды ашық әрі ыңғайлы ететін озық технологиялардың дамуымен тұтынушыларда мобильді төлем жүйелерін пайдалану сенімі мен әдеті қалыптасты. Тұтынушылардың мінез-құлқының дәстүрлі төлем әдістерінен заманауи онлайн төлем жүйелеріне ауысуы банктік және бөлшек саудада, сондай-ақ қол жетімді мобильді құрылғылардың көпшілігінде анық байқалады. Мобильді құрылғылар әр адамның дерлік өмірінің ажырамас бөлігіне айналғаны және бұл технологияның ыңғайлылық пен қауіпсіздік тұрғысынан онлайн және офлайн төлемдерді қамтамасыз ететін мүмкіндіктері анық болғандықтан, мобильді төлем жүйелерін пайдалану сөзсіз. қолма-қол ақшаны және басқа қолма-қол

ақшасыз төлем опцияларынан асып түсу немесе тіпті ауыстыру амбицияларымен одан әрі өсіңіз. Зерттеу сонымен қатар осы саланың болашағы үшін мобильді төлем жүйелерін қолданыстағы телекоммуникация және қаржылық инфрақұрылымдармен жақсырақ біріктіру қажет деген қорытындыға келді. Пайдаланушылардың кең ауқымымен өзара әрекеттесу мүмкіндігін арттыру, соңғы технологияларды пайдалану және қызмет жеткізушілері арасында ортақ стандарттарды орнату, қауіпсіздік пен құпиялылық мәселелерін еңсеру электрондық төлем әдістерін қабылдауды жеделдетуге және мобильді төлемдердің өсіп келе жатқан нарығын ілгерілетуге көмектеседі.

3 Тікелей жанаусыз, сауда жүргізуге арналған қосымшаны құру

3.1Байланыссыз төлем жүйесін жобалау

Байланыссыз жүйені құрмастан бұрын оның жобасымен таныса кеткен жөн. Бұл жүйенің басты құралдары (сурет 3.1) бұл:

-Python 3.9

-PyCharm IDE

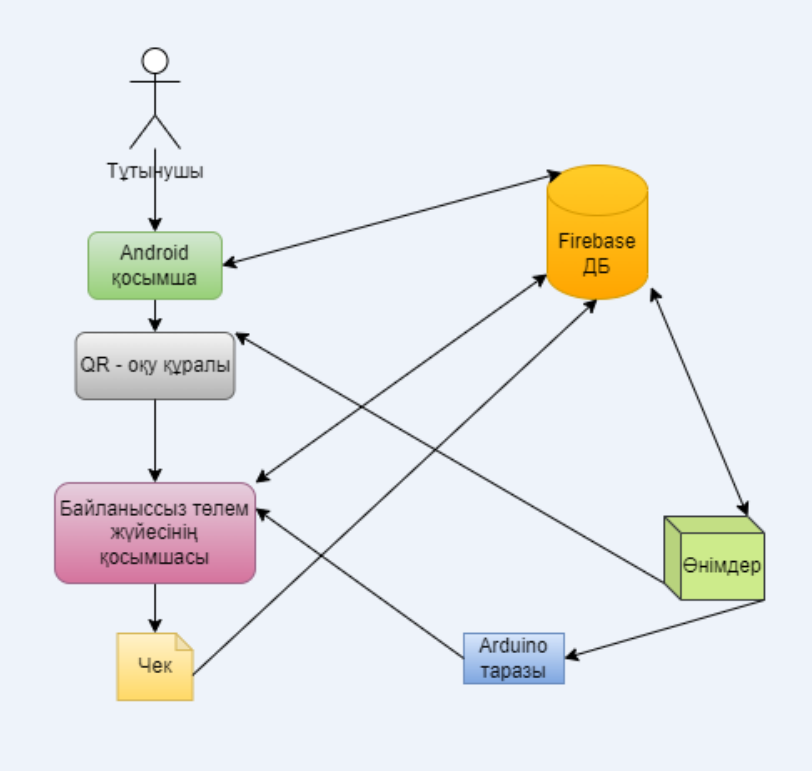
-python-opencv кітапқанасы

-PyQT қосымша құру және моделдеу ортасы

-Google Fireabase нақты уақыттағы деректер базасы және оның python мен android жалғау тәсілдері

-Android Studio - Java программалау ортасы

-Arduino Uno және Arduino бағдарламалау жүйесі



Сурет 3.1 Жүйенің блоктық-схемасы

Python-бұл объектіге бағытталған, процедуралық, функционалды, жалпы мақсаттағы ашық коды бар бағдарламалау тілі. Бірнеше түрлі парадигмаларды қолдайтын динамикалық бағдарламалау тілі:

1)Процедуралық бағдарламалау

2)Объектіге бағытталған бағдарламалау

3)Функционалдық бағдарламалау

PyCharm-бұл JetBrains компаниясы Python үшін IDE ретінде жасалған гибридті платформа. Ол Python қосымшаларын жасау үшін кеңінен қолданылады. Twitter, Facebook, Amazon және Pinterest сияқты кейбір"біртұтас" ұйымдар PyCharm-ді Python үшін IDE ретінде пайдаланады!

PyCharm-ді Windows, Linux немесе Mac OS-де іске қосуға болады. Сонымен қатар, онда бағдарламашыларға Python бағдарламалық жасақтамасын аз уақыт ішінде және аз күш жұмсау арқылы жасауға көмектесетін модульдер мен пакеттер бар. Сонымен қатар, ол әзірлеушілердің талаптарына сәйкес реттеле алады.

OpenCV (Open Source Computer Vision Library) - бұл компьютерлік көру және машиналық оқытудың ашық көзі. OpenCV компьютерлік көру қосымшаларына арналған жалпы инфрақұрылымды қамтамасыз ету және коммерциялық өнімдерде машинаны қабылдауды тездету үшін жасалған. BSD лицензиясы бар өнім бола отырып, OpenCV коммерциялық ұйымдар үшін кодты қолдануды және өзгертуді жеңілдетеді.

PyQt-бұл Qt құралдарын қолдана отырып, GUI қосымшаларын құруға арналған Python кітапханасы. Riverbank Computing-те құрылған PyQt ақысыз бағдарламалық жасақтама (GPL лицензиясы бойынша) және 1999 жылдан бері дамып келеді. PyQt6-дің соңғы нұсқасы-Qt 6 негізінде-2021 жылы шығарылды және кітапхана жаңаруды жалғастыруда. Бұл нұсқаулықты PySide 2, PySide 6 және PyQt5 үшін де қолдануға болады.

Firebase Дерекқоры Realtime Database сізге клиенттік кодтан тікелей дерекқорға қауіпсіз қол жетімділікті қамтамасыз ете отырып, бай бірлескен қосымшаларды құруға мүмкіндік береді. Деректер Жергілікті деңгейде сақталады, тіпті офлайн режимінде де нақты уақыттағы оқиғалар соңғы қолданушыға тез жауап беруді қамтамасыз етеді.

Android Studio-бұл Google өндірісінің интеграцияланған даму ортасы, оның көмегімен Android OS платформасында қосымшалар құруға арналған құралдар әзірлеушілерге қол жетімді болады. Android Studio-ны Windows, Mac және Linux - қа орнатуға болады.

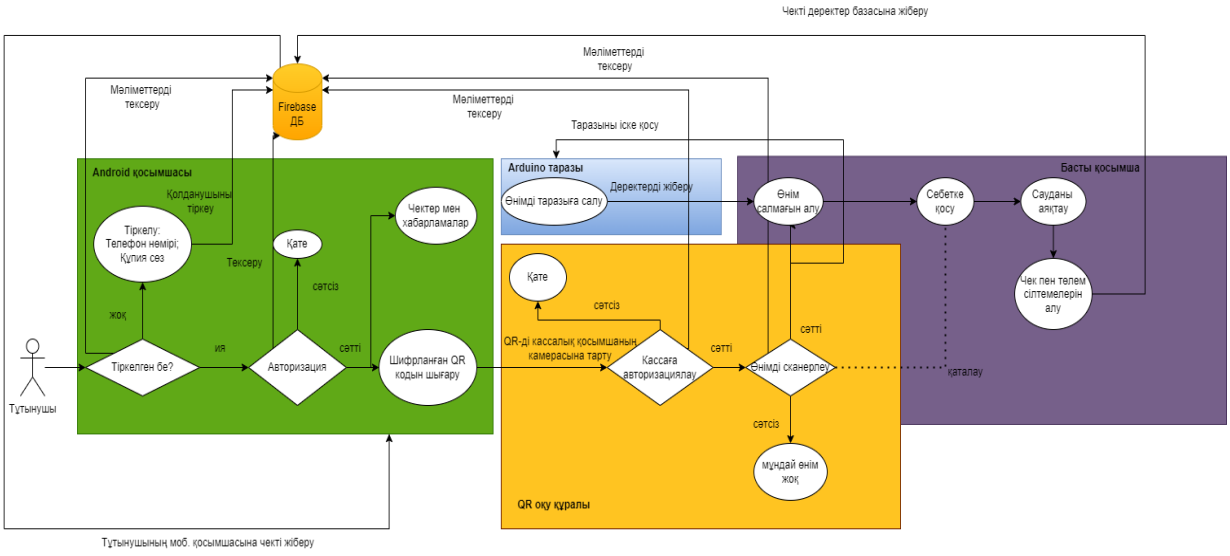
Arduino-бұл, ең алдымен, ашық бастапқы компьютерлік жабдықтар мен бағдарламалық жасақтама компаниясы. Arduino қауымдастығы-бұл микроконтроллерлер негізінде даму тақталарын жасайтын және пайдаланатын жоба және пайдаланушылар қауымдастығы. Бұл тақталар ашық бастапқы прототиптік платформалар болып табылатын Arduino модульдері ретінде белгілі. Жеңілдетілген микроконтроллер тақтасы әр түрлі даму тақталарында келеді.

3.2 Жүйенің программалық бөлігі

Жүйенің программалық бөлігі бірнеше бағдарлама-қосымшалардан тұрады,егер маңыздылығынан бастап айтатын болсақ,олар:

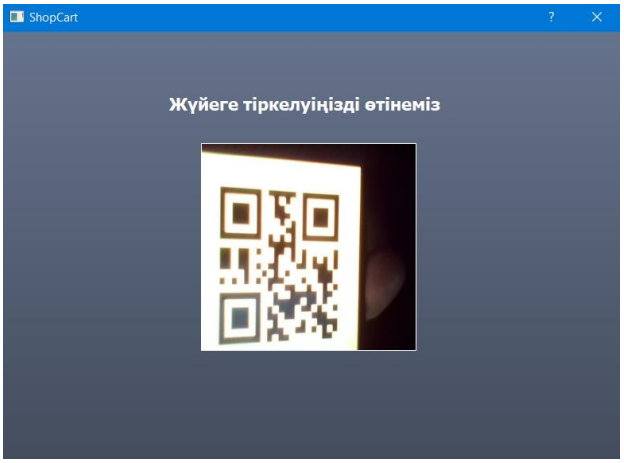
- Негізгі қосымша(Python,PyQT,Firebase)
- Тұтынушының мобильді қосымшасы(Android Studio,Java)

Жүйенің толықтырылған сұлбасы (сурет 3.2) көрсетілген.



Сурет 3.2 Жүйенің UML сұлбасы.

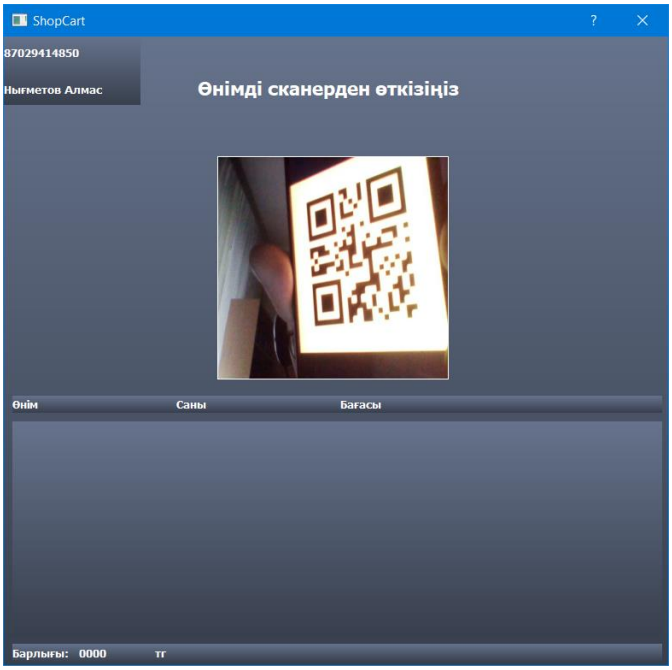
Негізгі қосымшада тұтынушы жұмысқа кіріспестен бұрын өзінің смартфонына мобильдік қосымшаны құрып, деректер базасына тіркелу керек, содан соң тұтынушыға авторизация процесін өтуіне мүмкіндік беретін QR коды беріледі. Сол QR кодын қолданып ол төлем қосымшасына тіркеле алады(сурет 3.3).



Сурет 3.3 Тұтынушының негізгі қосымшаға тіркелу процессі.

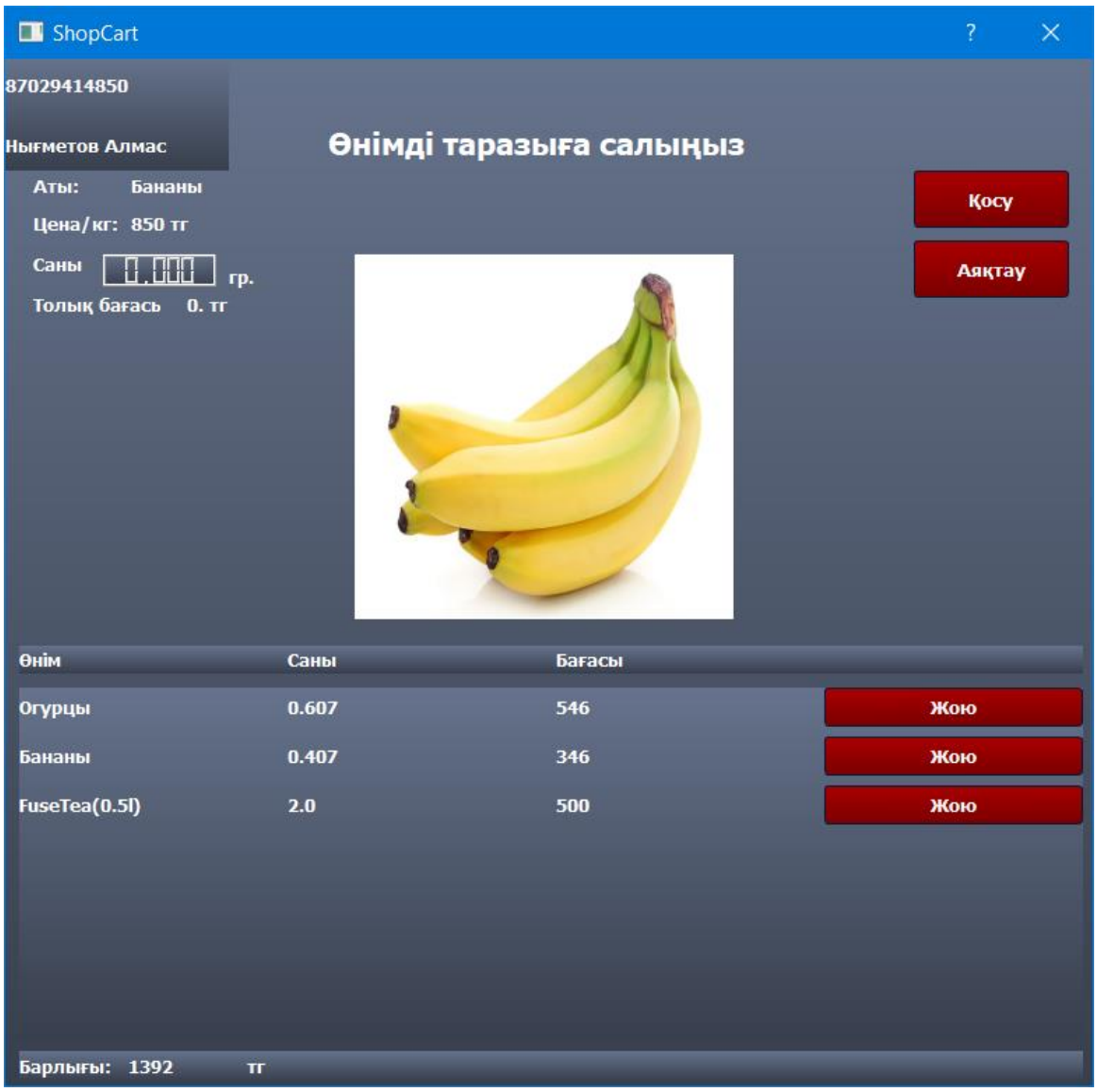
Қабылданған QR коды есептелініп, алынған мәлімет деректер базасына жіберіліп,тексеріледі.Дұрыстығы расталған соң тұтынушы әрі қарай қолданыс процессін жалғастырады.Келесі бетте бізде тағы QR оқитын шағын терезе, өнімді себетке қосу,алу, және сауданы аяқтау батырмалары бар, сонымен қатар себет өнімдер тізі ретінде көрсетілген.

Өнімді себетке қосу процессі екі этаптан тұрады. Біріншісі ол өнімнің сыртында орнатылған QR кодын сканерге жақындатып, өнімді тіркеу.Екіншісі ол тіркелген өнімнің салмағын алу арқылы оның санын және салмағын алу. Сол арқылы сол өнімге деген бағаны экранға шығарып себетке қосылады.Нақтырақ (сурет 3.4)-те көрсетілген



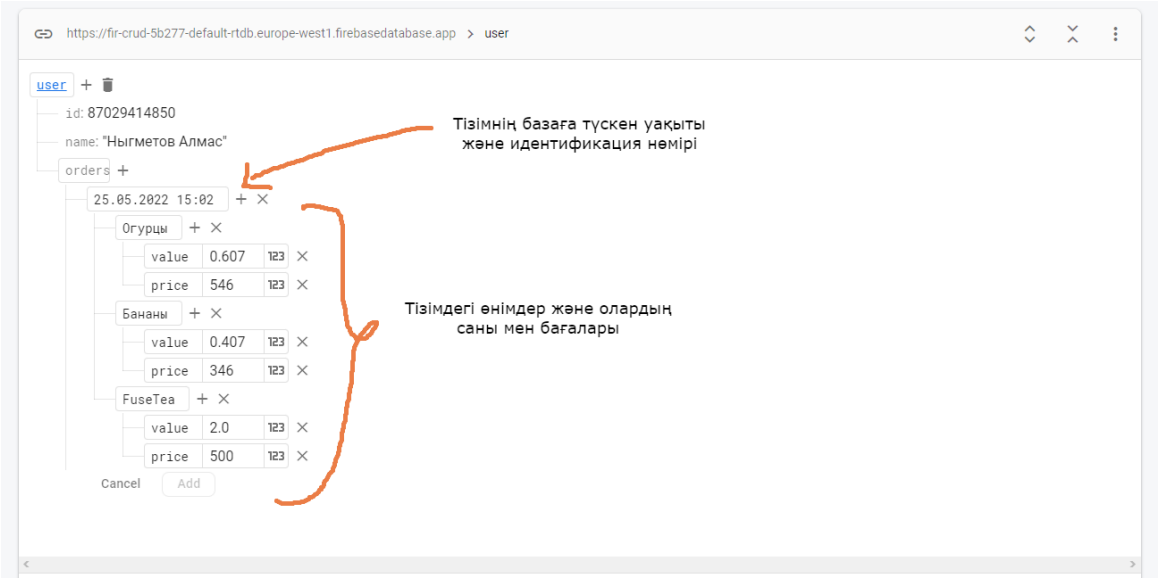
Сурет 3.4 Қосымшаның басты беті, өнімді сканерлеу процессі.

Қосылған өнімдер тізімі құрылғаннан кейін, ол тізім деректер базасына жіберіледі. Сол база артқылы тура уақыт ішінде қолданушының мобильдік қосымшасына хаттама болып келіп, төлем жасауын талап етеді.(сурет 3.5)



Сурет 3.5 Өнімдерді тіркеп себетке қосу процессі.

Керек өнімдерді тірке болғаннан кейін “Аяқтау” батырмасын басып,өнімдер тізімін деректер базасына жібереміз.Ол жерде олар (сурет3.6) тегідей сақталады

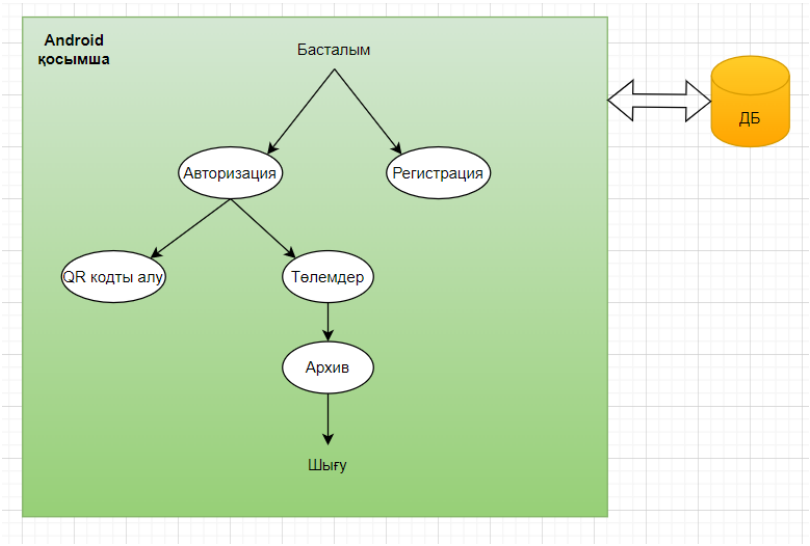


Сурет 3.6 Өнімдер тізімінің деректер базасында орналасуы.

Осы жерден тұтынушы қосымшаның авторизация жүйесінен шығып, әрі қарай кете береді.Ал қосымша бастапқы бетіне ауысады. Алыңған өнімдердің ақысын төлем мобильді қосымшада жалғасады.

Мобильді қосымша Android Studio ортасында құрылады және де Firebase деректер базасымен жалғанады. Ол жерде жаңа тұтынушылар регистрациядан өте алады және өзінің сатып алған өнімдерінің ақысын төлей алады.

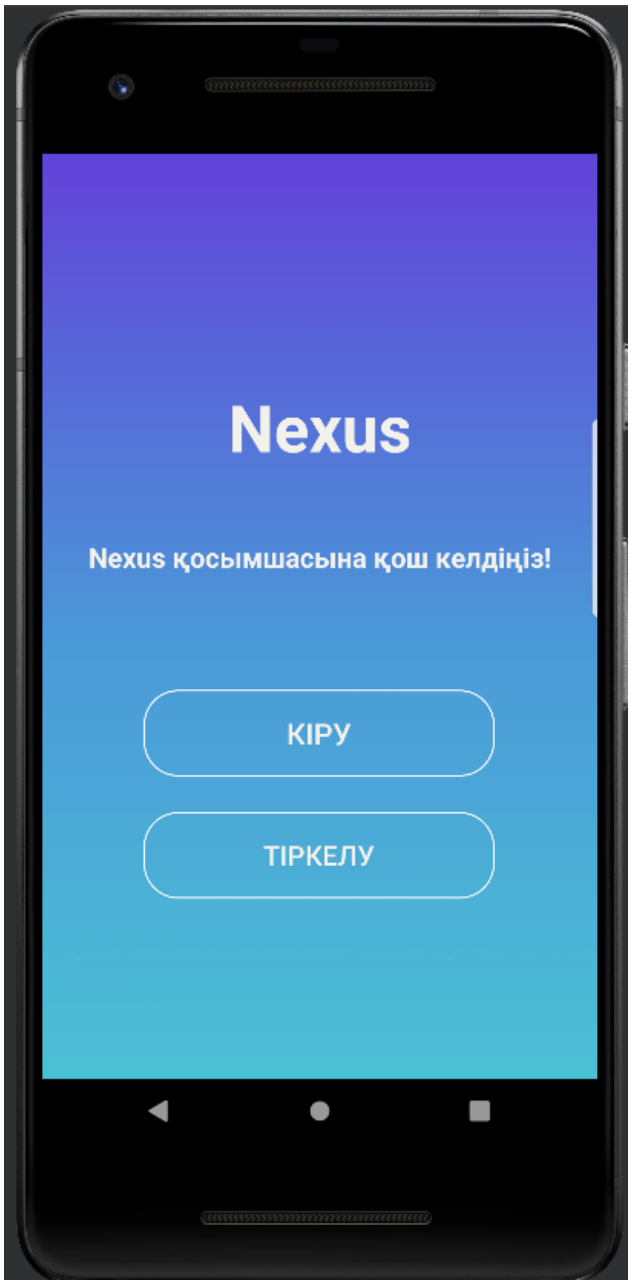
Қосымшаның өзіне келетін болсақ онда бастапқы бет және негізгі бет болады. Бастапқы бетте авторизация немесе регистрация батырмалары болса, негізгі бетте QR идентификаторын алу және сатылымдардың ақысы төлеу атты екі батырма болады.(сурет 3.7) де нақтырақ көрсетілген.



Сурет 3.7 Мобильді қосымша интерфейсінің сұлбасы.

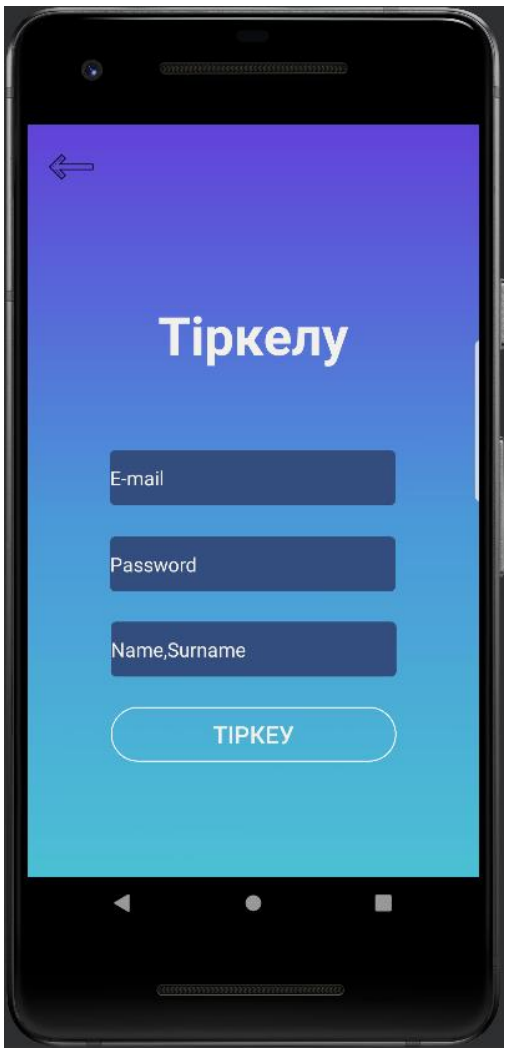
Бастапқы бет көп қосымшаларда ұқсас болып келеді негізгі көңіл аударатын нәрселер бұл авторизация дәне регистрация батырмалаыр болып

табылады.(сурет 3.8)



Сурет 3.8 Бастапқы парақша.

ViewGroup - тың бұл түрі жаңа layout файлдарын жасау кезінде әдепкі бойынша ұсынылады. Бұл әр түрлі күрделіліктегі экрандар жасау үшін өте ыңғайлы және икемді. LL – де Orientation қасиеті бар,(сурет 3.9) ол еншілес элементтердің қалай орналасатынын анықтайды-көлденең немесе тік сызық.



Сурет 3.9 Тіркелу парақшасы.

Мобильді қосымшаның бұл жердегі маңыздылығы зор және де негізге рөлі бұл-тұтынушыны идентификациялау және төлем мәселесін шешу.Төлемнің бірнеше жолдары бар. Электрондық әмиян, NFC немесе банк сервистері. Осының бәрі тез және жылдам, өзін – өзі қамтамасыз ету, және де байланыссыз төлем жүйсін құрады.

3.3 Жүйенің аппараттық бөлігі

Arduino-бұл электронды конструктор және жаңадан бастаушылар мен кәсіпқойлар үшін электронды құрылғылардың жылдам дамуының ыңғайлы платформасы. Платформа бағдарламалау тілінің ыңғайлылығы мен қарапайымдылығына, сондай-ақ ашық архитектурасы мен бағдарламалық кодына байланысты бүкіл әлемде өте танымал. Құрылғы USB арқылы бағдарламалаушыларды пайдаланбай бағдарламаланады.

Таразы Arduino ортасында іске асырылған. Басты элемент – Тензодатчик.Arduino таразысы үш элементтен тұрады,олар:

- Arduino UNO – негізгі микроконтроллер, таразының миы.
- Тензодатчик - деформация шамасын өлшеуге ыңғайлы сигналға (әдетте электрлік) түрлендіретін сенсор, тензометрдің негізгі компоненті (деформацияны өлшейтін құрал).
- Тензометр – тензодатчик жіберген мәліметтерді аналогты түрден цифлық түрге ауыстырады.

Таразының құрылысы (сурет 3.10) келтірілген

Сурет 3.10 Arduino ортасында құрылған таразы.

Кодқа келетін болсақ, жұмыс атқару үшін бізге "HX711.h" кітапханасын орнату қажет. Бұл кітапхана бізге тензометрмен жұмыс істеуге мүмкіндік береді. Негізгі функциялары олар:

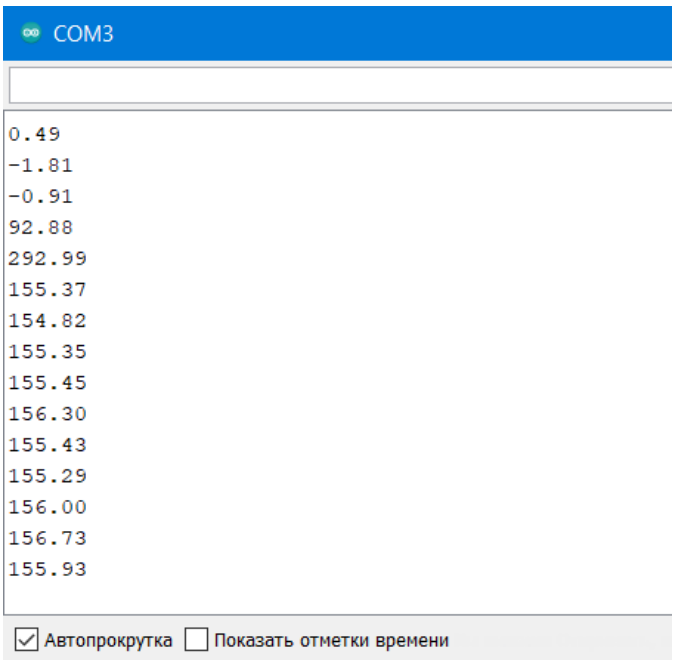
scale.begin – бұл функция жалғанған тензодатчикті іске қосады;

scale.set_scale() – бұл функция арқылы біз тензометрге калибрлеу коэффицентін енгіземіз;

scale.get_units() – бұл функция арқылы біз тензометрдің цифрлық мәліметтерін ала аламыз;

Жұмыс нәтижесін порттың мониторында көре аламыз (сурет 3.10)

Arduino Uno-бұл atmega328 негізіндегі микроконтроллер тақталарының бір түрі,ал Uno - итальяндық термин. Arduino Uno микроконтроллер тақтасының алдағы шығарылымын белгілеу үшін аталған, атап айтқанда Arduino Uno Board 1.0. Бұл тақтаға сандық і / о түйреуіштері - 14, қуат қосқышы, аналогтық I/O түйреуіштері - 6, керамикалық резонатор - 16 МГц, USB коннекторы, RST түймесі және ICSP тақырыбы кіреді. Мұның бәрі осы тақтаны компьютерге қосқан кезде одан әрі жұмыс істеу үшін микроконтроллерді қолдай алады. Бұл тақтаны айнымалы және тұрақты ток адаптері, USB кабелі немесе батарея арқылы қуаттауға болады. (сурет 3.11)



Сурет 3.11 Arduino портының мониторы.

ATmega328-бұл megaAVR отбасының бір бөлігі ретінде Atmel жасаған бір чипті микроконтроллерлердің бірі. Бұл Arduino UNO архитектурасы-8 биттік RISC процессорының өзегі бар бейімделген Гарвард архитектурасы. Басқа Arduino UNO тақталарына Arduino Pro Mini, Arduino Nano, Arduino Due, Arduino Mega және Arduino Leonardo кіреді.

Arduino Uno ATmega328 сипаттамаларына мыналар кіреді.

- Жұмыс кернеуі 5 В құрайды
- Ұсынылатын кіріс кернеуі-7В-ден 12В-ға дейін
- Кіріс кернеуі 6В-тан 20В-қа дейін өзгереді
- Сандық енгізу/шығару контактілері-14
- Аналогтық кіріс / шығыс – 6
- Әр кіріс/шығыс үшін Тұрақты ток 40 мА құрайды
- 3,3 в - 50 мА шығаруға арналған тұрақты ток
- Флэш-жад-32 КБ
- SRAM-2 КБ
- EEPROM-1 КБЖылдамдығы CLK-16 МГц

Arduino UNO қуатын USB кабелі немесе сыртқы қуат көзі арқылы алуға болады. Сыртқы қуат көздеріне негізінен айнымалы және тұрақты ток адаптері немесе батарея кіреді. Адаптерді Arduino UNO-ға Arduino тақтасының қуат коннекторына салу арқылы қосуға болады. Сол сияқты, батарея сымдарын VIN контактісіне және POWER коннекторының GND контактісіне қосуға болады. Болжалды кернеу диапазоны 7-ден 12 Вольтқа дейін болады.

HX711-бұл жиынтықта алдын-ала күшейткіші бар ADC чипі. Чип таразыда қолдану үшін арнайы жасалған. Әдетте салмақты өлшейтін жүктеме жасушалары милливольтадағы кернеуді шығарады. Бұл шығуларды тікелей

контроллерлермен өңдеу қиын, сондықтан біз осы кернеу сигналдарын қабылдайтын және микроконтроллер қолдана алатын стандартты сандық мәндерді шығаратын hx711 чипін қолдана аламыз. Микросхемада осындай төмен кернеулерді өңдеу үшін арнайы алдын-ала күшейткіш бар.

Қорытынды

Дипломдық жұмыста қойылған мақсаттар орындалып, міндеттер жүзеге асырылды. Соңғы бір-екі жылда әлемдегі жағдайдың күрт өзгеруіне байланысты байланыссыз жұмыс атқаратын технологиялардың рөлдері тез артуына куә болдық. Тек сауда ортасында емес, жалпы мемлекеттік деңгейде жаппай енгізілуі жақсы шешім болғанына тағы да көз жеткізіп отырмыз. Әсіресе QR технологиясының енгізілуі бірнеше өзгерістерге алып келді. Біріншіден Covid 19 пандемиясының тарауына жол бермеді, екіншіден халық ішінде және мемлекеттік деңгейде технологияларды модернизациялау процессін жылдамдатты. Есеп бойынша Қазақстанда шағын төлемдердің шамамен 75% -ы мобильді QR төлем арқылы іске асуда, және маршруттық төлемдердің шамамен жартысы байланыссыз төлеммен, ал қалған жартысы RFID картасымен төленді. Бұл дегеніміз қолма-қол ақшаның маңыздылығы азайғанын байқадық. Ендігі бір екі жылда қолма қол ақшадан бастарту процессі басталады деген болжам бар.

QR-кодты қолдану оқу процесінің тиімділігі мен нәтижелілігін арттыра алады. Мұғалімдер мен оқытушылар өзгерісті бағыттаушы ретінде қызықты, инновациялық және мағыналы оқытуды, әсіресе математика мен басқа да пәндерді жасай алады. Сонымен қатар, студенттер қазіргі дамуға бейімделген нақты және жағымды оқу тәжірибесін ала алады.

Осы жұмыстың орындау барысында мен бірнеше жүйелермен жұмыс атқарып, оларды жалғауды үйрендім. Python,PyQT,Android және де Firebase жүйелері кең дамыған, ашық кодты және көптеген кітапханалары бар екеніне көз жеткіздім.

Байланыссыз төлемдер дегеніміз негізінде бір ғана технология емес, бірнеше технологияларының жиынтығы болып табылады. Интерфейсқа бір фреймворк жауап берсе, деректер айналымымен, қауіпсіздікке басқа фреймворк жауап береді.Бүткіл жүйеге нақты қадағалау қажет, өйткені төлем бар жерде, қауіпсіздік деңгейі жоғары.

Байланыссыз төлем әдістері күнделікті саудада жиі қолданылады. Бұл жұмыста онлайн төлемдермен, сондай-ақ клиенттердің төлемдерін жүзеге асыру үшін электрондық коммерцияны енгізумен байланысты мәселелер талқыланады. Сонымен қатар, мобильді транзакцияларды қолдайтын және оларды ыңғайлы және мөлдір ететін технологиялардың дамуы осы төлем әдісін қолдануға дағдыланған сатып алушылардың сенімін арттырады. Бұл клиенттердің мінез-құлқындағы өзгеріс, бұл бөлшек сауда мен банк ісінде, сондай-ақ барлық қол жетімді мобильді құрылғыларда дәстүрлі онлайн төлем әдісіне ауысуды көрсетеді. Осы зерттеуде келтірілген статистика онлайн төлем әдісін қолданатын және онлайн-транзакциялар жасайтын клиенттердің саны үнемі өсіп келе жатқанын көрсетеді, бұл академияда да, өнеркәсіпте де онлайн төлем жүйелерінің тұрақты танылуын көрсетеді. Алайда, бірқатар жаңа технологияларды қабылдау және енгізу қазіргі уақытта да, жақын болашақта да

қауіпсіз онлайн төлем жүйелерін енгізу және дамыту үшін жаңа мүмкіндіктер мен қиындықтар туғызады. Бұл зерттеу осы төлем әдісінің қолайлы болашағы үшін қолданыстағы қаржылық және телекоммуникациялық инфрақұрылыммен онлайн төлем жүйелерін жақсырақ интеграциялау қажет деген қорытындыға келді. Сонымен қатар, әртүрлі қызмет провайдерлері үшін жалпы стандартты құру, көптеген тұтынушылармен үйлесімділікті жақсарту, құпиялылық пен қауіпсіздік мәселелерін жеңу және ең жаңа технологияларды пайдалану онлайн төлем әдістерін тез қабылдауға және осы төлем әдісінің нарығын кеңейтуге ықпал етуі мүмкін. Болашақ жұмыс бүкіл әлемде онлайн-төлем жүйелерін тиімді енгізуге ықпал ететін түрлі факторларды заңдастыруға бағытталуы мүмкін.

Пайдаланылған әдебиеттер тізімі

1. Coppola R., Ardito L., Torchiano M.Characterizing the transition to kotlin of android apps: A study on F-droid, play store, and GitHubInt. Workshop on App Market Analytics (WAMA) (2019), pp. 8-14
2. J. Oliveira, D. Borges, T. Silva, N. Cacho, F. CastorDo android developers neglect error handling? A maintenance-centric study on the relationship between android abstractions and uncaught exceptions
3. M. Banerjee, S. Bose, A. Kundu, M. MukherjeeA comparative study: Java vs kotlin programming in android application developmentInt. J. Adv. Res. Comput. Sci., 9 (3) (2018), p. 41
4. Enck W., Octeau D., McDaniel P.D., Chaudhuri S.A study of android application securityUSENIX Security Symposium, Vol. 2 (2011), p. 2
5. Mazuera-Rozo A., Bautista-Mora J., Linares-Vásquez M., Rueda S., Bavota G.The android OS stack and its vulnerabilities: an empirical studyEmpir. Softw. Eng. (2019)
6. Ponzanelli L., Bavota G., Penta M.D., Oliveto R., Lanza M.Prompter - turning the IDE into a self-confident programming assistantEmpir. Softw. Eng., 21 (5) (2016), pp. 2190-2231
7. Rosen S., Qian Z., Mao Z.M.AppProfiler: A flexible method of exposing privacy-related behavior in android applications to end usersInt. Conference on Data and Application Security and Privacy (CODASPY) (2013), pp. 221-232
8. Singleton L., Zhao R., Song M., Siy H.FireBugs: finding and repairing bugs with security patternsInt. Conference on Mobile Software Engineering and Systems (MOBILESoft) (2019)Google Scholar
9. StatCounter, 2020bStatCounter, ., 2020. Desktop vs Mobile vs Tablet vs Console Market Share Worldwide, https://gs.statcounter.com/platform-market-share.Google Scholar
10. Thomas et al., 2015Thomas D.R., Beresford A.R., Rice A.Security metrics for the android ecosystemInt. Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM) (2015), pp. 87-98
11. P. Sommerhoff, January, 2018, “Kotlin vs. Java: 9 Benefits of Kotlin for Your Business”, from https://business.udemy.com/blog/kotlin-vs-java-9-benefitsof-kotlin-for-your-business/
12. R.K. Panchal, and, A.K. Patel, 2017, A comparative study: Java Vs kotlin Programming in Android , in International Journal of Innovative Trends in Engineering & Research, September 2017, vol 2 Issue 9, pp 4 – 10.
13. S. Alani, S. N. Mahmood, S. Z. Attaallah, H. S. Mhmood, Z. A. Khudhur, A. A. Dhannoon, International Journal of Electrical Computer Engineering 2021, 11.
14. C.J. Hoofnagle, J.M. Urban and S. Li, “Mobile Payments: Consumer benefits and new privacy concerns”, BCLT Research Paper, pp. 1-19, 2012
15. A BREAKTHROUGH FOR CONTACTLESS PAYMENTS https://www.dynata.com/content/Dynata-Global-Consumer-Trends-COVID-19-The-

New-Normal-Breakthrough-for-Contactless-Payments.pdf

16. SmartLab Kazakhstan" LLP: [Online resource]. A., 2015-2021.URL: http://lis.kz.

17. Health Level Seven International: [Online resource]. 2013-2021. URL: https://wiki.hl7.org/.

18. Global Mobile Money Initiative – MEF [Online resource]URL: https://mobileecosystemforum.com/mobile-money-report/

19. PricewaterhouseCoopers. (2016) Mobile proximity payment: 5 things retailers should know. Retrieved from https://www.pwc.com/it/it/publications/assets/docs/mobileproximity.pdf

20. Mun, Y. P., Khalid, H., & Nadarajah, D. (2017). Millennials' perception on mobile payment services in Malaysia. Procedia Computer Science, 124, 397-404

21. Ntaukira, J., Khomba, J. K., & Maliwichi, P. (2019). Investigating Factors That Determine Continuous Intention Behaviour To Use Mobile Payment Services In Malawi (No. 2110). EasyChair

22. Ovum. (2012), Digital Wallet Dynamics., pp. 1–12. Retrieved from http://www.mahindracomviva.com/wp-content/uploads/2015/02/MahindraComviva-Digital-Wallet-Whitepaper.pdf

23. Phuah, K. T., TingJL, J. L., & Wong, K. K. S. (2018). Understanding customer intention to use mobile payment services in Nanjing, China. International Journal of Community Development and Management Studies, 2, 049-060.

24. K. Cash, "Stratos, Coin, Plastc, SWYP: Sizing up multiaccount cards"(2016). [Online]. Available: https://www.nerdwallet.com/blog/credit cards/stratos-coin-plastc-swyp-sizing-multiaccount-cards.

25. Consumer payments study". [Online]. Available: http://tsys.com/Assets/TSYS/downloads/rs_2014-consumer paymentsstudy.pdf.

26. "What is an E-Payment System?" [Online]. SecurionPay - Payment Gateway. Available: https://securionpay.com/blog/e-payment-system/

27. D. Fernandez and D. Fernandez, "The Future of Cashless Economies: Why Governments and Consumers Should Migrate to Cashless Payments", Netclearance Systems, 2017. [Online]. Available: http://www.netclearance.com/blog/2017/1/6/the-future-of-cashless economies-why-governments-and-consumers-should-migrate-to cashless-payments. [Accessed: 30- Apr- 2017].

28. J. Tellez Isaac and Z. Sherali, "Secure Mobile Payment Systems", IT Professional, vol. 16, no. 3, pp. 36-43, 2014.

29. D. Pavithra, R. Balakrishnan, in 2015 global conference on communication technologies (GCCT), IEEE, 2015, pp. 169-173.

30. P.M. Ogedebe and B.P. Jacob, "E-payment: Prospects and Challenges in Nigerian Public Sector", International Journal of Modern Engineering Research,vol. 2, no. 5, pp. 3104-3106, 2012.

31. I. G. M. N. Desnanjaya, I. N. A. Arsana, Indonesian Journal of Electrical Engineering Computer Science 2021, 22, 1295-1302.

32. M.A. Kabir, S.Z. Saidin and A. Ahmi, "Adoption of e-Payment Systems: A

Review of Literature", International Conference on E-Commerce, Kuching, Sarawak, 2015, pp. 112-1

Қосымша

Python тілінде бағдарламалық коды

Main.py

```
from PyQt5 import QtWidgets,uic
from PyQt5.QtSerialPort import QSerialPort,QSerialPortInfo
from PyQt5.QtCore import QIODevice, QByteArray,QThread,Qt,QFile,QTimer,pyqtSignal
from PyQt5.QtGui import QImage,QPixmap
from PyQt5.QtWidgets import *
import cv2
import pyrebase
import re
class camThread(QThread):
    def __init__(self,mainwindow,parent=None):
        super().__init__()
        self.mainwindow = mainwindow
    def run(self):
        cap = cv2.VideoCapture(0)
        detector = cv2.QRCodeDetector()
        def displayimage(img, window=1):
            if len(img.shape) == 3:
                if (img.shape) == 4:
                    qformat = QImage.Format_RGBA8888
                else:
                    qformat = QImage.Format_RGB888
            img = QImage(img, img.shape[1], img.shape[0], qformat)
            img = img.rgbSwapped()
            ui.imglabel.setPixmap(QPixmap.fromImage(img))
            ui.imglabel.setMinimumSize(1, 1)
            ui.imglabel.setScaledContents(True)
        while (cap.isOpened()):
            ret, frame = cap.read()
            if ret == True:
                displayimage(frame, 1)
                cv2.waitKey()
                data, one, ret = detector.detectAndDecode(frame)
                if data:
                    cv2.destroyAllWindows()
                    print("got it")
                    itemid = data
                    readQR(itemid)
                    cap.release()
                    cv2.destroyAllWindows()
            else:
                print('return not found')
    def stop(self):
        self.terminate()
app = QtWidgets.QApplication([])
ui = uic.loadUi("cart2.ui")
ui.setWindowTitle("ShopCart")
buttontoLayout = {}
```

```
from PyQt5 import QtWidgets,uic
from PyQt5.QtSerialPort import QSerialPort,QSerialPortInfo
from PyQt5.QtCore import QIODevice, QByteArray,QThread,Qt,QFile,QTimer,pyqtSignal
from PyQt5.QtGui import QImage,QPixmap
from PyQt5.QtWidgets import *
import cv2
import pyrebase
import re
class camThread(QThread):
    def __init__(self,mainwindow,parent=None):
        super().__init__()
        self.mainwindow = mainwindow
    def run(self):
        cap = cv2.VideoCapture(0)
        detector = cv2.QRCodeDetector()
        def displayimage(img, window=1):
            if len(img.shape) == 3:
                if (img.shape) == 4:
                    qformat = QImage.Format_RGBA8888
                else:
                    qformat = QImage.Format_RGB888
            img = QImage(img, img.shape[1], img.shape[0], qformat)
            img = img.rgbSwapped()
            ui.imglabel.setPixmap(QPixmap.fromImage(img))
            ui.imglabel.setMinimumSize(1, 1)
            ui.imglabel.setScaledContents(True)
        while (cap.isOpened()):
            ret, frame = cap.read()
            if ret == True:
                displayimage(frame, 1)
                cv2.waitKey()
                data, one, ret = detector.detectAndDecode(frame)
                if data:
                    cv2.destroyAllWindows()
                    print("got it")
                    itemid = data
                    readQR(itemid)
                    cap.release()
                    cv2.destroyAllWindows()
            else:
                print('return not found')
    def stop(self):
        self.terminate()
app = QtWidgets.QApplication([])
ui = uic.loadUi("cart2.ui")
ui.setWindowTitle("ShopCart")
buttontoLayout = {}
serial=QSerialPort()
serial.setBaudRate(9600)
sshFile="Adaptic.qss"
with open(sshFile,"r") as fh:
    app.setStyleSheet(fh.read())
firebaseConfig = {'apiKey': "AIzaSyADtjjQDQdbvNEAUJzan3_XMS6zQEOLGsA",
```

```
··'authDomain':·"fir-crud-5b277.firebaseapp.com",↵
··'databaseURL':·"https://fir-crud-5b277-default-rtdb.europe-west1.firebasedatabase.app",↵
··'projectId':·"fir-crud-5b277",↵
··'storageBucket':·"fir-crud-5b277.appspot.com",↵
··'messagingSenderId':·"1064906260461",↵
··'appId':·"1:1064906260461:web:28b16483fe17252476f1e4",↵
··'measurementId':·"G-LE7ZJDG8FE"}↵
firebase·=·pyrebase.initialize_app(firebaseConfig)↵
db=firebase.database()↵
auth=firebase.auth()↵
storage=firebase.storage()↵
ui.datalabel.hide()↵
ui.datalabel_2.hide()↵
ui.datalabel_3.hide()↵
ui.nameinfolabel.hide()↵
ui.typelabel.hide()↵
ui.pnamelabel.hide()↵
ui.priceinfolabel.hide()↵
ui.pricelabel.hide()↵
ui.amountinfolabel.hide()↵
ui.overallpricelabel.hide()↵
ui.overallpriceinfolabel.hide()↵
ui.lcdN.hide()↵
ui.nextbtn.hide()↵
ui.endbtn.hide()↵
ui.controlbtn_2.hide()↵
def·readQR(itemid):↵
····imageidstr·=·str(itemid)·+·".jpg"↵
····storage.child("product_images/"·+·imageidstr).download("",·imageidstr)↵
····imageid·=·QImage(imageidstr)↵
····ui.imglabel.setPixmap(QPixmap.fromImage(imageid))↵
····ui.imglabel.setMinimumSize(1,·1)↵
····ui.imglabel.setScaledContents(True)↵
····ui.nameinfolabel.show()↵
····ui.infolabel.show()↵
····ui.pnamelabel.show()↵
····ui.priceinfolabel.show()↵
····ui.pricelabel.show()↵
····ui.amountinfolabel.show()↵
····ui.overallpricelabel.show()↵
····ui.overallpriceinfolabel.show()↵
····ui.typelabel.show()↵
····ui.lcdN.show()↵
····ui.nextbtn.show()↵
····ui.endbtn.show()↵
····ui.infolabel.setText("Өнімді·таразыға·салыңыз")↵
····productinfo·=·db.child("products").order_by_child("id").equal_to(int(itemid)).get()↵
····for·product·in·productinfo.each():↵
········productname·=·product.val()['name']↵
········producttype·=·product.val()['type']↵
········productprice·=·product.val()['price']↵
········productweight·=·product.val()['weightperproduct']↵
····ui.pnamelabel.setText(productname)↵
```

```
    if (producttype == "countable"):
        ui.priceinfolabel.setText("Цена шт.:")
        ui.pricelabel.setText(str(productprice) + " гр")
        ui.typelabel.setText("ШТ")
        ui.controlbtn_2.clicked.connect(lambda :onUpdate(productweight,productprice,producttype))
        ui.controlbtn_2.click()
    if(producttype == "uncountable"):
        ui.priceinfolabel.setText("Цена/кг:")
        ui.pricelabel.setText(str(productprice)+" гр")
        ui.typelabel.setText("гр.")
        ui.controlbtn_2.clicked.connect(lambda :onUpdate(productweight,productprice,producttype))
        ui.controlbtn_2.click()
def onUpdate(productweight,productprice,producttype):
    ui.datalabel.setText(str(productprice))
    ui.datalabel_2.setText(str(productweight))
    ui.datalabel_3.setText(str(producttype))
def onRead():
    if not serial.canReadLine(): return
    rx = serial.readLine()
    rxs = str(rx,'utf-8')
    if(ui.datalabel_3.text()=="countable"):
        if( isfloat(rxs)):
            if(float(rxs)>0.005):
                count=round(float(rxs)*3571.4/float(ui.datalabel_2.text()))
                ui.lcdN.display(count)
                ui.overallpricelabel.setText(str(round((count*float(ui.datalabel.text())),3)))
            else:
                ui.lcdN.display("0.000")
                ui.overallpricelabel.setText(str("0.000"))
    elif(ui.datalabel_3.text()=="uncountable"):
        if (isfloat(rxs)):
            if (float(rxs) > 0.005):
                count = float(rxs) * 3571.4 / float(ui.datalabel_2.text())
                ui.lcdN.display(float(rxs)*3.5714)
                ui.overallpricelabel.setText(str(round((count * float(ui.datalabel.text())))) + " гр")
            else:
                ui.lcdN.display("0.000")
                ui.overallpricelabel.setText(str("0. гр"))
list=[]
class items:
    def __init__(self,name,weight,price):
        self.name = name
        self.weight = weight
        self.price = price
def isfloat(num):
    try:
        float(num)
        return True
    except ValueError:
        return False
def onOpen():
    serial.setPortName("COM3")
    serial.open(QIODevice.ReadWrite)
```

```
def sendcheck():
    for obj in list:
        print(obj.name,obj.weight,obj.price)
def onClose():
    serial.close()
def onAdd():
    print('Clicked')
    horizontalLayout=QHBoxLayout()
    buttonText=("Хоso")
    buttonS=QPushButton(buttonText,ui)
    label_pname = QLabel(ui.pnamelabel.text())
    label_count=QLabel(str(round(ui.lcdN.value(),3)))
    label_overall=QLabel(str(int(re.search(r'\d+',ui.overallpricelabel.text()).group())))
    horizontalLayout.addWidget(label_pname)
    horizontalLayout.addWidget(label_count)
    horizontalLayout.addWidget(label_overall)
    horizontalLayout.addWidget(buttonS)
    ui.verticalLayout.insertLayout(0,horizontalLayout)
    buttontoLayout[buttonS]=horizontalLayout
    print(ui.totallabel.text())
    print(label_overall.text())
    ui.totallabel.setText(str(int(int(ui.totallabel.text())+int(label_overall.text()))))
    list.append(items(label_pname.text(),label_count.text(),label_overall.text()))
    buttonS.clicked.connect(onDelete)
    camThreadinstance.stop()
    camThreadinstance.start()
def onDelete():
    rbt=ui.sender()
    hlt=buttontoLayout.get(rbt)
    while(hlt.count()!= 0):
        item=hlt.takeAt(0)
        widget=item.widget()
        widget.deleteLater()
    hlt.deleteLater()
camThreadinstance = camThread(mainwindow=ui)
camThreadinstance.setTerminationEnabled(True)
camThreadinstance.start()
ui.endbtn.clicked.connect(sendcheck)
ui.nextbtn.clicked.connect(onAdd)
ui.controlbtn.clicked.connect(onOpen)
serial.readyRead.connect(onRead)
ui.controlbtn.click()
ui.controlbtn.hide()
ui.show()
app.exec()
¶
```