AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əsgərov Ruslan Əfqan oğlu
Ağayev Hüseynbala Şöhrət oğlu
Zeynalova Gülnar Vəli qızı
Qarayev Cabir Oqtay oğlu

İnternet bankçılıq sistemində istifadəçi məxfiliyinin çoxsəviyyəli autentifikasiya tətbiqli model və alqoritminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter texnikasının lahiyələndirilməsi və konstruksiya edilməsi"

Elmi rəhbər: t.e.n, dosent **İsgəndərzadə Hüseyn Qasım oğlu**

BAKI – 2023

GİRİŞ

GİRİŞ

Müştərinin bank fəaliyyətini həyata keçirməsinin iki yolu var. Birincisi, bank işçiləri ilə fiziki qarşılıqlı əlaqə, ikincisi isə elektron əməliyyatdır (ATM əməliyyatı, onlayn əməliyyat və E-coin). Birinci halda bank işçiləri çek kitabçası, müştəri imzası və fotoşəkil əsasında istifadəçinin autentifikasiyasını əl ilə həyata keçirir. Elektron əməliyyat vəziyyətində bank, istifadəçinin identifikatoru və PİN kodu (şəxsi identifikasiya nömrəsi) əsasında istifadəçinin autentifikasiyasını həyata keçirən ənənəvi metodu tətbiq edir. Lakin bu halda təhlükəsizlik elektron əməliyyatla bağlı əsas məsələlərdən biridir. Hal-hazırda Bank ənənəvi təhlükəsizliyi təmin edir (istifadəçi adı və şifrə ilə istifadəçinin autentifikasiyası). Son illərdə kibercinayətkarlıq halları günü-gündən artır. Cinayətkar hücum təkcə kibertəhlükəsizlik və kiberməlumat deyil, həm də şəxsi məlumatları toplayır və elektron bank sisteminə hücum edir. Bir çox cinayətkarlar təhlükəsizliyi pozaraq Bankçılıq məlumat bazasına daxil olur və qeyri-qanuni yollarla müştərilərin şəxsi məlumatlarını (hesab məlumatları, kart məlumatları, istifadəçi identifikatoru, parol və s.) oğurlayırlar. Cinayətkar şəxsi məlumatları əldə etdikdən sonra istifadəçilərin hesabı hücuma məruz qalır. Bu, təkcə istifadəçi üçün deyil, həm də bank olmaq üçün təhdiddir. Şifrələrdən və istifadəçi identifikatorlarından (identifikatorlar) və ya identifikasiya kartlarından və PIN-lərdən (şəxsi identifikasiya nömrələri) istifadəni nəzərdə tutan istifadəçi autentifikasiyasının üstünlük təşkil edən üsulları bir sıra məhdudiyyətlərdən əziyyət çəkir. Parollar və PİN-lər birbaşa gizli müşahidə yolu ilə qeyri-qanuni şəkildə əldə edilə bilər. Hal-hazırda onlayn əməliyyat təhlükəsizliyi üzərində işləyən çoxlu alim var. Burada biz elektron əməliyyatda istifadəçinin autentifikasiyası üçün üç səviyyəli təhlükəsizlik sistemi hazırlamışıq.

Bu işin əsas məqsədi həm istifadəçi, həm də bank üçün etibarlı olan elektron əməliyyat sistemini müəyyən etməkdir.

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əsgərov Ruslan Əfqan oğlu

İnternet bankçılıq sistemində istifadəçi məxfiliyinin çoxsəviyyəli autentifikasiya tətbiqli model və alqoritminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter texnikasının lahiyələndirilməsi və konstruksiya edilməsi"

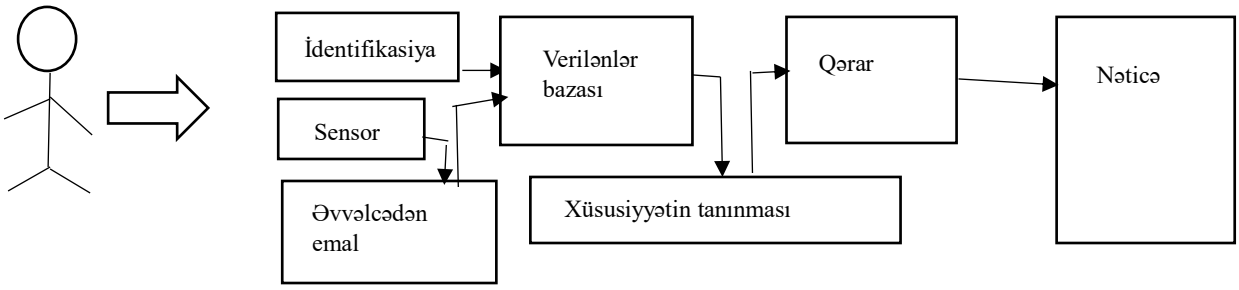
Elmi rəhbər: t.e.n, dosent İsgəndərzadə Hüseyn Qasım oğlu

BAKI – 2023

I FƏSİL. BİOMETRİKA VƏ MOBİL BANKÇILIQ

1.1. Biometrik metodların tədqiqi

Biometriklər mobil bankçılıq müştərisinin fiziki və elektron şəxsiyyəti arasında autentifikasiya məqsədi ilə çox mühüm rol oynayır. Xüsusilə autentifikasiya üsulları üçün biometrik tanınma mexanizmlərinin müxtəlif növləri var. Hər bir insanın bioloji xüsusiyyətləri digərlərindən fərqlidir, ona görə də deyə bilərik ki, biometrik identifikasiya autentifikasiya üçün faydalı bir üsuldur, çünki təhlükəsizlik məqsədi ilə autentifikasiyanı unikal şəkildə müəyyən etmək lazımdır. Bəzi biometrik metodlar səsin tanınması, əl əsaslı tanınması, barmaq izinin tanınması, üz tanınması və s., lakin saxlama məqsədi ilə verilənlər bazasında ən uyğun və daha az məlumat istehlakçısı və əksər istifadəçilər üçün dost və asan üsul barmaq izinin tanınmasıdır. Barmaq izi texnologiyasında araşdırmalar davam edir, buna görə də bir çox fərqli sensorlar hazırlanır. 1998-ci ildə Siemens PSE və Trio datası sensoru olan ilk mobil telefonu inkişaf etdirdi. Ümumi biometrik mexanizm aşağıda göstərilmişdir (şəkil 1.1.1).



Şəkil 1.1.1. Sadə biometrik sistem arxitekturası

Elektron bankçılıq təhlükəsizliyinin biometrik metodlarla təkmilləşdirilməsi cədvəl 1.1.1-də verilmişdir.

Cədvəl 1.1.1

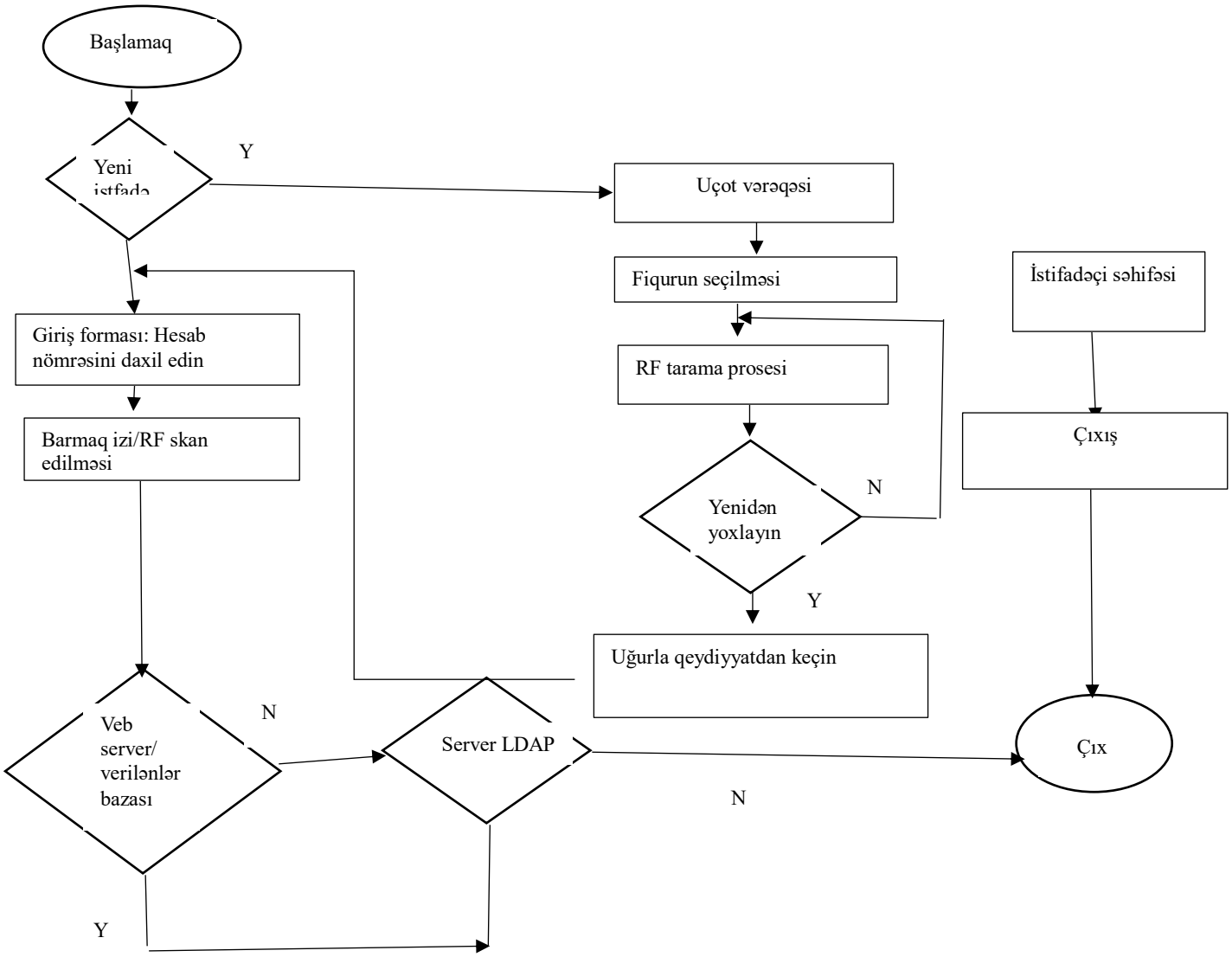
Mobil bankçılığın qəbulu	Görünüş
Təhlükəsiz ödəniş əməliyyatları tələb olunur	Təhlükəsiz identifikasiya üsulu Barmaq izi kimi biometrik metodun qeydiyyatı Mobil bankçılıqda saxtakarlığın minumuma edirilməsi Məxfilik Məlumatların bütövlüyü Səmərəlilik Vius hücumlarının qarşısının alınması

İki növ istifadəçi (1) qeydiyyatdan keçmiş istifadəçi və (2) yeni istifadəçilər var.

1. RF skanerindən istifadə olunur, çünki RF tarama vasitəsilə canlı hüceyrələr və ölü və ya kopyalanan hüceyrələr arasında fərq qoymaq mümkündür. Beləliklə, səlahiyyətli şəxsin mobil bankçılıq xidmətindən istifadə etməsini təmin etmək üçün biometrikdə RF Scanning texnologiyasından istifadə olunur.
2. Məlumatların yoxlanılmasından sonra müştəri vasitəsilə verilənlər bazasına daxil olmaq olar.
3. Əgər barmaq izi verilənlər bazasına uyğun gələrsə, müştəri mobil telefona başlaya biləcək.
4. Əlavə təhlükəsizlik üçün LDAP serverindən istifadə olunur. Birinci barmaq izi identifikasiyası olmadıqda verilənlər bazasında aşkar edildikdə, daha çox yoxlama üçün LDAP serverində yoxlanılacaq.

Yeni istifadəçilər verilənlər bazasında istənilən üç barmaq izini qeydiyyatdan keçirməli və həmçinin qeydiyyat formasını doldurmalıdırlar. Bank müştərisinin barmaq izi uğurla qeydiyyatdan keçərsə, müştəri mobil bank xidmətlərindən istifadə edə biləcək.

Təklif olunan Biometrik Mobil Bankçılıq Sistemi diaqramı aşağıakı kimidir (Şəkil 1.1.2)



Şəkil 1.1.2. Təklif olunan biometrik mobil bankçılıq sisteminin axın alqoritmi

1.2. Biometrik mexanizmlərin bank sektoruna inteqrasiyası

Mobil bankçılıqda yeni model barmaq skaneri qurğusu təklif olunur. Biometrik barmaq izi skaneri qurğusu mobil şirkətlərə barmaq izi mexanizminin tətbiqi ilə mobil telefon dizaynına kömək edəcək. Mobil qurğu istehsalçılarından biometrik barmaq izi skaneri cihazını dəstəkləyən mobil qurğu dizayn etmələri tələb olunur.

[1]Təklif olunan Barmaq izi skaneri qurğusu fenomenləri:

1. Mobil istehsal şirkətləri biometrik skaner qurğusu ilə edəcək mobil əl dəsti. Mobil müştəri ondan autentifikasiya məqsədləri üçün istifadə edəcək.
2. Biometrik barmaq izi skaneri qurğusu PİN (Şəxsi identifikasiya nömrəsi) kimi məlumatları qoruyan ənənəvi üsulu əvəz edəcək.
3. Barmaq izini çəkmək üçün bir sensor olacaq. Çünki indiki vaxtda hardware platformalar verilənləri tutmaq üçün müxtəlif növ sensor interfeysləri dəstəkləyir.
4. Barmaq izi çəkildikdən sonra məlumatlar internet vasitəsilə ötürüləcək. Və məlumatlara bank serveri vasitəsilə daxil olmaq mümkündür.
5. Server sonunda verilənlər bazasında barmaq izi müqayisə edilərək olub olmadığı təsdiqlənəcək və ya səlahiyyətli şəxs mobil bankçılıq sisteminə daxil olur.
6. Barmaq izi skaneri qurğusu Port vasitəsilə mobil telefona qoşula bilər.
7. Məxfilik və etibar səviyyəsi yüksək olacaq, çünki biometrik yenilənə və ya ləğv edilə bilməz.

---

1. [1] F.-M. E. Uzoka and T. Ndzinge, “Empirical analysis of biometric technology adoption and acceptance in Botswana,” J. Syst. Softw., vol. 82, no. 9, pp. 1550– 1564, 2009.

8. Biometrik mexanizmdə barmaq izi skaneri bir çox təşkilatlarda, xüsusən də milli sərhəd nəzarəti, pasport idarələri, hava limanları və s. geniş istifadə olunur. İndi mobil ödəniş etmək və mobil xidmətlərdən istifadə etmək üçün belə biometrik mexanizmləri bank sektoruna inteqrasiya etmək lazımdır.

9. Barmaq izi qurğusunu doldurmaq üçün doldurulan ucuz batareya istifadə olunacaq.

10.Barmaq izi aparatının sensoru var. Sensorda Kapasitans lövhəsi var. Kapasitans elektrik yükünü saxlamaq qabiliyyətinə malikdir.

1.3. Tətbiqi casus proqramları

Spyware, İnternetdə olarkən istifadəçi məlumatlarını gizli şəkildə toplayan bir proqram növüdür. Reklam proqramı marketoloqlar tərəfindən gələcək reklam materialını fərdiləşdirmək məqsədilə İnternet istifadəçisinin vərdişlərini və maraqlarını izləmək üçün istifadə olunan bir növ casus proqramdır. Daha sonra məlumat istifadəçiyə yönəldilmiş gələcək reklamları fərdiləşdirmək üçün istifadə olunur və ya eyni məqsədlə üçüncü tərəfə satıla bilər.

Siz kompüterinizə, cihazlarınıza təsadüfən casus proqramı yükləmək şansınızı minimuma endirə bilərsiniz.

Kompüterinizin viruslardan azad olmasını təmin etmək şansınızı aşağıdakılarla artıra bilərsiniz:

-Antivirus proqram təminatının quraşdırılması və onun ən son virus tərifləri ilə yenilənməsi.

-Əməliyyat sisteminiz üçün təhlükəsizlik yamalarını yüklədikdən sonra yükləyin və quraşdırın.

-Naməlum mənbələrin e-poçtlarından əlavələrin qəbul edilməməsi.

-Proqram təminatının yalnız etibarlı mənbələrdən quraşdırılması.

Trojan, zərərsiz bir tətbiq kimi görünən dağıdıcı bir proqramdır. Viruslardan fərqli olaraq, troyanlar özlərini təkrarlamırlar və əlavə etmək üçün host proqramına ehtiyac duymurlar. Bəzi troyanlar kompüteri viruslardan və ya

digər zərərli proqramlardan təmizləyəcəklərini iddia edəcək, əksinə virusları təqdim edəcək və onu hakerlər və müdaxilə edənlərin hücumlarına qarşı həssas qoyacaqlar. Trojanları təsadüfən yükləmək şansınızı minimuma endirə bilərsiniz.

Əgər fırıldaqçı kompüterdə və ya müştərinin Onlayn Bankçılıq xidmətinə daxil olduğu cihazda "keylogger" adlı proqram təminatı quraşdırırsa, proqram fayla kopyalayır, hər bir düyməni basmaqla həmin fayla kopyalanıb. Bu həssas məlumat ələ keçirilir ki, fırıldaqçı sonradan saxta məqsədlər və hesabınıza qeyri-qanuni giriş üçün istifadə edə bilər.

Bunun qarşısını almağın yolları var.

-Etibar olunmayan hesablara daxil olmaq üçün kompüterlərdən istifadə etməməlisiniz (məsələn, Onlayn Bankçılıq xidmətinə daxil olmaq üçün kiberkafe və ya digər insanların kompüterlərindən istifadə etməyin).

-Sisteminizi qorumaq və sisteminizin virussuz olmasını təmin etmək üçün antivirus proqramını hər gün yeniləyin.

IBS hücumları İnternet bankçılıq tətbiqini saxlayan serverlərə qarşı oflayn hücumlardır. Bunlara daxildir:

-IBS1: Müəyyən parol əsaslı mexanizmlərdə kobud güc hücumlarının təsadüfi istifadəçi adları və parollar göndərməklə mümkün olduğu bildirilir. Hücum edilən mexanizmlər təxmin edilən istifadəçi adlarına və dörd rəqəmli parollara əsaslanan sxem həyata keçirir. Hücum mexanizmi istifadəçi adı və ya parola əsaslanan hesablama üçün avtomatlaşdırılmış proqramların yerləşdiyi paylanmış zombi fərdi kompüterlərinə əsaslanır. Bu hücum istifadəçinin kimliyini müəyyən etmək üçün istifadəçi adı filtrləmə üsulları ilə birləşdirilə bilər. Bu üsullar etibarlı və ya etibarsız istifadəçi adları halında serverin müxtəlif cavablarını süzür.

-IBS2: Bank təhlükəsizlik siyasətinin pozulması – Zəif giriş nəzarəti və qeyd mexanizmləri ilə birlikdə bankın təhlükəsizlik siyasətini pozaraq, işçi daxili təhlükəsizlik insidentinə səbəb ola və müştərinin hesabını ifşa edə bilər.

-IBS3: Veb sayt manipulyasiyası—İnternet bankçılıq veb serverinin zəifliklərindən istifadə onun məzmununun, məsələn, İnternet bankçılığına giriş səhifəsinə keçidlərin dəyişdirilməsinə icazə verə bilər. Bu, istifadəçini onun etimadnaməsinin tutula biləcəyi saxta veb saytına yönləndirə bilər.

1.4. Kredit kartlarının təkrarlanmasında biometrikanın tətbiqi ilə cinayətkarlığın qarşısının alınmasının üsul və vasitələri

Çip və PİN-in tətbiqinə qədər bütün üz-üzə kredit və ya debet kartı əməliyyatları hesab məlumatlarını oxumaq və qeyd etmək üçün maqnit zolaqdan və ya mexaniki izdən və yoxlama üçün imzadan istifadə edirdi. Bu sistemə əsasən, müştəri öz kartını satış məntəqəsindəki məmura verir, o, kartı ya maqnit oxuyucu vasitəsilə "sildirir", ya da kartın qaldırılmış mətnindən iz qoyur. Əvvəlki halda hesab rekvizitləri yoxlanılır və müştərinin imzalaması üçün slip çap olunur. Mexanik çap halında, əməliyyatın təfərrüatları doldurulur və müştəri çap edilmiş slipi imzalayır. Hər iki halda, məmur əməliyyatı təsdiqləmək üçün imzanın kartın arxasındakı imzaya uyğun olduğunu yoxlayır. Bu sistem səmərəsiz olduğunu sübut etdi, çünki onun bir sıra təhlükəsizlik qüsurları var, o cümlədən postda kartı oğurlamaq və ya kartdakı imzanı saxtalaşdırmağı öyrənmək. Bu yaxınlarda qara bazarda maqnit zolaqlarını oxumaq və yazmaq üçün texnologiya əlçatan olub, kartları asanlıqla klonlaşdırmaq və sahibinin xəbəri olmadan istifadə etmək imkanı verir. Barmaq izləri fərdləri müəyyən etmək və onların kimliyini yoxlamaq üçün istifadə edilən bir çox üsullardan biridir. İdentifikasiya məqsədləri üçün əvvəllər saxlanılan barmaq izləri şablonlarını namizədin barmaq izləri ilə müqayisə etmək üçün istifadə edilən uyğunluq alqoritmləri. Nümunə əsaslanan alqoritmlər əvvəllər saxlanmış şablon və namizəd barmaq izi arasında əsas barmaq izi nümunələrini (arx, bütöv və döngə) müqayisə edir. Namizədin barmaq izi şəkli onların uyğunluq dərəcəsini müəyyən etmək üçün şablonla qrafik olaraq müqayisə edilir. Burada əsas çatışmazlıq odur ki, istifadəçinin barmağında

bant yardımı varsa, Barmaq izi identifikasiyası uğurlu ola bilməz. Başqa bir dezavantaj, insan huşsuz və ya ölü olsa belə, barmaq izinin eyni qalmasıdır. Bu, şəxsin razılığı olmadan barmaq izinin icazəsiz istifadəsinə gətirib çıxarır. Kredit kartlarından istifadənin mövcud autentifikasiya sistemlərinin məhdudiyyətlərini aradan qaldırmaq üçün autentifikasiyanın iki mərhələdə həyata keçirildiyi yeni autentifikasiya sistemi təklif edilmişdir. Birinci mərhələ irisin tanınmasından istifadə edərək istifadəçinin şəxsiyyətinin yoxlanması, ikinci mərhələ isə palma damarı texnologiyasından istifadə edərək autentifikasiyadır.

Əvvəlcə istifadəçidən kartını daxil etməsi tələb olunacaq. Belə bir hesabın olub-olmadığını yoxlamaq üçün verilənlər bazası yoxlanılır. Əgər varsa, istifadəçi irisin tanınması ilə autentifikasiya ediləcək. Əgər istifadəçi bu mərhələdə autentifikasiya olunubsa, ondan damar nümunəsinin autentifikasiyası üçün ovucunu uzatması tələb olunacaq. Bu, saxlanılan nümunə ilə müqayisə edilir və əgər istifadəçiyə uyğun gəlirsə, təsdiqlənir.

Bu gün istifadəçilər əsasən şifrələmə alqoritmini izləyən mətn parollarından istifadə edirlər. Əsasən mətn parolları, bu gün çox sadə saxlanılır, lüğətdən bir söz demək və ya onların ev heyvanlarının adları, qız yoldaşları və s. Tipik irisin tanınması sistemi üç əsas moduldan ibarətdir:

-Şəklin əldə edilməsi xüsusi hazırlanmış sensordan istifadə edərək obyektdən iris şəkillərinin ardıcıllığını çəkməkdir.

-Əvvəlcədən İşləmə Mərhələsi göz təsviri daxilində irisin sərhədinin müəyyən edilməsini əhatə edir və onun işlənməsini asanlaşdırmaq üçün şəkildən iris hissəsini çıxarır. Buraya müxtəlif mərhələlər daxildir: irisin seqmentasiyası, irisin normallaşdırılması, təsvirin gücləndirilməsi.

-Xüsusiyyətlərin çıxarılması və kodlaşdırılması irisin tanınması sisteminin ən əsas komponentidir və sistemin işini böyük ölçüdə müəyyən edir. Süsən tanınması istehsal edirdaxil edilmiş şəkillərin xüsusiyyətlərini çıxarmaqla və

bu xüsusiyyətləri xüsusiyyətlər bazasında məlum nümunələrlə uyğunlaşdırmaqla düzgün nəticə əldə etmək.

Bu gün istifadəçilər əsasən şifrələmə alqoritmini izləyən mətn parollarından istifadə edirlər. İndiki vaxtda əsasən mətn parolları çox sadə saxlanılır. İndi texnologiya dəyişikliyi, sürətli prosessorlar və İnternetdəki bir çox alətlə bu, daha sadə oldu. Buna görə də, biz autentifikasiyamızda daha çox fərdiləşdirilə bilən və çox maraqlı autentifikasiya üsulu olan Biometrikdan istifadə edirik. Damar uyğunluğu, həmçinin damar texnologiyası adlanır, dərinin səthindən görünən qan damarlarının nümunələrinin təhlili vasitəsilə biometrik identifikasiya üsuludur. Bir şəxs əvvəlcə biləyini bəzi cihazlara dayadır ki, xurma cihazın skanerindən santimetr yuxarıda tutulur, bu da xurma üzərində yaxın infraqırmızı şüalar saçır.

Yaxın infraqırmızı işığın keçdiyi dəridən fərqli olaraq, damarlardan axan qanda oksigensizləşdirilmiş hemoglobin yaxın infraqırmızı şüaları udur, hemoglobini işıqlandırır və onun skanerə görünməsinə səbəb olur. Qanında yaxın infraqırmızı işığı udmayan oksigenli hemoglobin olan arteriyalar və kapilyarlar sensora görünməzdir. Yaxın infraqırmızı diapazonda fotoşəkil çəkən kamera tərəfindən çəkilmiş hərəkətsiz görüntü xurmanın daha açıq fonunda xurma damarlarının naxışını əks etdirən qara şəbəkə kimi görünür.

1.5. Onlayn bankçılıq sistemindən istifadənin obyektyönümlü tədqiqi

Şri Lankada bank sənayesi maliyyə aktivlərinin idarə olunmasında mühüm rol oynayır. O, maliyyə vasitəçiliyi rolunu yerinə yetirməkdə davam etdi, lakin ona təklif olunan məhsul və xidmətlərin çeşidi daha da genişləndi. Adi bank fəaliyyəti həm müştəri, həm də bank üçün çox vaxt və xərc tələb edir. İnternet bankçılıq indi Şri-Lankada bank sənayesini əhatə edir və ənənəvi bank fəaliyyətini internet əsaslı onlayn sistemə çevirir. 1988-ci ildə Sampath bankından bildirilən internet bankçılığının tətbiqi. Şri-Lankada əldə edilən son tapıntı göstərir ki, müştərilər bu texnologiyanın daha kifayət qədər nisbi

üstünlüklərə malik olmasına baxmayaraq daha çox müqavimət göstərirlər. Müəyyən edilmişdir ki, bank müştərilərinin yalnız 1%-dən az hissəsi, ümumiyyətlə, onlayn bankçılıq, mobil bankçılıq, telefon bankçılığı və internet ödəniş qapısından istifadə edir.

Tədqiqat məlumatları strukturlaşdırılmış sorğu və müsahibə yolu ilə toplanmışdır. Sorğu Şri-Lankanın Kelaniya Universitetində dörd fakültədən təsadüfi seçilmiş 100 nümunəyə aparılıb. Hazırkı məqalədə sorğu məlumatlarının yalnız seçilmiş hissələrinə istinad ediləcək. Kəmiyyət məlumatları təsviri tədqiqat metodundan istifadə etməklə təhlil edilmişdir.

Cədvəl 1.5.1 və 1.5.2-də göstərildiyi kimi, akademik üzvlərin 48 faizi dörd fakültədə bank əməliyyatlarının aparılması üçün onlayn bankçılıq imkanlarından istifadə edir. 52 faiz isə bankçılıqla bağlı xidmətlər üçün onlayn bankçılıqdan istifadə etmir.

Cədvəl 1.5.1

İstifadəçilər	Faiz%	İstifadəçi olmayanlar	Faiz%
96	48	104	52

Cədvəl 1.5.2

Fakultə	İstifadəçilərin sayı	%	İstifadəçi olmayanların sayı	%
Sosial Elmlər	18	18.75	32	30.77
Humanitar Elmlər	12	12.5	38	36.53
Ticarət və idarəetmə	36	37.5	14	13.47
Digər Elmlər	30	31.25	20	19.23
Cəm	96	100	4	100

Yuxarıdakı cədvələ əsasən, Ticarət və İdarəetmə və Digər Elmlər fakültələrindəki akademik üzvlərin demək olar ki, çoxu onlayn bankçılıq imkanlarından istifadə edir, onlayn bankçılıq istifadəçilərinin 68-dən çoxu hər iki

fakültəyə qoşulub. Bununla belə, Sosial Elmlər üzrə akademiklərin yüzdə 18-dən çoxu və Humanitar Elmlər üzrə akademiklərin yüzdə 12,5-i bank fəaliyyətləri üçün bu imkandan istifadə edir. Tədqiqat fakültənin akademik üzvlər arasında onlayn bankçılıqdan istifadəsinə təsir edən mühüm amilin olduğunu müəyyən etmişdir. Buna görə də fakültə onlayn bankçılıqdan istifadə sürətinə birbaşa təsir göstərir. Ticarət və İdarəetmə və Elm üzvləri onlayn əsaslı akademik tədris metodları ilə daha çox tanış olduqları üçün maliyyə institutları və onların imkanları haqqında kifayət qədər məlumatlı olduqları üçün. Beləliklə, onlar digər iki fakültədən daha çox elektron bankçılıqdan istifadə edirlər.

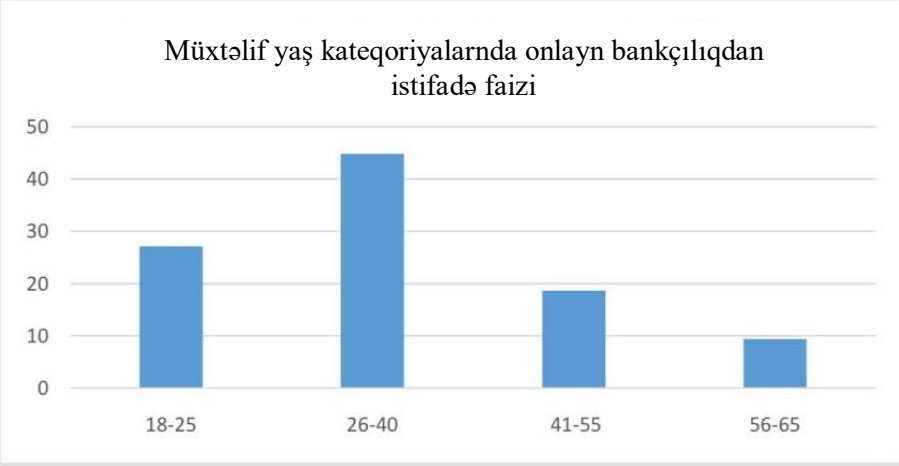
Cədvəl 1.5.3

Bankın adı	Hesabların sayı	Onlayn Bankçılıqdan istifdə üçün hesab nömrəsi	%
Dövlət bankları			
Peoples' Bank	182	28	15.4
NSB	71	20	28.2
Bank of Ceylon	63	16	25.4
Cəm	316	64	20.2
Özəl banklar			
Kommersiya Bankı	127	41	32.3
Sampath Bank	174	43	24.7
Seylan Bank	46	15	32.6
HNB	38	8	21
NDB	32	5	15.6
Başqa banklar	17	2	11.7
Cəm	434	114	26.2

Cədvəl 1.5.3-də göstərilir ki, universitet alimlərinin elektron bankçılıqdan istifadəsi əsasən həmin bankların dövlət və ya özəl mülkiyyətdə olmasından asılıdır. Yuxarıdakı cədvələ əsasən, özəl banklarda 200 akademik üzv tərəfindən 316 hesab, dövlət banklarında isə 434 hesab saxlanılmışdır. İki özəl bankın, Sampath və Kommersiya Bankının müştəriləri e-bankçılıq imkanlarından yüksək həzz alırlar və digər banklar onları izləyir. Sampath və Kommersiya banklarında onlayn bankçılıq üçün 57 faiz hesab istifadə edir. Sampath bank, Şri Lanka bank sektoruna onlayn bankçılığı təqdim edən ilk bankdır. Tədqiqatın nəticələrinə

görə, özəl banklar dövlət bankları ilə müqayisədə geniş çeşiddə elektron bankçılıq imkanları təqdim edir. Həm Sampath, həm də Kommersiya bankı rəqabət qabiliyyətli onlayn bankçılıq imkanları və müştərilərini cəlb etmək üçün motivasiya təklif edir, digər dövlət kommersiya bankları isə elektron bankçılığa daha az diqqət yetirirlər.

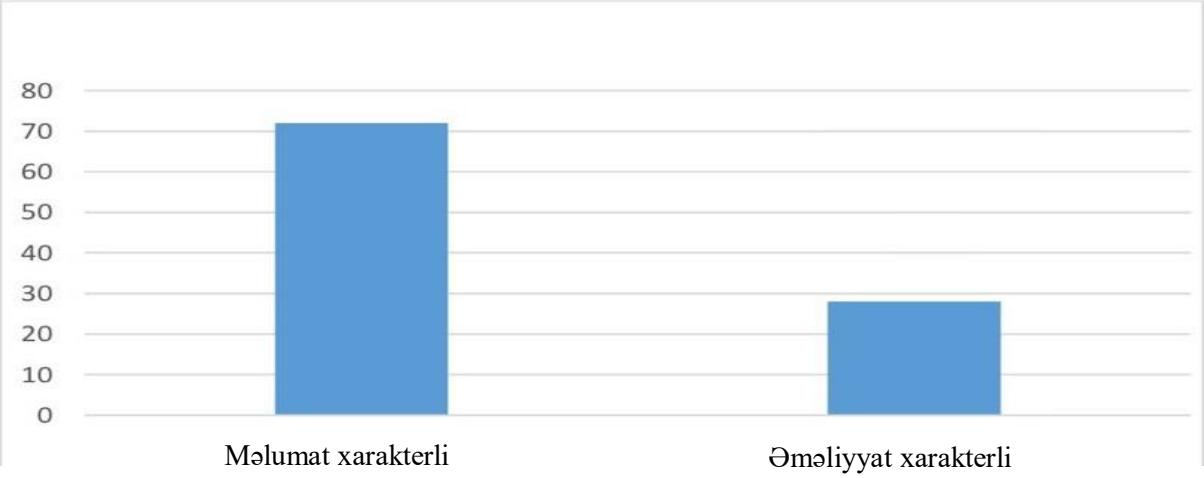
Aşağıdakı diaqrama əsasən, 200 akademik istifadəçidən ibarət 69 gənc və orta yaşlı akademik öz bank fəaliyyətləri üçün onlayn bankçılıq imkanlarından istifadə edirdi. Akademiklərin yüzdə 44-dən çoxu 26-40 yaş kateqoriyasında e-bankçılıqdan istifadə edirdi. Bundan əlavə, 56-65 yaş qruplarında akademik üzvlər nəzərə alındıqda müxtəlif yaş qrupları arasında ən az istifadə edən yaş qrupunu təmsil edir. Tədqiqat kompüter savadlılığını, texnoloji bacarıqları və elektron bankçılıq imkanları haqqında məlumatlılığı müəyyən etmişdir (şəkil 1.5.1).



Şəkil 1.5.1. Müxtəlif yaş qruplarında onlayn bankçılıqdan istifadə

Tədqiqatın nəticələri göstərir ki, alimlər yalnız məlumat və əməliyyat mərhələsində onlayn bankçılıq imkanlarından istifadə ediblər. Müəyyən edilmişdir ki, akademiklər İnteraktiv mərhələdə onlayn bankçılıq imkanlarını cəlb etmirlər. Alimlərin 72 faizi çek hesabının qalıqları, hesab tarixçəsi haqqında məlumat, ATM və filialların yerləşdirilməsi haqqında məlumat, Çek kitabçası sorğusu, PIN/şifrəni dəyişdirmək, Yoxlama statusu sorğusu və s. kimi məlumat

səviyyəli onlayn bankçılıq imkanlarından istifadə edib. 28 indiki akademik əməliyyat fəaliyyəti üçün onlayn bankçılıq imkanlarından istifadə etmişdir, məsələn, kredit kartı və kommunal ödənişlər, öz və üçüncü tərəf hesabları arasında vəsait köçürmələri, səhm ödənişləri və s (şəkil 1.5.2).



Şəkil 1.5.2.Müxtəlif xidmətlərdə onlayn bankçılıq imkanlarından istifadə

Müştərilərin onlayn bankçılıq imkanlarından məmnunluq səviyyəsi cədvəl 1.5.4-də göstərilmişdir. cədvəl 1.5.4

Fakültə	Onlayn bankılıq imkanlarından istifadədən məmnunluq				Cəm
	Çox yaxşı	Yaxşı	Orta	Zəif	
Sosial Elmlər	3	8	6	1	18
Humanitar Elmlər	2	4	6	0	12
Ticarət və idarəetmə	5	14	15	2	36
Digər Elmlər	2	12	30	1	30
Cəm	14	38	40	4	96

Bu araşdırma göstərdi ki, dörd fakültənin 14 akademik üzvü istifadə etdikləri onlayn bankçılıq imkanlarından "Çox yaxşı" razıdır. Bütün fakültələrdə akademik üzvlərin əksəriyyəti "yaxşı" və normal məmnuniyyətə üstünlük verdilər, ondan sonra ümumi istifadəçilərdən 38 və 40-ı gəlir. Alimlərdən bir neçəsi 4 nəfərdən ibarət "çox zəif" məmnunluq nümayiş etdirdi.

Bu araşdırma, dörd fakültədəki 52 akademik üzvünün hələ də bank fəaliyyətləri üçün onlayn bankçılıq imkanlarından istifadə etmədiyini müəyyən

etdi. Onlayn bankçılıqdan daha az istifadə etməyin əsas beş səbəbi müəyyən edilmişdir. Mürəkkəblik və nasazlıq, risk, təhlükəsizlik, daha az məlumatlılıq və təlimatlar. Təhlükəsizlik və risk məsələsi tapıldı.

90 faizdən çox akademik risk və təhlükəsizlik səbəbindən onlayn bankçılıqdan istifadə etmir. Mürəkkəblik və nasazlıq onlayn bankçılıqdan istifadə edilməməsinin üçüncü əsas səbəbi olub.

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Ağayev Hüseynbala Şöhrət oğlu

İnternet bankçılıq sistemində istifadəçi məxfiliyinin çoxsəviyyəli autentifikasiya tətbiqli model və alqoritminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter texnikasının lahiyələndirilməsi və konstruksiya edilməsi"

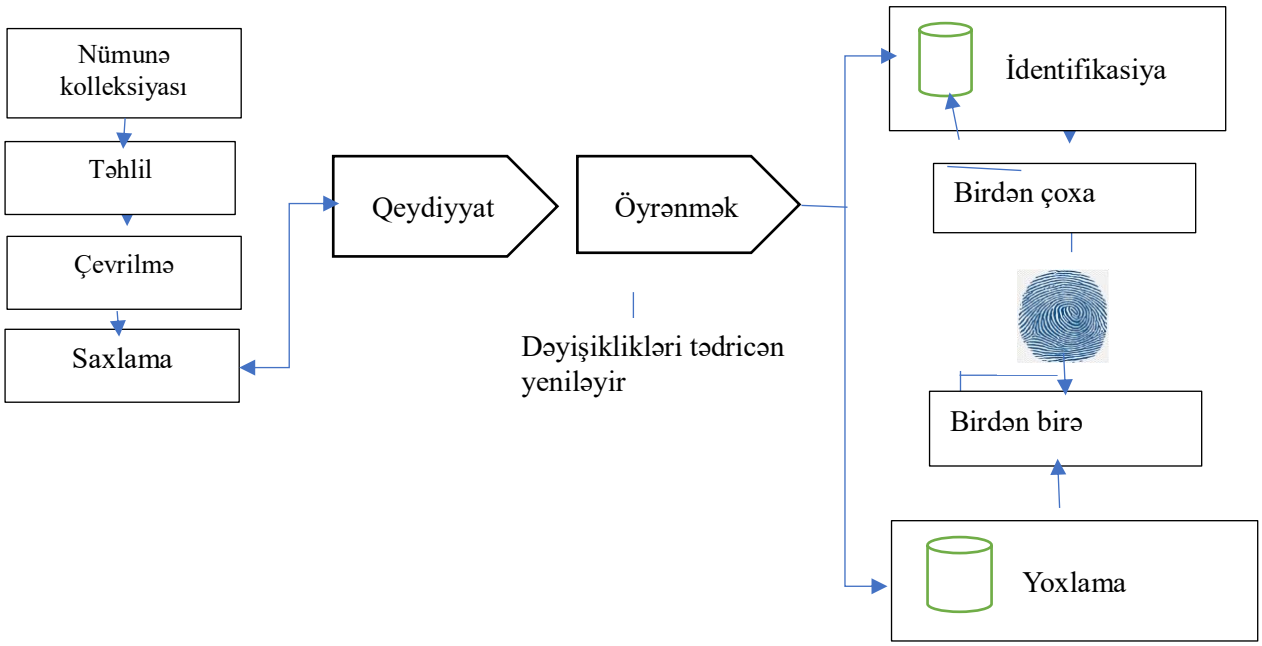
Elmi rəhbər: t.e.n, dosent İsgəndərzadə Hüseyn Qasım oğlu

BAKI – 2023

II FƏSİL. BİOMETRİK DOĞRULAMA VƏ MULTİ HESABLI ATM KARTI İLƏ TƏKMİLLƏŞDİRİLMİŞ BANKÇILIQ SİSTEMİ

2.1.Biometrik (barmaq izi) çoxsəviyyəli autentifikasiya

Biometrik avadanlıq ölçmə, kodlaşdırma qabiliyyətinə malikdir, müqayisə etmək, saxlamaq, ötürmək və/və ya tanımaq a yüksək səviyyəli bir insanın spesifik xüsusiyyəti dəqiqlik və etibarlılıq. Biometrik texnologiyanın orada olması elmi həqiqətə əsaslanır olan canlı formalarının müəyyən xüsusiyyətləridir unikal və hər bir fərd üçün təkrarlanmayan; bunlar xüsusiyyətlər texniki cəhətdən mümkün olan yeganə xüsusiyyətdir olmayan bir insanı müsbət müəyyən etmək üçün alternativ identifikasiyanın digər formalarından daha çox istifadə fırıldaqçı davranışlara həssasdır. Biometrik texnikanın iki var kateqoriyası əsas: fizioloji (barmaq izi yoxlanışı, iris analiz, əl həndəsə-damar naxışları, qulaq tanınması, qoxunun aşkarlanması, DNT nümunəsinin analizi və tər məsamələrinin təhlili) və davranış (əl yazısı ilə imzanın yoxlanılması, düymələrin basılması təhlil və nitq təhlili)(şəkil 2.1.1).



Şəkil 2.1.1. Biometrik metodologiyanın prosesləri

Tranzaksiya identifikasiyası əməliyyatları ehtiva etdiyi üçün böyük bir bazarı təmsil edir avtomat kassada (ATM), electron fond köçürmələri, kredit kartı və smart kart əməliyyatlar, əməliyyatlar telefonda və ya İnternet və s. MasterCard ağıllı olduğunu təxmin edir. Barmaq izi yoxlanışını özündə birləşdirən kredit kartı saxta ittihamların 80%-ni aradan qaldıra bilər. Barmaq izi həlləri autentifikasiyanın insan faktorlarına müraciət edən bir çox üstünlüklər təklif edir və o, aşağıdakı fərqli xüsusiyyətlərə malikdir:

Bir növ identifikator- On barmağımızın hər birinin barmaq izləribir-birindən və digər şəxslərin barmaq izlərindən fərqlidir.

Daha çox rahatlıq- İstifadəçilər artıq mürəkkəb və uzun, tez-tez dəyişən parolları yadda saxlamalı vədaşımalı deyillər.

Sistemdəki bütün istifadəçilər üçün nisbi bərabər təhlükəsizlik səviyyəsi – Hər hansı digər hesabdan (məsələn, asanlıqla təxmin edilən parol və ya social şəbəkə vasitəsilə) bir hesaba daxil olmaz asan deyil.

Parollar, PİN kodlar və smart kartlardan fərqli olaraq paylaşıla, itirilə, oğurlana, kopyalana, paylana və unudula bilməz. Barmaq izləri şəxsiyyəti fiziki insana güclü şəkildə bağlayır və bunu çətinləşdirir.

Identifikasiya tapşırıqlarında uğurlu istifadənin uzun tarixi- Barmaq izləri bir əsrdən çoxdur ki, məhkəmədə, tibbdə istifadə olunur və barmaq izlərinin fərqliliyini və qalıcılığını dəstəkləyən çoxlu elmi araşdırmalar mövcuddur.

2.2. Maliyyə təşkilatlarında biometrik doğrulama

Sistemin autentifikasiyası subyektin elektron vasitələrdən istifadə etməklə şəxsən müəyyən edilə bildiyi prosesə aiddir. Bu autentifikasiya müxtəlif üsullardan istifadə etməklə həyata keçirilə bilər: (1) sahib olduğunuz bir şey

(Token, şəxsiyyət vəsiqəsi/çarpma kartları), (2) bildiyiniz bir şey (parol, PIN) və (3) olduğunuz bir şey (biometrik). Bu üsullar arasında biometrik autentifikasiyadan istifadə ən yaxşı üsul hesab olunur, çünki o, insanın itirilməsi, unudulması və oğurlanması mümkün olmayan fiziologiya və davranışlarından istifadə edir. Əksinə, sahib olduğunuz bir şey oğurlana bilər və bildiyiniz bir şey unudula bilər.

Biometrik sistem, bir şəxsdən toplanan məlumatların tələb olunan xüsusiyyət məlumatını çıxarmaq üçün istifadə edildiyi bir nümunə tanıma sistemindən istifadə edir, daha sonra verilənlər bazasında saxlanılan şablon ilə müqayisə edilir və bu uyğunluq sistemi vasitəsilə həqiqət müəyyən edilir. Biometrik sistem iki rejimdə işləyə bilər: yoxlama rejimi və ya identifikasiya rejimi. Doğrulama rejimində şəxsiyyətini müəyyənləşdirmək istəyən şəxs saxlanılan biometrik şablonu əldə etmək üçün öz şəxsi xüsusiyyətlərindən istifadə edir, sonra isə ələ keçirilən biometrik məlumatla müqayisə edilir. Bu rejimdə məlumatların müqayisəsi iddianın doğru olub-olmadığını müəyyən etmək üçün bir-bir müqayisə kimi aparılır. Doğrulama rejiminin məqsədi birdən çox istifadəçinin eyni şəxsiyyətdən istifadə etməsinin qarşısını almaqdır. İdentifikasiya rejimində alınan biometrik məlumatlar uyğunluq üçün verilənlər bazasında tapılan bütün biometrik məlumatlarla müqayisə edilir. Bu sonrakı rejimdə fərdi şəxsiyyəti müəyyən etmək üçün müqayisə birdən çoxa hesab olunur. İdentifikasiya rejiminin məqsədi tək istifadəçinin çoxsaylı identifikasiyalardan istifadə etməsinin qarşısını almaqdır.

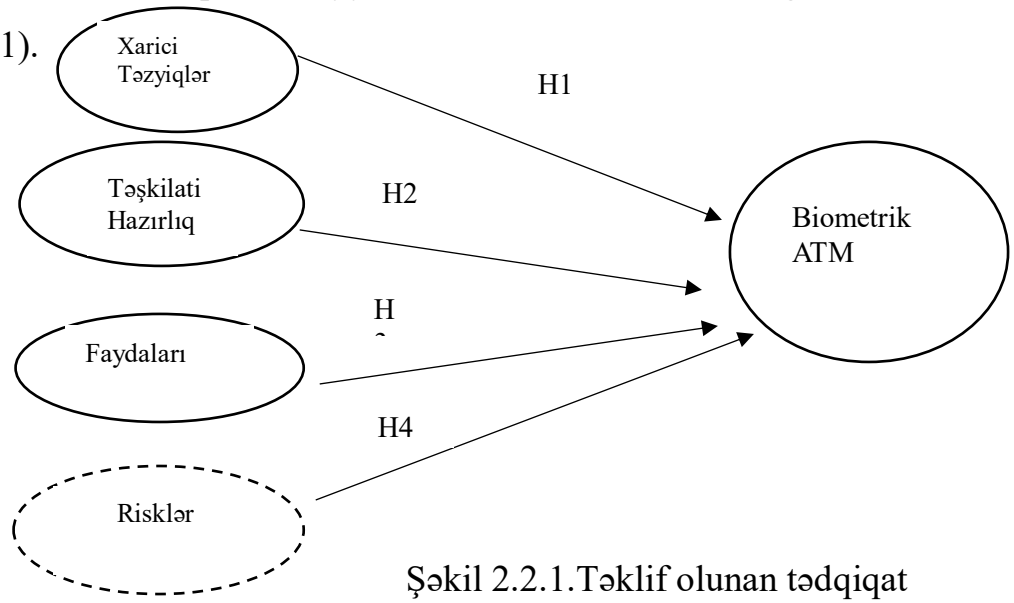
Banklar, səhiyyə və dövlət qurumlarında müxtəlif sistemlər öz müştərilərinə autentifikasiya təmin etmək üçün barmaq izləri və ya səsin tanınması kimi biometrik sistemdən istifadə edir. Aparılan araşdırma göstərir ki, dünya üzrə xidmət istehlakçılarının 66%-i müxtəlif sistemlərə qiymətli kağızların verilməsində biometrik sistemlərdən istifadəyə üstünlük verir. Xüsusilə bankomatlarda onlayn fırıldaqçılığın artması səbəbindən təhlükəsizliyin

gücləndirilməsində biometrik texnologiyanın tətbiqi maliyyə institutlarında mühüm tədqiqat sahəsinə çevrilmişdir. [2]Hər hansı bir təşkilatda təhlükəsizliyin təmin edilməsində biometrik texnologiyanın tətbiqinə dair qərar bir sıra amilləri əhatə edə bilər. Bu amillər Texnologiya Qəbul Modeli (TAM) , Planlaşdırılmış Davranış Nəzəriyyəsi (TPB) , Əsaslandırılmış Fəaliyyət Nəzəriyyəsi (TRA) , İnnovasiyaların Yayılması (DOI) kimi müxtəlif qəbuletmə nəzəriyyələrində müəyyən edilmişdir. Texnologiyanın Qəbul və İstifadəsinin Vahid Nəzəriyyəsi (UTAUT) və Elektron Məlumat Mübadiləsi (EDI) qəbulu Modeli. Tanzaniya maliyyə institutlarında biometrik texnologiyanın qəbulu davranışını anlamaq üçün hazırkı tədqiqat konseptual çərçivəni inkişaf etdirmək üçün EDI modelini qəbul edir. EDI modeli ona görə qəbul edilmişdir ki, o, təsərrüfat subyektləri arasında məlumat mübadiləsində təşkilatlararası əlaqəyə imkan verən modellərdən biridir. Buna görə də, o, ayrı-ayrı banka və ya əməkdaşlıq edən banklara ATM-lərdən istifadə zamanı təhlükəsizliyi gücləndirmək üçün biometrik texnologiya tətbiq etməyə imkan verə bilər.

Xarici təzyiqlər banklarda biometrik enerji ilə işləyən bankomatların qəbulu niyyətinə müsbət və birbaşa təsir göstərir. Mövcud kontekstdə təşkilati hazırlıq bir təşkilatın İT layihəsini həyata keçirmək qabiliyyətinə və qabiliyyətinə aiddir, o, İT-nin mükəmməlliyi, insan resursları və maliyyə resursları ilə ölçülür. İKT texnologiyasının mənimsənilməsinə digər amillərlə yanaşı, daha çox təşkilati hazırlıq təsir göstərir. İKT texnologiyasında təşkilati hazırlığın təsiri digər tədqiqatlarda da görünür. Biz həmçinin gözləyirik ki, əgər təşkilat infrastruktur, idarəetmə dəstəyi, insan resursları və maliyyə resursları baxımından hazırdırsa, biometrik enerji ilə işləyən bankomatı qəbul etmək üçün yaxşı vəziyyətdədir.

2. [2] J. Y. L. Thong and C. S. Yap, “Information technology adoption by small business: An empirical study,” in Diffusion and adoption of information technology, Springer, 1996, pp. 160–175.

Buna görə də fərz edirik ki: Təşkilati hazırlıq banklarda biometrik enerji ilə işləyən bankomatların tətbiqi niyyətinə müsbət və birbaşa təsir göstərir. Qəbul edilən faydalar təşkilatda texnologiyanın mənimsənilməsi nəticəsində əldə edilən üstünlüklərlə bağlı qavrayışlara aiddir. Bu araşdırmada, əvvəlki tədqiqatlara uyğun olaraq, biz gözləyirik ki, performansın artırılması, məxfiliyin artırılması və müştəri əməliyyatlarının təhlükəsizliyi baxımından biometrikanın qəbul edilən faydaları bankları biometrika ilə işləyən ATM-ləri qəbul etməyə sövq edəcək. Beləliklə, proqnozlaşdırırıq: Qəbul edilən faydalar banklarda biometrik enerji ilə işləyən ATM qəbul etmək niyyətinə müsbət və birbaşa təsir göstərir Qəbul edilən risk İKT layihəsinə, bu kontekstdə biometrik enerji ilə işləyən ATM-ə girişməyin gözlənilən mənfi nəticələrinə aiddir. Mənfi nəticələr, əgər İKT sistemi müştərinin məlumatını qoruya bilmirsə, müştəri etibarının itirilməsi, tətbiq edilən İKT sistemi təşkilata maliyyə faydalarını qaytara bilmədikdə təşkilatın maliyyə itkisi ola bilər. Təşkilatlarda İKT sistemlərinin tətbiqi ilə bağlı qərar həmişə bir əsasa əsaslanır. İKT sərmayəsi üzrə gözlənilən risklərin qiymətləndirilməsi. İT-nin qəbulu üzrə ədəbiyyat göstərir ki, qəbul edilən risklər təşkilatlarda İKT sisteminin mənimsənilməsinə birbaşa və mənfi təsir göstərir. Buna görə də, banklarda biometrik sistemli bankomatların qəbulu risklərin qəbuluna mənfi təsir göstərir. Beləliklə, biz fərz edirik ki, Qəbul edilən risklər banklarda biometrik enerji ilə işləyən bankomatların qəbulu niyyətinə mənfi və birbaşa təsir göstərir (şəkil 2.2.1).



Şəkil 2.2.1.Təklif olunan tədqiqat

Bu işdə əsasən kəmiyyət yanaşması ilə təsviri dizayn istifadə edilmişdir. İştirakçı təşkilatlar Tanzaniya Bankının (BOT) məlumat bazasından qeydiyyatdan keçmiş banklar siyahısından əldə edilmişdir. Məqsədli seçilmiş bankomatlardan istifadə edən 47 Bank və Maliyyə Qurumuna 141 sorğu anketi paylanmışdır. Tədqiqatda hər Bankdan üç respondent iştirak etmişdir. Respondentlər İKT departamentlərinin yüksək vəzifəli əməkdaşları idi. Respondentlərin bu kateqoriyası iki səbəbə görə seçilib: (1) biometrik texnologiya İKT texnologiyasının bir hissəsidir, beləliklə, İKT personalının bankdakı digər respondentlərlə müqayisədə texnologiya haqqında daha çox biliyi var; və (2) İKT departamenti xüsusilə İKT texnologiyasının əldə edilməsi, inkişafı və tətbiqi zamanı İKT ilə bağlı məsələlərdə rəhbərliyə məsləhət vermək üçün əsas rol oynayır. Tədqiqat təxminlərinin etibarlılığını zəiflədə bilən arzuolunan qərəzdən qaçmaq üçün çoxlu respondent yanaşmasından istifadə edilmişdir.

İştirakçı təşkilatlar arasında yüz on (110) sorğu vərəqi toplanmışdır ki, bu da 78% cavab nisbətini bildirir. Səkkiz (8) iş natamam və çatışmayan məlumatlar səbəbindən ləğv edildi, 102 iş tam və sonrakı təhlillər üçün etibarlı hesab edildi. Toplanmış məlumatların normal şəkildə paylandığını və buna görə də reqressiyanın aparılması üçün uyğun olub olmadığını müəyyən etmək üçün məlumatların normallığının qiymətləndirilməsini apardıq. Məlumatlar normal şəkildə paylanmırsa, tədqiqatın nəticələrini ümumiləşdirmək mümkün deyil. Məlumat elementlərinin normal paylandığını yoxlamaq üçün standart kənarlaşma, əyilmə və kurtoz hesablanmışdır. Nəticələr göstərir ki, əyrilik və kurtoz göstəricisi müvafiq olaraq -1 ilə +1 və -3 ilə +3 arasında məqbul diapazonda olduğu üçün məlumatlar normal şəkildə paylanır. Amil analizinin aparılması üçün məlumatların adekvatlığı və uyğunluğu Kaiser-Meyer-Olkin Ölçüsü (KMO) Nümunə Alma Adekvatlığı və Bartlett Sferiklik Testindən istifadə etməklə yoxlanılmışdır. Nəticələr göstərir ki, KMO 0,725-dir ki, bu da 0,6 həddən

yuxarıdır və Bartlett Testinin əhəmiyyətli olduğu aşkar edilmişdir (x2 = 1705 p <0,01). Bu o deməkdir ki, verilənlər faktor analizi üçün kifayət qədər yaxşı idi.

Ölçülməli olanın ölçülməsində sorğu vərəqələrinin uyğunluğunu qiymətləndirmək üçün etibarlılıq təhlili aparılmışdır. Kronbax alfasının geniş məqbul diapazonu 0,70-dir. Etibarlılıq təhlili nəticələri göstərir ki, bütün maddələr üçün ümumi Cronbach alpha (a) 0,840 olmuşdur ki, bu da məqbul səviyyədən xeyli yuxarıdır. Bu, sorğu vərəqələrinin kifayət qədər etibarlı olduğunu göstərir.

Faktor təhlili amil çıxarma üsulu kimi Əsas Komponent Analizi (PCA) vasitəsilə əldə edilmişdir. PCA sosial elmlərdə geniş istifadə olunan ümumi faktor çıxarma üsuludur. Faktorları seçmək üçün 1-dən böyük xüsusi qiymətlər və Kaiser Normalization ilə Varimax fırlanması istifadə edilmişdir. Faktor təhlilinin əsas məqsədi hər bir elementin konstruksiyasına düzgün yüklənməsini təmin etməkdir . Beş amil istehsal edilmiş və ümumi dispersiyanın 64,15%-ni təşkil etmişdir.

Bütün zəruri şərtlərin qənaətbəxş olduğundan əmin olduqdan sonra təklif olunan model fərziyyələri çoxlu reqressiya analizindən istifadə etməklə sınaqdan keçirilmişdir. Xarici Təzyiq (EXP), Təşkilati Hazırlıq (OR), Hiss olunan Fayda (PB) və Hiss olunan Risk (PR) olan model konstruksiyalar Davranış Niyyəti (BI) üzrə geri çəkilmişdir. Tədqiqatın nəticələri göstərir ki, EXP (t = 2.741, p < 0.01) və PB (t = 2.26 p < 0.05), PR (t = 2.13, p < 0.05) isə birbaşa və müsbət təsirə malikdir. banklarda biometrik enerji ilə işləyən bankomatın tətbiqi niyyətinə birbaşa və mənfi təsir göstərir. Lakin gözlədiyimizdən fərqli olaraq, banklarda biometrik enerji ilə işləyən bankomatların tətbiqi niyyəti ilə bağlı təşkilatın hazırlığı əhəmiyyətsiz olduğu müəyyən edilib. Bundan əlavə, tapıntılar ümumi modelin statistik əhəmiyyətli olduğunu göstərir (R2=0,23 p<0,01). Modelin qısa təsviri cədvəl 2.3.1-də göstərilmişdir.

Cədvəl 2.3.1

Model	R	R^2	Tənzimləndi R^2	STD. Səhv
	483[a]	0.233	0.2	0.874

Nəticələri isə cədvəl 2.3.2-də verimişdir.

Cədvəl 2.3.2

	Məbləğ Kvadratlar	df	Sahə	F	Sig.
Reqressiya	21.783	4	5.446	7.136	.000[b]
Qalıq	71.732	94	0.763		
Cəm	93.515	98			

Reqressiya əmsalı ilə nəticələri cədvəl 2.3.3-də qeyd olunmşdur.

Cədvəl 2.3.3

	UC		SC		
	B	S.E	Beta	t	Sig.
C	0.88	0.492		1.788	0.077
EP	0.271	0.099	0.265	2.741	0.007
OR	0.033	0.094	0.033	0.347	0.729
PB	0.229	0.101	0.224	2.264	0.026
PR	-0.182	0.086	-0.196	-2.128	0.036

Açar sözlər: C: daimi; ER: xarici təzyiq; və ya: təşkilati Hazırlıq; PB: təxmini fayda; PR: təxmini risk; UC:Standartlaşdırılmamış əmsal; SC: standartlaşdırılmış əmsal; S.E: standart səhv

Bu tədqiqatın əsas məqsədi bank sektorunda biometrik enerji ilə işləyən bankomatların qəbuluna təsir edən antesedentləri müəyyən etməklə bankların biometrik enerji ilə işləyən bankomatları qəbul etmək niyyətini qiymətləndirmək olmuşdur. Ədəbiyyat təhlili əsasında biz tədqiqat modeli və fərziyyələr

hazırlamışıq ki, burada xarici təzyiq, təşkilatın hazırlığı və qəbul edilən fayda birbaşa və müsbət təsir göstərir, qəbul edilən risk isə biometrik enerji ilə işləyən ATM-i qəbul etmək niyyətinə birbaşa və mənfi təsir göstərir. cmal ns var 5 idi model (EXP), t (PB) ovçu <P (t = d olmaq Nəticələr göstərdi ki, xarici təzyiq biometrik enerjili ATM-i qəbul etmək niyyətinə müsbət və birbaşa təsir göstərir. Xarici təzyiqin digər dəyişənlərlə müqayisədə güclü proqnozlaşdırıcı olduğu aşkar edilmişdir, bu o deməkdir ki, bankların əksəriyyəti bankomatların təhlükəsizliyini yaxşılaşdırmaq üçün biometrik enerji ilə işləyən bankomatın tətbiqini tələb edən müxtəlif maraqlı tərəflərin xarici təzyiqləri ilə daha çox maraqlanır. Bundan əlavə, daha etibarlı bankomat texnologiyasının tətbiqi ilə rəqiblərin təzyiqinin artması banklara təzyiqi artıra bilər. Bu o deməkdir ki, xarici təzyiq artdıqca bankın biometrik enerjili bankomatları qəbul etmə şansı yüksək olur. Bu tədqiqatda göstərildiyi kimi xarici təzyiqin əhəmiyyəti Thong & Yap (1996) və Websterin (1994) digər əvvəlki nəticələri ilə uyğundur. Bu tədqiqatlar müxtəlif ölkələrdə aparılsa da, müxtəlif texnologiyaların tətbiqində xarici təzyiqin mühüm amil olduğunu göstərir.

2.3.Təsvirin tanınması və istifadəçinin qurulan əlaqələri arasında çox faktorlu autentifikasiya alqoritmi

Təsvirin tanınması alqoritmləri, istifadəçinin unikal biometrik xüsusiyyətlərini analiz edir və onları məlumat bazası ilə müqayisə edir. Bu, istifadəçilərə daha güvənilir və çətinliklə qopyalanabilən bir autentifikasiya məkanizması təmin edir. Məsələn, barmaq izi skanı, istifadəçinin parmak izinin unikal xüsusiyyətlərini müəyyənləşdirir və onları məlumat bazası ilə müqayisə edir. Bu, istifadəçinin həqiqi olduğunu təsdiq edir və məlumatlara güvənilir girişini təmin edir.

Əlavə olaraq, istifadəçinin qurulan əlaqələri də çox faktorlu autentifikasiya alqoritmlərində istifadə edilən bir başqa faktordur. Bu, istifadəçinin əlavə

təhlükəsizlik mənbələrindən (məsələn, mobil telefon, e-poçt ünvanı) birini və ya daha çoxunu istifadə edir. İstifadəçi, autentifikasiya prosesində məlumatlara giriş edərkən, müvafiq qurulan əlaqəni təyin edən bir məlumatı daxil etməlidir. Bu, istifadəçinin məlumatlara girişinin təsdiq edilməsi üçün bir addımdır. Məsələn, sistem, istifadəçiyə mobil telefonuna göndərilən bir təsdiq kodu daxil etməsini tələb edə bilər. Bu, istifadəçinin kimlik təsdiqini tamamlamaq üçün ikinci bir faktor kimi funksiya edir.

Çox faktorlu autentifikasiya alqoritmləri, güclü bir təhlükəsizlik səviyyəsi təmin edir. Birdən çox faktorun istifadə edilməsi, bir mənbənin kompromet uğraması halında dəfələrlə təhlükənin azalmasını təmin edir. Həmçinin, biometrik məlumatların istifadəsi, şifrə və ya PIN kimi məlumatların unudulmasını, itirilməsini və ya başkaları tərəfindən öyrənilməsini aradan qaldırır.

Bu yeni çox faktorlu autentifikasiya alqoritmləri, bankçılıq, sağlamlıq, e-ticarət, sosial mediya və digər bir çox sahədə tətbiq edilir. İstifadəçilərə daha güvənli bir giriş təcrübəsi təqdim edir və məlumatların təhlükəsizliyini artırır.

Yeni çox faktorlu autentifikasiya alqoritmlərinin inkişafı, təsvirin tanınması və istifadəçinin qurulan əlaqələri ilə əlaqədardir. Bu alqoritmlər, müxtəlif faktorlardan istifadə edərək istifadəçilərin kimliklərinin daha güvənli bir şəkildə təsdiq edilməsinə imkan verir. Aşağıda, yeni çox faktorlu autentifikasiya alqoritminin qurulmasında əsas addımları təsvir edən bir nümunə verilmişdir:

1. Faktorların seçilməsi:

Alqoritm üçün istifadə ediləcək faktorlar seçilməlidir. Bu faktorlar şəxsi məlumatlar, barmaq izi, yüz tanıma, parol, SMS təsdiqi, biometrik məlumatlar və s. ola bilər.

Mümkün olan fərqli faktorların bir kombinasiyası, daha təhlükəsiz bir autentifikasiya təcrübəsi yaradır.

2. Verilənlərin toplanması və analizi:

Müştəri ilə əlaqəli olan fərqli verilər toplanır. Bu verilər müştəri hesab məlumatları, əməliyyat tarixi, istifadəçinin davranışı və digər məlumatları əhatə edə bilər.

Toplanan verilər alqoritmin analiz üçün istifadə ediləcək və müştərinin davranışının normal və anormal olduğunu müəyyənləşdirəcək.

3. Modelin təyin edilməsi:

Verilənlər əsasında, alqoritm modeli təyin edilir. Bu model, müştərinin təsvirini və davranışını anlamaq üçün statistik və maşın öyrənmə texnikalarından istifadə edir.

Təyin edilən model, fərqli faktorları dəyərləndirərək müştəri autentifikasiyasını təhlil edir və müştərinin kimliyinin təsdiq edilməsinə qərar verir.

4. Autentifikasiya təsdiq prosesi:

Müştəri autentifikasiya etmək üçün alqoritm dəyərləndirməni aparır.

Faktorların bir kombinasiyası, müştərinin identifikasiya olunmasına və təsdiqlənməsinə kömək edir.

Alqoritm müştəriyi autentifikasiya edərkən dəqiqlik və səmərəlilik təmin edir.

Təsvirin tanınması və istifadəçinin qurulan əlaqələri əsasında yeni çox faktorlu autentifikasiya alqoritmləri, məlumatların təhlükəsizliyini və gizliliyini təmin etmək üçün effektiv və inkişaf etmiş bir yoldur. Bu, istifadəçilərin güvənilir və təhlükəsiz girişini təmin edir və təhlükəsizlik tədbirləri ilə birgə çalışaraq məlumatların qorunmasına kömək edir. Bu alqoritmlər, digər autentifikasiya metodlarına nisbətən daha güclü bir təhlükəsizlik səviyyəsi təmin edir və günümüzün digər təhlükəsizlik tədbirləri ilə birlikdə istifadə edildikdə daha effektiv bir məlumat tələyinə çatışır. Bu sayədə istifadəçilər, məlumatlarına daha çox güvənə bilər və potensial təhlükələrdən daha çox qorunurlar.

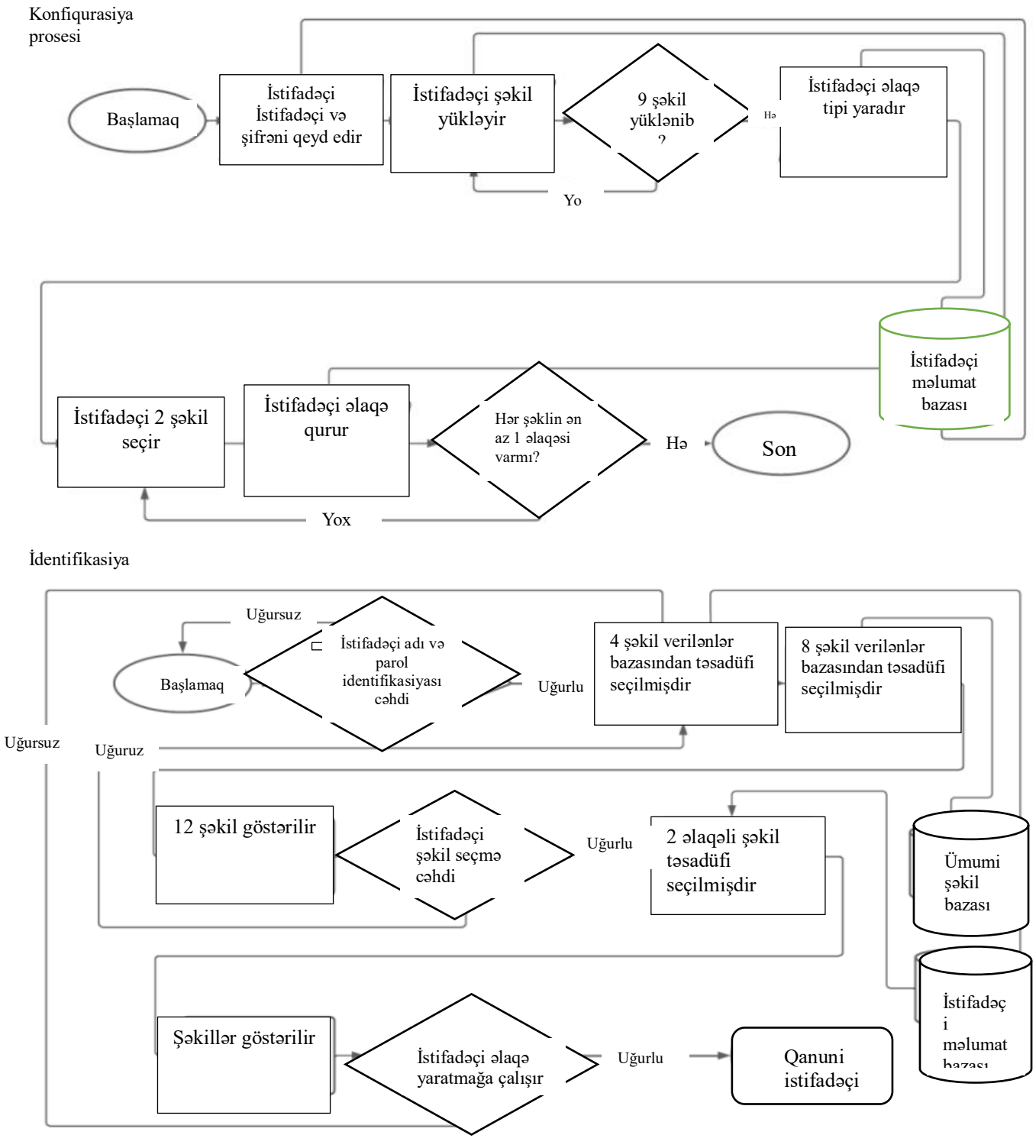
Yeni çox faktorlu autentifikasiya alqoritmləri təhlükəsizlik tədbirlərinin möhkəmlənməsinə kömək edir. Biometrik məlumatların istifadəsi, istifadəçilərin kimlik təsdiqini daha sürətli və daha asan bir şəkildə tamamlamasına imkan verir. Bu, işləri təkmilləşdirir və istifadəçilərin həyatını daha asanlaşdırır.

Həmçinin, bu alqoritmlər, istifadəçilərə uyğunluq və rahatlıq təmin edir. Biometrik məlumatların istifadəsi, şifrələr və PIN-lər kimi məlumatların yaddaşda saxlanması və yaddaşdan silinməsi məsələlərini aradan qaldırır. İstifadəçilər, yalnız biometrik məlumatlarını təmin etməklə autentifikasiya prosesini başa vuraraq məlumatlarına giriş edə bilərlər.

2.4. MFA tətbiqli alqoritm dizaynı

Mexanizmin funksional prototipi React Native-də hazırlanmış və tətbiq edilmişdir. Expo Go müştərisindən istifadə edərək həm Android, həm də İOS üçün mobil proqram kimi həm istifadəçilərin autentifikasiya məlumatlarını, həm də ümumi şəkilləri saxlamaq üçün Back4App-da yerləşdirilib. Ümumi şəkil bazası Google-dan 110 şəkildən ibarət idi. Bu görüntülər internet istifadəçilərinin mobil telefon qalereyasından yüklənib. Bu verilənlər bazası üçün şəkillərin seçilməsində mühüm amil idi, çünkü identifikasiya zamanıbu şəkillərin istifadəçinin şəkilləri ilə problemsiz qarışması nəzərdə tutulmuşdu.

Mexanizmin həm konfiqurasiya, həm də autentifikasiya prosesləri aşağıda ətraflı təsvir edilmişdir. Şəkil 2.4.1 mexanizmin axını prosesini təsvir edir.



Şəkil 2.4.1. Təklif olunan mexanizm üçün axın diaqramı

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Zeynalova Gülnar Vəli qızı

İnternet bankçılıq sistemində istifadəçi məxfiliyinin çoxsəviyyəli autentifikasiya tətbiqli model və alqoritminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter texnikasının lahiyələndirilməsi və konstruksiya edilməsi"

Elmi rəhbər: t.e.n, dosent İsgəndərzadə Hüseyn Qasım oğlu

BAKI – 2023

III FƏSİL. ELEKTRON PUL ƏMƏLİYYATLARININ TƏHLÜKƏSİZLİYİ ALQORİTM

3.1. Bankçılıq sistemində kripto əməliyyatların təhlükəsizlik səviyyələri

Banklarda təhlükəsizlik tədbirləri müştərilərə hücumların qarşısının alınmasında mühüm rol oynaya bilər. Mülki məhkəmə çəkişmələrində zəifliklər və səbəbiyyət əlaqəsi nəzərə alınarkən bu tədbirlər böyük əhəmiyyət kəsb edir və banklar müştəriləri üçün təhlükəsiz və təhlükəsiz bank mühitini təmin etmək üçün müəyyən standartlara cavab verməlidirlər.

Elektron pul köçürmə sistemi internet üzərindən əməliyyatları asanlaşdırır. Elektron Məlumat Mübadiləsi (EDI) nümunəsi kimi də tanınan e-ödəniş sistemləri internet əsaslı alış-veriş və bankçılığın geniş yayılması səbəbindən getdikcə populyarlaşır. Onlayn əməliyyatın əsas problemlərinin təhlükəsizlik olduğunu artıq təsvir etdik. Burada ənənəvi və qabaqcıl təhlükəsizliyi təmin edən texnologiyanın kombinasiyası ilə bir alqoritm hazırlanmışdır. Bu tərtib edilmiş alqoritm üç səviyyəli təhlükəsizlik sistemlərindən istifadə etməklə e-təhlükəsizliyi təmin edir (şəkil 3.1.1). [3]Bu üç təbəqə aşağıdakılardır:

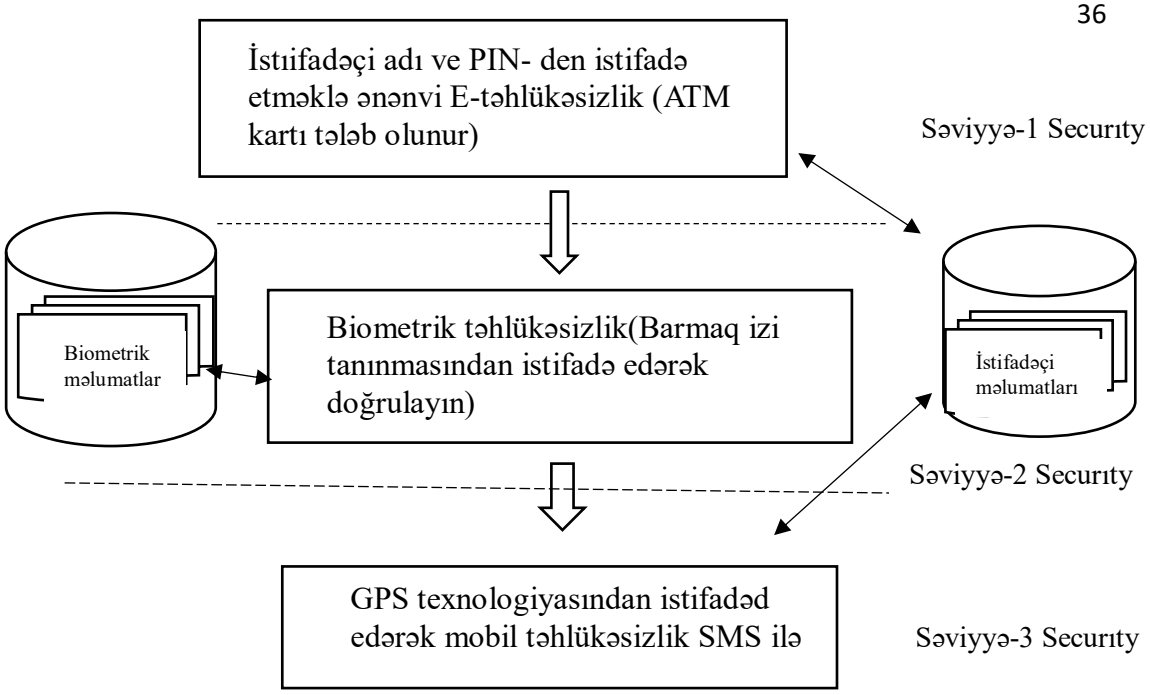
-Səviyyə -1: İstifadəçi adı və PİN nömrəsindən istifadə etməklə ənənəvi E-təhlükəsizlik.

-Səviyyə -2: Barmaq izi və ya irisin tanınmasından istifadə edərək biometrik təhlükəsizlik.

-Səviyyə-3: GPS və ya mobil SMS istifadə edərək mobil təhlükəsizlik.

---

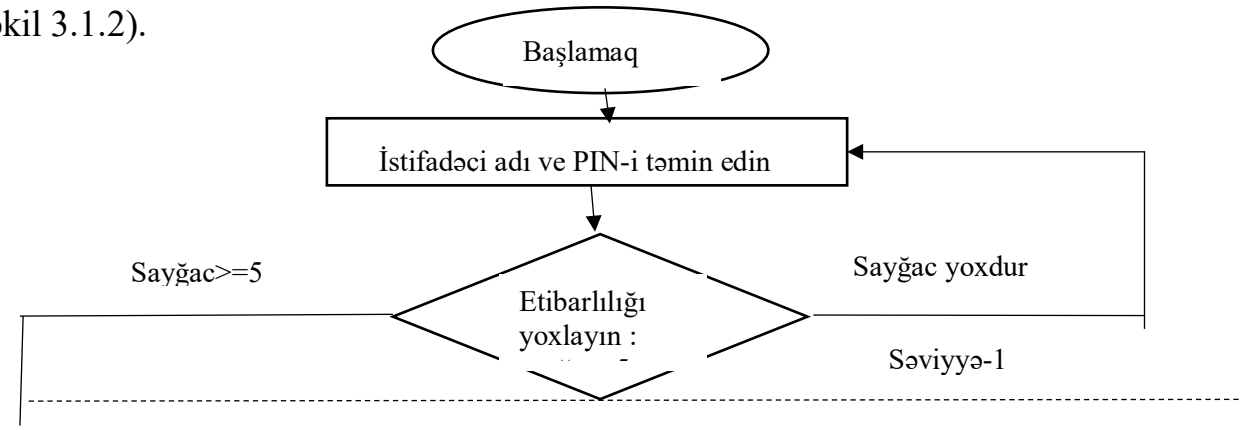
3. [3] Murdoch, S. J. “Reliability of chip & PIN evidence in banking disputes”. Digital Evidence and Electronic Signature Law Review, vol. 6, Pario Communications, pp. 98-115 [Nov, 2010].



Şəkil 3.1.1. Üç laylı təhlükəsizlik sistemi axını

Ənənvi E-təhlükəsizlik, onlayn istifadəçinin autentifikasiyası üçün ənənəvi sistemdir. Təkcə elektron əməliyyat sistemi deyil, sistemin əksəriyyəti istifadəçi adı və paroldan istifadə edərək istifadəçinin autentifikasiyasını həyata keçirir. Bu təklif olunan alqoritmdə əsas olaraq 1-ci addımlar müştəri ATM sistemindən istifadəçi adı və PİN kodu ilə istifadə edir. ATM kartı kimi hər hansı fiziki cihazın ötürülməsinə ehtiyac yoxdur. Təklif olunan sistemin adi ATM kartlarını aradan qaldırması bizim əsas çətinliklərimizdir. Müştəri istənilən bankda əməliyyat üçün hesab açdıqda istifadəçi adı və PİN kodu alır. PİN-in yaradılması texnologiyası sistemin PİN kodu yaratmaq və onu müvafiq müştəri mobil telefonuna göndərməkdir. Müştəri sistemə daxil olaraq PİN kodu dəyişə bilər. Müştəri ATM sistemində istifadəçi adı və PİN kodu təqdim etdikdə bank serverindən istifadəçi məlumat cədvəlindən istifadəçinin autentifikasiyasını həyata keçirir. Əgər autentifikasiya olunarsa, bu, müştəriyə 2-ci səviyyənin təhlükəsizliyini davam etdirməyə imkan verir, əks halda istifadəçi adı və PİN kodunu 5 dəfə təkrar təqdim edir. 4 dəfə cəhd etdikdən sonra əməliyyatı dayandırır və bu istifadəçi üçün 30 dəqiqə oflayn olur. Bu zaman müştəri heç bir bankomat sistemindən

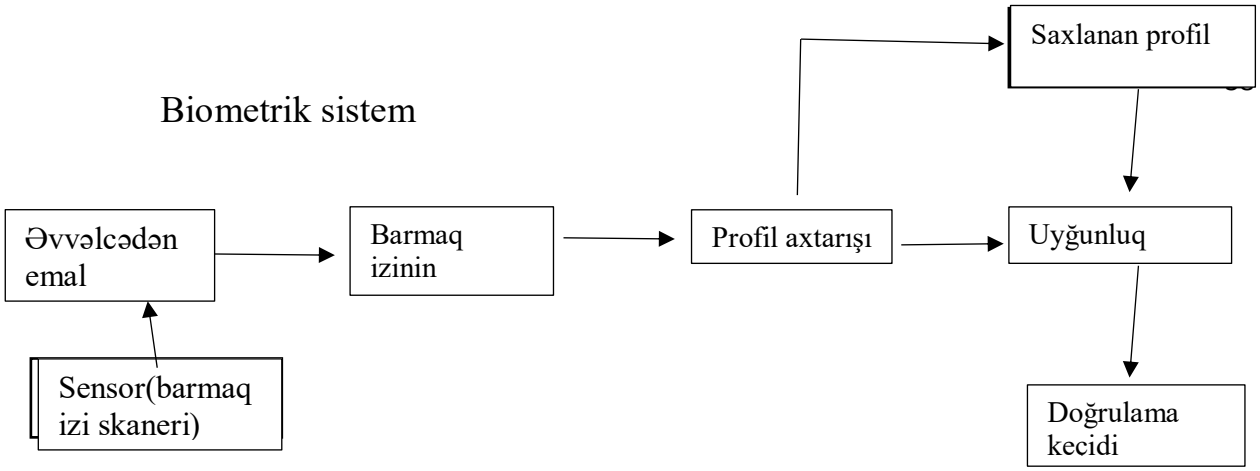
əməliyyat apara bilməz. Zəruri hallarda müştəri bankla fiziki əlaqə saxlamalıdır (şəkil 3.1.2).



Şəkil 3.1.2. Səviyyə 1 təhlükəsizlik sistemi alqoritmi

1-ci səviyyəni keçdikdən sonra sistem istifadəçiyə 2-ci səviyyəli qiymətli kağızlara daxil olmaq imkanı verir. Bu biometrik təhlükəsizlik sistemidir. Müasir texnologiyada bir neçə biometrik təhlükəsizlik sistemi mövcuddur. Lakin ən çox yayılmış və etibarlı təhlükəsizlik sistemi Barmaq izi və İrisin tanınmasıdır. Bu təbəqə 2 həm satıcıya əsaslanan biometrik texnikaları qəbul edə bilər, həm də müştəri seçimi. Burada mən yalnız barmaq izini biometrik təhlükəsizliyi təmin edən texnika kimi təsvir etdim.

Bank sistemində Biometrika müxtəlif tətbiqlər üçün sürətli, istifadəsi asan, dəqiq, etibarlı və daha ucuz autentifikasiya vəd edir. Müştərilər əməliyyat zamanı barmaq izini yüksək ayırdetməli barmaq izi skanerinə yazır. Barmaq izi təsviri qorunan kanal vasitəsilə mərkəzi serverə ötürülür. Bank terminalında təqdim olunan barmaq izi şəklinin bank məlumat bazasında iddia edilən istifadəçiyə aid olduğunu yoxlamaq üçün detalların çıxarılması və uyğunlaşdırılması həyata keçirilir. Dəqiqliklərin uyğunluğu uğurlu olarsa, identifikasiya imzalanır. Təklif olunan sxem sürətli və daha təhlükəsizdir (şəkil 3.1.3).



Şəkil 3.1.3. Biometrik təhlükəsizlik

Əsas biometrik autentifikasiya sistemi altı əsas komponentdən ibarətdir. Bunlar: Barmaq izi skaneri, preprosessor, xüsusiyyət çıxaran, verilənlər bazası və uyğunlaşdırıcı və qərar modulu. Skanerin funksiyası müştərinin biometrik xüsusiyyətini skan etməkdir. Sonra ön prosessor biometrik məlumatları emal edir və funksiyaların çıxarılmasına hazırdır. Xüsusiyyətlərin çıxarılması modulunun funksiyası skan edilmiş biometrik məlumatlardan xüsusiyyətlər dəstini çıxarmaqdır. Bu xüsusiyyət dəsti daha sonra şablon verilənlər bazasında saxlanılır. Uyğunlaşdırıcı modullar iki giriş alır, yəni şablon verilənlər bazasından xüsusiyyətlər dəsti və onu autentifikasiya etmək istəyən istifadəçinin xüsusiyyətlər dəsti və iki dəst arasındakı oxşarlığı müqayisə edir. Sonuncu modul, yəni yoxlama modulu iki xüsusiyyət dəstinin uyğunluğu barədə qərar qəbul edir. Biometrika cinayətlərin müəyyən edilməsi və həbsxana təhlükəsizliyi kimi kriminalistikada geniş şəkildə istifadə edilən və geniş mülki tətbiq sahələrində istifadə olunma potensialına malik sürətlə inkişaf edən texnologiyadır. Biometrikadan bankomatlara, mobil telefonlara, smart kartlara, masaüstü kompüterlərə, iş stansiyalarına və kompüter şəbəkələrinə icazəsiz girişin qarşısını almaq üçün istifadə edilə bilər.

Sistemdə ilk 2 dəfə etibarlı müştərinin autentifikasiyası uğursuz olarsa, barmaq izini daxil etməyə 3 dəfə icazə vermişəm. Müştəri sınaq limitini qəbul edərsə, 30 dəqiqə ərzində 1-ci səviyyənin təhlükəsizliyi ilə eynidir. Əgər autentifikasiya keçərsə, o zaman 3-cü səviyyə təhlükəsizlik sisteminə keçir.

Bu təbəqə mobil istifadə edərək təhlükəsizliyi təmin edir. Müştəri seçiminə əsasən tamamilə isteğe bağlıdır. Müştərilər yüksək səviyyəli təhlükəsizliyi təmin etmək istəyirlərsə, o, mobil təhlükəsizliyə icazə verə bilər. 2-ci qatdan müvəffəqiyyətlə təsdiqləndikdən sonra 3-cü qatın aktiv olub olmadığını yoxlayın. Əks halda, o, birbaşa müştəri hesabına daxil olur. Əgər lay 3 aktivləşdirərsə, o zaman bu addımda autentifikasiyanı gözləyin. Burada 2 növ mobil təhlükəsizliyi təqdim etdim.

-GPS əsaslı autentifikasiya.

-Mobil mesajlaşma vasitəsilə doğrulayın

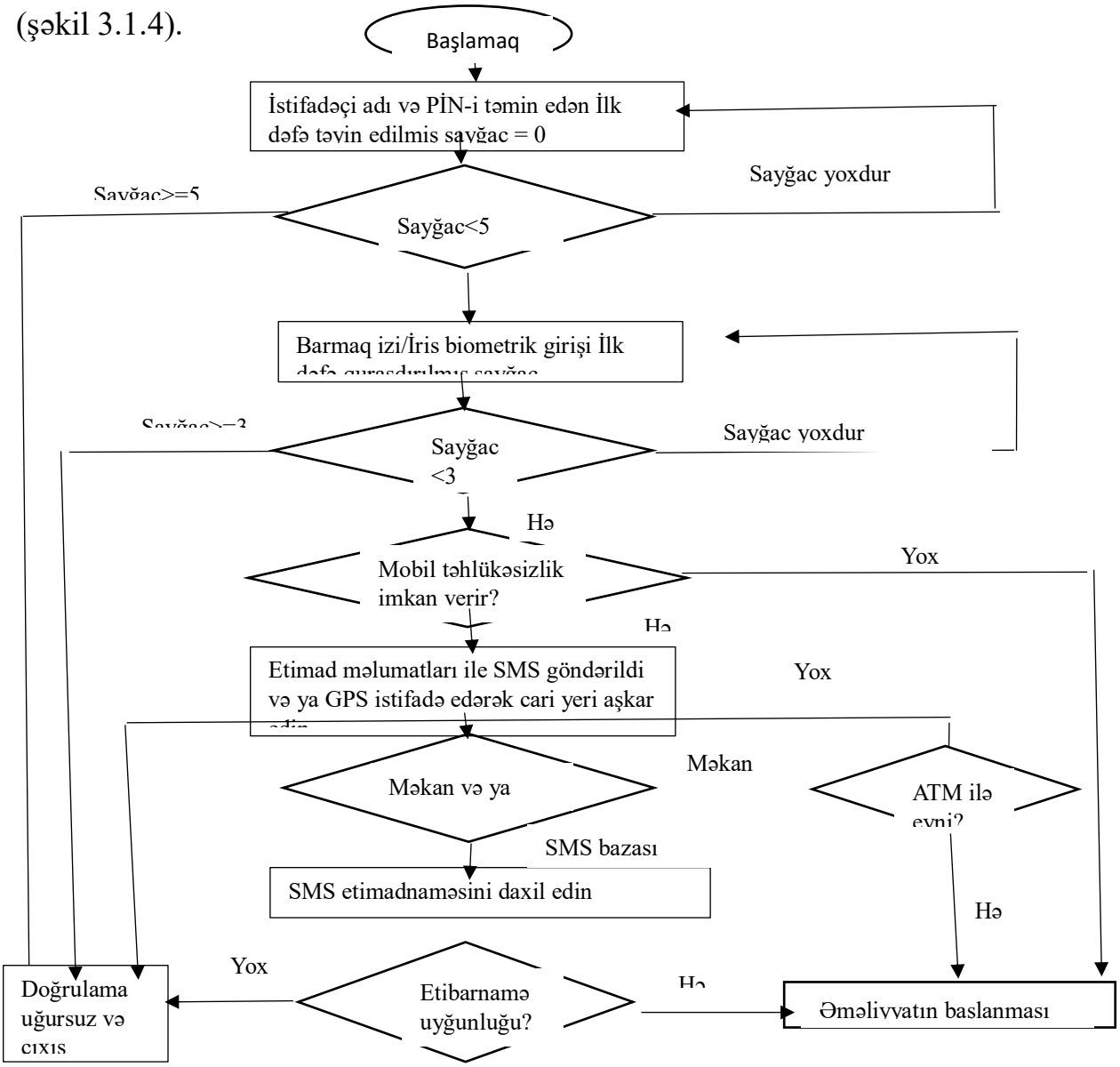
GPS əsaslı identifikasiya: Bu addım isteğe bağlıdır və istifadəçi seçiminə əsasən aktivləşdirilir. GPS əsaslı autentifikasiyada müştəri etibarlı mobil cihazı qeydiyyatdan keçirməlidir. sistemə. Və əməliyyat üçün gedərkən mobil telefon gətirmək məcburidir. ATM müştərinin mobil yeri əsasında etibarlı müştəri təmin edir. Müştərinin mobil yeri ATM yeri ilə eynidirsə, sistem bu müştərinin etibarlı olmasını təmin edir və müştəri hesabına daxil olmağa davam edir. Əks təqdirdə, əməliyyat prosesini rədd edir və oflayn rejimə keçir.

Mobil mesajlaşma vasitəsilə doğrulayın: Bu, həmçinin SMS vasitəsilə etimadnamə məlumatlarını göndərmək üçün etibarlı istifadəçinin autentifikasiyası üçün ümumi bir texnikadır. Onlayn identifikasiya sisteminin əksəriyyətində SMS əsaslı autentifikasiya istifadə olunur. Müasir sistemdə istifadəçi istənilən sistemə daxil olduqdan sonra autentifikasiya üçün SMS alır. SMS-də təhlükəsizliyi təmin etmək üçün təhlükəsizlik kodu var. İstifadəçi mobil telefonda mesaj aldıqdan sonra etimadnaməsini təmin edir. Əgər istifadəçi daxiletmə düzgündürsə, sistem bu istifadəçini etibarlı istifadəçi hesab edir.

Bu halda, digər mövcud SMS əsaslı autentifikasiya texnikası kimi, 2-ci səviyyənin təhlükəsizliyini keçdikdən sonra o, etimadnamə məlumatları (4 rəqəmli kod) ilə müştəri mobil telefonuna mesaj göndərir. Müştəri mesajı

aldıqdan sonra onu giriş kimi sistemə təqdim edir. Mache etimadnaməsi məlumatları varsa, o, müştərinin hesaba və əməliyyat pullarına daxil olmaq üçün icazənin təsdiqlənməsini təmin edir. İstifadəçi səhv kod təqdim edərsə, təhlükəsizlik məlumatlarını yenidən daxil etmək üçün üç dəfə seçim təqdim edir. Üç dəfə cəhd etdikdən sonra sistem əməliyyat prosesini dayandırır.

Bütün təbəqənin identifikasiyası sistemi keçdikdən sonra bu istifadəçinin etibarlı olduğuna və müştəri hesabının fırıldaqçılığa girişinə zəmanət verdi. Hər hansı bir müştəri autentifikasiyadan keçərsə, o, orada pulu elektron şəkildə əməliyyat edə bilər. Müştəri orada pul yatıra, çıxara və ya ödəniş edə bilər (şəkil 3.1.4).

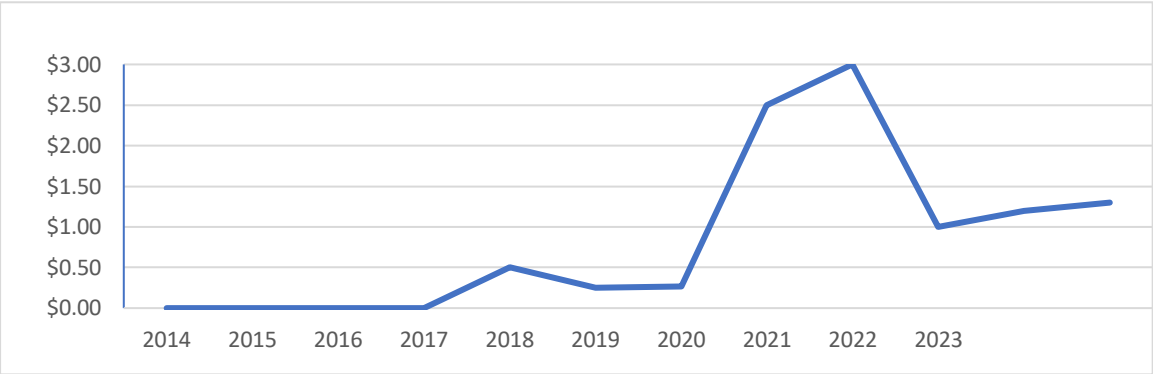


3.2. Kriptovalyutalar, rəqəmsal dollar

Bir neçə il ərzində kriptovalyutalar rəqəmsal yeniliklərdən qlobal maliyyə sistemini pozmaq potensialı olan trilyon dollarlıq texnologiyalara çevrildi. Bitcoin və yüzlərlə digər kriptovalyuta getdikcə daha çox investisiya kimi saxlanılır və proqram təminatı, rəqəmsal daşınmaz əmlak kimi bir çox mal və xidmətlərin alınması üçün valyuta kimi istifadə olunur.

Virtual sikkələrin zərb edilməsi üçün kriptoqrafiya prinsiplərindən istifadə etdikləri üçün kriptovalyutalar adətən virtual pul kisələri olan istifadəçilər arasında mərkəzləşdirilməmiş kompüter şəbəkələrində mübadilə edilir. Bu əməliyyatlar blokçeynlər kimi tanınan paylanmış, dəyişdirilməyə davamlı kitablarda açıq şəkildə qeyd olunur. Bu açıq mənbə çərçivə sikkələrin təkrarlanmasının qarşısını alır və əməliyyatları təsdiqləmək üçün bank kimi mərkəzi orqana ehtiyacı aradan qaldırır. 2009-cu ildə təxəllüslü proqram mühəndisi Satoshi Nakamoto tərəfindən yaradılan bitkoin indiyə qədər ən məşhur kriptovalyutadır və onun bazar kapitallaşması 1 trilyon dolları ötüb. İkinci ən populyar Ethereum da daxil olmaqla bir çox başqaları son illərdə çoxalıb. Kriptovalyuta istifadəçiləri rəqəmsal pul kisəsi ünvanları arasında vəsait göndərirlər. Bu əməliyyatlar daha sonra “blok” kimi tanınan nömrələr ardıcıllığına yazılır və şəbəkədə təsdiqlənir. Blokçeynlər real adları və ya fiziki ünvanları qeyd etmir, yalnız rəqəmsal pul kisələri arasında köçürmələri qeyd edir və beləliklə, istifadəçilərə müəyyən dərəcədə anonimlik verir. Monero kimi bəzi kriptovalyutalar əlavə məxfilik təmin etdiyini iddia edirlər. Lakin pul kisəsi

sahibinin kimliyi məlum olarsa, onların əməliyyatlarını izləmək olar (şəkil 3.2.1).



Şəkil 3.2.1. Kriptovalyutaların ümumi bazar dəyəri

[4] Fərqli valyutaların müxtəlif müraciətləri var, lakin kriptovalyutaların populyarlığı əsasən onların qeyri-mərkəzləşdirilmiş təbiətindən qaynaqlanır: Onlar əməliyyatı bloklaya biləcək və ya rüsum tələb edə biləcək banka ehtiyac duymadan nisbətən tez və anonim şəkildə, hətta sərhədlər boyu köçürülə bilər. Avtoritar ölkələrdəki dissidentlər ABŞ-ın Rusiyaya qarşı sanksiyalarından qaçmaq da daxil olmaqla, dövlət nəzarətindən yayınmaq üçün Bitcoin-də vəsait toplayıblar. Bir sıra Latın Amerikası və Afrika ölkələri də daxil olmaqla, tarixən zəif valyutaya malik olan ölkələrdə Bitcoin populist liderlər arasında populyarlaşıb. 2021-ci ildə El Salvador Bitcoin-i qanuni ödəniş vasitəsi edən ilk ölkə olmaqla dalğalar yaratdı (sakinlər bununla vergi ödəyə və borclarını ödəyə bilərlər), baxmayaraq ki, bu hərəkət etirazlara səbəb oldu. Bölgənin digər bölgələrindəki bəzi siyasətçilər bu ideyanı dəstəklədiklərini bildiriblər.

Kriptovalyutalar hökümətlər üçün cinayət fəaliyyəti, ətraf mühitə dəyən zərər və istehlakçıların müdafiəsi ilə bağlı narahatlıqlar da daxil olmaqla, mübarizə aparmalı olduqları yeni problemlər toplusuna səbəb olub. Bitcoin hasilatı çox enerji tələb edən bir prosesdir: şəbəkə indi bir çox ölkədən daha çox

4. [4] E. E. Grandon and J. M. Pearson, “Electronic commerce adoption: An empirical study of small and medium US businesses,” Inf. Manag., vol. 42, no. 1, pp. 197–216, 2004.

elektrik enerjisi istehlak edir. Bu, kriptovalyutanın iqlim dəyişikliyinə töhfəsi ilə bağlı qorxulara səbəb oldu. Kriptovalyuta tərəfdarları bu problemi bərpa olunan enerjidən istifadə etməklə həll etmək olar; El Salvador prezidenti, məsələn, Bitcoin hasilatı üçün vulkan enerjisindən istifadə edəcəyinə söz verdi. Ətraf mühitlə bağlı narahatlıqların Ethereum-un daha az enerji istifadə edən sübut modelinə keçməsinə səbəb olduğu bildirilir.

Bir çox hökumətlər kriptovalyutaya əlçatan bir yanaşma tətbiq etdilər, lakin onun sürətli yüksəlişi və təkamülü DeFi-nin yüksəlişi ilə birlikdə tənzimləyiciləri inkişaf etməkdə olan sektor üçün qaydalar hazırlamağa başlamağa məcbur etdi. Qaydalar bütün dünyada geniş şəkildə dəyişir, bəzi hökumətlər kriptovalyutaları qəbul edir, digərləri isə onları birbaşa qadağan edir. Tənzimləyicilərin qarşısında duran vəzifə, ekspertlərin fikrincə, innovasiyaları boğmadan ənənəvi maliyyə risklərini məhdudlaşdıran qaydaların işlənib hazırlanmasıdır.

ABŞ-da siyasətçilər kriptovalyutaları və inkişaf etməkdə olan DeFi sektorunu tənzimləmək üçün yavaş-yavaş hərəkət etdiklərini bildirdilər. Bununla belə, kriptovalyutalar mövcud tənzimləyici çərçivəyə tam uyğun gəlmir və bu, qanunvericilərin çox güman ki, həll etməli olacağı qeyri-müəyyənlik yaradır. ABŞ Qiymətli Kağızlar və Birja Komissiyasının (SEC) sədri Gary Gensler kriptovalyuta sektorunu "Vəhşi Qərb" adlandırdı və Konqresi SEC-ə daha çox səlahiyyətlər verməyə çağırdı. Federal Ehtiyatlar Sisteminin sədri Jerome Powell və Xəzinədarlıq katibi Janet Yellen hər ikisi stabilkoinlərin daha güclü tənzimlənməsinə çağırıblar. Lakin tənzimləyicilər indiyədək kriptovalyuta investorlarına əmanət sığortası kimi daha ənənəvi maliyyədə mövcud olan eyni qorumaları genişləndirməkdən çəkinirlər. Federal Ehtiyat Rəhbərlər Şurasının Kristofer J. Uoller 2023-cü ildə "Kripto-aktivlər alsanız və qiymət nə vaxtsa sıfıra düşərsə, lütfən təəccüblənməyin və vergi ödəyicilərinin sizin itkilərinizi ictimailəşdirməsini gözləməyin" dedi.

Qeyri-qanuni fəaliyyətləri məhdudlaşdırmaq üçün səlahiyyətlilər istifadəçilərə kriptovalyutaları ABŞ dollarına və digər milli valyutalara çevirməyə imkan verən birjaları hədəfə alıblar. Tənzimləyicilərin təzyiqi altında Coinbase, Binance və Gemini daxil olmaqla böyük birjalar "müştərinizi tanıyın" və çirkli pulların yuyulmasına qarşı digər tələblərə əməl edirlər. Bu arada hüquq-mühafizə orqanları və kəşfiyyat orqanları cinayət fəaliyyətini təhlil etmək və izləmək üçün blokçeynlərdən istifadə etməklə əksər kriptovalyutaların izlənilməsindən istifadə etməyi öyrəniblər. Məsələn, Colonial Pipeline hakerlərinə ödənilən fidyənin bir hissəsi daha sonra FTB tərəfindən bərpa edildi. 2022-ci ilin avqustunda Xəzinədarlıq Departamenti cinayətkarların blokçeyndəki əməliyyatları anonimləşdirmək üçün istifadə edə biləcəyi sözdə kriptovalyuta mikserlərinə qarşı repressiya elan etdi və onları "ABŞ-ın milli təhlükəsizliyinə təhdid" adlandırdı.

Suverenliyini təsdiq etmək üçün bir çox mərkəzi banklar, o cümlədən ABŞ Federal Ehtiyat Sistemi, mərkəzi bank rəqəmsal valyutası (CBDC) kimi tanınan öz rəqəmsal nağd pullarını təqdim etməyi düşünür. Tərəfdarlar üçün CBDC-lər əlaqəli risklər olmadan kriptovalyutanın sürətini və digər faydalarını vəd edir. Qlobal iqtisadiyyatın 90 faizindən çoxunu təmsil edən onlarla ölkə CBDC-ləri araşdırır. On bir ölkə CBDC-ləri tamamilə işə saldı. Hamısı aşağı gəlirli, on nəfər isə Karib hövzəsindədir (Nigeriya on birincidir). 2019-cu ildə rəqəmsal yuanı sınaqdan keçirdikdən sonra Çinin indi CBDC pilot proqramını 2023-cü ilin sonuna qədər bir milyarddan çox əhalisinə çatdıracağı gözlənilir. ABŞ-da Fed rəsmiləri arasında rəqəmsal dollara ehtiyacla bağlı fikir ayrılığı olduğu bildirilir.

Bəzi ekspertlər deyirlər ki, CBDC-lərin vasitəçi kimi kommersiya banklarını kəsmək potensialı risk daşıyır, çünki bu banklar kredit yaratmaq və ayırmaqla (yəni kredit verməklə) mühüm iqtisadi rol oynayırlar. İnsanlar birbaşa Fed-lə bank etməyi seçsəydilər, bu, mərkəzi bankdan ya istehlakçı borclanmağı asanlaşdırmasını tələb edərdi ki, bunu etmək üçün təchiz oluna bilməz, ya da

kredit yeritmək üçün yeni yollar tapmalıdır. Bu səbəblərə görə bəzi ekspertlər özəl, tənzimlənən rəqəmsal valyutaların CBDC-lərə üstünlük verildiyini söyləyirlər.

3.3. Üçsəviyyəli təhlükəsizlik tətbiqli internet bankçılıq sisteminin təkmilləşdirilməsi

Ümumiyyətlə, İnternet bankinq açarı iki müxtəlif moduldan, yəni təhlükəsizlik və şəbəkə/nəzarət modulundan istifadə edir. Təhlükəəsizlik modulu İnternet bankinq sistemi üçün əsas meyardır və üç alt modula bölünür:

İstifadəçinin autentifikasiyası (cihaz girişinə nəzarət)

Cihaz/server identifikasiyası modulu

Tranzaksiya məlumatlarının təhlükəsizliyi (şəbəkə təhlükəsizliyi)

Şəbəkə/nəzarət modulu da iki alt modula yəni, şəbəkə və idarəetmə altmodullatına bölünür. Nəzarət alt modulu İnternet bankinkşılıq serveri vəİnternet bankinq açarı arasında əlaqə yaratmaq üçün cavabdehdir. Həmçinin o anomaliyaları izləyir və aşkar edildikdə əlaqəni dayandırılır. Şəbəkə modulu ötürüləcək məlumatları əhatə edir. O. Həmçinin İnternet bankşılıq serverindən məlumatları ötürür və qəbul edir. Ötürmə uyğun Transmission Control Protocol/İnternet Protocol (TCP/İP) və TLS protokollarından istifadə etməklə həyata keçirilir. Bizim üçün ən önəmli detal təhlükəsizlik modulunun təhlilidir.

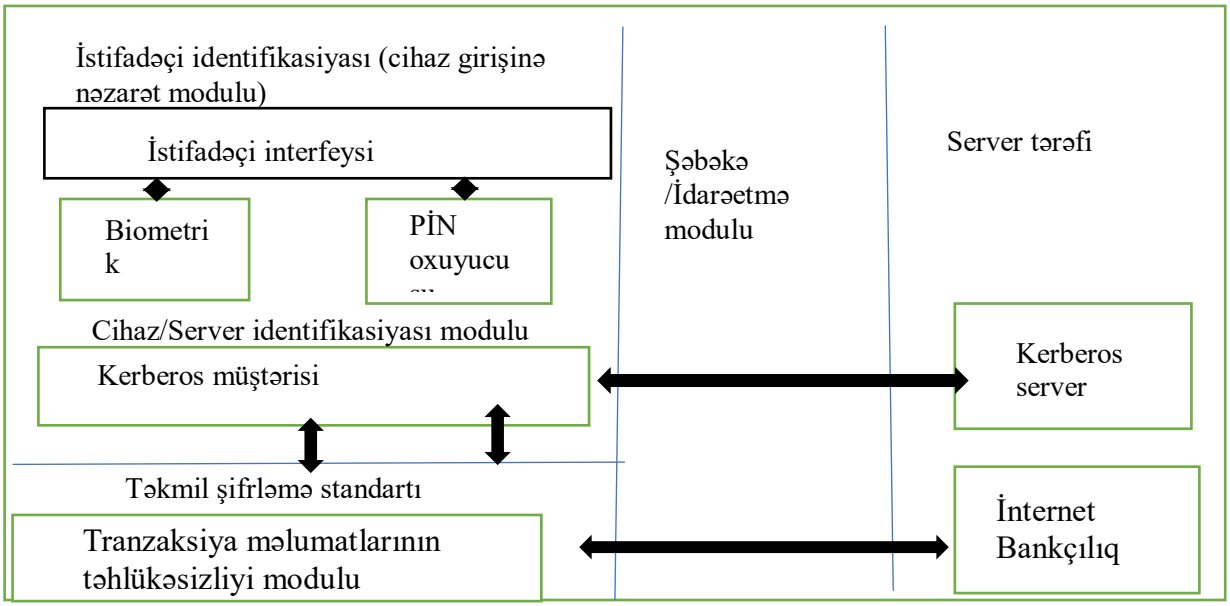
İstifadəçinin autentifikasiyası təhlükəsizlik alt modulu yalnız səlahiyyətli istifadəçilərin internet bançılıq sisteminə daxl olmasını təmin edir. Bu barmaq izi məlumatından və istifadəçinin şəxsi identifikasiya nömrəsindən (PİN) istifadə etməklə həyata keçiriləcək. Biometrik oxuyucu müştərinin biometrik məlumatlarını oxuyur və autentifikasiya üçün şəbəkə moduluna göndərir. Bjurad asistem elə qurulmuşdur ki, məlumat ələ keçirilərkən dərhal şifrlənir.

Qurğu/Server identifikasiyası alt təhlükəsizlik modulunyalnız səlahiyyətli qurğuların internet bankinq serverinə daxil olmasını təmin edir. Bu klonlaşıdırılmış qurğuların istifadəsinin qarşısının alınması üçündür. Kerberos serveri yalnız səlahiyyətli qurğuların daxil olduğuna əmin olmaq üçün onun Media girişinə Nəzarət (MAC) ünvanını yoxlayır. MAC ünvanın şifrlənməsi və müştərilərin barmaq izi məlumatlarının PİN kodu ilə birlikdə autentifikasiya üçün Kerberos serverinə göndərilməsi klonlaşdırılmış qurğuların autentifikasiya olunmamasına zəmanət verir.

Tranzaksiya məlumatlarının təhlükəsizliyi bu təhlükəsizlik alt modulu əməliyyat məlumatlarının internet bankinq serverindən başqa heç kim üçün əlçatan olmammasını təmin edir. Bu məlumatların məxfiliyinə zəmanət verir və tranzaksiya məlumatlarına hər hansımümkün girişi aradan qaldırır.

A. Sistem modullarının qarşılıqlı əlaqəsi: Aşağıdakı şəkildə təklif olunan sistem üçün modul qarşılıqlı əlaqəsinin diaqrammatik təsviri verilmişdir. Kerberos müştərisi bilavasitə istifadəçi interfeysi altında quraşdırılmışdır. Cihaz istifadəçisinin giriş məlumatı (barmaq izi və PİN) alındıqdan sonra Kerberos müştəri məlumatını şifrləyir və Şəbəkə nəzarət moduluna yerləşdirir. Bu məlumat MAC ünvanı ilə birlikdə Kerberos biletinin verilməsi üçün cihazın və istifadəçinin autentifikasiyası üçün istifadə olunur.

Ətraflı şifrlənmə əməliyyatı təhlükəsizlik modulunda həyata keçirilir. Bu modul cihazın/serverin autentifikasiyası modulunun altında yerləşir. Daha sonra Kerberos biletiinternet bankçılıq serveri tərəfindən qəbul edilidikdən sonra o, internet bankçılıq serveri ilə birbaşa əlaqə saxlayır. Bu modul əməliyyatların məxfiliyini təmin edir (şəkil 3.3.1).



Şəkil 3.3.1. Təhlükəsizlik modulu

3.4.İnternet Bankçılıq sisteminin təhlükəsizlik alqoritminin işlənməsi

Təklif olunan sistemdə informasiya axınını başa düşmək üçün sistemin işini aşağıda qeyd olunan alqoritmlə təqdim etmək olar:

1. İstənilən istifadəçi İnternet bağlantısı olan kompüter və ya planşetdə

USB İnternet bankinq açarını daxil edir; dongle istifadəçi üçün giriş interfeysi avtomatik olaraq işə salınır.

2. İnterfeys istifadəçidən PİN və barmaq izini təqdim etməyi təklif edir.

3. İlkin təhlükəsizlik yoxlaması dongle tətbiqi tərəfindən həyata keçirilir. Və müsbət nəticə verərsə dongle proqramı məlumatı bilet üçün autentifikasiya edən Kerberos serverinə göndərir

4. Kerberos serveri dongle cihazının və istifadəçinin şəxsiyyətini və icazələrini təsdiqlədikdə, biletin verilməsi prosesi başlayır.

5. Biletin verilməsi uğurlu olarsa dongle proqramı Kerberos serveri tərəfindən verilmiş biletdən istifadə edərək avtomatik olaraq internet bankinq serverinə qoşulur.

6. İnternet bankçılıq serverinin interfeysində istifadəçi internet bankçılıq menyusuna daxil olmaq üçün hesabına giriş məlumatlarını(istifadəçi adı və şifrə) təqdim edir və burada yerinə yetiriləcək əməliyyatları seçə bilər.

7. Hər bir əməliyyatı təsdiqləmək üçün müştərilərin ikin giriş PİN kodu daxil edilməli olan əməliyyatın təsdiq nömrəsi kimi xidmət edir.

8. İnternet Bankinq serveri məlumatları şifrləmək və deşifrləmək üçün yalnız iki əlaqə quran cihaza məlum olan simmetrik açardan istifadə edir.

9. Müştəri menyuda çıxışı seçdikdən sonra biletin müddəti başa çatır, server ilə dongle arasındakı əlaqə kəsilir və açar tətbiqi bildirişdən sonra avtomatik bağlanır. İstifadəçi əməliyyatın bitdiyini bildirir.

10. Müştəri öz dongle-ni kompüterdən çıxarır.

Kerberos bileti. Müştəri özünü yeni yoxlayıcıya autentifikasiya etdikdə o yeni şifrələmə açarı və autentifikasiya serverindən istifadə edir. Bu yeni şifrələmə açarı sessiya açarı adlanır və Kerberos bileti ony yoxlayıcıya paylamaq üçün istifadə edir. Kerberos bileti autentifikasiya serveri tərəfindən verilmiş və Server açarı ilə şifrlənmiş sertifikatdır. Bilet birbaşa yoxlayıcıya göndərilmir və əksinə ərizə sorğusunun bir hissəsi kimi onu yoxlaylclya yönləndirən müştəriyə göndərilir. Bilet yalnız autentifikasiya serveri (Kerberos server) və İnternet bankinq serveri tərəfindən tanınan server açarında şifrləndiyi üçün müştərinin bileti aşkar etmədən dəyişdirməsi mümkün deyil. Kerberos biletlətinin istifadə müddəti və istifadə parametrləri vardır.

Bir dəfə biletin müddəti bitdikdə, müştəri serverlə əlaqəni davam etdirmək üçün yenilənmə və ya yeni bilet tələb etməlidir.

Kerberos biletinin verilmə prosesi aşağıdakı kimidir:

1. İstifadəçi PİN kod daxil edərək Biometrik məlumatları qeyd edir.
2. Müştəri etimadnamələrini DES ilə şifrləyərək KDC-yə ötürür.
3. KDC istifadəçi etimadnaməsini yoxlayır.

4. KDC istifadəçi məlumatını hashing etməklə Bilet Təqdimat biletini (TGT) yaradır.

5. TGT müştəriyə ötürülməsi üçün DES ilə şifrlənir.

6. Müştəri TGT-nin istifadə müddəti bitənə qədər quraşdırır.

Bunlar bitdikdən sonra növbəti proses İnternet Bankçılıq xidmətinə müraciətdir:

1. Müştəri İnternet bankçılıq xidmətinə giriş sorğusu ilə öz TGT-ni KDC-yə geri göndərir.

2. KDC TGT-nin davam edən etibarlılığını yoxlayır və istifadəçinin resursa daxil olmaq üçün doğruluğunu yoxlamaq üçün onun girişə nəzarət matrisini yoxlayır.

3. Xidmət bileti (ST) yaradılır və müştəriyə göstərilir.

4. Müştəri ST-ni İnternet bankinq serverinə göndərir.

5. KDC ilə ST-nin server və ya xidmət hostu etibarlılğı yoxlanılır.6. Şəxsiyyət və icazə təsdiqləndikdən sonra Kerberos fəaliyyətini tamamlayır. İnternet bankçılıq serveri daha sonra müştəri ilə sessiya açır və rabitə və ya məlumat ötürülməsinə başlayır.

Açar Dağıtım Mərkəzi kriptoqrafik sessiya açarlarını saxlayan , paylayan və saxlayan serverlər qrupudur. Sistem Kerberos istifadə edən xidmətə daxil olamq istədikdə, sorğu KDC vasitəsilə edilir. KDC seans açarı yaradır. Bu da sistemin birləşdirilməsi prosesini asanlaşdırır. Bu iş bankdan asılı olmayaraq hər bir ölkədə bütün İnternet bankçılıq əməliyyatları üçün ehtiyat KDC-lər ilə vahid KDC təklif edir. Ehtiyat KDC-lər uğursuz olarsa vahid KDC-də uğursuz nəticə verəcəkdir. KDC-ılər onlarda yerləşən məlumatların eyni olması üçün sinxronlaşdırılacaqdır. KDc istifadəçinin autentifikasiyası və MAC ünvanından və istifadəçiinin PİN və barmaq izi məlumatından istifadə edəcək. Bununla biz əmin ola bilərik ki, dongle-də yalnış Pİn və barmaq izi məlumatının daxil edilməsi İnternet bankçılıq saytında xidmətdən imtina ilə nəticələnəcək. Bu da

İnternet Bankçılıq sisteminə başqa şəxsin açarı ilə daxil olmağım qeyri-mümkün edir. İstifadəçilər İnternet Bankinq açarını öz banklarından əldə etdikdə açar Distribution Mərkəzindəqeydiyyatdan keçirilir, istifadəçilər öz PİN və barmaq izi məlumatını Açar Dağıtım mərkəzinə təqdim edirlər. Dongle-nin MAC ünvanı daha sonra istifadəçilərin PİN kodu və barmaq izi ilə əlaqələndirilir. Daha sonra istifadəçinin autentifikasiyası və sorğu əsasında Kerberos biletiinin verilməsi üçün istifadə olunur. Qeydiyyat prosesi ərzində istifadəçilərdən İnternet bankinq sahibini izləməyə imkan verən açar əmanətdə saxlanılan şəkil və təhlükəsizlik məlumatlarını təqdim etmələri tələb olunur. Bunun sayəsində istifadəçi internet bankinqdə hər hansı əməliyyat yerinə yetirərkən təhlükəsizlik məlumatatları müəyyən ediləcək (şəkil 3.3.2).

3.3.2.Kerberos serverlər və açar əmanət funksiyası

Açar əmanət sistemi. Bu açarların verilənlər bazasında saxlandığı kriptoqrafik bərpa mexanizmidir. Açarın itirilməsi və ya zədələnməsi halında səlahiyyətli əsas agentlər tərəfindən bərpa edilir. Təklif olunan açar əmanəti müştərilərin İnternet bankinq açarından istifadə tarixini saxlaya biləcək çünki müştəri birdən çox internet bankinq açarından istifadə etmək qərarına gələ bilər. Bu mühasibat uçotu kimi tanınır. Bu cür tarix lazım gəldikdə xüsusilə internet bankçılıq fəaliyyətinin araşdırılması zamanı səlahiyyətli şəxslərə təqdim edilə

bilər. Müştəri internet bankinq açarını itirdikdə yeni açar əldə edir və sonra bank onu qeydiyyatdan keçirir.Bütün qeydiyyatdan keçmiş müştərilərin məlumatı əsas əmanəatdə saxlanılır.

AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Qarayev Cabir Oqtay oğlu

İnternet bankçılıq sistemində istifadəçi məxfiliyinin çoxsəviyyəli autentifikasiya tətbiqli model və alqoritminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631 – "Kompüter mühəndisliyi"

İxtisaslaşma: "Kompüter texnikasının lahiyələndirilməsi və konstruksiya edilməsi"

Elmi rəhbər: t.e.n, dosent İsgəndərzadə Hüseyn Qasım oğlu

BAKI – 2023

IV FƏSİL. İNTERNET BANKÇILIQ SİSTEMİNDƏ İSTİFADƏÇİ MƏXFİLİYİNİN ALQORİTMİNİN İŞLƏNMƏSİ

4.1.İnternet bankçılıq sistemində istifadəçi məxfiliyinin qorunması

Məxfiliyin qorunması istifadəçilərin maliyyə məlumatlarının təhlükəsizliyini və məxfiliyini təmin etmək üçün internet bankçılıq sistemlərinin mühüm aspektidir. Məxfiliyin qorunması üçün internet bankçılıq sistemlərində həyata keçirilən bəzi əsas tədbirlər bunlardır:

Şifrələmə: İnternet bankçılıq sistemləri istifadəçinin cihazı ilə bank serveri arasında məlumat ötürülməsini təmin etmək üçün şifrələmə üsullarından istifadə edir. Bu, giriş etimadnamələri, hesab təfərrüatları və əməliyyat məlumatları kimi mübadilə edilən məlumatların məxfi qalmasını və icazəsiz şəxslər tərəfindən ələ keçirilməməsini təmin edir.

Secure Sockets Layer (SSL) və ya Nəqliyyat Layer Security (TLS): SSL/TLS protokolları istifadəçinin veb brauzeri ilə bank serveri arasında təhlükəsiz əlaqə yaradır. Şəbəkə üzərindən ötürülən məlumatların şifrlənməsini təmin edir, onların təcavüzkarlar tərəfindən əldə edilməsinin və ya dəyişdirilməsinin qarşısını alır.

İki faktorlu identifikasiya (2FA): İnternet bankçılıq sistemləri çox vaxt əlavə təhlükəsizlik qatını əlavə etmək üçün birdəfəlik parollar (OTP), biometrik doğrulama və ya aparat nişanları kimi 2FA metodlarından istifadə edir. Bu, kimsə istifadəçinin giriş etimadnaməsini əldə etsə belə, ikinci autentifikasiya faktoru olmadan daxil ola bilməyəcəyini təmin edir.

Firewalllar: Banklar şəbəkə trafikinə nəzarət etmək və izləmək üçün firewall tətbiq edirlər. Firewalllar internet və bank sistemi arasında maneə rolunu oynayır, icazəsiz girişin qarşısını alır və zərərli fəaliyyətləri bloklayır.

Intrusion Detection and Prevention Systems (IDPS): IDPS alətləri potensial təhlükəsizlik təhdidlərini və ya icazəsiz giriş cəhdlərini müəyyən etmək və onlara cavab vermək üçün istifadə olunur. Bu sistemlər şəbəkə trafikinə nəzarət edir,

nümunələri təhlil edir və inzibatçıları şübhəli fəaliyyətlər barədə xəbərdar edir, məlumatların pozulmasının qarşısını almağa kömək edir.

Təhlükəsiz İnkişaf Təcrübələri: Banklar təhlükəsiz kodlaşdırma təcrübələrinə əməl edir və internet bankçılıq sistemlərində zəiflikləri müəyyən etmək və aradan qaldırmaq üçün müntəzəm təhlükəsizlik auditləri aparırlar. Sistemlərin məlum təhlükəsizlik risklərinə qarşı qorunmasını təmin etmək üçün müntəzəm yeniləmələr və yamalar tətbiq edilir.

Məxfilik Siyasətləri və Razılıq: İnternet bankçılıq sistemləri adətən müştəri məlumatlarının necə toplandığını, saxlandığını və istifadə edildiyini təsvir edən məxfilik siyasətlərinə malikdir. Banklar məlumatların toplanması üçün müştərinin razılığını almalı və məlumatın necə qorunacağını və istifadə olunacağını aydın şəkildə bildirməlidir.

İstirahət zamanı məlumatların şifrələnməsi: Banklar sistemlərində saxlanılan müştəri məlumatlarını qorumaq üçün şifrələmə üsullarından istifadə edirlər. Bu, məlumatların oğurlanması halında belə, onların şifrələnmiş və şifrə açma açarları olmadan istifadə edilə bilməyəcəyini təmin edir.

Daimi Monitorinq və İnsidentlərə Müdaxilə: Banklar öz sistemlərini hər hansı şübhəli fəaliyyət və ya pozuntular üçün aktiv şəkildə izləyirlər. Onların hər hansı potensial zərəri azaltmaq və müştəri məlumatlarını qorumaq üçün müvafiq tədbirlər görmək üçün insidentlərə cavab planları var.

Tənzimləmə Uyğunluğu: Banklar müştəri məlumatlarının qorunmasını təmin etmək və məxfilik standartlarını qorumaq üçün Ümumi Məlumatların Qorunması Qaydası (GDPR) və Ödəniş Kartı Sənayesi Məlumat Təhlükəsizliyi Standartı (PCI DSS) kimi müxtəlif məxfilik və təhlükəsizlik qaydalarına riayət edirlər.

Güclü parollardan istifadə etməklə, cihazlarını və bank proqramlarını mütəmadi olaraq güncəlləmək, şübhəli e-poçt və ya keçidlərdən qaçınmaq və ictimai şəbəkələrdə internet bankçılıq sistemlərinə daxil olarkən ehtiyatlı olmaq yolu ilə insanların təhlükəsizlik gigiyenasına riayət etmələri də vacibdir.

4.2.Məxfilik məlumatları üzrə tədqiqat mühafizə sistemi

İnternet bankçılıqda blokchain alqoritmləri mövzusu son illərdə artan maraqı ilə diqqət çəkən bir sahədir. Blokchain, dağıtılmış bir ledjer sistemi olaraq bilinən və kriptovalyuta transaksiyalarının qeydiyyatını və doğrulamağa imkan verən bir texnologiyadır. Bu texnologiya, internet bankçılığı sahəsində məxfilik təhlükələrinin azaldılması və güvənli bir mühit yaratılması üçün potensial imkanlar təklif edir.

Blokchain, məxfilik və təhlükəsizlik prinsipləri üzrə inkişaf etmiş bir texnologiya olduğundan, internet bankçılığında tətbiqi ilə bir sıra faydalar gətirir. Birincisi, blokchain tərəfindən təsdiqlənmiş və doğrulanmış blokların olması, hər bir əməliyyatın şifrələnməsi və dağıtılmış olaraq saxlanılması deməkdir. Bu, məxfilik məlumatlarının təhlükəsiz şəkildə saxlanılmasına və potensial məxfilik pozuntularının azalmasına imkan verir.

Blockchain açıq açar ünvanlarına əsaslanan autentifikasiya üsuludur. Şəbəkədəki istifadəçilərin açıq açar ünvanları ilə birdən çox əlaqəsi var. İstifadəçilərin məxfiliyinə bu psevdoanonimliyin mühafizəsi altında zəmanət verilir. Bununla belə, tədqiqat göstərir ki, blokçeynin psevdoanonimliyi məxfiliyin sızması riskini aradan qaldıra bilməz. Problemin mənbəyini izləmək faydalıdır, ona görə də anonimlik və izlənilmə problemlərini balanslaşdıra bilən təkmilləşdirilmiş autentifikasiya sxeminə ehtiyac vardır.

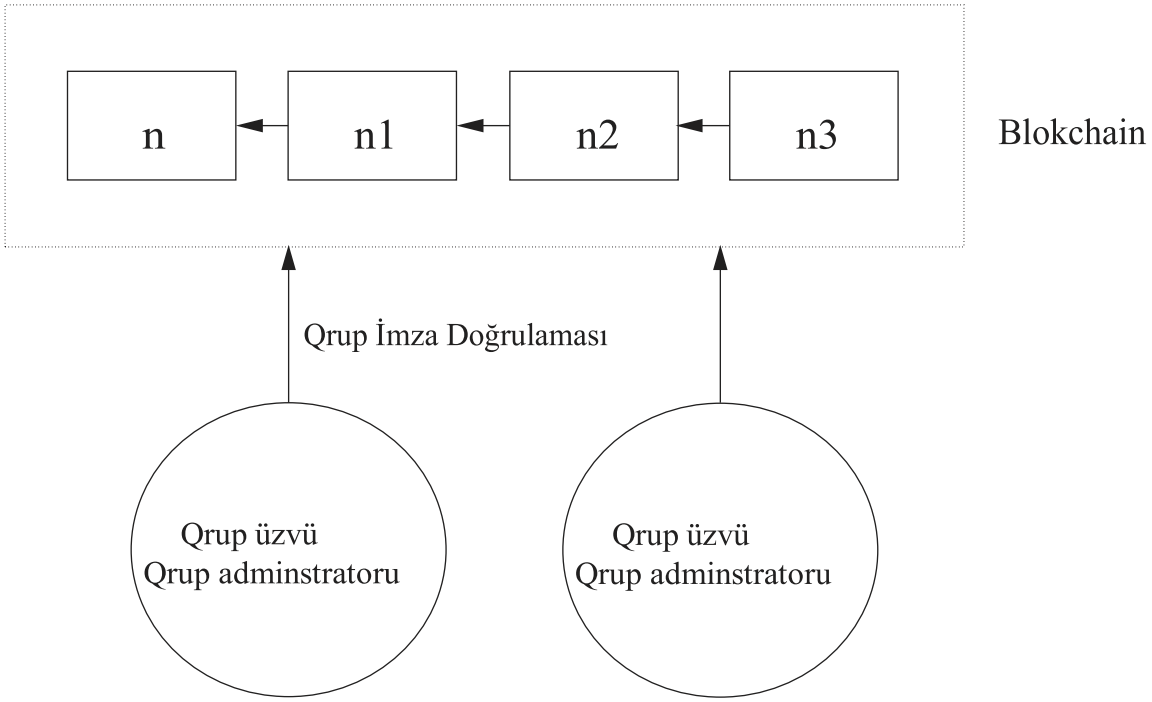
$$\min F\text{obj} = \min P + \lambda \sum_{\beta} \left[\frac{Vi - Vi\lim}{Vi\max - Vi\min} \right]^2$$

Blockchain autentifikasiya kimi istifadə edilə bilər və istifadəçilər açar cütlərindən istifadə edərək öz şəxsiyyətlərini blokçeyndə qeyd edirlər. Bu qeydə alınmış şəxsiyyət şəxsiyyətlə əlaqəli bir neçə atributun heşini ehtiva edən məlumatdır. Bundan sonra belə istifadəçilər blokçeynində əvvəllər qeydə alınmış heşləri yoxlayan tanınmış qrupa qoşula və sonra identifikasiya edən tərəfin həmin məlumatı blokçeyndə həqiqət kimi təsdiqləməsini tələb edə bilər. Müəyyən

müəyyən edilmiş tərəfə güvənən digər tərəflər indi blokçeyndəki şəxsiyyətə etibar edə və ondan autentifikasiya və ya identifikasiya mexanizmi kimi istifadə edə bilər, lakin istifadəçilər öz identifikasiyalarını itirə bilər, məsələn, mobil telefonun və ya şəxsi məlumatları saxlayan digər məlumat daşıyıcısının itirilməsi. şəxsiyyətin əsas hissəsi və ya daha da pisi: rəqəmsal şəxsiyyətin məlumat oğurluğu. Blockchain texnologiyasına əsaslanan qeyri-mərkəzləşdirilmiş autentifikasiya vəziyyətində, heç bir mərkəzi qurum yeni şəxsiyyətin tələb oluna biləcəyi və köhnə şəxsiyyətimin blokçeynində oğurlanmış və ya itirilmiş kimi qeyd oluna biləcəyi şəxsiyyətə nəzarət etmir. Başqa bir halda, blokçeyn psevdo-anonimliyi təmin etdiyinə görə, hər kəs blokçeyndəki bir və ya bir neçə açıq açar ünvanına, yəni virtual şəxsiyyətə uyğun gəlir, baxmayaraq ki, bir neçə açıq açar ünvana malik olmaq anonimliyi gücləndirə bilər. Bununla belə, tədqiqatlar göstərdi ki, zəncir üzərindəki əməliyyatlar zəncirdənkənar əməliyyatlarla əlaqələndirildikdə, virtual şəxsiyyətin arxasındakı həqiqi şəxsiyyət böyük miqdarda əməliyyat məlumatlarının təhlili ilə aşkar edilə bilər və bununla da istifadəçi məxfiliyini ifşa edir.

$$\theta^{e+1} = \theta^{e} + \frac{\alpha}{|B|} (X^{B})^{T} (X^{B}\theta^{e} - y^{B})$$

Məlumatlar yalnız etibarlı blokçeyn imzaları və qrup imzaları halında etibarlı məlumat hesab olunur. Zərərli istifadəçilər öz istəyi ilə bloka məlumat göndərirsə, zəncir sistemin sabitliyini poza bilər və imzalayanı cəzalandırmaq üçün xüsusi qrup menecerinin şəxsi açarı vasitəsilə izləmək olar. Blockchain texnologiyasının özü izlənilmə xüsusiyyətinə malik olmadığı üçün sistemin sabitliyini pozan zərərli istifadəçiləri effektiv şəkildə cəzalandıra bilməz. Qrup imzasının izlənəbilirlik xüsusiyyəti yalnız bu qüsuru tamamlayır və sistemin effektiv idarə olunmasını təmin edir. Şəkil 4.2.1-də göstərilmişdir.



Şəkil 4.2.1. İstifadəçi autentifikasiyası

4.3. İstifadəçi məxfilik məlumatlarının bütövlüyünün yoxlanması

İnternet bankçılıq sistemlərində istifadə edilən məxfiliyin qorunması alqoritminə bir nümunə Qabaqcıl Şifrələmə Standartıdır (AES). AES simmetrik şifrələmə alqoritmidir və verilənlərin ötürülməsi və saxlanmasını təmin etmək üçün geniş istifadə olunur.

AES, adətən 128 bit ölçüsündə olan məlumat blokları üzərində işləyir və məlumatları şifrələmək və deşifrə etmək üçün gizli şifrələmə açarından istifadə edir. Alqoritm yüksək səviyyəli təhlükəsizlik təmin edən bir neçə növbəli əvəzetmə, dəyişdirmə və qarışdırma əməliyyatlarından ibarətdir.

AES-in necə işlədiyinə dair sadələşdirilmiş icmal:

Açarın genişləndirilməsi: Yalnız banka və istifadəçiyə məlum olan əvvəlcədən təyin edilmiş gizli açar olan şifrələmə açarı dəyirmi açarlar dəsti yaratmaq üçün açar genişləndirmə prosesindən keçir. Bu dəyirmi açarlar sonrakı şifrələmə və deşifrə əməliyyatlarında istifadə olunur.

İlkin raund: Giriş məlumat bloku (açıq mətn) birinci dövrə düyməsi ilə XORed (birləşdirilmişdir).

Dəyirmi: AES hər biri dörd əməliyyatdan ibarət bir neçə dövrədən ibarətdir: SubBytes, ShiftRows, MixColumns və AddRoundKey. Bu əməliyyatlar məlumat blokunu kriptoqrafik hücumlara davamlı edəcək şəkildə çevirir.

Subbaytlar: Məlumat blokunun hər bir baytı şifrələmə prosesində çaşqınlığı təmin edən əvəzetmə cədvəlindən (S-Box) müvafiq baytla əvəz olunur.

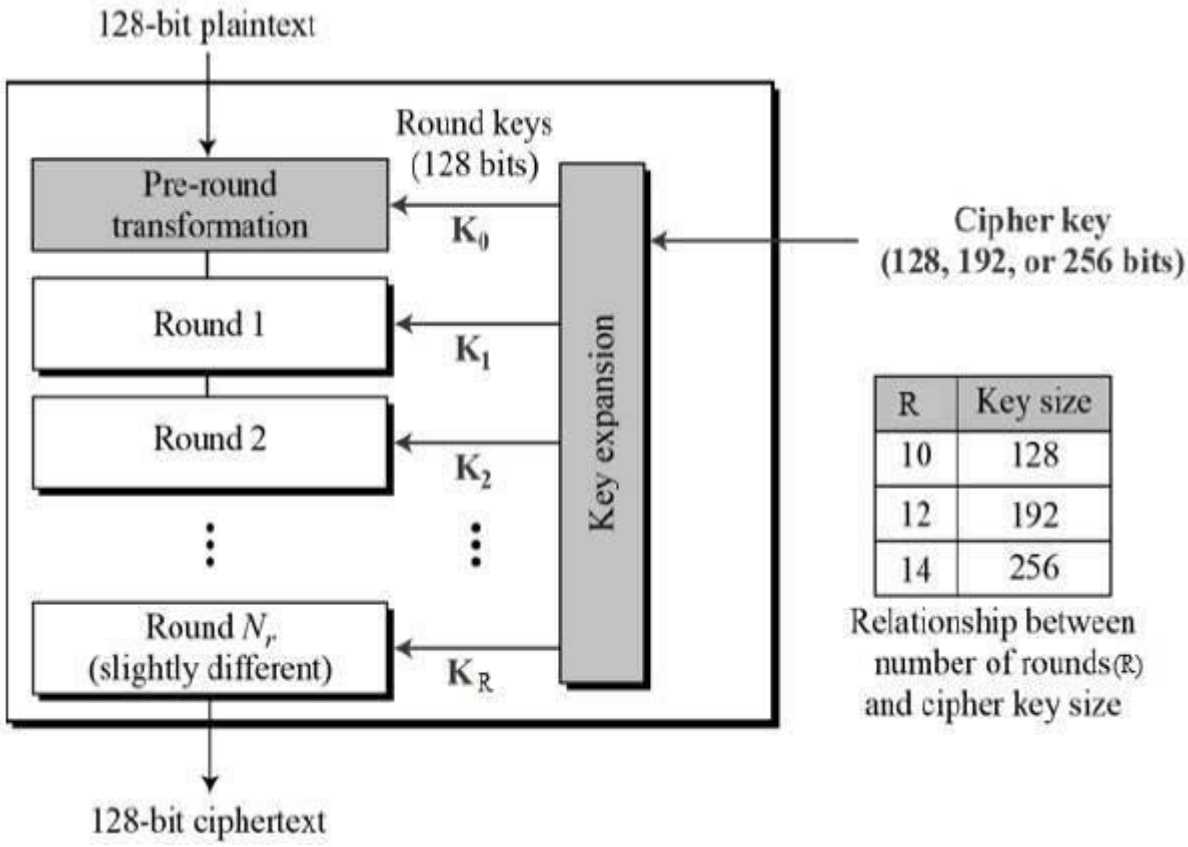
ShiftRows: Məlumat blokunun hər bir cərgəsindəki baytlar siklik olaraq dəyişdirilir və şifrələmə prosesində diffuziya təmin edilir.

Qarışıq Sütunlar: Məlumat blokunun hər bir sütunu əlavə diffuziya təmin edən riyazi əməliyyatdan istifadə edərək çevrilir.

AddRoundKey: Cari raund üçün dəyirmi açar dəyişdirilmiş məlumat bloku ilə XORed.

Son raund: Son tur alqoritmi sadələşdirmək üçün MixColumns əməliyyatını istisna edir. O, əvvəlki turlarda olduğu kimi SubBytes, ShiftRows və AddRoundKey əməliyyatlarını yerinə yetirir.

Nəticə: Son turdan sonra əldə edilən məlumat bloku şifrələnmiş şifrəli mətndir (şəkil 4.3.1-də göstərilmişdir).



Şəkil 4.3.1. Advanced Encryption Standard (AES)

Şifrə mətninin şifrəsini açmaq üçün eyni AES alqoritmi şifrləmə açarından əldə edilən deşifrə açarından istifadə edərək tərsinə tətbiq edilir.

AES geniş şəkildə təhlükəsiz şifrələmə alqoritmi kimi qəbul edilir və o, müxtəlif təşkilatlar və standart qurumlar tərəfindən internet bankçılıq sistemləri daxil olmaqla, həssas məlumatların qorunması üçün etibarlı üsul kimi qəbul edilmişdir.

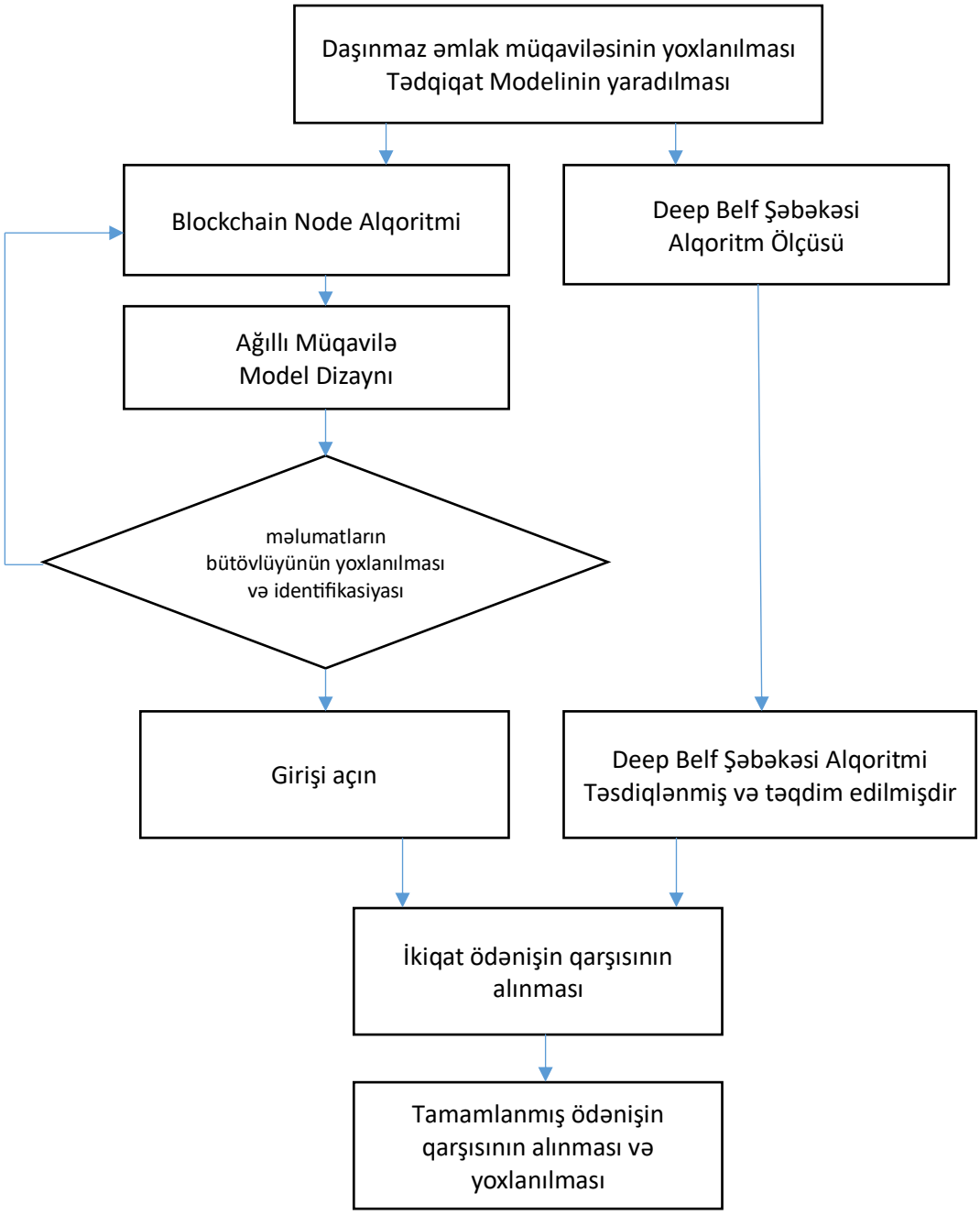
Alqoritmlər, internet bankçılıqda əməliyyatların effektiv şəkildə həyata keçirilməsinə kömək edən tədqiqat proseslərdir. Bu alqoritmlər, məsələn, hesab kitabxanası alqoritmləri, tranzaksiya verifikasiyası alqoritmləri, risk idarəetmə alqoritmləri və s. kimi fərqli sahələrdə tətbiq olunurlar.

Hesab kitabxanası alqoritmləri, internet bankçılıq sistemlərində müştərilərin hesablarının idarə olunmasına və maliyyə əməliyyatlarının düzgün şəkildə aparılmasına kömək edir. Bu alqoritmlər, hesab məlumatlarının saxlanılması, əlavə edilməsi, dəyişdirilməsi və silinməsi proseslərini avtomatlaşdırır və təhlükəsizliyini təmin edir.

Tranzaksiya verifikasiyası alqoritmləri, internet bankçılıq sistemlərində həyata keçirilən maliyyə əməliyyatlarının doğrulama prosesinə kömək edir. Bu alqoritmlər, məsələn, müştərilərin əməliyyatlarının şifrələnməsi və təsdiqlənməsi, hesabların məxfilik məlumatlarının təhlükəsizliyinin təmin edilməsi və tranzaksiyaların güvənli şəkildə icrasını nəzərdə tutur.

Bu araşdırmada ilk olaraq daşınmaz əmlak əməliyyatlarındakı problemlərin diaqnozu qoyuldu. Bu problemləri aradan qaldırmaq üçün süni intellektin dizayn modeli olaraq Blockchain alqoritmi təqdim edildi. Bundan əlavə, bu tədqiqat tədqiqat modelləri və mühüm mühasibat kitabçası məlumatları təsvirinin korreksiyası və blokların yoxlanılması üçün Blockchain smart müqaviləsinin yaradılması üçün nəzərdə tutulmuşdur. Tələb olunan daşınmaz əmlak müqaviləsinin direktorunun müqayisəli yoxlanılması üçün Deep Belief şəbəkə alqoritmi də tətbiq edilmişdir. Buna görə də, məlumatların tutarlılığı düzəliş şəklinin yoxlanılması müqayisə alqoritmi ilə təsdiqləndi və daha sonra Blockchain razılaşma prosesi vasitəsilə Hyperledger-in praktiki Bizans qüsurlarına dözümlülük alqoritmini müqayisə etmək və yoxlamaq üçün qeyri-maddi tədqiqat quruldu. Sonradan daşınmaz əmlak müqaviləsinin yoxlanılması prosesi quruldu (Şəkil 3-ə baxın).

Risk idarəetmə alqoritmləri, internet bankçılıq sistemlərində məxfilik risklərinin və potensial maliyyə təhlükələrinin idarə edilməsinə yardımçı olur. Bu alqoritmlər, müştərilərin əməliyyat tarixini analiz edir, şübhəli və riskli əməliyyatları təhlil edir və hüquqi qaydalara əsaslanan risk qiymətləndirmələri aparır.



Şəkil 4.3.2. Tədqiqat planı

Bu işin məqsədi Blockchain-də ağıllı müqavilələr etmək üçün daha təhlükəsiz şifrələmə alqoritmindən istifadə etməkdir. Bu şifrələmə alqoritmləri ElGamal şifrələmə sistemi əsasında həyata keçirilir. Kvant biliyi sertifikatı üçün də faydalı ElGamal kommutasiyası təmin edilir. Bu, BLS (Sümük-Linn-Schacham) istifadə

edərək elliptik əyrinin bağlama xüsusiyyətlərindən istifadə edərək qısa imza tətbiq edir. O, həmçinin sertifikata əsaslanan texnologiyanı tətbiq etmək üçün daha sabit elastik əyri Qu-Vanstone (ECQV) sisteminin texnologiyasından istifadə edir. Bu ağıllı konturlar şifrələmədən sonra yaradılmış skript formatını VM-nin içərisinə yükləməyə imkan verir və proqramçıdan müstəqil işləməyə imkan verir. O, həmçinin daşınmaz əmlak müqavilələrinin yoxlanılması üçün şifrələmə kitabxanası API-lərini tətbiq edir ki, şifrələmənin həyata keçirilməsi üçün tələb olunan asılılıqlarla bağlı problemlər yaranmaması üçün onlar öz daxil edilmiş formalarında yerinə yetirilə bilsinlər. Bu tədqiqat bu daşınmaz əmlak müqavilələrini təsdiqləmək üçün əmlaka əsaslanan metodologiyadan və Blockchain-dəki bütün qovşaqların emitentə, sübutları təsdiqləmək üçün yoxlayıcıya və emitentə sübut təqdim etdiyinə dair sübut yaradan bir sahibdən ibarətdir. Sahibinin sertifikatı ola bilər, ardınca aşağıdakı məlumatların sübutu:

1. Etibarnamə
2. Etibarnamələr üçün açar cütü
3. Doğrulayıcı məlumat
4. Etibarnamənin nəticəsi
5. Doğrulayıcı məlumat nəticəsi

İnternet bankçılıq sistemlərdə tətbiqi alqoritmlər, məxfilik təhlükələrinin azaldılması və müştərilərə daha yüksək səviyyədə xidmət təqdim etmək üçün əhəmiyyətli rol oynayır. Bu alqoritmlər, müştərilərin hesablarını və maliyyə əməliyyatlarını idarəetməyə kömək edir və təhlükəsizlik, effektivlik və etibarlılığı təmin edir.

Kirayə blok zəncirinin mənbə kodunu ortaya qoyur. O, həmçinin smart müqavilənin daşınmaz əmlak kimi idxalını kəskinləşdirir və stil “əməliyyat” mənbə kodunu göndərir. Beləliklə, bu smart contract.java kodları açılır (bax şəkil 4).

Smart Contract.Java

```
import Smart Contract as Real Estate
RealEstate.set(style="transaction")
tips = RealEstate.load_dataset("tips")
 g = Real Estate.jointplot("total_bill", "tip",
            data=tips,  kind="reg",
                truncate=False,
            xlim=(0, 60), ylim=(0, 12),
            color="m", height=7)
```

```
V[0,0,0] = np.sum(X[:5,:5,:]  * W0) + b0 # np.dot(X[:5,:5,:],W0) + b0

V[1,0,0] = np.sum(X[2:7,:5,:] * W0) + b0

V[2,0,0] = np.sum(X[4:9,:5,:] * W0) + b0

V[3,0,0] = np.sum(X[6:11,:5,:]* W0) + b0
```

Şəkil 4.3.3. Ağıllı müqavilə mənbə kodu

İnternet bankçılıqda tətbiqi alqoritmlər, bank təşkilatları üçün də bir sıra faydalar ilə gəlir. Bu alqoritmlər, bankların əməliyyatlarını effektiv idarə etmək və potensial riskləri azaltmaq üçün istifadə edilir. Banklar, alqoritmlər vasitəsilə tranzaksiya verifikasiyasını, məxfilik pozuntularının aşkar edilməsini və məlumatlara əsaslanan risk qiymətləndirmələri apararaq daha səmərəli bir şəkildə işləyə bilirlər.

Tranzaksiya verifikasiyası alqoritmləri, bankların müştərilərinin əməliyyatlarını şifrələmək və doğrulamaq üçün istifadə etdiyi bir texnologiyadır. Bu alqoritmlər, əməliyyatların etibarlı şəkildə həyata keçirilməsini, identifikasiya və avtorizasiya proseslərini asanlaşdırmağa və həddindən artıq məxfilik təhlükələrini qarşılamağa kömək edir.

Məxfilik pozuntularının aşkar edilməsi, bank təşkilatlarının məlumatları və tranzaksiyaları izləyərək potensial dolandırıcılıq, kimlik hırsızlığı və digər məxfilik risklərini aşkar etmək üçün tətbiq etdiyi bir prosesdir. Bu məqsədlə, banklar

alqoritmlərdən istifadə edərək şübhəli əməliyyatları, anormal maliyyə hərəkətlərini və digər potensial riskləri təhlil edə bilirlər.

Tətbiqi alqoritmlər, internet bankçılıq sistemlərində istifadə olunan müxtəlif funksiyalar üçün məsələn, maliyyə hesab-kitabxanası idarəetməsi, tranzaksiya verifikasiyası, risk idarəetməsi, müştəri məlumatlarının idarə olunması və istifadəçi təcrübəsinin yaxşılaşdırılması kimi mühüm sahələrdə tətbiq olunur.

Maliyyə hesab-kitabxanası idarəetməsi alqoritmləri, bankların müştəri hesablarının idarə olunması və maliyyə əməliyyatlarının düzgün şəkildə aparılması üçün istifadə olunur. Bu alqoritmlər, müştəri hesab məlumatlarının avtomatik olaraq saxlanılması, əlavə edilməsi, dəyişdirilməsi və silinməsi proseslərini təşkil edir. Hesab-kitabxana alqoritmləri eyni zamanda hesab balansının və hesab məlumatlarının müştərilər tərəfindən real vaxtında izlənməsinə imkan verir.

Tranzaksiya verifikasiyası alqoritmləri, internet bankçılıq sistemlərində yerləşən maliyyə əməliyyatlarının doğrulama prosesinə kömək edir. Bu alqoritmlər, əməliyyatların şifrələnməsi, autentifikasiya və avtorizasiya proseslərinin icrası, məxfilik təhlükələrinin təhlil edilməsi və müştərilərin təsdiq proseslərinin avtomatik olaraq aparılması ilə məşğuldur.

Risk idarəetmə alqoritmləri, bankların məxfilik risklərini idarə etməyə kömək edərək. Bu alqoritmlər, müştəri əməliyyat tarixini analiz edir, şübhəli və riskli əməliyyatları aşkar edir və risk qiymətləndirmələri aparır. Buna əsasən, banklar məxfilik pozuntularını minimuma endirmək üçün tədbirlər görə bilir və potensial məxfilik təhlükələrinin qarşısını almaq üçün etibarlı bir risk idarəetmə sistemindən istifadə edir.

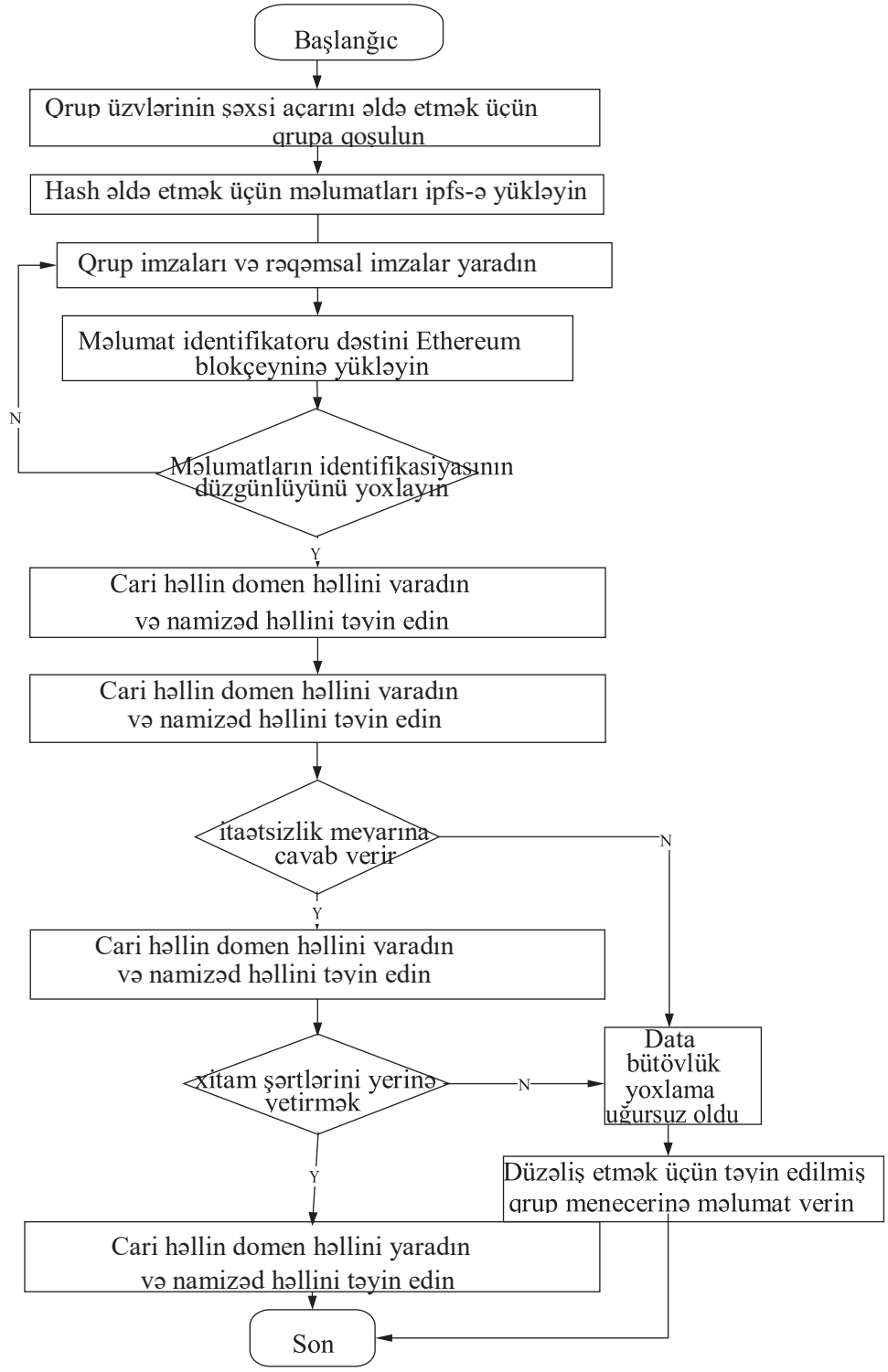
[5]İnternet bankçılıqda tətbiqi alqoritmlər eyni zamanda müştəri məlumatlarının idarə olunması üçün də əhəmiyyətli bir rol oynayır. Bu alqoritmlər, müştəri məlumatlarının saxlanılmasını, yenilənməsini və təhlükəsizliyini təmin edir. Müştərilərin şəxsi məlumatları, bank hesab nömrələri, əlaqə məlumatları və digər məlumatlar, alqoritmlər vasitəsilə mühafizə olunur. Bu, müştərilərə məxfilik və gizlilik təminatı verir və potensial məlumat sızıntılarına qarşı önəmli bir təhlükəsizlik tədbiri kimi xidmət edir.

Son olaraq, internet bankçılıqda tətbiqi alqoritmlər müştərilərə daha yüksək səviyyədə xidmət təqdim etmək üçün bir sıra imkanlar yaradır. Bu alqoritmlər, müştərilərə mobil tətbiqlər vasitəsilə istədikləri zaman və yerlərdə bank əməliyyatlarını icra etmə imkanı verir. Bu, müştərilərə hər hansı bir cihazdan bank hesablarına giriş, əməliyyatlarını idarə etmə və maliyyə statistikasına çatma imkanı verir. Böyleliklə, müştərilər bankla əlaqədə olmaq üçün fərqli kanallardan istifadə edə bilir və daha çox rahatlıq və əlçatanlıq hissi yaşayır.

4.4. İstifadəçi məxfiliyinin alqoritminin işlənməsi

IoT istifadəçilərinin şəxsiyyətinin autentifikasiyasını və IoT istifadəçi məxfilik məlumatlarının saxlanma üsulunu təqdim etdikdən sonra biz əsasən IoTuser məxfilik məlumatlarının bütövlüyünün yoxlanılmasını və istifadəçi məxfiliyinin necə təmin olunacağını təhlil edirik və ətraflı iş axını diaqramı Şəkil 3-də göstərilmişdir.

5. [5] L. O'Gorman, "Seven issues with human authentication technologies," in Workshop Automatic Identification Advanced Technologies (AutoID), 2002, pp. 185–186.



Şəkil 4.4.1. Blockchain əsaslı istifadəçi məxfilik məlumatlarının bütövlüyünün yoxlanılması prosesi

Bu, protokolun etibarlılığını gücləndirir və istifadəçilərin məxfiliyinin qorunmasına zəmanət verir. Bu araşdırmada təklif olunan çoxfaktorlu yüngül anonim şəxsiyyət identifikasiyası protokolunda istifadəçi mobil cihazın

şəxsiyyətinin legitimliyini yoxlamaq üçün əvvəlcə şəxsi biometrik şablonu daxil etməli, sonra isə yalnız ən yaxın autentifikasiya qovşağına tam hesablama aparmalıdır.

Son olaraq, blokchain alqoritmləri ilə internet bankçılıq sistemlərində məxfilik təhlükələrinin azaldılması mövzusu, günümüzün texnologiya dünyasında ardıcıllığı artan bir sahədir. Həm bank təşkilatları, həm də müştərilər, blokchainin potensial tətbiqindən maksimum fayda götürmək üçün bu texnologiyaların ətraflı şəkildə araşdırılması və tətbiq edilməsinə ehtiyac duyurlar. Bu dissertasiya işi, internet bankçılıqda blokchain alqoritmlərinin əhəmiyyətini, tətbiq edilə biləcəyi prosesləri və məxfilik üçün gələcəkdəki potensial faydalarını aydın şəkildə təsvir edir.

Cədvəl 4.4.2-dəki sorğunun nəticələrinə görə, bizim təklif etdiyimiz sxem digər blokçeyn əsaslı sxemlərlə müqayisədə məlumatların səmərəli saxlanmasına əsaslanan ehtimal edilən hücumların qarşısını ala bilər. Digər üsullarla müqayisədə bizim metodumuz istifadəçi məxfiliyini üzə çıxarmadan məlumatların dəyişdirilməsinin qarşısını ala bilər, IoT istifadəçiləri məlumatlara sahibdirlər və ağıllı müqavilələrin dəstəklənməsi sistemin təkmilləşdirilməsi üçün daha çox yer olması deməkdir. Cədvəldə “Y” və “N” müvafiq olaraq məmnunluq və narazılığı, “L” sxemin müəyyən performans qüsurlarının olduğunu, “H” sxemin səmərəli olduğunu, “M” isə metodun mümkün olduğunu göstərir. ; hələ də təkmilləşdirmə üçün yer var.

Cədvəl 4.4.2

Qrup	Fırıldaqçılığın qarşısının alınması	Tamper sübutu	İzlənilə bilən	AntiReplay
1	Y	47.2	0.82	H
2	Y	55.3	0.92	H
3	Y	50.5	0.84	L
4	N	58.3	0.92	L
5	N	52.2	0.82	M
6	N	61.2	0.92	M
7	N	62.1	0.94	H
8	N	55.6	0.82	L
9	Y	65.9	0.94	L
10	Y	79.0	0.91	M
11	N	60.3	0.82	M
12	Y	75.4	0.94	H
13	N	78.7	0.74	111.5

NƏTİCƏ

I fəsildə biometrik tanınma mexanizmlərinin müxtəlif növlərinin effektivlik səviyyəsi təyin edilməklə biometrikanın tətbiqi ilə cinayətkarlığın qarşısının alınmasının üsul və vasitələri araşdırılmış, biometrika və mobil bankçılıq üzrə tədqiqat obyekti təyin edilmiş, tətbiqi Casus proramları əsasında biometrik mobil bankçılıq sisteminin axın alqoritmi işlənmişdir.

II fəsildə biometrik doğrulama və multi hesablı ATM kartları ilə təkmilləşdirilmiş bankçılıq sistemi tədqiq edilməklə biometrik metodologiyanın prosesləri araşdırılmış, maliyyə təşkilatlarında biometrik doğrulama prosesi tədqiq edilmiş, biometrik doğrulama axın diaqramı quruulmuş və MFA tətbiqli alqoritm işlənmişdir.

III fəsildə İnternet bankçılıq sistemində üçlaylı təhlükəsizik sistem axını araşdırılmış, çoxfaktorlu autentifikasiya alqoritmi qurulmuş və kriptovalyutaların ümumi bazar dəyəri araşdırılmışdır.

IV fəsildə internet bankçılıq sistemində tətbiqi alqoritmlər, məxfilik təhlükələrinin azaldılması araşdırılmış və nəticədə tətbiqi alqoritmlərdən istifadə edilməklə risklərin qiymətləndirilməsi və tranzaksiyaların təyin edilməsi prosesinin tətbiqi göstərilmişdir.

Ümumiyyətlə, dissertasiya işində İnternet bankçılıq sistemində istifadəçi məxfiliyinin təmin edilməsində və eləcə də bank təhlükəsizliyi probleminin həllində ödəniş təhlükəsizliyi və problemləri müəyyən edilməklə mövcud təhlükəsizlik həlləri araşdırılaraq təhlil edilmiş, biometrik dizaynın istifadəçi ilə bank arasında təhlükəsizlik səviyyəsinin artdığı müəyyən edilmişdir.

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT

1. F.-M. E. Uzoka and T. Ndzinge, “Empirical analysis of biometric technology adoption and acceptance in Botswana,” J. Syst. Softw., vol. 82, no. 9, pp. 1550– 1564, 2009.
2. J. Munilla and A. Peinado, “HB-MP: A further step in the HB-family of lightweight authentication protocols,” Comput. Networks, vol. 51, no. 9, pp. 2262–2267, 2007.
3. L. O’Gorman, “Seven issues with human authentication technologies,” in Workshop Automatic Identification Advanced Technologies (AutoID), 2002, pp. 185–186.
4. J. Y. L. Thong and C. S. Yap, “Information technology adoption by small business: An empirical study,” in Diffusion and adoption of information technology, Springer, 1996, pp. 160–175.
5. S. S. Alam and M. K. M. Noor, “ICT Adoption in Small and Medium Enterprises : an Empirical Evidence of Service Sectors in Malaysia,” Int. J. Bus. Manag., vol. 4, no. 2, pp. 112–125, 2009.
6. E. E. Grandon and J. M. Pearson, “Electronic commerce adoption: An empirical study of small and medium US businesses,” Inf. Manag., vol. 42, no. 1, pp. 197–216, 2004.
7. Murdoch, S. J. “Reliability of chip & PIN evidence in banking disputes”. Digital Evidence and Electronic Signature Law Review, vol. 6, Pario Communications, pp. 98-115 [Nov, 2010].
8. Drimer, S., Murdoch, S.J. “Keep your enemies close: Distance bounding against smartcard relay attacks”. In: USENIX Security Symposium [Aug, 2007].
9. Anderson, R.J., Needham, R.M. “Robustness principles for public key protocols”, CRYPTO 1995. LNCS, vol. 963, pp. 236–247 [1995].

10. Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Comput. Secur. 2011, 30, 208–220.
11. February 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 405–421. 6. Kim, J.J.; Hong, S.P. A method of risk assessment for multi-factor authentication. J. Inf. Process. Syst. 2011, 7, 187–198. [CrossRef] 7. Sinha, A.; Shrivastava, G.; Kumar, P. A Pattern-Based Multi-Factor Authentication System. Scalable Comput. Pract. Exp. 2019, 20, 101–112.