Метод Ідентифікації в Безконтакних Платежах

Олег Золотухін
кафедра штучного інтелекту
Харківський національний університет
радіоелектроніки
Харків, Україна
oleg.zolotukhin@nure.ua

Олексій Лановий
кафедра програмної інженерії
Харківський національний університет
радіоелектроніки
Харків, Україна
oleksiy.lanovyy@nure.ua

The Method of Identification in Contactless Payments

Oleg Zolotukhin
Artificial Intelligence Department
Kharkiv National University
of Radio Electronics
Kharkiv, Ukraine
oleg.zolotukhin@nure.ua

Oleksiy Lanovyy
Software Engineering Department
Kharkiv National University
of Radio Electronics
Kharkiv, Ukraine
oleksiy.lanovyy@nure.ua

***Анотація*—Даному електронному документі є опис метода для підвищення ефективності ідентифікації та безпеки платежів у системах безконтактних платежів за рахунок вдосконалення методу ідентифікації клієнтів в частині біометричної ідентифікації та геолокації користувача.**

***Abstract*—This electronic document describes a method for increasing the efficiency of identification and security of payments in contactless payments systems by improving the method of identifying clients in terms of biometric identification and user geolocation.**

Ключові слова— система безконтактних платежів, геолокація, біометрична ідентифікація, метод ідентифікації безконтактних платежів, NFC.

Keywords— contcless paymentt system, geolocation, biometric identity, method of free contact network identification, NFC.

I. Вступ

Система електронних платежів - це спеціалізована інформаційна система безготівкових розрахунків, укладання контрактів і переказу грошей між продавцями і покупцями, банками і їх клієнтами за допомогою засобів електронної комунікації для здійснення взаєморозрахунків у мережі Інтернет із застосуванням засобів кодуванні інформації та її автоматичної обробки.

Масове поширення в світі банківських карт в розрахунках, платежах, кредитних відносинах доводить, що використання цього банківського інструменту істотно спрощує взаємини продавців і покупців товарів, робіт, послуг, зняття з рахунків фізичних осіб готівкових коштів.

Підвищення ефективності економіки багато в чому залежить від організації платіжних систем, їх надійності та зручності для всіх учасників ринку. Країни, зацікавлені в прозорості фінансових потоків (зокрема, роздрібної торгівлі, громадського харчування, транспорту), зниженні витрат платіжної системи, зростанні споживчого кредиту та розвитку роздрібної банківської мережі, зазвичай прагнуть розвинути систему розрахунків банківськими картами, включаючи спеціальні заходи для скорочення сфери готівкових розрахунків .

Разом з платіжними системами розвиваються і технології забезпечення їх безпеки. Оскільки на сьогоднішній день жодна електронна платіжна система не може існувати без хороших технологій і систем безпеки, які в свою чергу забезпечують безпечну транзакцію грошових операцій, проблема безпеки і підвищення рівня вимог з безпеки є актуальними. Так як інтернет одночасно є і надзвичайно ефективним комунікативним засобом і середовищем, що викликає досить велика недовіра у користувачів, безпеку електронних платежів є досить серйозним критерієм успіху конкретної системи і використовує її електронного бізнесу. Важливо, щоб при будь-якої реалізації в системі не залишалося погано захищених ділянок, здатних привести до великомасштабного шахрайства.

II. Опис методу

Пропонується використання біометричної ідентифікації - процес доказу і перевірки автентичності через пред'явлення користувачем свого біометричного образу і шляхом перетворення цього образу відповідно до заздалегідь визначених протоколом аутентифікації. Біометричні системи аутентифікації - системи аутентифікації, що використовують для посвідчення особи людей їх біометричні дані, тому що кожна людина володіє унікальними вимірюємими характеристиками.

Біометричні системи складаються з двох частин: апаратних засобів і спеціалізованого програмного забезпечення. Апаратні засоби включають в себе біометричні сканери і термінали. Вони фіксують той чи інший біометричний параметр (відбиток пальця, райдужну оболонку очей, рисунок вен на долоні або пальці, ДНК, голос) і перетворять отриману інформацію в цифрову модель, доступну для комп'ютера. А програмні засоби ці дані обробляють, співвідносять з базою даних і визначають, авторизований клієнт знаходиться перед сканером чи ні.

В якості методів, пропонованих в якості удосконалення процедури ідентифікації, пропонується, крім основних і додаткових методів, використовувати методи ідентифікації за становищем і методи біометричної ідентифікації.

Пропонується використовувати наступні методи:

− ідентифікація по фотографії - метод біометричної ідентифікації. Під час здійснення платежу з додатком необхідно надати фотокартку особи користувача. Цю фотографію аналізують нейронні мережі та набір алгоритмів для визначення параметрів особи. В результаті оцінки виходить ймовірність того, що людина, яка робить платіж, є власником карти. Для цього попередньо потрібно зробити кілька знімків особи власника картки під час реєстрації в платіжній системі.

Метод має обмеження:

а) не використовується перевірка властивостей, які можуть бути вкрадені під час перевірки, наприклад, PIN код може бути підглянут;

б) недосконаліть алгоритмів обробки і аналізу особи по фотографії. На даний момент для того, щоб точно визначити по фотографії, чи є людина власником карти, чи ні, необхідно провести складні і «важкі» обчислення, навантажуючи процесор мобільного пристрою, витрачаючи багато енергії акумулятора мобільного пристрою, а також тривалий час на якісну обробку;

в) особу просто «підробити». Зловмисник може поставити фотографію власника карти перед камерою мобільного пристрою в момент скоєння фінансової транзакції, і на поточному рівні розвитку мобільних пристроїв буде дуже складно або навіть неможливо визначити ідентифіковану особистість;

− ідентифікація по ході - метод біометричної ідентифікації. У фоновому режимі мобільний пристрій, з якого здійснюються платежі, відстежує дані з датчиків прискорення (акселерометрів). Ці дані зберігаються в одному великому масиві. Після з цього масиву за допомогою статистичних методів рядів Фур'є відбувається виділення патернів ходи власника карти. У момент скоєння фінансової транзакції мобільний пристрій бере дані з акселерометрів за останні дві хвилини і звіряє їх з існуючими довіреними паттернами. На підставі цього виходить імовірнісна оцінка того, що останні дві хвилини телефон був у руках у свого власника, відповідно саме він і робить платіж.

Метод не вимагає ніяких дій від користувача. Для оплати необхідно лише піднести телефон до терміналу. У цьому методі не використовується перевірка властивостей, які можуть бути вкрадені під час перевірки. Наприклад, PIN код може бути підглянут. Дані акселерометрів дуже складно підробити через відмінності в анатомії двох будь-яких людей. І навіть якщо вдасться підібрати потрібні параметри, то це буде дуже складно для крадіжки одного телефону, і майже неможливо для систематичних крадіжок. Не дає хибно позитивних результатів.

Метод має недоліки. Через постійне відстежування даних акселерометра відбувається постійний розряд батареї пристрою, що негативно позначається на тривалість періоду, після і стан батареї.

Незважаючи на те, що метод не дає помилково позитивних результатів, метод дуже часто дає помилково негативні результати, через що його дуже складно застосовувати як основний метод ідентифікації. Як правило, його застосовують у сукупності з іншими методами. Наприклад, з перевіркою PIN коду застосовують тоді, коли оцінка ходи вказує, що платіж виконує не власник карти;

− ідентифікація за даними про пересування - метод ідентифікації за становищем (геолокація). У фоновому режимі мобільний пристрій, з якого здійснюються платежі, відстежує дані про переміщення власника пристрою за допомогою отримання даних з датчиків системи глобального позиціювання GPS (Global Positioning System), а також отримання ідентифікаторів всіх найближчих WI-FI точок. Ці дані зберігаються в одному великому масиві. Після цього за допомогою різних методів, наприклад, методів машинного навчання або простого статистичного аналізу, визначаються патерни переміщення людини в залежності від часу доби і дня тижня. На підставі цих даних можна визначити ймовірність того, що власник карти буде здійснювати фінансову транзакцію в даному місці, в даний час доби, на дану суму. На підставі цього можна оцінити в момент скоєння користувачем фінансової транзакції, ймовірність того, що людина, яка виконує платіж є власником мобільного пристрою.

Для користувача платіжної системи недоліки відсутні. Недоліки практично відсутні для банку-клієнта платіжної системи. Єдині недоліки - необхідність використання спеціально розробленого програмного забезпечення разом

з навченими операторами, перевіряючими підозрілі транзакції.

На основі дослідження існуючих систем безконтактних електронних платежів: Google Pay, Apple Pay, Samsung Pay, MasterCard Contactless визначені характеристики, переваги та критичні недоліки систем у вигляді рекомендацій вибору конкретного рішення.

Процес ідентифікації складається реєстрації користувача в відділенні банку-клієнта системи MasterCard Contactless, установки платіжного додатка користувачем на мобільний пристрій, спостереження за користувачем платіжної системи і збір масиву ідентифікуючої інформації, обчислення ймовірнісної оцінки ідентифікації користувача в момент вчинення ним платежу за допомогою безконтактної системи.

Таким чином, перевагами і вдосконаленнями запропонованого методу ідентифікації користувача є наступні:

− отримуючи від терміналу тип платежу (інформацію, чи потрібно його підтверджувати паролем чи ні, надає банк клієнту, на підставі зібраної раніше інформації про попередні транзакції і переміщеннях користувача), тобто виконується перевірка на серверній стороні.

Якщо сервер на підставі зібраної інформації вимагає пароль, - однозначно запитується пароль у користувача.

Якщо сервер не вимагає пароля, додаток вирішує, чи потрібно запитувати у користувача пароль на підставі вже своїх даних.

− якщо додаток приймає рішення, що користувач ідентифікований правильно, тоді програма не запитує пароль і просто робить платіж, інакше, - вимагає пароль.

Ухвалення рішення про ідентифікацію користувача здійснюється наступним чином:

1) звіряються дані про дату, суму, місці поточного платежу, перелік оточуючих wifi точок з даними, накопиченими в пункті 3 Підготовчий етап (збір даних для ідентифікації).

Визначаємо ймовірність того, що користувач авторизований, інакше запитується пароль.

2) Якщо користувач пройшов перевірку пункту 1, перевіряються дані за останні дві хвилини з його акселерометрів.

Звіряються з даними з пункту 3 «Спостереження за користувачем платіжної системи і збір масиву ідентифікуючої інформації».

3) Якщо п.1 та п.2 пройдені з імовірністю більше 95%, то здійснюється платіж без пароля.

III. Висновки

Виявлення та протидія шахрайським операціям−одна з ключових завдань всіх міжнародних платіжних систем. Безпека онлайн-платіжних транзакцій відстежується безліччю систем на різних рівнях і етапах проходження платежу.

На сьогоднішній день з використанням безконтактної технології платіжні технології мають безліч переваг, серед яких інноваційність, оперативність здійснення платежів, простота, зручність, швидкість проведення операцій, значна економія часу, зниження черг і, в результаті використання модифікації методу ідентифікації платежів, більш високий рівень безпеки проведення операцій, зниження злочинності.

Запропонована в роботі система безконтактних електронних платежів дозволяє підвищити ефективність роботи більшості сучасних телефонів і планшетів, оснащених NFC адаптерами, з можливістю швидкого обміну контентом і безконтактної оплати послуг.

Актуальність завдання обумовлена гнучкістю використання даної технології, сумісністю з різними пристроями, спрощення процесів оплати, що сприяють підвищенню привабливості впровадження даної технології банками.

Актуальність завдання обумовлена гнучкістю використання даної технології, сумісністю з різними пристроями, спрощення процесів оплати, що сприяють підвищенню привабливості впровадження даної технології банками.

Література References

[1] MasterCard Cloud-Based Payments Product Description, MasterCard Digital Enablemet Service, 2015.

[2] M. Kulkarni, "SamsungPay Payment Method", Maheshkk.github.io, 2018. [Online]. Available: https://maheshkk.github.io/webpayments/proposals/ SamsungPay-payment-method.html. [Accessed: 18- Jul- 2018]. Android Pay XML Integration Guide

[3] MasterCard Cloud-Based Payments Credential Managment System Functional Description, MasterCard Digital Enablemet Service, 2015.

[4] *Contactless integrated circuit cards*, ISO Standard IEC_14443-2011, 2011 року.

[5] MasterCard Cloud-Based Payments Issuer Cryptographic Algorithms Specification, MasterCard Digital Enablemet Service, 2015.

[6] V. Filatov, D. Rudenko and E. Grinyova, "Means of integration of heterogeneous data corporate information and telecommunication systems," Proceedings of the 24th Intern. Crimean Conference Microwave and Telecommunication Technology CriMiCo., 7-13 sept. 2014 року, Sevastopol, Ukraine, pp. 399-400.