Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)
Кафедра Штучного інтелекту
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Створення інтелектуального web-сервісу для діагностики банківських транзакцій у середовищі інтернет магазину
(тема)

Виконав:
студент 2 курсу, групи СШІм-22-1
Лизогубов М.В.
(прізвище, ініціали)

Спеціальність 122 Комп'ютерні науки
(код і повна назва спеціальності)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Системи штучного інтелекту
(повна назва спеціалізації)
Керівник доц. Золотухін О.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ В.О. Філатов
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Штучного інтелекту
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системи штучного інтелекту
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____» _____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Лизогубову Микиті Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Створення інтелектуального web-сервісу для діагностики банківських транзацій у середовищі інтернет магазину

затверджена наказом університету від 1 квітня 20 24 р. № 260Ст
2. Термін подання студентом роботи до екзаменаційної комісії 7 червня 20 24 р.
3. Вихідні дані до роботи Науково-технічні публікації та дані статей щодо технології побудови системи для захисту банківських транзакцій, результати експериментальних досліджень по технологіям, методам, моделям

4. Перелік питань, що потрібно опрацювати в роботі
1) Вступ, мета роботи та постановка задачі, визначення систем банківського захисту
2) Теоретичні дослідження
3) Аналіз технологій та засобів реалізації для побудови сервісу

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання на кваліфікаційну роботу	01.04.2024	виконано
2	Анализ предметної галузі та постановка задачі	10.04.2024	виконано
3	Теоретичні дослідження	20.04.2024	виконано
4	Проектування веб-додатку	30.04.2024	виконано
5	Розробка методу захисту	10.05.2024	виконано
6	Підготовка пояснювальної записки	31.05.2024	виконано
7	Попередній захист кваліфікаційної роботи	05.06.2024	виконано
8	Захист перед ЕК	12.06.2024	

Дата видачі завдання 1 квітня 2024 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Золотухін О.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 81 сторінку, 19 малюнки, 5 таблиць, 18 джерел.

WEB-СЕРВІС, БАНКІВСЬКА ТРАНЗАКЦІЯ, ІНТЕРНЕТ-МАГАЗИН, ЗАХИСТ ІНФОРМАЦІЇ, ІНТЕЛЕКТУАЛЬНА СИСТЕМА.

Метою кваліфікаційної роботи є аналіз технологій та методів побудови Web-сервісів; застосування даних технологій практично, створення інтелектуального Web-сервісу діагностики банківської транзакції серед інтернет-магазину.

Об'єктом дослідження є предметна область, яка охоплює розробку семантичних Web-сервісів та конкретних методів створення Web-сервісів.

Результатом дослідження є розробка захищеного Web-сервісу за допомогою технології PHP.

ABSTRACT

Master`s thesis contains: 81 pages, 19 figures, 5 tables, 18 sources.

WEB SERVICE, BANK TRANSACTION, INTERNET SHOP, INFORMATION PROTECTION, INTELLIGENT SYSTEM.

The purpose of the Master`s thesis is the analysis of technologies and methods of building Web services; practical application of these technologies, creation of an intelligent Web service for bank transaction diagnostics among online stores.

The object of research is a subject area that covers the development of semantic Web services and specific methods of creating Web services.

The result of the research is the development of a protected Web service using PHP technology.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛОВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SOAP - SIMPLE OBJECT ACCESS PROTOCOL;

XML RPC – EXTENSIBLE MARKUP LANGUAGE REMOTE PROCEDURE CALL;

WSDL – WEB SERVICES DESCRIPTION LANGUAGE;

UDDI – UNIVERSAL DESCRIPTION DISCOVERY & INTEGRATION;

DF – DETECT FRAUD;

CVV2 – CARD VERIFICATION VALUE 2

BIN – BANK IDENTIFICATION NUMBER

VBV – VERIFIED BY VISA.

ВСТУП

В даний час система захисту банківської інформації є популярною темою, оскільки щодня з карток користувачів списуються величезні суми без їхньої участі. Знайти і повернути гроші практично неможливо, оскільки шахраї користуються різними системами анонімності, а банки та інтернет-магазини зазнають величезних збитків.

Залишається безліч способів отримання конфіденційної інформації банківських систем. Тому не можна обгородити звичайного користувача кредитної картки від потрапляння особистої інформації в чужі руки; потрібен сервіс який зміг би розпізнавати та визначати ймовірність того, що транзакція є не шахрайською, ґрунтуючись на різних факторах.

Але, як і в реальному житті, в системі захисту інформації існує жорстка конкуренція, не програти в якій допомагає постійне вдосконалення системи, виходячи від методів шахраїв. Так само слід з обережністю ставиться до визначення програм анонімності, невміле їх обчислення може згубно позначитися на всьому сервісі і, як наслідок, сервіс працюватиме некоректно.

Шахрайство з платіжними картками, кардинг(від англ.carding) - виглядшахрайства, при якому проводиться операція з використаннямплатіжної карткиабо її реквізитів, не ініційована чи не підтверджена її власником. Реквізити платіжних карток, як правило, беруть зі зламаних серверівінтернет-магазинів,платіжнихта розрахункових систем, а також з персональних комп'ютерів (або безпосередньо, або черезпрограми віддаленого доступу, «трояни», «боти» з функцією формграбера). Крім того, найпоширенішим методом викрадення номерів платіжних карток на сьогодні єфішинг(англ.phishing, спотворене "fishing" - "рибалка") - створення шахраямисайту, який буде користуватися довірою у користувача, наприклад, сайт, схожий на сайт банку користувача, через який і відбувається викрадення реквізитів.платіжних карток.

Вкрадена або втрачена карта може використовуватися злочинцями лише доти, доки власник не повідомить свого банку про зникнення або в офлайнових операціях. Більшість банків надають цілодобову телефонну лінію для таких повідомлень.

Основним захисним заходом є наявність підпису на карті та вимога підписування чеків. У деяких магазинах при оплаті карткою потрібне надання документів, що засвідчують особу. Проте вимога документа в деяких юрисдикціях є незаконною.

Викрадені картки можуть використовуватися в деяких терміналах самообслуговування, які не потребують введення PIN-коду. У Європі більшість карток оснащені чіпом, який зазвичай запитує введення 4-значного цифрового PIN-коду при здійсненні покупок. Якщо код не зберігався разом із вкраденою картою, то шахрай зможе використовувати її лише в операціях, де код не потрібен, наприклад, в онлайнових (електронних) транзакціях, або в POS-терміналах, оснащених тільки зчитувачем магнітної смуги.

Існують програмні системи та комплекс організаційних заходів, спрямованих на запобігання чи ускладнення можливих шахрайських операцій. Наприклад, велика транзакція, здійснена далеко від місця проживання власника — як варіант — в іншій країні, може бути визнана такою, що не відбулася або навіть призвести до тимчасового блокування карти.

На початку 2010-х у США із 5,6 мільярдів дійсних банківських карток, лише близько 20 мільйонів є смарт-картками (містять чіп). За період із 2007 по 2011 рік секретна служба США заарештувала понад 5 тисяч злочинців, замішаних у скіммінгу. Втрати за 2012 рік оцінюються в 11,3 млрд. доларів. У рік у країні виявляють близько 20 тисяч скімерів.

У Великій Британії з 2005 по 2020 роки шахрайство з пластиковими картками призводило до втрат у 300—900 млн фунтів щорічно. Значна частка злочинів здійснювалася за даними карти в операціях, у яких не потрібне пред'явлення картки (наприклад, покупка через Інтернет). Втрати від скіммінгу, що становили щорічно від 100 до 170 мільйонів фунтів у 2001-2008 роках, значно

знизилися в 2010-2011 роках, до 47-36 мільйонів фунтів завдяки широкому впровадженню чіпованих карт і чіпів з підтримкою iCVV і DDA.

Метою даної роботи є розробка інтелектуальної системи захисту Detect Fraud для зниження кількості зворотних платежів, розпізнаючи замовлення групи ризику та зупиняючи їх до подальшого розгляду. Цей проект орієнтований на захист банківської інформації при використанні інтернет-магазинів.

Актуальність даної роботи виявляється у тому, що кожен день інтернет магазини та банки втрачають гроші через дії шахраїв і для того, щоб обмежити помилкові платежі, необхідно створити оптимальний сервіс для розпізнавання шахрайської діяльності в електронно-комерційних транзакціях, партнерських посиланнях, опитуваннях, входах у систему, інтернет-магазинах, соціальних мережах та реєстраціях.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Розробка Web-сервісів

Архітектура Web-сервісів є однією з реалізацій сервіс-орієнтованої архітектури (SOA).

Концепція Web-сервісіввиникла ще наприкінці 90-х років XX ст. Однак зараз ця концепція встигла встоятись і архітектура, яку вона пропонує, стала галузевим стандартом у сфері IT. Стандартизацією архітектури Web-сервісів займаються робочі групи комітету W3C [1]. Вони пропонують таке визначення поняття «Web-сервіс»: Web-сервіс – це система, що реалізується програмними засобами для підтримки міжмашинної взаємодії через мережу. Інтерфейс сервісу описується машинозрозумілою мовою, наприклад, WSDL.

Інші системи взаємодіють з Web-сервісом способом, зазначеним у його описі, використовуючи повідомлення у стандарті SOAP, що передаються з використанням HTTP та XML та у поєднанні з іншими стандартами, що стосуються Web. Фізично Web-сервіс є фрагментом програмного забезпечення, званий «агентом». Агент здатний передавати та приймати повідомлення, він реалізує функціональність сервісу.

Існує різницю між агентом і сервісом – той самий сервіс може бути забезпечений різними агентами. Механізм обміну повідомленнями визначається описі сервісів (Web Services Description), що є специфікацію інтерфейсу сервісу і охоплює формати повідомлень, типи даних, транспортні протоколи, способи серіалізації, використовувані під час обміну між агентами замовника і постачальника послуг.

Web-сервіс – будь-яка служба, яка доступна в Інтернеті, використовує стандартизований XML обмін повідомленнями системи, і не пов'язаний з жодною операційною системою або мовою програмування. Загальна схема роботи Web-сервісів представлена рисунку 1.1.

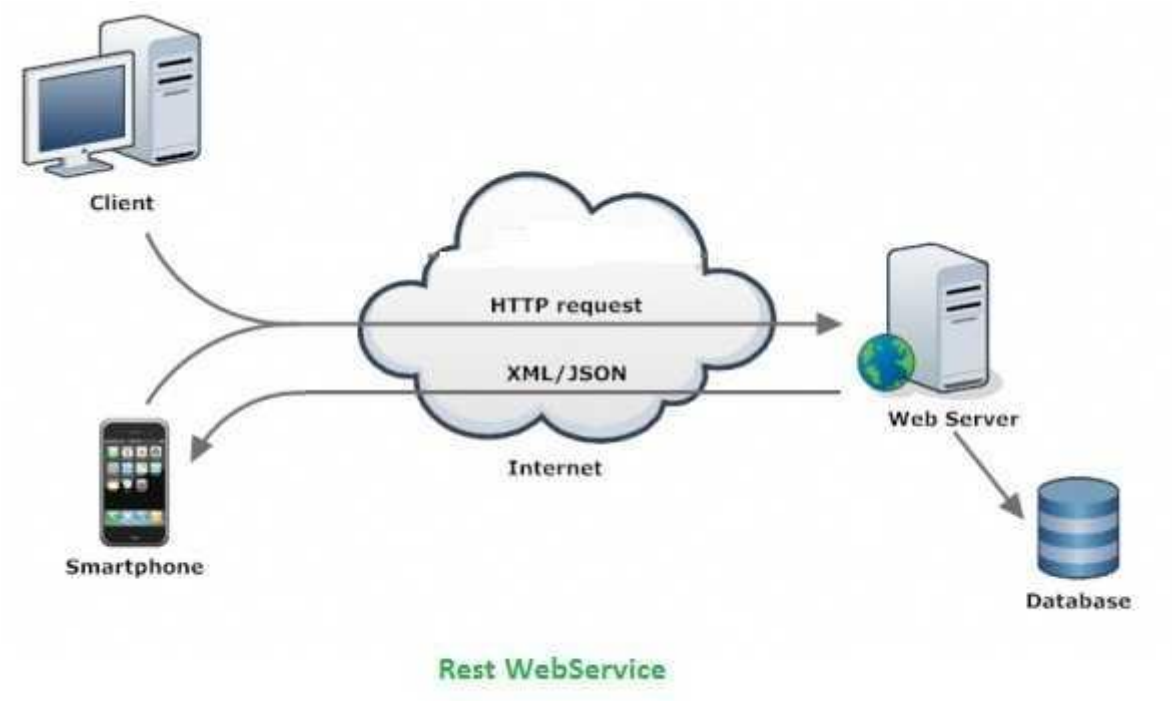

Рисунок 1.1 – Загальна схема роботи Web-сервісу

Web-сервісу необхідно мати дві необхідні властивості.

Web-сервіс повинен мати функцію самоописання. Якщо публікується новий Web-сервіс, він має бути відкритий для служби інтерфейс. Служба повинна включати документацію, що читається так, щоб інші розробники могли інтегрувати цю службу. Граматика XML може використовуватися, щоб ідентифікувати всі відкриті методи, параметри методу, і значення, що повертаються [2].

Web-сервіс має бути легко доступним. Якщо створюється Web-сервіс, то він повинен мати простий механізм подальшої публікації, а також механізм, за допомогою якого зацікавлені сторони можуть знайти службу та визначити розташування її відкритого інтерфейсу. Точний механізм може бути здійснений через повністю децентралізовану систему чи логічно централізовану систему реєстру.

Переваги Web-сервісів:

- web-сервісизабезпечують взаємодію програмних систем незалежно від платформи;

- web-сервіси засновані на базі відкритих стандартів та протоколів, завдяки використанню XML досягається простота розробки та налагодження Web-служб;

- використання інтернет-протоколу забезпечує HTTP-взаємодія програмних систем через міжмережевий екран.

Недоліки Web-сервісів:

- менша продуктивність та більший розмір мережевого трафіку в порівнянні з технологіями RMI, CORBA, DCOM за рахунок використання текстових XML-повідомлень, проте на деяких Web-серверах можливе налаштування стиснення мережного трафіку;

- сервіси передають дані у форматі SOAP/WDDX/XML, що потребує деякого додаткового програмування для розпакування даних;

- з'єднання з сервісами може становити проблему у разі наявності проксі-сервера.

PHP (англ. PHP: Hypertext Preprocessor – «PHP: препроцесор гіпертексту», англ. Personal Home Page Tools – «Інструменти для створення персональних Web-сторінок») – скриптова мова програмування загального призначення, що інтенсивно застосовується для розробки Web-додатків. В даний час підтримується переважна більшість хостинг-провайдерів і є одним з лідерів серед мов програмування, що застосовуються для створення динамічних сайтів.

В області програмування для Web PHP – одна з найпопулярніших скриптових мов (поряд з JSP, Perl та мовами, що використовуються в ASP.NET) завдяки своїй простоті, швидкості виконання, багатої функціональності, кросплатформенності та поширенню вихідних кодів на основі ліцензії PHP.

Популярність у галузі побудови сайтів визначається наявністю великого набору вбудованих засобів для розробки Web-додатків. Основними є:

- автоматичне вилучення POST та GET-параметрів;

- файлові функції успішно обробляють як локальні, так і видалені файли;

- автоматичне відправлення HTTP-заголовків;

- робота з cookies та сесіями;

- обробка файлів, що завантажуються на сервер;
- робота з HTTP заголовками та HTTP авторизацією;
- робота з XForms;
- робота з віддаленими файлами та сокетами.

1.2 Стандарти створення Web-сервісів

На сьогоднішній день існує безліч стандартів створення Web-сервісів. Найпопулярнішими є XML RPC, SOAP, WSDL, UDDI.

XML RPC. XML RPC є механізмом, заснованим на XML і HTTP, для створення методів або віддаленого виклику функцій через мережу. XML RPC пропонує набір інструментів для того, щоб з'єднати системи та для того, щоб опубліковувати машинозрозумілу інформацію. XML RPC дозволяє програмам виконувати функції або виклики процедур через мережу. XML RPC використовує протокол HTTP для передачі інформації від клієнтського комп'ютера до сервера, описуючи запити та відповіді на мові XML.

Дві основні складові XML RPC повідомлення – це методи та параметри. Параметри можуть бути різного типу: рядки, цілі числа, масиви. Крім того, у XML RPC визначено інші теги для різних цілей, таких як обробка помилок.

У XML RPC спілкування між двома системами починається із запиту (request) від XML RPC-клієнта, якому сервер надсилає відповідь (response). Запит містить назву методу та необхідні параметри. У відповіді виводиться набір параметрів, в яких і містяться дані, що запитуються. Весь процес дуже нагадує використання функцій у PHP-скриптах: викликається функція, куди передаються деякі змінні. Потім функція у відповідь повертає кілька змінних.

Клієнти визначають ім'я процедури та параметри у запиті XML, сервер повертає відмову чи відповідь у XML вигляді. Параметри XML RPC – простий список типів та контенту – структури та масиви, що є найскладніше доступними типами.

XML RPC з'явився на початку 1998 року; він був опублікований програмним забезпеченням UserLand.

Переваги XML RPC такі: вибір XML RPC типів даних є відносно невеликим, але забезпечує достатню гранулярність; розробники можуть висловити інформацію будь-якими мовами програмування; системні інтегратори та програмісти, що створюють розподілені системи, використовують XML RPC як код сполучної ланки, з'єднуючи різнотипні частини в приватній мережі; при використанні XML RPC основною проблемою розробників є інтерфейси взаємодії між системами; розробники, які надають послуги загального використання, можуть також використовувати XML RPC, визначаючи інтерфейс та реалізовуючи його обраною ними мовою. Як тільки ця служба опублікована для мережі, будь-який XML RPC клієнт може з'єднатися зі службою, і розробники можуть створити власні програми, які використовують цю службу.

XML RPC складається з трьох деталей:

- моделі даних XML RPC;

- набору типів для використання параметрів, що повертають значення та відмови (помилка повідомлення);

- Структура запиту XML RPC;

- запиту POST HTTP, що містить метод та інформацію про параметр;

- Структури відповіді XML RPC;

- відповіді HTTP, що містить інформацію про відмову або значення, що повертаються;

- структур даних, що використовуються і запитом та відповіддю.

SOAP. SOAP – заснований на протокол XML. Хоча SOAP може використовуватися різними системами обміну повідомленнями і може постачатися через різноманітні транспортні протоколи, головною метою SOAP є виклики віддаленої процедури, що транспортується через HTTP [3].

Специфікація SOAP визначає XML - «конверт» передачі повідомлень, метод для кодування програмних структур даних у форматі XML, і навіть засоби зв'язку за протоколом HTTP. SOAP-повідомлення бувають двох типів: запит

(Request) та відповідь (Response). Запит викликає метод віддаленого об'єкта, відповідь повертає результат виконання цього методу. Нижче наведено приклади запиту та відповіді у форматі SOAP.

Специфікація SOAP визначає три основні частини.

Специфікація конверта SOAP. XML SOAP Конверт визначає певні правила для того, щоб інкапсулювати дані, що передаються між комп'ютерами, що включає спеціалізовані дані, такі як ім'я методу, щоб викликати, параметри методу, або значення, що повертаються. А може також включати інформацію про те, хто має обробити зміст конверта та, у разі відмови, як закодувати повідомлення про помилки.

Правила кодування даних. Щоб обмінюватися даними, комп'ютери повинні домовитися про правила, щоб закодувати певні типи даних.

Угоди RPC. SOAP може використовуватися в багатьох системах обміну повідомленнями, включаючи односторонній та двосторонній обмін повідомленнями. Для двостороннього обміну повідомленнями SOAP визначає просту угоду для надання викликів віддаленої процедури та відповідей [4]. Це дозволяє клієнтському додатку визначати віддалене ім'я методу, включаючи будь-яку кількість параметрів, та отримання відповіді сервера.

WSDL. WSDL – специфікація опису Web-сервісів у спільній XML граматиці. WSDL описує чотири критичні частини даних:

- інтерфейсна інформація, що описує публічно доступні функції;
- інформація про тип даних для всіх запитів та відповідей повідомлення;
- інформація про транспортний протокол, який використовуватиметься;
- адресна інформація для того, щоб визначити місцезнаходження служби.

WSDL представляє контракт між запитуючим сервісом та сервісом-провайдером. WSDL - платформонезалежна і використовується перш за все, щоб описати SOAP служби [5]. Використовуючи WSDL, клієнт може визначити розташування Web-сервісу і викликати будь-яку з його публічно доступних функцій. За допомогою інструментів WSDL можна також автоматизувати цей процес, включаючи програми, для легкої інтеграції нових служб з невеликим або

мінімальним ручним кодом.

Специфікаціяділиться на шість основних елементів.

Визначення. Елементвизначення має бути кореневим елементом усіх документів WSDL. Він визначає назву Web-сервісу, заявляє, кілька просторів імен, що використовуються в частині документа, що залишилася, і містить всі елементи послуг, описаних тут.

Типи. Елемент типів описує всі типи даних, що використовуються між клієнтом та сервером. WSDL не прив'язаний виключно до певного типу системи, але використовує специфікацію W3C XML Schema за умовчанням. Якщо сервіс використовує лише XML Schema, вбудовану у прості типи, тип елементів не потрібний.

Повідомлення. Елемент повідомлення описує одностороннє повідомлення, це простим повідомленням-запитом чи єдине повідомлення – відповідь. Він визначає назву повідомлення і містить нуль або більше елементів частин повідомлення, які можуть звернутися до параметрів повідомлення або значення повідомлення, що повертаються.

PortType. PortType елемент комбінує багаторазові елементи повідомлення, щоб сформувати повну односторонню дію чи дію «туди й назад». Наприклад, portType може об'єднати один запит і одне повідомлення відповіді на єдину операцію запиту/відповіді, яка зазвичай використовується в SOAP [6]. Зазначимо, що portType може (і часто робить) визначати багаторазові операції.

Закріплення. Обов'язковий елемент описує конкретні специфічні особливості того, як буде здійснено сервіс в мережі. WSDL включає вбудовані розширення для того, щоб визначити послуги SOAP та спеціальну SOAP інформацію.

Обслуговування. ЕлементСервіс визначає адресу виклику зазначеного сервісу. Найчастіше включає URL для виклику сервісу SOAP.

На додачу до шести головних елементів специфікація WSDL також визначає наступні сервісні елементи:

документація. Елемент документації використовується, щоб забезпечити

документацію, що зручно читається, і може бути включений в будь-якому іншому елементі WSDL.

Передача. Елемент передачі використовується для імпорту інших документів WSDL або XML схеми. Це дозволяє більше модулювати документи WSDL. Наприклад, два документи WSDL можуть імпортувати ті самі основні елементи і все ж таки включати їх власні елементи обслуговування, щоб зробити те саме обслуговування доступним у двох фізичних адресах. Однак, не всі інструменти WSDL підтримують функціональні можливості передачі.

WSDL – не офіційна рекомендація W3C та не має офіційного статусу в межах W3C. Версія 1.1 WSDL була представлена на W3C у березні 2001 року.

UDDI. UDDI – технічна специфікація, що описує, виявлення та об'єднання Web-служб. UDDI – частина стеку протоколу Web-сервісів, що дозволяє компаніям опубліковувати та знаходити Web-сервіси. UDDI складається із двох частин.

Перша – технічна специфікація побудови розподіленого довідника Web-сервисов. Дані зберігаються в межах певного формату XML і специфікація UDDI включає деталі API для того, щоб шукати існуючі дані та опублікувати нові дані.

Друга - бізнес реєстрація UDDI є повністю реалізацією специфікації UDDI. Реєстрація UDDI дозволяє шукати існуючі дані UDDI, а також зареєструвати компанію та її послуги.

Дані, отримані у UDDI, поділені на три основні категорії.

Білі сторінки. Включає в себезагальну інформацію про конкретну компанію – наприклад, назву компанії, описи бізнесу, контактну інформацію, адреси та номери телефонів. Може також містити унікальні ідентифікатори бізнесу, такі як Dun & Bradstreet DUNS.

Жовтісторінки включають загальні дані класифікації компанії або пропонованих послуг [7]. Наприклад, ці дані можуть включати інформацію про промисловість, продукти та географічні коди, засновані на стандартній таксономії.

Зеленісторінки містять технічну інформацію щодо Web-служби. Як

правило, включає вказівник на зовнішні специфікації та адресу для виклику Web-сервісу. UDDI не обмежується описом Web-сервісів на основі SOAP. UDDI може використовуватися для опису будь-яких послуг, від однієї Web-сторінки або адреси електронної пошти до SOAP, CORBA, Java RMI та послуг.

1.3 Існуючі програмні рішення щодо банківських транзакцій

Є деякі програмні продукти щодо безпечних банківських транзакцій. Одним із них є засіб прийому платежів «2checkout».

"2checkout.com" - засіб прийому платежів в інтернеті, причому без особливо жорстких вимог до продавця.

«2checkout» вимагає окремий обліковий запис на кожен сайт, кожен обслуговуваний домен. За великим рахунком, це логічно, оскільки у разі проблем в одному бізнесі у вас завжди залишаться інші облікові записи.

Цей сервіс має афілієйну програму, і клієнт стає її учасником автоматично після отримання першого облікового запису [8]. Кожен наступний обліковий запис обходиться на величину агентської комісії дешевше — економія близько 15 доларів. Цю комісію вони повертають тобі через кілька днів на ту картку, якою оплачував клієнт покупку облікового запису.

"2checkout" - посередник, хоча останнім часом вони змушують всіх клієнтів писати у себе на сайті, що "2checkout.com - магазин. По суті, "2checkout" - точка, в яку відправляється клієнт, що клікнув по кнопці "Купити". Є багато варіантів, у тому числі текстові посилання, і інтеграція з кошиками.

Є API повідомлення, причому досить просте через параметри POST-запиту на сайті клієнта. Тестовий режим теж можна включити, в тому числі і з генерацією номерів кредиток, щоб пройти процес замовлення від початку і до кінця.

Можна налаштувати або редирект на сайт клієнта після покупки, або стандартне повідомлення про минулий платеж - краще залишати саме його так, щоб у разі проблем на сайті клієнт не біг у банк робити чарджбек.

Цей сервіс — не «параноїк», на відміну від багатьох інших систем, які існують. У них цілком осудний фродчек, хибних спрацьовувань практично немає. Якщо вони сумніваються – дзвонять клієнту. У випадку з Plimus чи не кожен третій ордер викликав якісь проблеми.

Фроди (шахрайські ордери) проходять досить часто. Їхня кількість може досягати двадцяти відсотків, що є дуже високим показником і вказує на слабку орієнтацію у боротьбі з шахрайськими транзакціями. Так само даний сервіс повідомляє, що при великій кількості шахрайських транзакцій вони закривають акаунт користувача. Це з обмеженнями, накладаними ними платіжними системами [9]. Причому цей відсоток розраховується за кожною з платіжних систем окремо.

Гроші виводяться автоматично щотижня, якщо клієнт перевищив встановлений мінімальний рівень виведення. Гроші вирушають увечері у середу, у четвер увечері вони приходять на карту. З валютним рахунком гроші приходять за 4-5 днів.

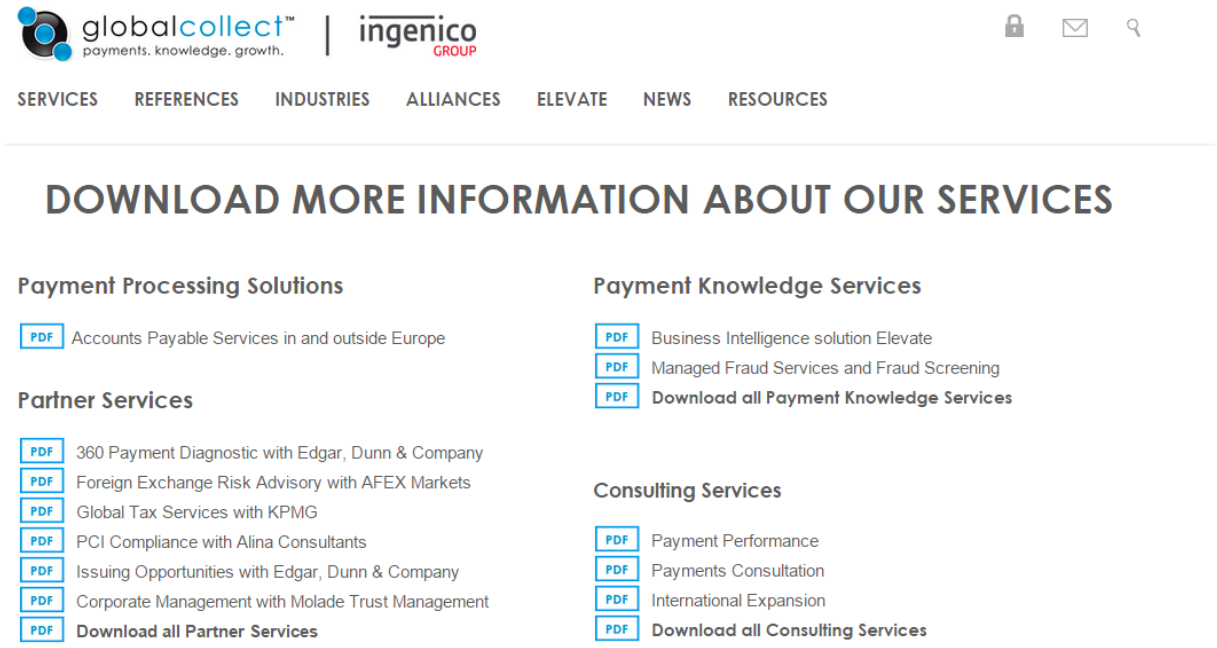

Рисунок 1.2 – Сервіси системи «GlobalCollect»

Також існує система «GlobalCollect». Це система обробки платежів, яка спеціалізується на електронних методах оплати в різних галузях, включаючи транспорт, телекомунікації, роздрібну торгівлю, Інтернет-портали, ігри та інформацію. Але вона захищає своїх клієнтів лише за допомогою того, що має доступ до баз різних банківських систем і на основі цього робить висновок, чи є платіж достовірним чи ні.

Однією з перших систем захисту комерційних структур від шахраїв є «Plimus». Система є посередником між інтернет-магазином та власне банківською транзакцією. Сервіс обіцяє своїм клієнтам високий захист, але на практиці блокує багато платежів, якщо, наприклад, білінг адреса не збігається з шипінг адресою, щоб не ризикувати чужими засобами. Простота і зручність інтерфейсу приваблює користувачів, але не можна говорити про передові методи захисту транзакції.

1.4. Постановка задачі

У роботі поставленим завданням було реалізувати інтелектуальну систему захисту під назвою Detect Fraud.

Сервіс Detect Fraud знижує кількість зворотних платежів, розпізнаючи замовлення групи ризику та зупиняючи їх до подальшого розгляду. Ця служба використовується для розпізнавання шахрайської діяльності в електронно-комерційних транзакціях, партнерських посиланнях, опитуваннях, входах у систему та реєстраціях.

Detect Fraud визначає ймовірність того, що транзакція є шахрайською, ґрунтуючись на різних факторах, включаючи те, чи надходить онлайн-транзакція з IP-адреси, електронної адреси або пристрою підвищеного ризику або з анонімного проксі-сервера. Однією з ключових функцій сервісу Detect Fraud є мережа, яка дозволяє визначати та зберігати репутації IP-адрес, адрес електронної пошти та інших параметрів.

Користувачі служби отримують користь з динамічного та адаптивного підходу до виявлення шахрайської діяльності та взаємного захисту мережі Detect Fraud. Наприклад, якщо буде виявлена підозріла діяльність з певної IP-адреси, вона буде позначена як адреса підвищеного ризику у всій мережі Detect Fraud у режимі реального часу. Таким чином, відгуки продавців є попереджувальними сигналами для решти всіх членів мережі Detect Fraud.

Сервіс може використовуватися сам по собі або як доповнення до існуючої корпоративної системи відстеження шахрайської діяльності.

У процесі досягнення поставленої мети необхідно вирішити такі завдання:

- Вивчити технології створення Web-сервісів;
- Вивчити внутрішню структуру Web-сервісів;
- Вивчити принципи роботи Web-сервісів;
- розробити алгоритм визначення шахраїв у системі;
- Розробити власний Web-сервіс Detect Fraud.

Даний Web-сервіс буде оснащений зручною системою керування вмістом. У цьому проекті мається на увазі реалізувати адміністративну частину, таким чином, що адміністратор зможе легко переглядати, видаляти або редагувати інформацію, що надходить від сервісу та пересилати далі інформацію потрібним службам залежно від рівня платежу.

2 ОГЛЯД КАРДИНГУ В ІНТЕРНЕТІ

2.1. Визначення кардингу

На сьогоднішній день кардинг – це не просто окремі шахраї, це організована злочинна спільнота. Воно має свої сайти та форуми, на яких новачки долучаються до обрядів ремесла, а професіонали обмінюються корисними порадами.

У середині 1990-х років ніхто ще не чув про махінації з кредитними картками, а поодинокі випадки зникнення грошей були помилками магазинів та банків. Тому інтернет-магазини охоче приймали неіснуючі згенеровані кредитні картки, алгоритм яких був таким самим, як і справжні карти. Перевіривши алгоритм, інтернет-магазини надсилали замовлений товар. Обман розкривався лише наприкінці місяця, коли магазини вимагали у банків переказ грошей з карток на оплату товару. Природно, що грошей магазин не отримував, оскільки запитаних кредитних карток немає [10].

У цей час у країнах СНД стало можливим отримати доступ до Інтернету. Першими користувачами були переважно викладачі та студенти вузів. Ці студенти і становили основу кардерства СНД, що зароджується. Студенти кардили все, що тільки можна, спираючись на електроніку та ювелірні вироби. Особливою запопадливістю відрізнялися українські кардери, які організували в Києві цілу мережу з транспортування, зберігання та збуту вкраденого товару. Десятки квартир купувалися під склади для зберігання електроніки, яку не встигали збувати за дешевшими цінами. На митному терміналі у київському міжнародному аеропорту Бориспіль цілодобово чергували кілька вантажівок, які вивозили вантаж після кожного міжнародного рейсу. Товар із європейських магазинів переважно доставлявся наземним шляхом. Обсяг товару був настільки великий, що нерідко магазини відправляли свої фури прямо на Україну, не вдаючись до послуг пошти. Багато магазинів серйозно замислилися про відкриття своїх філій у СНД.

Товар збувався за підробленими документами через оптові та роздрібні магазини, які були зацікавлені у купівлі фірмової електроніки за низькими цінами. Величезний потік вкраденої електроніки призвів до затоварювання українського ринку. Склалася парадоксальна ситуація, коли можна було купити оперативну пам'ять за ціною вдвічі дешевшою від відпускної ціни виробника. Легальне постачання електроніки, особливо комп'ютерів, практично припинилося.

Так не могло тривати вічно. ФСБ спільно з Інтерполом вже деякий час стежили за кардерами, що викликає діяльністю. 1996 року країнами СНД прокотилася хвиля арештів. Творці кардерських угруповань та їх наближені було заарештовано. Про подальше існування таких угруповань не могло бути й мови, тепер кожен був сам за себе. Товар намагалися збути одразу після отримання, працювали в основному поодинці чи невеликими групами, не залучаючи зайвих людей.

Наступним ударом по кардерському ремеслу стала поступова відмова у прийомі згенерованих кредиток. У зв'язку з великими збитками магазинів, у банків з'явилися нові сервіси, що дозволяють магазину перевіряти достовірність даних про кредитну картку моментально або в розумні терміни (раніше магазин дізнавався, що його обікрали вже після того, як покупка надсилалася замовнику). І тепер магазин міг відсіяти неіснуючу кредитку ще до надсилання товару. Але й цю перепону вдалося подолати. Через недосконалість захисту інтернет-магазинів можна було стягнути в них базу даних з інформацією про кредитні картки клієнтів, які робили у них покупки.

З цього моменту багато доброчесних американців боялися робити покупки в інтернет-магазинах. І правильно робили. Кожен магазин запевняє покупців, що має найнадійніший захист. Але було б набагато краще, якби магазини просто не зберігали інформацію про покупців у себе на сервері. Іноді можна, ввівши в пошуковій системі "credit card name adress", вийти на список кредитних карток, який зберігається на сервері інтернет-магазину. Тобто інформація про кредитні картки в цьому випадку настільки незахищена, що навіть індексується

пошуковими системами. Тепер, коли в магазині робили замовлення на існуючій карті, він знімав із неї гроші (або просто перевіряв її існування, а гроші знімав наприкінці місяця) [11]. Через деякий час справжній власник картки звертався до банку та опротестовував транзакцію. Банк, своєю чергою, розбирався з магазином. Але товар висланий, а магазин знову у збитку.

Новим кроком захисту від підробок став запит магазинами коду CVV2 при покупці. CVV2 код – це 3 останні цифри номера на задній стороні картки, знати його може лише власник картки, який тримає її в руках. Тепер будь-які махінації з кредитними картками стали в принципі неможливі, оскільки код CVV2 не можна дізнатися ніяк. Спочатку планувалося, що CVV2 не зберігатиметься на жодній стадії обробки кредитної картки. Тобто він повідомлявся лише банківській системі обробки карток, а вже з банку йшло підтвердження чи відмова. Але цей спосіб захисту не виправдав своїх очікувань. Інтернет-магазини, порушуючи всі вимоги банків, стали зберігати код CVV2 з рештою інформації про кредитні картки у своїх базах даних. Бази, своєю чергою, так само спокійно, як і раніше, вкралися, а кардери отримували доступ до CVV2.

Щодня фахівці у банках працюють над тим, щоб ускладнити кардерам життя. На початку 21 століття вони вигадали VBV - Verified by Visa. Суть системи в тому, що при оплаті товарів або послуг в інтернеті необхідно ввести додатковий код перевірки, який власник картки отримує від банку, який випустив картку. Однак, це не вирішує проблеми безпеки платежів. Проблема полягає в тому, що клієнт не може заборонити проведення операцій, що не захищені Verified by Visa. І навіть розплачуючись тільки в тих інтернет магазинах, де використовується Verified by Visa [12], у клієнта з легкістю можуть бути викрадені дані (номер картки, ім'я власника, термін дії, CVV2 код) достатні для проведення законних платежів від імені клієнта.

Зі зростанням кількості пластикових карток у світі втрати від кардингу стають все більш відчутними. Щороку у світі шахраї викрадають за допомогою пластикових карток систем Visa та Europay близько $2 млрд. Найчастіше подібні злочини відбуваються останнім часом у країнах, де пластикові картки вже досить

поширені, але спецслужби ще не навчилися ефективно боротися із пов'язаними з ними аферами.

2.2 Способи списання коштів із кредитної картки

Існує десятки способів зняття грошей з кредитної картки, але найпопулярнішим залишається речовий кардинг. Речовий кардинг набув найбільшого поширення серед кардерів. Його суть полягає у замовленні товарів в інтернет-магазинах за чужими кредитними картками з метою подальшого збуту.

Схема роботи речового, начебто, лежить на поверхні. Це приваблює багатьох кардерів-початківців, яким все здається зрозумілим і простим [13]. Насправді займатися речовим кардинг не так легко. Щоб отримувати дохід, потрібний ланцюжок людей, які злагоджено працюватимуть.

Сьогодні значна частина кардерів так само займається "віртуальним" різновидом свого ремесла - тобто скуповує не "товари народного споживання", а корисні йому мережеві речі такі як домени, паролі, хости, енроли і т.д. До речі, дещо з цього легально не купиш, оскільки воно не повинно і не може продаватися. Наприклад, енрол (від англ. enroll – ввести обліковий запис) – це зв'язок кредитної картки (рахунки) з онлайн доступом, можливістю дізнаватися та змінювати дані користувача через інтернет. Тобто це те, що робить кредитку «живою» та банківська таємниця – повністю вся інформація про вас, включаючи ПІН-код. Як можна дізнатися такі подробиці – досконало відомо лише самим кардерам. Дані від розблокування кредитки їх задовольняють, у своїй видається лише частина особистих даних власника - наприклад Credit card/debit card number: ******0299584**. Частина даних все одно залишилася зашифрованою, і не факт, що їх вдасться підібрати. Тому кардер продовжує пошук потрібних відомостей про картку. Спочатку він встановить, який банк випустив цю карту (втім, ця інформація є на всіх картах відкрито), потім заходить на сайт цього банку і знаходить кнопочку з аналогічною назвою «енрол» (віртуальний кабінет

користувача). Якщо карта жива, тобто. ніхто інший ще використовував її тих самих цілей, він авторизується. Авторизуватись у системі набагато простіше, ніж підбирати комбінації картки – треба ввести пароль [14]. Це може бути пін-код, дівоче прізвище матері тощо. Після чого сайт буквально на блюдечку видасть кардеру всю інформацію, аж до адреси та телефону. Щоправда, більшість сайтів російських та українських банків опцію enroll не передбачають, тож кардеру необхідно купити клієнтську базу даних банку. Але оскільки є попит, є і пропозиція – саме тому раз на квартал можна почути про черговий крадіжку баз даних із серверів великих інтернет-магазинів. Проте будь-якого фахівця чи потерпілого більше цікавить не це – а те, як кардерам вдається безкарно «зливати» великі суми грошей із чужого банківського рахунку. Тих, хто «працює» з банкоматами та отримує інформацію при зніманні клієнтом грошей із картки, залишилося небагато – змонтувати свої пристрої на банкоматі не можна, оскільки майже всі банкомати давно отримали відеозйомку. Тому кардерам нічого не залишилося, як «перебазуватися» в Інтернет і скуповувати віртуальні товари в інтернет магазинах.

2.3 Способи отримання кредитної картки

Для отримання інформації необхідної проведення успішної транзакції кардери використовують різні способи їх видобутку. Найчастіше вони створюють інтернет-магазини, оскільки саме в ньому можна розплачуватися кредитними картками. Принадою служать зазначені ціни - на 30-70% нижче, ніж у звичайних магазинах, причому з правдоподібним поясненням: "конфіскат з митниці", "ліквідація складу" і т.п. А далі все залежить від нахабства кардерів. Деякі, крім реквізитів кредитної картки, відразу вимагають ПІН-код – щоб потім оперативно витратити чи зняти всі гроші з рахунку [14]. Інші доповнюють інформацію користувача зі зламаних серверів «чесних» інтернет-магазинів, платіжних та розрахункових систем. Отже, гроші з кредитки можуть «плисти» і без заходу користувача на кардерський сайт. Дехто може поєднати в собі навички

кардера та хакера та отримати потрібну інформацію прямо з комп'ютера – запустивши в нього "трояна" або "хробака".

«Класичний» кардинг, який відмирає нині за вказаними вище причинами, ще відомий під назвою «скіммінг». Назва йде від «скіммеру» - інструменту для зчитування, наприклад, магнітної доріжки кредитної картки. Це портативний пристрій з магнітною головкою, що зчитує, підсилювачем - перетворювачем, пам'яттю і перехідником для підключення до комп'ютера. Причому скіммери можуть бути як портативними, так і мініатюрними - і цілком здатні знімати інформацію, коли клієнт вставляє картку в банкомат. Однак оскільки, як уже говорилося, більшість банкоматів обзавелося відеокамерами, встановити скіммер стало дещо проблематично - і кардери йдуть в інші місця, зокрема великі магазини.

Отримавши дані про банківську картку або її саму, кардер спочатку перевіряє рахунок на працездатність - робить з картки певний платіж. При цьому він «вбиває» всю інформацію про видобуток: ім'я власника, країну, місто тощо. Якщо платіж пройшов, то карта працює і тепер можна приступати до «справжньої справи». Тобто: знайшовши в будь-якій пошуковій системі «потрібні» сайти, кардер скуповує (за краденою кредиткою, звичайно) все, що бачить у мережі – вже згадані хостинги, домени, всілякі доступи тощо. Далі кардер перепродує «віртуальний товар» та отримує необхідний прибуток. Що стосується реальних товарів, то кардери ніколи не висилають його на себе для повної безпеки.

2.4 Проведення шахрайської операції в інтернет-магазині

Кредитну картку для покупки в інтернет-магазині досвідчені кардери підбирають дуже ретельно. Карта повинна відповідати штату, а краще місту дропа, тоді можна спробувати вказати при замовленні різні адреси дропа та власника картки та постаратися переконати магазин, що кардер (нібито власник картки) вирішив зробити подарунок своєму племіннику на іншому кінці міста.

Якщо адресу змінити на адресу дропа, то у магазину в принципі відпадуть будь-які сумніви в легальності покупки, оскільки він надсилає покупку на адресу власника картки. Але й тут все не так просто. Іноді адреса на карті змінюється без питань, інколи ж банк починає сумніватися і нічого не виходить [15]. Що стосується «дропу» (від англійського drop – скидаючий), то це громадяни країни, в якій здійснюється закупівля товарів за чужими або краденими кредитними картками.

Основне завдання «Дропів» - отримати товар і переправити його адресату, тобто організатору мережі. Як правило, ці люди не знають, що вони фактично беруть участь у злочині. Справа в тому, що компанія при прийомі нового співробітника зазвичай укладає з ним усі необхідні за трудовим правом договору – і людина щиро впевнена, що працює кур'єром чи дилером. Кандидатів хоч греблю гати - і в Росії і в світі багато людей постійно шукає роботу. І побачивши невигадливе оголошення типу: «Потрібен менеджер з персоналу або обробки кореспонденції, робота вдома», практично будь-який претендент без проблем погодиться на таку посадку.

Щоправда, період «працевлаштованості» рідко триває довше за три-чотири місяці – далі на мережу зазвичай виходить поліція. До речі, найчастіше це відбувається через те, що при вже описаному вище «розблокуванні» кредитки кардер замість імені реального власника картки вносить дані свого «дропа». І добре, якщо він зможе довести, що вважав себе звичайним працівником у такій самій звичайній фірмі (наприклад, трудовим договором та віддаленістю роботи) і про махінації від свого імені поняття не мав. Для слідства «дроп» зазвичай марний – оскільки всі контакти з ним начальство здійснювало лише електронною поштою і розплачувалося електронними грошима.

Інтернет-магазин, в якому буде зроблено замовлення, також ретельно підбирається. Кардери не роблять замовлення у великих інтернет-магазинах із гарною службою безпеки. Вони вибирають невеликий інтернет-магазин, який є лише інтернет-вітриною звичайного магазину [16]. Частка покупок через інтернет у такому магазині дуже мала, тому немає кваліфікованого персоналу,

який відстежує покупки кардерів. На рисунку 2.1 зображено «вбивши» інформації про власника картки в типовий інтернет магазин.

Якщо інтернет-магазин щось здається підозрілим, він може вимагати вислати йому відскановану кредитну картку або запитає телефон, або запропонує кардеру самому зателефонувати в магазин. Скан кредитної картки за кілька десятків доларів зазвичай підробляють а ось з телефоном іноді виникають проблеми. Кардери іноді домовляються зі своїми дропами про підтвердження по телефону, іноді знаходять окрему людину. І якщо з дропом все просто, то окрема людина може жити в іншому штаті. Тоді їм доведеться користуватися антиаонами, які підмінять номер телефону на той, який буде відповідати штату дропу.

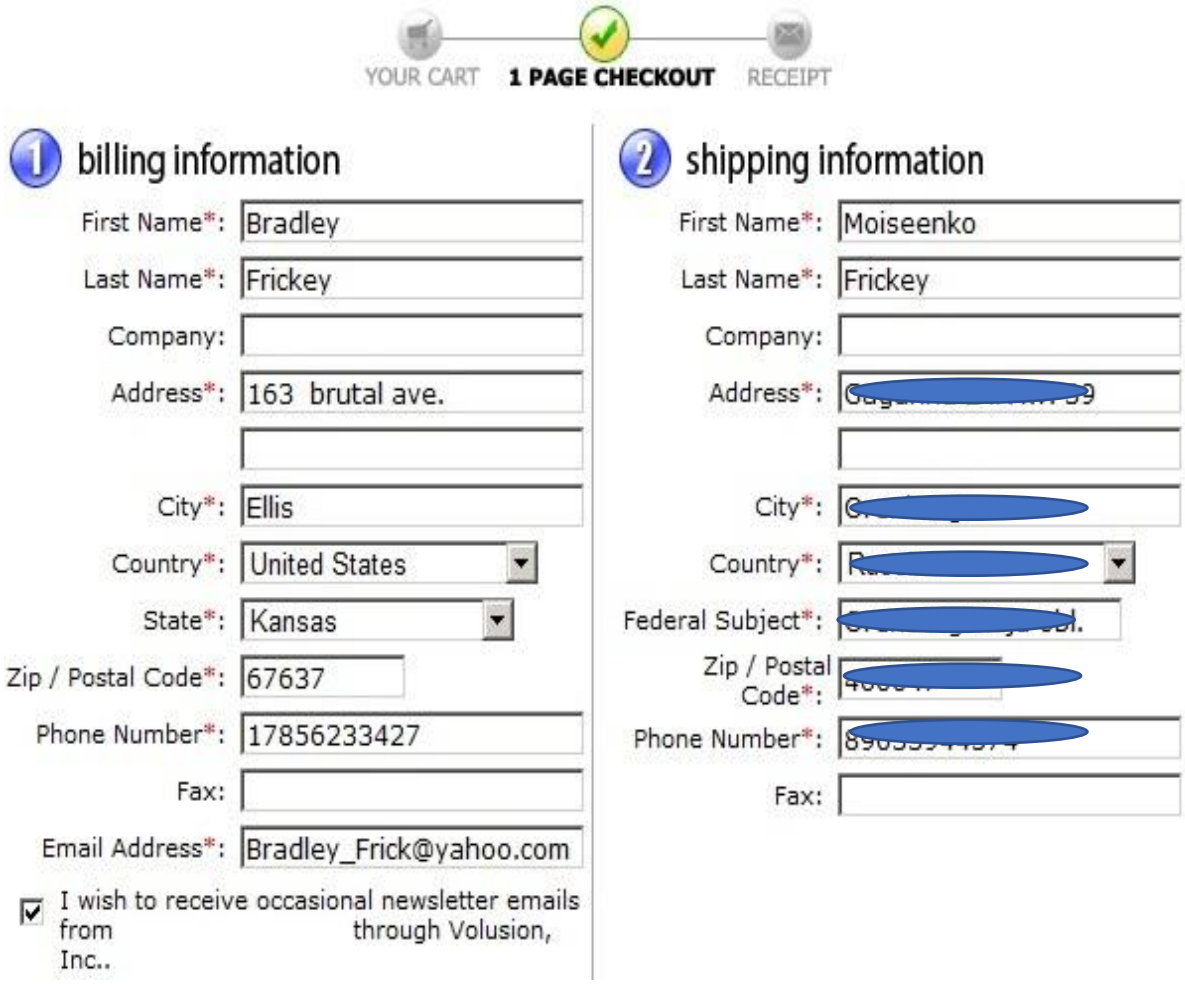

Рисунок 2.1 - Повна інформація про власника картки

Останнім часом стала дуже актуальною тема з інтернет-магазинів Австралії та Нової Зеландії. Через їхню віддаленість від інших країн там існує лише нечисленний місцевий речовий кардинг, який контролюється китайською мафією. Тому магазини без зайвих питань шлють товар не лише своїми країнами, а й за кордон, навіть до Росії. Щоправда, термін доставки в Росію набагато більший, ніж з Америки, через гірше розвинені служби поштової доставки. Ще однією проблемою є видобуток австралійських та новозеландських кредитних карток. Через те, що з цих країн мало хто кардить, дуже малу кількість карток можна придбати. А якщо у продавця і з'являються австралійські кредитки, то за цінами у кілька разів більше.

2.5 Огляд кредитної картки

На рисунку 2.2 зображено приклад інформації, необхідної для здійснення успішної транзакції.

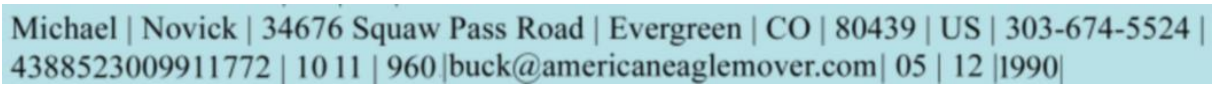

Рисунок 2.2 – Приклад інформації про кредитну картку для кардингу

Розшифрування даних зображених рисунку 2.2 надано у таблиці 2.1

Таблиця 2.1 – Дані про кредитну картку

Назва даних	Позначення
Michael Novick	Ім'я та прізвище власника картки
34676 Squaw Pass Road	Вулиця проживання картки власника.
Evergreen	Місто картхолдера
CO	Штат власника кредитки

80439	Zip cod, postal cod або поштовий індекс власника картки
US	Країна проживання картхолдера
303-674-5524	Номер телефону власника
4388523009911772	Номер кредитки
10 24	Дата закінчення терміну дії картки
Назва даних	Позначення
960	CVV2 або захисний код картки
buck@americaneaglemover.com	Email власника кредитки
05 12 1990	Рік та дата народження картхолдера

3 РОЗРОБКА АРХІТЕКТУРИ WEB-СЕРВІСІВ

3.1 Загальна структура Web-сервісу

Для реалізації Web-сервісу зазвичай використовують серверну, адміністративну, користувальницьку частини. Враховуючи особливості даного Web-сервісу, реалізовано серверну частину, частину, що відповідає за збір та обробку отриманої інформації та адміністративну частину – комп'ютер користувача або служби підтримки.

На рисунку 3.1 представлено загальний вигляд системи обробки банківських транзакцій.

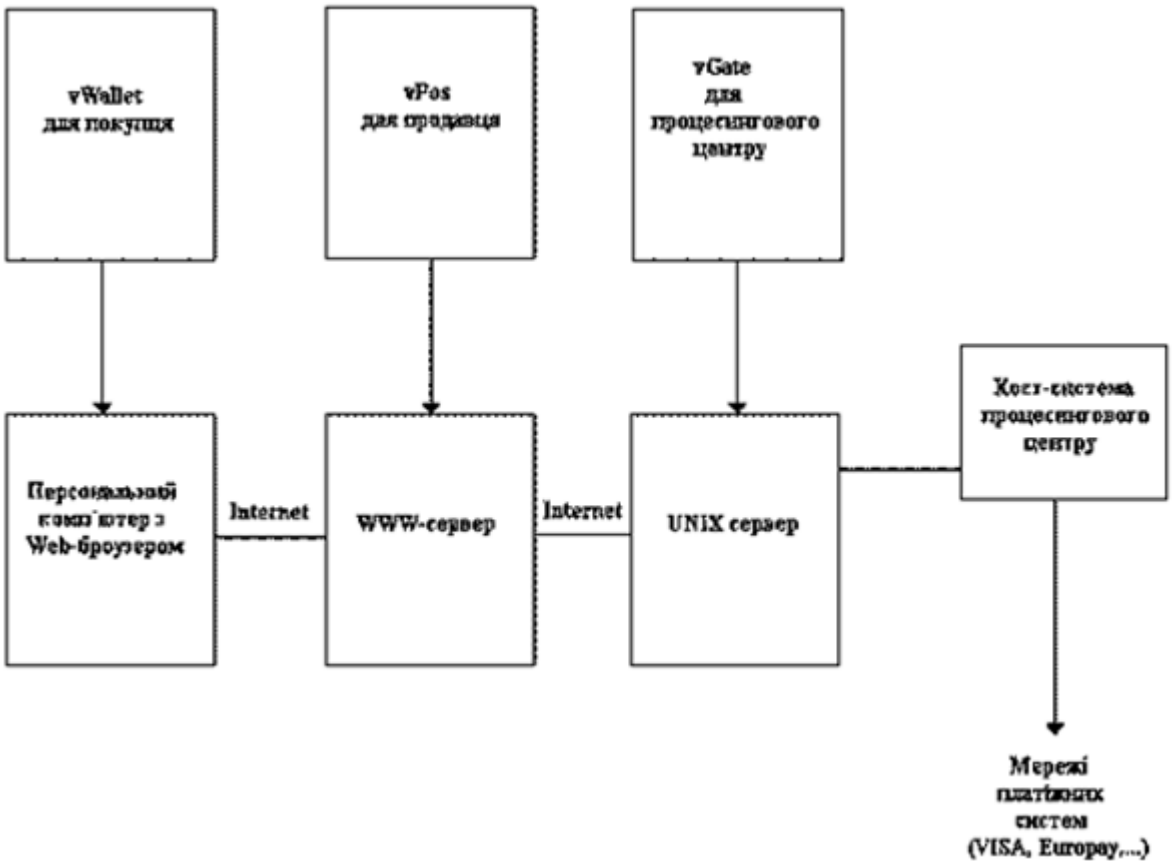

Рисунок 3.1 – Загальна схема роботи Web-сервісу обробки банківських транзакій

У таблиці 3.1 надано всі функції сервісу DetectFraud.

Таблиці 3.1 – функції сервісу DetectFraud

riskScore	Дане поле містить рівень ризику, від 0.01 до 100. Чим вище рівень тим більша ймовірність, що транзакція є шахрайською. Рівень ризику не може дорівнювати нулю.
Збіг країни	Це поле може містити відповідь ТАК або НІ. Висновок робиться за рахунок збігу IP адреси країни та адреси відправлення товару. Невідповідність вказує на вищий ризик шахрайства. Якщо не вдається визначити IP адресу, то поле залишається не заповненим.
Країни з високим ризиком	Це поле може містити відповідь ТАК або НІ. Якщо поле містить ТАК то це означає, що IP адреса або адреса доставки товару належить країні, де високий рівень шахрайства.
Відстань	Відстань між локацією IP адреси та адресою доставки, у кілометрах. Чим більша відстань, тим більший ризик шахрайства.
Радіус IP-адреси	Радіус у кілометрах навколо вказаного розташування, де знаходиться користувач IP-адреси.
IP міста	Місто до якого належить IP-адреса.
IP індекс	Індекс пов'язаний з IP-адресою. Вони доступні для деяких IP-адрес в Австралії, Канаді, Франції, Німеччині, Італії, Іспанії, Швейцарії, Сполученому Королівстві та США.
IP Телефонний код	Телефонний код області пов'язаний з IP-адресою. Вони лише доступні для IP-адрес у США.

<table>
<tr><td></td><td></td></tr>
<tr><td>Часовий пояс</td><td>Показує часовий пояс, виставлений користувачем на його комп'ютері.</td></tr>
<tr><td>Анонімні проксі</td><td>Це поле може містити відповідь ТАК або НІ. Якщо користувач використовує анонімні проксі, це вказує на високий ризик помилкової транзакції.</td></tr>
<tr><td>proxyScore</td><td>Оцінка від 0.00 до 4.00 вказує на можливість користування відкритим проксі. Нижче наведено можливість у відсотковому співвідношенні.

<table><tr><td>proxyScore</td><td>Імовірність шахрайської діяльності</td></tr><tr><td>0.5</td><td>15%</td></tr><tr><td>1.0</td><td>30%</td></tr><tr><td>2.0</td><td>60%</td></tr><tr><td>3.0+</td><td>90%</td></tr></table>
Примітка: анонімним проксі присуджується оцінка 0.</td></tr>
<tr><td>Корпоративний проксі</td><td>Це поле може містити відповідь ТАК або НІ. За допомогою цієї функції можна зрозуміти, чи користується користувач корпоративний проксі.</td></tr>
<tr><td>Безкоштовна пошта</td><td>Це поле може містити відповідь ТАК або НІ. Якщо користувач використовує поштовий сервіс з поганою репутацією, то інтернет магазин буде про це повідомлений.</td></tr>
<tr><td>БІН</td><td>Це поле може містити відповідь ТАК, НІ або ВІДСТУВАЄ. Функція повідомляє про перші шість цифр зазначених на кредитній картці покупця.</td></tr>
</table>

binCountry	Це поле показує якій країні належить банк. Ця функція доступна для 99% номерів БІН. Функція доступна лише для преміум користувачів.
binNameMatch	Це поле може містити відповідь ТАК або НІ або ВІДСТУВАЄ. Воно вказує чи збігається чи ім'я власника картки з одержувачем товару. У полі вказується ВІДСУТНО якщо дані не були знайдені в базі. Функція доступна лише для преміум користувачів.
binName	Це поле показує якому банку належить карта. Ця функція доступна для 96% номерів БІН. Функція доступна лише для преміум користувачів.
binPhoneMatch	Це поле може містити відповідь ТАК або НІ або ВІДСТУВАЄ. Воно показує телефон гарячої лінії банку Функція доступна лише преміум користувачів.
binPhone	Це поле містить телефонний номер (гарячу лінію) банку. Ця функція доступна для 90% номерів БІН. Функція доступна лише для преміум користувачів.
prepaid	Це поле може містити відповідь ТАК або НІ. Поле вказує чи карта кредитної (дебетової) чи подарункової. Якщо достовірної інформації немає, поле буде порожнім. Функція доступна лише для преміум користувачів.
custPhoneInBillingLoc	Це поле може містити відповідь ТАК, НІ або ВІДСТУВАЄ. Ця функція повідомляє, чи збігається вказаний номер телефону зі штатом доставки. У полі вказується НІ, якщо код телефону не співпадає зі штатом. У полі вказується ВІДСУТНО якщо цей телефонний код відсутній в базі. Ця функція лише для телефонних номерів у США. Для решти країн поле буде порожнім. Функція доступна лише для преміум користувачів.

shipForward	Це поле може містити відповідь ТАК або НІ. Поле показує, чи складається ця адреса доставки в базі адрес з поганою репутацією. Відповідь позитивна, якщо адреса доставки полягає у списку адрес з високим ризиком обману.
cityPostalMatch	Це поле може містити відповідь ТАК або НІ. Дана функція повідомляє чи збігаються білінг адресу та штат доставки товару. Ця функція доступна лише для адрес США. Для решти країн поле буде порожнім.
shipCityPostalMatch	Це поле може містити відповідь ТАК або НІ. Дана функція повідомляє, чи збігаються адреса доставки і штат доставки товару. Ця функція доступна лише для адрес США. Для решти країн поле буде порожнім.

3.2 Структура роботи Web-сервісу

Оцінка riskScore, що видається службою DetectFraud, Висловлює ймовірність того, що конкретна транзакція є шахрайською. Продавці використовують оцінку riskScore, щоб визначити, чи варто їм прийняти, відхилити, фізично розглянути чи надіслати транзакції до додаткових служб на подальший розгляд.

Оцінка riskScore дається у вигляді відсотка, і як така коливається від 0,01 до 100,00. Наприклад, замовлення з оцінкою riskScore 20,00 має 20-відсоткову ймовірність того, що воно шахрайське, а замовлення з оцінкою riskScore 0,10 – 0,1-відсоткову ймовірність шахрайства.

Оцінка riskScore ґрунтується на статистичному аналізі. Репутація та моніторинг у реальному часі:

- IP-адреси;
- пристрої;
- адреси електронної пошти;
- перевірки геопозиціонування;
- виявлення проксі-серверів;

- перевірки банківських ідентифікаційних номерів;

- мережа DetectFraud.

Не існує однієї строго встановленої системи показників оцінки riskScore, яку можна використовувати при ухваленні рішення про прийняття, відхилення, фізичний розгляд транзакцій або передачі їх у додаткові служби на подальший аналіз. При визначенні того, які граничні значення встановити, слід брати до уваги вартість повернення платежів та втраченого товару, вартість фізичної перевірки та послуг додаткових служб, а також вартість потенційного відхилення хороших замовлень.

Рекомендована стратегія – спочатку автоматично приймати лише замовлення з низькою оцінкою riskScore (наприклад, 3,00), автоматично відхиляти тільки замовлення з дуже високою оцінкою riskScore (наприклад, 70,00), і фізично розглядати решту всіх транзакцій. Після моніторингу оцінок riskScore, отриманих для фізично розглянутих замовлень, можна відрегулювати граничні значення належним чином, щоб скоротити кількість необхідних фізичних розглядів.

Нижче наводиться розподіл оцінок riskScore, виданий службою minFraud, всім користувачам. Ці дані можна використовувати, щоб оцінити кількість замовлень, які будуть схвалені, відхилені або призупинені до подальшого розгляду відповідно до встановлених вами граничних значень.

Таблиця 3.2. – Приблизний розподіл оцінок riskScore для DetectFraud

Діапазон оцінок riskScore	Відсоток замовлень у діапазоні
0.10 – 4.99	90%
5.00 – 9.99	5%
10.00 – 29.99	3%
30.00 – 99.99	2%

Надбудова відстеження пристроїв для служби DetectFraud розпізнає пристрої під час їхнього руху по мережах і розширює можливість служби

DetectFraud розпізнати шахрайську діяльність. Якщо шахрай змінює проксі-сервери під час перегляду веб-сайту або між відвідуваннями, будуть підвищені оцінки proxyScore та riskScore у вихідних даних DetectFraud, пов'язані з їх транзакціями.

Виконання відстеження пристроїв потребує лише використання коду JavaScripty веб-сайті, який передає інформацію про пристрої вашого клієнта (ноутбуки, планшети тощо) до служби DetectFraud для виявлення шахрайства.

DetectFraud видає поля оцінка та опис. Оцінка ґрунтується на простій, стійкій формулі, а опис надає її словесне пояснення. Не можна повністю покладатися на оцінку, яку видає DetectFraud, для підвищення безпеки транзакції варто також дотримуватися інших правил, які описані у вкладці Help.

3.3 SOAP – повідомлення у Web –сервісі

Відомо, що SOAP-додатки створювалися та створюються у взаємодії з PHP. Однак не може не залишитись непоміченим той факт, що з'явилися розширення SOAP для PHP-5, які організовують підтримку SOAP у PHP на Сі. Основна перевага даних релізів – їх швидкість. З урахуванням Web-сервісу контролю несправності автомобіля, це дає безліч переваг. Використання SOAP-рішень спільно з PHP відкриває практично безмежні функціональні можливості для створення серверів такого типу, як використовуються у вищезгаданому сервісі.

Нижче розглянемо принцип роботи такого веб-сервісу. До його складу входить SOAP-сервер, WSDL-файл, SOAP-клієнт, набір допоміжних PHP-файлів. Обмін даними відбувається за допомогою XML.

Зазвичай у заголовку SOAP-клієнта вказуються URI-сервер, простір імен, заголовок SOAPAction, спосіб кодування, типи параметрів, тобто. дані, необхідних функціонування всього сервісу [17]. Набагато зручніше це робити безпосередньо в тексті SOAP-коду, а скористатися таким засобом як WSDL-файл. Вся зазначена вище інформація буде братися з файлу WSDL. Цей файл

буде в тій же директорії, що і SOAP-сервер.

На рисунку 3.2 представлено SOAP-клієнт (відправник).

```
<?php
$client=
newSoapClient("http://our_server.net/soap/urn:information_observe.wsdl");
$object_info =($client->getInfo("object_id"));
?>
```

Рисунок 3.2 – SOAP-клієнт (відправник)

На рисунку 3.3 наведено приклад WSDL файлу.

```
<?xml version ='1.0' encoding ='UTF-8' ?> <definitions
name='StockQuote' targetNamespace='http://

our_server.net/GetInfo' xmlns:tns=' http://
our_server.net/GetInfo'
xmlns:soap='http://schemas.xmlsoap.org/wsdl/soap/'
xmlns:xsd='http://www.w3.org/2001/XMLSchema' xmlns:soapenc='http:/
/schemas.xmlsoap.org/soap/encoding/'
xmlns:wsdl='http://schemas.xmlsoap.org/wsdl/'
xmlns='http://schemas.xmlsoap.org/wsdl/'> <message name
='getInfoService'> <part name='symbol' type='xsd:string'/>
</message> <message name='getInfoService'> <part name='Result'
type='xsd:float'/> < /message> <portType
name='InfoServicePortType'> <operation name='getInfo'> <input
message='tns:getInfoService'/> <output
message='tns:getInfoResponse'/> </operation> </portType> < binding
name='InfoServiceBind' type='tns:InfoServicePortType'>
<soap:binding style='rpc'
transport='http://schemas.xmlsoap.org/soap/http'/> <operation
name='getInfo'> <soap:operation
soapAction='urn:information_observe#getInfo'/>


<input> <soap:body use='encoded'
namespace='urn:information_observe'
encodingStyle='http://schemas.xmlsoap.org/soap/encoding/'/>
</input>



<output> <soap:body use='encoded'
namespace='urn:information_observe'
encodingStyle='http://schemas.xmlsoap.org/soap/encoding/'/>
</output> </operation> </binding >
```

```
<service name='WEBService'> <port name='WEBServicePort'
binding='WEBService'> <soap:address
location='http://our_server.net/get_info.php'/> </port> </service>
</definitions>
```

Рисунок 3.3 – WSDL-файл

На рисунку 3.4 представлено листинг самого SOAP-сервера.

```
<?php class InfoService { private $info = array("object_id" =>
$data_array); function getInfo($object_id) { if (isset($this-
>quotes[$object_id ])) { return $this->quotes[$object_id ]; } else {
throw new SoapFault("Server","Unknown Symbol 'object_id'."); } } }
$server = new SoapServer("information_observe.wsdl"); $server-
>setClass("InfoService"); $server->handle(); ?>
```

Рисунок 3.4 – SOAP-сервер

Основна функція протоколу SOAP – забезпечувати обмін інформацією між програмами на різних платформах. На рисунку 3.5 показано, що за допомогою SOAP-сервера взаємодіють два агенти, які працюють на різних платформах і принципах. Клієнтські програми спецслужб можуть бути виконані на різних основах (DELPHI, VB, PHP та ін.), у той час як база даних MySQL працює на SQL-командах. «Адаптером» між ними є SOAP-сервер, який обробляє запити спецслужб і повертає відповідні дані про об'єкти (ті об'єкти, про які йдеться в запитах, що надсилаються додатками в спецслужбах). Більш детальна робота всіх повідомлень представлена рисунку 3.5.

SOAP заснований на синтаксисі XML. Між відправником та одержувачем SOAP-повідомлень курсують листи XML. Запит від спецслужби надходить у середовище SOAP, інтерпретується в XML-повідомлення, що генерується

сервером SOAP, відправляється одержувачу (досі серед SOAP), де воно інтерпретується у команди PHP містять SQL запити. Ці SQL запити «витягують» дані з БД, а PHP формує їх масив, який зберігається в змінної. У даному масиві міститься так само клітинка з номером об'єкта, інформацію про який необхідно передати спецслужбі.

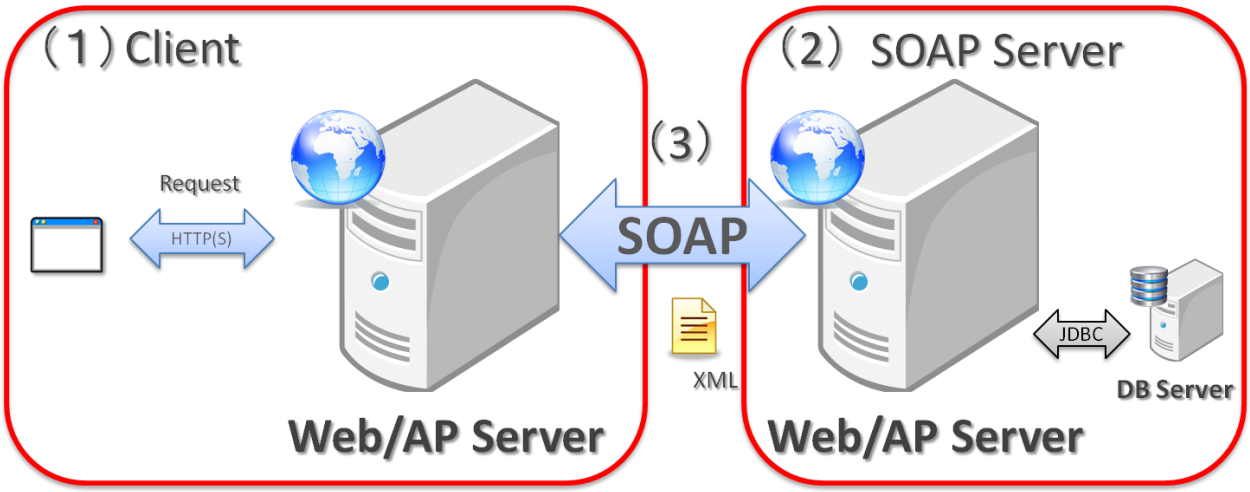

Рисунок 3.5 - Web-сервіс на SOAP-сервері

Взаємодія цих даних видно у списку SOAP-сервера вище. Тепер SOAP-сервер формує повідомлення у відповідь. Отриманий масив даних оговтується в XML-повідомленні у зворотному напрямку, серед SOAP йому надається вигляд, зрозумілий клієнтському додатку спецслужби. Ця програма приймає дані і вже аналізує їх у тому порядку, який у ньому передбачено.

Всі описані операції передачі даних відбуваються в середовищі HTML, таким чином немає необхідності відкривати безліч портів і, крім того, брандмауери, у зв'язку з цим, не є перешкодою.

Лістинги XML-повідомлень, які становлять основу передачі в даному Web-сервісі представлені рисунку 3.6.

```
<?xml version="1.0" encoding="UTF-8" ?>
<SOAP-ENV:Envelope
xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="urn: information_observe "
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body>
<ns1:getInfo>
<object_id xsi:type="xsd:string">XXXX</object_id>
</ns1:getInfo>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Рисунок 3.6 – XML-повідомлення запиту

Як відомо, тіло SOAP-повідомлення складається з «конверта» (SOAP-ENV:Envelope), заголовка (необов'язковий елемент) і тіла повідомлення (SOAP-ENV:Body), в якому, власне, і міститься весь зміст листа [18]. На рисунку 3.7 зображено XML повідомлення відповіді.

У цьому повідомленні у відповідь виходить масив, що містить дані про запитуваному об'єкті. Можна реалізувати відображення не змінної, що містить масив, а весь масив з назвами полів. Але це важливо. Далі слідує обробка масиву передачі його у зрозумілому вигляді для програми спецслужби, де вже й відбувається аналіз отриманих даних.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="urn: information_observe"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body>
<ns1:getInfoResponse>
<Result xsi:type="xsd:array">data_array</Result>
</ns1:getInfoResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Рисунок 3.7 – XML-повідомлення відповіді

Отриманий масив даних оговтується в XML-повідомленні у зворотному напрямку, серед SOAP йому надається вигляд, зрозумілий клієнтському додатку. Ця програма приймає дані і вже аналізує їх у тому порядку, який у ньому передбачено.

SOAP заснований на синтаксисі XML. Між відправником та одержувачем SOAP-повідомлень курсують листи XML. Запит від спецслужби надходить у середовище SOAP, інтерпретується в XML-повідомлення, що генерується сервером SOAP, відправляється одержувачу (досі серед SOAP), де воно інтерпретується у команди PHP містять SQL запити. Ці SQL запити «витягують» дані з БД, а PHP формує їх масив, який зберігається в змінної. У даному масиві міститься так само клітинка з номером об'єкта, інформацію про який необхідно передати спецслужбі. Тепер SOAP-сервер формує повідомлення у відповідь. Отриманий масив даних оговтується в XML-повідомленні у зворотному напрямку, серед SOAP йому надається вигляд, зрозумілий клієнтському додатку

спецслужби. Ця програма приймає дані і вже аналізує їх у тому порядку, який у ньому передбачено.

4 ОПИС ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

4.1 Види пакетів

"Standard Pack".

Цей пакет забезпечує можливість підтверджувати, що країна, назва та номер телефону БІН відповідають інформації, наданої клієнтом, для оцінки riskScore.

"Premium Pack".

Заснований на «Standard Pack», але при цьому додаються деякі опції для можливості визначити конкретніше транзакція шахрайської чи ні. Служба класу Premium підтверджує відповідність цих факторів, а також видає країну, назву, номер телефону БІН, і відомості про те, чи є картка передплаченою. Номер телефону БІН можна використовувати для дзвінка до банку для підтвердження відомостей про власника картки.

"Premium + Pack".

Цей продукт заснований на «Premium Pack», але доступні більш вдосконалені та розширені функції. Цей пакет дає можливість відправляти запити відразу експерту для максимального забезпечення безпеки.

4.2 Робота Web-сервісу DetectFraud

Даний Web-сервіс має кілька частин: адміністративну та користувальницьку.

Адміністративна панель полегшує користувачеві додавати нові новини, виправляти інформацію, робити розсилку та стежити за надходженням транзакцій, які є небезпечними виходячи з результату riskScore.

На рисунку 4.1 представлено адміністративну частину в режимі онлайн-спостереження за транзакціями:

DetectFrID	IP	Domain	City	Region	Postal	Country	BIN	Distance	Score	Time	ProxyScore	RiskScore
891HGBJ8	99.103.173.247	earthlink.net	Spring	TX	77379	us	401174	1	0	2012-01-16 08:59:34	0	0.1
IV8H03D7	99.103.173.247	earthlink.net	Spring	TX	77379	us	401174	1	0	2012-01-16 08:02:06	0	0.1
VRSTDB4N	41.206.12.18	yahoo.com	Crivitz	WI	54114	us	601100	9645	10	2012-01-15 03:04:21	0	56.01
WJ1PU954	41.206.12.18	yahoo.com	Omaha	NE	68116	us	601100	10337	10	2012-01-15 03:01:26	0	56.01
YSLC5XSG	70.160.222.49	MPSIntelligence.com	Virginia Beach	VA	23462	us	424631	27	0.01	2012-01-11 21:46:19	0	0.24
RMCKMRCK	72.49.40.4	enginepartswholesale.com	Owensville	Oh	45160	us	544928	13	0.01	2012-01-10 00:30:16	0	0.1
0MEVCKZC	98.116.85.78	gmail.com	Oceanside	New York	11572	us	431307	11	2.51	2012-01-09 13:15:53	0	0.1
D172L6P6	173.72.31.178	ameridiscorp.com	Ewing	NJ	08628	us	431247	5	0	2012-01-05 07:39:05	0	0.1
S082FTGO	173.72.31.178	ameridiscorp.com	Ewing	NJ	08628	us	431247	5	0	2012-01-05 07:38:54	0	0.1
WZCEB0IM	24.25.223.217	webcolamedia.com	Jericho	New York	11753	us	431231	3935	1.96	2012-01-02 12:52:02	0	4.18
ILH0M43V	24.25.223.217	boydsbearsonline.com	Mount Sinai	NY	11766	us	480213	3978	1.99	2012-01-02 12:50:27	0	5.5
DXFQHGRZ	24.25.223.217	onsitelogic.com	Leawood	KS	66224	us	601139	2124	1.06	2012-01-02 12:49:36	0	5.06
72ZMIOYK	24.25.223.217	neldasvintageclothing.com	san antonio	texas	78250	us	465548	1790	0.89	2012-01-02 12:47:54	0	6.61
22ZVIX39	24.25.223.217	gmail.com	Irvine	CA	92618	us	372340	107	2.55	2012-01-02 12:46:10	0	1
Q09HGIKD	24.25.223.217	comcast.net	White House	TN	37188	us	376750	2798	1.4	2012-01-02 12:45:20	0	1.02

Рисунок 4.1 – Адміністративна частина у режимі онлайн-спостереження за транзакціями

Ця частина має таблицю, що складається з таких розділів як: DetectfraudID, IP, Domain, City, Postal, Region, Country, BIN, Distance, Score, Time, ProxyScore, RiskScore. Розділ «DetectfraudID» – це ідентифікаційний номер транзакції, «IP» показує IP-адресу покупця в момент здійснення покупки, «Domain» уточнює який поштовий сервіс був вказаний при здійсненні транзакції, «City» - місто покупця, вказане в доставці, «Postal» є індексом доставки, «Region» - регіон доставки, «Country» - країна доставки, «BIN» - банківський ідентифікаційний номер картки якої був оплачений товар в інтернет-магазині, «Distance» - це відстань між адресою доставки товару та IP адресою, «Score » є оцінкою ступеня

шахрайства, «Time» - час здійснення покупки, «ProxyScore» - оцінка яка вказує на ймовірність використання проксі, «RiskScore» є основною оцінкою ступеня шахрайства за стобальною шкалою.

Оцінка riskScore, що видається службою DetectFraud, Висловлює ймовірність того, що конкретна транзакція є шахрайською. Продавці використовують оцінку riskScore, щоб визначити, чи варто їм прийняти, відхилити, фізично розглянути чи надіслати транзакції до додаткових служб на подальший розгляд. Не існує однієї строго встановленої системи показників оцінки riskScore, яку можна використовувати при ухваленні рішення про прийняття, відхилення, фізичний розгляд транзакцій або передачі їх у додаткові служби на подальший аналіз.

При виборі транзакції з розділу DetectfraudID відбувається перехід на сторінку Fraud Score з докладним описом інформації про IP користувача, використанням анонімних або відкритих проксі, чи був використаний ним безкоштовний email сервіс або email сервіс, що знаходиться у списку з високою ймовірністю шахрайства, інформація про БІН (номер) БІН, назва банку, гаряча лінія банку, країна походження банку), чи складається адреса доставки товару в чорному списку, чи код телефону вказаний при покупці зі штатом БІН. У розділі «Inputs» показуються дані, які вводив користувач картки при здійсненні покупки, а також IP адреса та БІН, які були отримані.

На рисунку 4.2 зображено транзакцію з низьким рівнем ймовірності шахрайства. Як видно, відстань між IP адресою та білінг адресою 1 км, що є низьким показником. IP адреса країни збігається з адресою білінгу; US не є країною з високим ризиком шахрайства; користувач не використовував безкоштовний електронний сервіс; не користувався анонімними та відкритими проксі; БІН також збігається з білінг адресою; адреса доставки відсутня у чорному списку; телефонний код не збігається з локацією адреси білінгу.

На рисунку 4.3 зображено транзакцію із середнім рівнем ймовірності шахрайства. Як видно, відстань між IP адресою та білінг адресою 9645 км, що є дуже високим показником шахрайської транзакції. IP адреса країни не

збігаються з білінг адресою; Нігерія є країною з високим ризиком шахрайства; Користувач використовував безкоштовний email сервіс; не користувався анонімними та відкритими проксі; адреса доставки відсутня у чорному списку; телефонний код збігається із локацією білінг адреси; БІН збігається з білінг адресою.

На рисунку 4.4 зображено транзакцію з високим рівнем ймовірності шахрайства. Як видно, відстань між IP адресою та білінг адресою 37 км, що є не високим показником шахрайської транзакції. IP адреса країни збігаються з білінг адресою; US не є країною з високим ризиком шахрайства; користувач використовував безкоштовний email сервіс, такий як mail.ru, даний email сервіс внесений до бази як сервіс з поганою репутацією; був використаний анонімний проксі зокрема VPN; адреса доставки полягає у чорному списку shipping адрес; БІН збігається з білінг адресою. Враховуючи в сукупності всі фактори, можна зробити висновки, що транзакція є з ймовірністю 94% шахрайської, оскільки був використаний VPN сервіс, електронна пошта була використана з російського email сервісу, адреса доставки занесена в чорний список, що вказує на неодноразовий обман з боку одержувача.

Fraud Score low risk 0 1 2 3 4 5 6 7 8 9 10 high risk

Estimated distance from IP Address to Billing Address, in Kilometers:	1
Country Match	Yes
IP Country Code	US
High Risk Country	No
Free E-mail Provider	No
Anonymous Proxy	No
BIN Country Code	US
BIN Match	Yes
BIN Name	Whitney bank
BIN Phone	(504) 5867543
Ship Forward	No
Customer Phone in Billing Location	No
Open Proxy Score (0 low risk, 3 and above high risk)	0
Carder Email	No
Fraud Score (0 low risk, 10 high risk)	0
riskScore	5,00

Inputs

IP Address	99.103.173.247
Domain of E-mail address	earthlink.net
Billing City/Region/Postal	Spring TX 77379
Billing Country	US
BIN Number	401174
BIN Name	Whitney bank
BIN Phone	(504)5867543
Customer Phone	(305)2842211
Ship Address	Twister Tr 20
Ship City	Spring
Ship Region	TX
Ship Postal	77379
Ship Country	US
Requested Type	standard
Transaction ID	24291
Session ID	891HGBJ8
Accept Language	English

Рисунок 4.2 – Докладний опис транзакції з низьким рівнем ймовірності шахрайства

Fraud Score low risk 0 1 2 3 4 5 6 7 8 9 10 high risk

Estimated distance from IP Address to Billing Address, in Kilometers:	9645
Country Match	No
IP Country Code	NG
High Risk Country	Yes
Free E-mail Provider	Yes
Anonymous Proxy	No
BIN Country Code	US
BIN Match	Yes
BIN Name	Discover Bank
BIN Phone	1-800-347-74-49
Ship Forward	No
Customer Phone in Billing Location	Yes
Open Proxy Score (0 low risk, 3 and above high risk)	No
Carder Email	No
Fraud Score (0 low risk, 10 high risk)	10
riskScore	56,01

Inputs

IP Address	41.206.12.18
Domain of E-mail address	yahoo.com
Billing City/Region/Postal	Crivitz WI 54114
Billing Country	US
BIN Number	601100
BIN Name	Discover Bank
BIN Phone	1-800-347-74-49
Customer Phone	717-22-5683
Ship Address	Fritzie Ave 7
Ship City	Crivitz
Ship Region	WI
Ship Postal	54114
Ship Country	USA
Requested Type	Standard
Transaction ID	24291
Session ID	VRSTDB4N
Accept Language	English

Рисунок 4.3– Детальний опис транзакції із середнім рівнем ймовірності шахрайства

Fraud Score low risk 0 1 2 3 4 5 6 7 8 9 10 high risk

Estimated distance from IP Address to Billing Address, in Kilometers:	37
Country Match	Yes
IP Country Code	US
High Risk Country	No
Free E-mail Provider	Yes
Anonymous Proxy	Yes
BIN Country Code	US
BIN Match	Yes
BIN Name	Bank of America
BIN Phone	1-888-222-10-12
Ship Forward	Yes
Customer Phone in Billing Location	Yes
Open Proxy Score (0 low risk, 3 and above high risk)	0
Carder Email	Yes
Fraud Score (0 low risk, 10 high risk)	10
riskScore	94,15

Inputs

IP Address	72.49.40.4
Domain of E-mail address	mail.ru
Billing City/Region/Postal	Omaha NE 68116
Billing Country	US
BIN Number	431307
BIN Name	BOF
BIN Phone	1-888-222-10-12
Customer Phone	717-22-56-83
Ship Address	Charles St 18
Ship City	Omaha
Ship Region	NE
Ship Postal	68116
Ship Country	USA
Requested Type	Standard
Transaction ID	45142
Session ID	IE23AQ80
Accept Language	English

Рисунок 4.4 – Детальний опис транзакції з високим рівнем ймовірності шахрайства

Що стосується користувальницької частини, то вона була створена з комерційними цілями, щоб представляти продукцію DetectFraud та здійснювати продаж через Інтернет. На рисунку 4.5 представлено головну сторінку сайту для продажу продукту DF.

Рисунок 4.5 – Головна сторінка сайту DetectFraud

На головній сторінці є такі блоки, такі як: DetectFraud service overview (огляд служби DetectFraud), packs (пакети), feature comparison (порівняння параметрів), registration (реєстрація), trial account (пробний обліковий запис), news (новини), blog (блог), help (допомога), contacts (контакти), popular request (популярні запити).

DetectFraud service overview – у цьому блоці описується служба DetectFraud, як вона працює, з якого принципу працює, що її відрізняє від інших подібних служб та її ключові функції.

Packs – блок описує види та пакети умов служби, кожен пакет має різну

ціну та свої особливості та доповнення. Для кожного пакета створена окрема сторінка, яка представлятиме продукт, де описано, що це продукт його властивості, можливості.

Feature comparison – цей блок докладно порівнює параметри пакетів для більш простого вибору.

Help – цей блок представляє найчастіші запити на сайті як гостей, так і користувачів, які зареєстровані на сайті. Тут люди залишають свої питання, пропозиції, враження про наш продукт (якщо це користувачі).

Most popular requests – цей блок представляє найчастіші запити на сайті як гостей, так і користувачів, які зареєстровані на сайті. Тут люди залишають свої питання, пропозиції, враження про наш продукт (якщо це користувачі).

Registration – блок реєстрації, де реєструються користувачі.

News – цей блок має окрему сторінку, містить інформацію про погодні умови та новини на дорогах, що є важливим для водіїв.

Blog – цей блок має окрему сторінку, тут гості та користувачі сайту залишають свої побажання, питання та враження про продукт.

Trial account – цей блок пропонує користувачам спробувати службу DetectFraud абсолютно безкоштовно для ознайомлення та пропонує пройти реєстрацію в обмін на обмежену кількість запитів.

На рисунку 4.6 зображено блок Feature Comparison з докладним описом параметрів пакетів, що передалися.

На рисунку 4.7 представлена сторінка сайту «DetectFraud», де користувач може скористатися можливістю реєстрації пробного облікового запису та отримати безкоштовно 1000 стандартних та 100 преміум запитів служби DetectFraud.

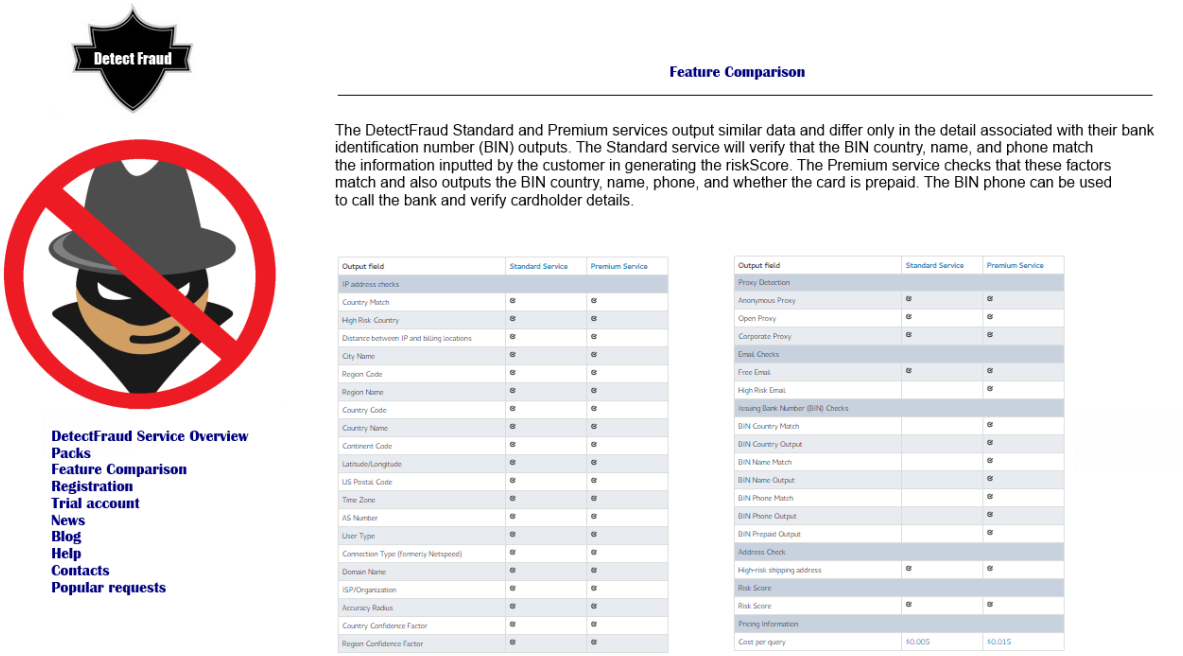

Рисунок 4.6 – Сторінка Feature Comparison сайту «DetectFraud»

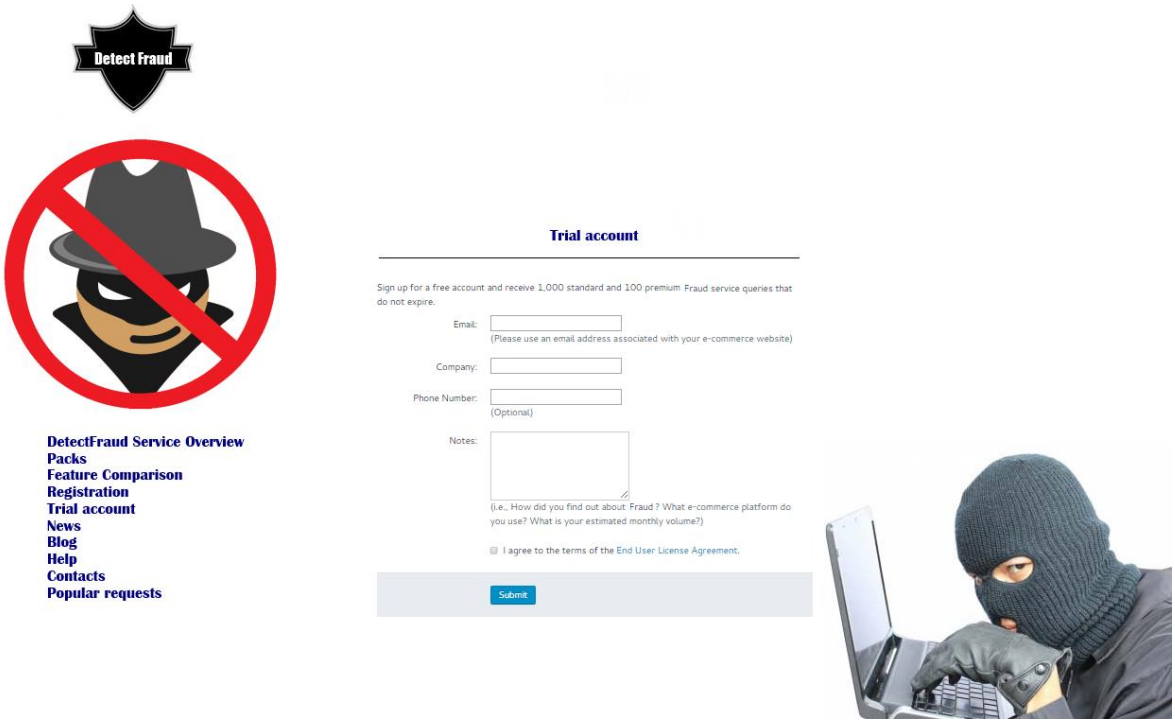

Рисунок 4.7 – Сторінка реєстрації пробного облікового запису

На рисунку 4.8 представлений один із пакетів пристрою, а саме Standard

Pack, подібним чином створені сторінки для Premium Pack, Premium + Pack тільки зі своїм описом, особливостями та доповненнями. Користувач вибирає собі пакет із наданих та система його переводить на сторінку реєстрації нового користувача.

Рисунок 4.8 – Сторінка Standard Pack сайту DetectFraud

На рисунку 4.9 знаходиться інформація з формою реєстрації, де користувач реєструє себе та вказує своє ім'я, прізвище, країну проживання, поштовий індекс, контактний телефон, електронну пошту та який пакет він вибирає, якщо ще не був обраний.

Після успішної реєстрації користувачеві доступна адміністративна частина і може проводити безпечні транзакції залежно кількості куплених їм запитів.

Рисунок 4.9 – Сторінка реєстрації нового користувача

DetectFraud service overview – у цьому блоці описується служба DetectFraud, як вона працює, з якого принципу працює, що її відрізняє від інших подібних служб та її ключові функції.

Packs – блок описує види та пакети умов служби, кожен пакет має різну ціну та свої особливості та доповнення. Для кожного пакета створена окрема сторінка, яка представлятиме продукт, де описано, що це продукт його властивості, можливості.

Feature comparison – цей блок докладно порівнює параметри пакетів для більш простого вибору.

ВИСНОВКИ

На сьогоднішній день залишається безліч способів отримання конфіденційної інформації банківських систем. Тому не можна захистити звичайного користувача кредитної картки від попадання особистої інформації в чужі руки. Тому потрібен сервіс, який зміг би розпізнавати та визначати ймовірність того, що транзакція є не шахрайською, ґрунтуючись на різних факторах.

Але, як і в реальному житті, в системі захисту інформації існує жорстка конкуренція, не програти в якій допомагає постійне вдосконалення системи, виходячи від методів шахраїв. Так само слід з обережністю ставиться до визначення програм анонімності, невміле їх обчислення може згубно позначитися на всьому сервісі і, як наслідок, сервіс працюватиме некоректно.

Залишається безліч способів отримання конфіденційної інформації банківських систем. Тому не можна обгородити звичайного користувача кредитної картки від потрапляння особистої інформації в чужі руки; потрібен сервіс який зміг би розпізнавати та визначати ймовірність того, що транзакція є не шахрайською, ґрунтуючись на різних факторах.

У роботі поставленим завданням було реалізувати інтелектуальну систему захисту під назвою Detect Fraud.

Сервіс Detect Fraud знизив кількість зворотних платежів, розпізнаючи замовлення групи ризику та зупиняючи їх до подальшого розгляду. Ця служба використовується для розпізнавання шахрайської діяльності в електронно-комерційних транзакціях, партнерських посиланнях, опитуваннях, входах у систему та реєстраціях.

Detect Fraud визначає ймовірність того, що транзакція є шахрайською, ґрунтуючись на різних факторах, включаючи те, чи надходить онлайн-транзакція з IP-адреси, електронної адреси або пристрою підвищеного ризику або з анонімного проксі-сервера. Однією з ключових функцій сервісу Detect Fraud є

мережа, яка дозволяє визначати та зберігати репутації IP-адрес, адрес електронної пошти та інших параметрів.

Користувачі служби отримують користь з динамічного та адаптивного підходу до виявлення шахрайської діяльності та взаємного захисту мережі Detect Fraud. Наприклад, якщо буде виявлена підозріла діяльність з певної IP-адреси, вона буде позначена як адреса підвищеного ризику у всій мережі Detect Fraud у режимі реального часу. Таким чином, відгуки продавців є попереджувальними сигналами для решти всіх членів мережі Detect Fraud.

Сервіс може використовуватися сам по собі або як доповнення до існуючої корпоративної системи відстеження шахрайської діяльності.

У процесі досягнення поставленої мети було вирішено такі завдання, як вивчення технології створення Web-сервісів, вивчення внутрішньої структури Web-сервісів, вивчення принципів роботи Web-сервісів, розробка алгоритму визначення шахраїв у системі, розробка власного Web-сервіс Detect Fraud.

Даний Web-сервіс оснащений зручною системою керування вмістом. У цьому проекті реалізована адміністративна частина, таким чином, що адміністратор зможе легко переглядати, видаляти чи редагувати інформацію, що надходить від сервісу та пересилати далі інформацію потрібним службам залежно від рівня платежу.

На сьогоднішній день кардинг – це не просто окремі шахраї, це організована злочинна спільнота. Воно має свої сайти та форуми, на яких новачки долучаються до обрядів ремесла, а професіонали обмінюються корисними порадами.

Але, як і в реальному житті, в системі захисту інформації існує жорстка конкуренція, не програти в якій допомагає постійне вдосконалення системи, виходячи від методів шахраїв. Так само слід з обережністю ставиться до визначення програм анонімності, невміле їх обчислення може згубно позначитися на всьому сервісі і, як наслідок, сервіс працюватиме некоректно.

Тільки грамотне використання сукупності методів дасть позитивний ефект.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Платіжні технології [Електронний ресурс] / Режим доступу: www/ URL: http://bankir.ru/tehnologii/s/zaschita-ot-kardera-9057392/ – Загл. з екрану.

2. Web Services Architecture [Електронний ресурс] / Режим доступу: www/ URL: http://www.w3.org/TR/ws-arch/ – Загл. з екрану.

3. Web Services Essentials Distributed Applications with XML-RPC, SOAP, UDDI & WSDL [Text] / Ethan Cerami / Publisher: O'Reilly // First Edition. - February 2002 . - 304 pages. - ISBN: 0-596-00224-6

4. Web Services Implementation Guide [Text] / Brian E. Travis, Mae Ozkan / March 2002 – 352 pages. - ISBN-10: 0964960230

5. LAN/журнал мережевих рішень[Текст], вересень 2013

6. Вікіпедія, вільна енциклопедія [Електронний ресурс] / Режим доступу: www/ URL: http://ua.wikipedia.org – Загл. з екрану

7. Azuma, R. Survey of Augmented Reality [Text] / R. Azuma. - London: AR, 1997. - P.355-385.

8. Ray Casting for Modeling Solids [Електронний ресурс] / Google Books. – Режим доступу: www/ URL: https://books.google.com.ua/books/about/Multiple_View_Geometry_in_Computer_Visio.html?id=si3R3Pfa98QC&hl=ua – Загл. з екрану.

9. Bigtable: A Distributed Storage System for Structured Data [Електронний ресурс] – Електрон. текст. дано. – режим доступу: www/ URL: http://static.googleusercontent.com/media/research.google.com/en/ /archive/bigtable-osdi06.pdf– Загл. з екрану.

10. Думки експертів про CC [Електронний ресурс] / AR-Conference – Режим доступу: www/ URL: http://ar-conf.ru/ru/news/virtualnaya-realnost-mneniya-ekspertov-o-budushchem – Загл. з екрану.

11. Bin Database - Credit Card Bin Checker[Електронний ресурс] / Режим доступу: www/ URL: https://bindb.com/bin-database.html – Загл. з екрану.

12. Кардинг – реальний бізнес для віртуальних шахраїв [Електронний ресурс] / Режим доступу: www/ URL: http://bank-stories.blogspot.com/2008/03/blog-post_03.html– – Загл. з екрану.

13. Кардинг або як крадуть гроші з кредиток [Електронний ресурс] Зв'язок та віртуальна валюта Режим доступу: www/ URL: http://www.prostobank.ua/kreditnye_karty/stati/karding_ili_kak_voruyut_dengi_s_kreditok– Загл. з екрану.

14. Речовий кардинг або сумнівний продаж [Електронний ресурс] / Режим доступу: www/ URL: http://webplot.ru/lrub2part4.html– Загл. з екрану.

15. Шиммінг - новий різновид скіммінгу [Електронний ресурс] Основи захисту від скімерів / Режим доступу: www/ URL: http://securitylab.ru/news/395811.php– Загл. з екрану.

16. Речовий кардинг продажу [Електронний ресурс] / Режим доступу: www/ URL:http://ccc.mn/forum/24-речовий-кардинг/– Загл. з екрану.

17. Рассел, С. Штучний інтелект: сучасний підхід [Текст]: навч. посібник / С. Рассел, П. Норвіг. - 2-ге вид., перероб. - М.: Вільямс, 2006. - 1408 с.