**COURSEWORK SUBMISSION FORM**

|  |  |  |  |
| --- | --- | --- | --- |
| **STUDENT USE** | | **STAFF USE** | |
| Module Name | Business Information Systems Project | First Marker’s  (acts as signature) |  |
| Module Code | 6BUIS007C-n - | Second Marker’s  (acts as signature) |  |
| Lecturer Name | Shodiyabegim Bakhtiyorzoda  Shirin Primkulova (supervisor) | Agreed Mark |  |
| Student Email Address | labdukhalilova@students.wiut.uz | **For Registrar’s office use only (hard copy submission)** | |
| WIUT Student Name | Laylo Abdukhalilova |
| Deadline Date | 09-02-2023 |
| Assignment Type | ☐ Group ☑ Individual |
| Word Count | 2000 |
| Project Title | Development of a system for detecting fraudulent activities in online payments |  | |

**SUBMISSION INSTRUCTIONS**

**COURSEWORKS *must* be submitted in *both* HARD COPY (to the Registrar’s Office) *and* ELECTRONIC unless instructed otherwise.**

For hardcopy submission instructions refer to: <http://intranet.wiut.uz/Shared%20Documents/Forms/AllItems.aspx> - Coursework hard copy submission instructions.doc

For online submission instructions refer to: <http://intranet.wiut.uz/Shared%20Documents/Forms/AllItems.aspx> - Coursework online submission instructions.doc

|  |
| --- |
| **MARKERS FEEDBACK (Continued on the next page)** |
|  |

**Table of Contents**

[Introduction with analysis 2](#_Toc66622086)

[SWOT analysis 6](#_Toc66622087)

[Rationale for choosing a programming language 9](#_Toc66622088)

[Conclusion 12](#_Toc66622089)

[Reference list 13](#_Toc66622091)

**Introduction and Analysis**

Online payments offer an easy and convenient way to shop. Due to the increase in the use of payment cards, especially in online purchases, cases of fraud have become more frequent. Growth creates financial risk and uncertainty as billions of dollars in losses occur annually in the commercial sector. However, actual transaction records, which can facilitate the development of effective predictive models for fraud detection, are difficult to obtain, mainly due to privacy concerns about customer information.

In this thesis, we apply a total of 13 statistical and machine learning models to detect payment card fraud using both public and real transaction records. The results of both initial and aggregated features are analyzed and compared. Statistical hypothesis testing is performed to evaluate whether the aggregated features identified by the genetic algorithm can provide better discrimination power than the original features in fraud detection. The results positively confirm the effectiveness of using aggregated functions to solve real-world problems of payment card fraud detection.

Many types of payment cards are now widely available, including credit, charge, debit, and prepaid cards, and they are one of the most popular payment methods in some countries. Indeed, advances in digital technology have changed the way we handle money. Payment methods have changed from physical activity to a digital transaction using electronic means. This has revolutionized the monetary policy of both large and small companies, including the business strategies and operations of banks.

According to Forbes, American bankers estimate that every second there are 10,000 payment card transactions in the world. Thanks to such a high transaction speed, payment cards have become a target for fraud. Fraud has been a major problem in most commercial and business environments. Indeed, ever since the Diners Club issued the first credit card in 1950, credit card companies have been constantly fighting fraud.

Every year, payment card fraud results in billions of dollars in losses. These losses create risk and uncertainty for financial institutions. Fraud occurs under different conditions, such as point-of-sale (POS) transactions, online or telephone transactions, i.e. Card Not Pre Send (CNP) cases or transactions involving lost or stolen cards. Losses from payment card fraud in 2015 amounted to $21.84 billion (Nilson report, 2016). According to the European Central Bank in 2012, the majority (60%) of fraud cases involved CNP transactions, with another 23% involving POS terminals.

The potential for generating significant cash income, combined with the ever-changing nature of financial services, creates a wide range of opportunities for fraud. Funds from payment card fraud are often used in criminal activities, such as supporting terrorist activities. Over the years, fraud mechanisms have evolved along with the models used by banks to avoid fraud detection. Therefore, it is essential to develop effective and efficient methods for detecting payment card fraud. Developed methods also need to be constantly reviewed in line with advances in technology. There are many challenges in developing effective fraud detection methods. Among them, researchers are having difficulty obtaining real samples of payment card transaction data as financial institutions are reluctant to share their data due to privacy concerns. As a result, only limited studies with real data are available in this area.

Some research on machine learning and related fraud detection research has been done using publicly available datasets. SVMs (Support Vector Machines), ANNs (Artificial Neural Networks), Decision Trees, and regression and rule-based methods.

This thesis implements thirteen widely used statistical and machine methods for detecting payment card fraud. Methods used include SVM and ANN as well as more advanced deep learning methodologies. Two data sources used for evaluation: public repositories and a database of real payment cards. In this study, the availability of real payment card data for evaluation is of particular importance, which ensures that the methods developed are applicable and useful in real situations. In other words, the developed methods should be applicable in the financial sector to detect payment card fraud, which will reduce financial losses and mitigate risks and uncertainty in the business world. The main contributions of the paper are twofold. First, the feature aggregation method is designed to process payment transaction records. A key benefit of aggregating different features from transaction data is increased robustness to counter the effects of concept drift. In addition, feature selection is applied to the transaction data using optimization techniques. Second, a real payment card database is used to analyze the performance of various data-driven statistical and intelligent fraud detection algorithms, in addition to using reference data. Since obtaining real financial statements for analysis is different (due to privacy concerns), the results of our study are important to provide valuable insight into the reliability of various data-driven methods using aggregate functions to detect fraud in real-world payment card transactions.

The relevance of my project is to identify fraudulent activities in online payments and analyze modern systems. Online payments provide convenience for both consumers and business owners. This is due to the fact that online payment systems provide an instant payment verification process. Consumers don't need to manually submit proof of payment. Also, payment systems are necessary for our individual life and for the normal functioning of the economy. They allow money to fulfill its role as the accepted medium of exchange in the purchase of goods or services. If money is the lifeblood of the modern money economy, then payment systems are the circulation system.

The main objectives are, firstly, to identify different types of online payment fraud and, secondly, to review alternative methods that have been used to detect fraud. On the other hand, other products such as consumer loans and retail are also at risk and have serious ethical implications for banks and credit card companies paying online. Also develop a system for detecting fraudulent activities in online payments. Online payment fraud can occur in a variety of ways, depending on the type of fraud in question; it covers bankruptcy scams, theft/counterfeiting scams, application scams, and behavioral scams. Each of these sub-categories of fraud has its own definition and specifics.

**The Importance of Online Payments**

What actually happens during an online payment?

The customer transfers money from their bank account or credit card account to the supplier's or merchant's bank account. Online payment can be made by credit card, checking account or other means such as PayPal.

Merchants or dealers accepting online payments must comply with security requirements. There are many cases of digital theft and hacking, as well as many other types of fraud, so it is important to follow the rules for the security of online payments.

A secure encrypted connection must be established for the transaction. Merchants must implement a long list of security features and protocols, also known as PCI compliance requirements, for recurring billing where customer data is stored.

For the online payment process, the merchant needs to have access to the online payment gateway. It is a service provider that is integrated with a credit card and communicates online payment information between the owner/merchant and the payment processor.

**SWOT analysis**

The **advantages** of online payments are as follows:

• Increases sales;

• Access to the global market;

• Reduced transaction costs;

• Security of payments;

• Credit cards to facilitate purchases with a low balance;

• Acceptance of payment method;

• Marketing tool;

• More attractive for impulsive buyers;

• Opportunities for regular payments;

• Increased speed and convenience;

• Low labor costs;

• Obtaining a competitive advantage.

Online payments allow you to pay for goods and services non-cash using cards, mobile phones or the Internet. The main benefits of using online payments are saving money and time, increasing sales and reducing transaction costs.

**Flaws**

Also, there are several issues to consider when making online payments. Such as:

1. technical problems;

2. Vulnerability to cybercriminals.

**Technical problems.**

Each system has its own technical problems.

Similarly, online payment methods must also face technical difficulties.

Vulnerability to cybercriminals.

As the online process increases, cybercrime and scams are also on the rise. Cybercriminals try to disable online payment methods or steal people's money or information using their hacking skills.

A business organization must protect its business from these cyber attacks. To do this, they have to invest more money in additional online security.

**Weak sides**

The fact is that many of the largest online payment servers have already implemented security systems in their transaction schemes that block third parties that threaten the personal data of buyers.

Also, our project is intended only for online payments for online purchases. The website will not be able to protect the personal data of users who simply make transactions and money transfers.

**Threats**

The main threat is what our website is fighting against. That is, in this project, I considered only 4 types of threats. In reality, there are many more of them. If scammers study the security system, they can easily find new ways to avoid protecting our users' sensitive information.

**Rationale for choosing a programming language**

When developing a system for detecting fraud in online payments, we design it using the following programming languages:

• PHP

• Apache

• HTML, CSS, JS

• OpenServer

• MySQL

PHP

PHP is an open source server-side scripting language that many developers use for web development. It is also a general purpose language that you can use to create many projects including graphical user interfaces (GUIs)

HTML, CSS and Javascript

Hyper Text Markup Language (HTML), Cascading Style Sheets (CSS), and JavaScript are the languages ​​that run the web. They are very closely related, but they are also designed for very specific tasks. Understanding how they interact will go a long way in becoming a web developer.

MySQL is an Oracle-supported open source relational database management system

(RDBMS) based on the Structured Query Language (SQL). MySQL runs on almost all platforms, including Linux, UNIX, and Windows. While it can be used in a wide variety of applications, MySQL is most commonly associated with web applications and online publishing.

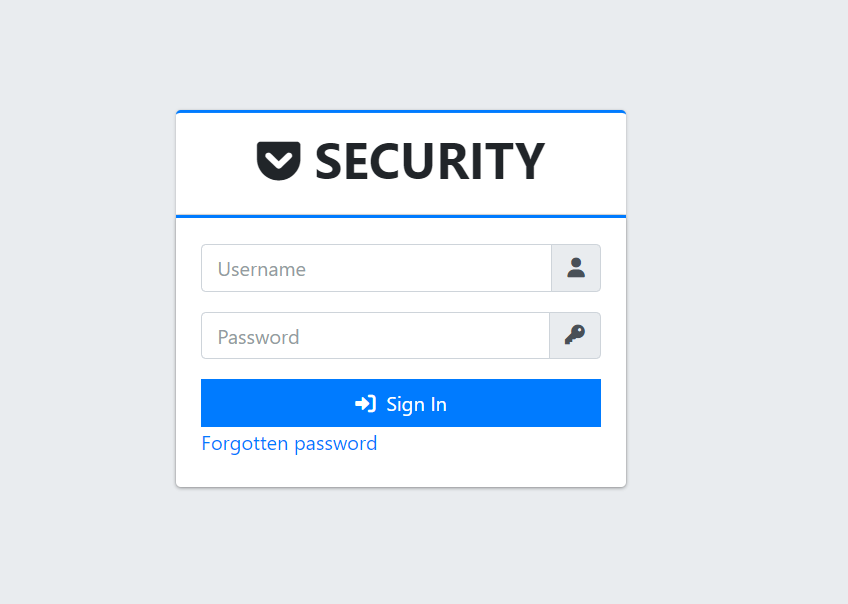
In the first part of PID, I presented a completely different project. In the second stage of the completion of the project, I decided to choose a more serious topic for my thesis.

The next two months I plan to develop the remaining pages and the database. In April, I will conduct an Audit - this is a comprehensive check of a website for technical vulnerabilities.

**Prototype**

Below is what has already been done.

In order to log in, user will need to enter username and password for account. This process is shown in the picture below.



Picture 2 shows the main page of the site, as well as the menu on the left side. The menu includes:

1. Site panel;

2. Information about the site;

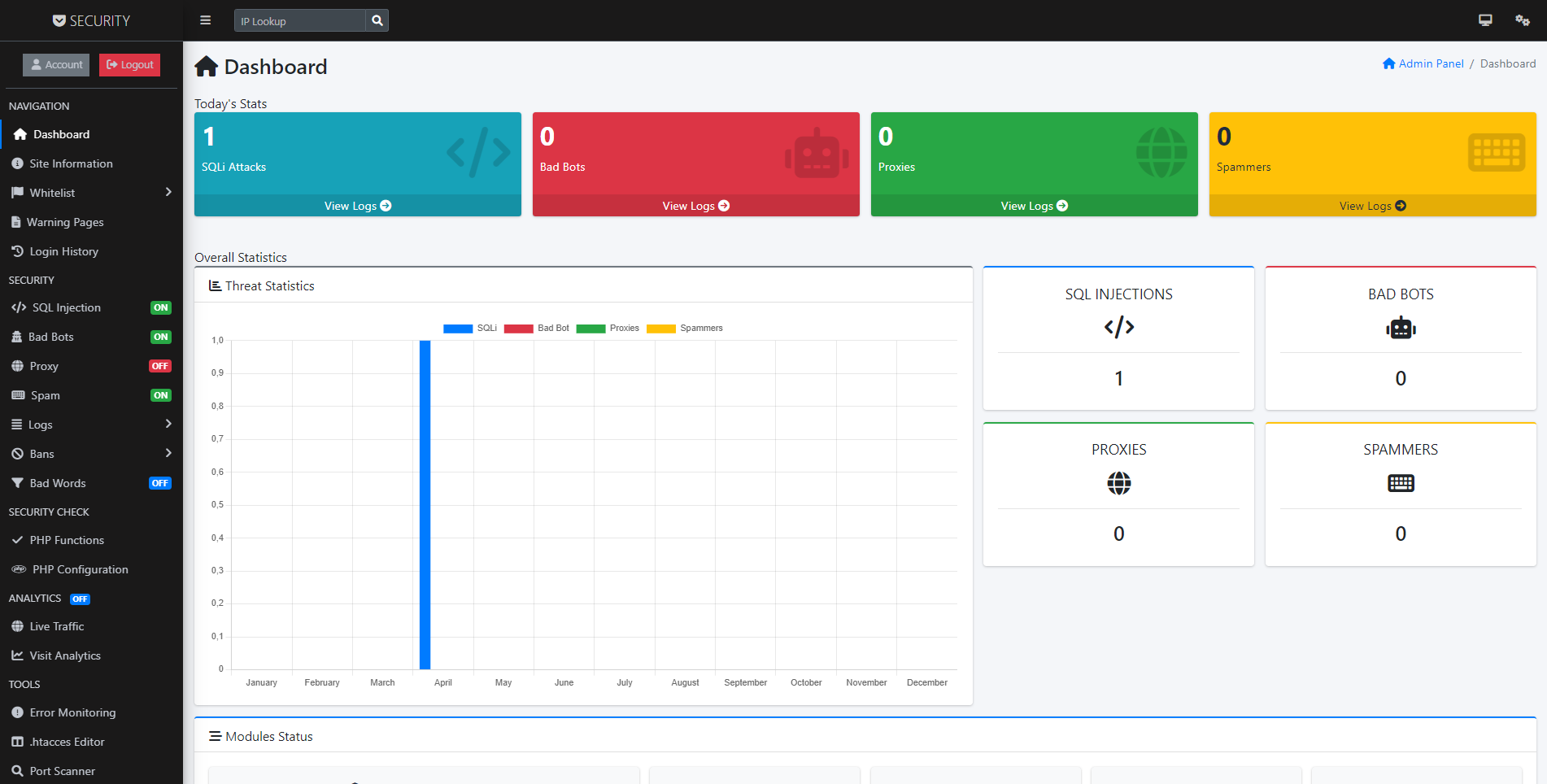
3. List of IP addresses;

4. Warning page;

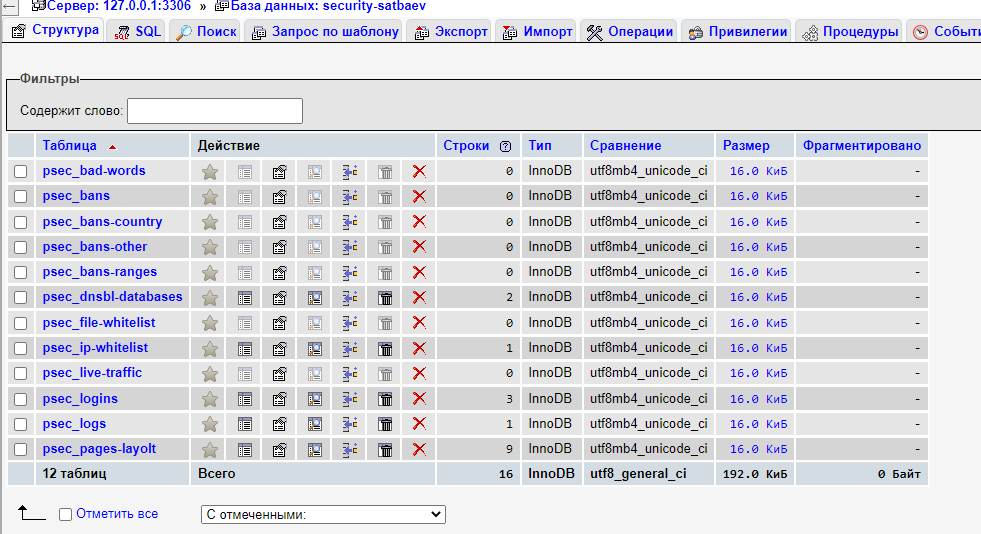
5. Login history;

6. Security.

In the site panel section, users can see information such as threat statistics, spammers and pro proxies.



The databases for the implementation of the site are shown next.



**Conclusion**

The change in technology has resulted in several improvements. In this thesis, we presented a study on the detection of fraud associated with payment card transactions. The main contribution is the development of a practical system using aggregate functions to detect payment card fraud and the use of real transaction records to evaluate and demonstrate the effectiveness of the developed system. Our research is important to mitigate the risks of financial loss as well as the uncertainties that institutions face in their day-to-day operations. A total of thirteen statistical and machine learning methods, ranging from ANNs to deep learning models, were used for estimation in our analysis. Three benchmark credit card datasets sourced from a public repository were used to evaluate performance.

**Reference list**

Moore, L. (2018) *What is mysql?: Definition from TechTarget*, *SearchOracle*. TechTarget. Available at: https://www.techtarget.com/searchoracle/definition/MySQL [Accessed: January 13, 2023].

*7 tips to improve your career development | indeed.com* (no date). Available at: https://www.indeed.com/career-advice/career-development/improve-your-career-development (Accessed: January 23, 2023).

Chris, K. (2021) *What is php? the PHP programming language meaning explained*, *freeCodeCamp.org*. freeCodeCamp.org. Available at: https://www.freecodecamp.org/news/what-is-php-the-php-programming-language-meaning-explained/ (Accessed: January 23, 2023).

*Fraud detection and verification system for online transactions: A ...* (no date). Available at: https://www.inderscienceonline.com/doi/abs/10.1504/IJEBANK.2020.114762 (Accessed: February 1, 2023).

L. (2018) *What is mysql?: Definition from TechTarget*, *SearchOracle*. TechTarget. Available at: https://www.techtarget.com/searchoracle/definition/MySQL (Accessed: February 5, 2023).

*PHP* (2023) *Wikipedia*. Wikimedia Foundation. Available at: https://en.wikipedia.org/wiki/PHP (Accessed: February 8, 2023).

*What is mysql? everything you need to know* (no date) *Talend*. Available at: https://www.talend.com/resources/what-is-mysql/#:~:text=MySQL%20is%20a%20relational%20database,information%20in%20a%20corporate%20network (Accessed: February 8, 2023).

*What is User Interface (UI)? | indeed.com - indeed career guide* (no date). Available at: https://www.indeed.com/career-advice/career-development/user-interface (Accessed: February 9, 2023).