ABSTRACT
Link Consulting is a Portuguese company that owns an internet banking application that allows users to remotely access their bank accounts via internet and do the same operations they would on ATM. But as many other applications this one can also be a victim of malicious users, therefore needing security mechanisms to prevent fraud attacks. The system BankOnBox Fraud Detector allows the detection of fraud in historical data or in a real time transaction. An interface was also designed to allow the Back Office users to keep track of possible malicious users or to perform maintenance of the BankOnBox Fraud Detector System. The evaluation of the system showed that all the planned functionalities were completed and also showed the potential of this system in a real internet banking application.

GOALS
The main goals defined before the development of the BankOnBox Fraud Detector system were:

- Obtain user behavior information through the bank’s historical data. Historical data should be processed in order to obtain information about the user’s behavior while using the BankOnBox application.
- Use the information that resulted from processing the bank’s historical data and use it to detect fraudulent transactions in a real time fraud detection module.
  - Detect fraudulent users.
  - Detect stolen accounts.
- Create an interface that allows maintenance of the BankOnBox Fraud Detector and to monitor possible fraudulent users. This interface should be used by the Back Office users of the BankOnBox application.

PROBLEM
Most new internet users do not gain knowledge about the potential dangers of using it. The information is available but in most cases there is no willingness on the part of users to take notice of them.

Unconscious action by a user may jeopardize your personal information and eventually lead to improper access to bank accounts. Among the several attacks that are carried out today are the following [1][2][3]:

Stolen Account
Attackers do not need to use special technologies to perform this type of fraud, it is only necessary that some kind of access to the account be provided, whether banking
or otherwise, through carelessness of the user, such as leaving the application page open in a browser or saving the password in the browser so that the attacker can change account information like the email address. The exchange of the email allows later change the access password, since most authentication systems in case of forgetting the password sends information to the email associated with the account so that the password can be reset or changed.

This type of fraud can occur in another format, the so-called Shoulder Surfing in which the attacker knows the victim, this can a family member, friend or acquaintance. Fraud is based on the knowledge that the attacker possesses or is able to acquire from the victim, such as your personal information or habits. This knowledge is subsequently used to gain access to the victim’s account or to take action according to the standards the victim regularly uses when accessing the account.

**Malware**
Malware is a malicious software that is created with the intention of gaining non authorized access to systems, databases or networks. Malware used to gain access to internet banking systems is very common nowadays and can configured to access a particular bank internet application. This type of attack uses mechanisms like Browser Injection or Session Hijacking.

**Pishing**
The most common method of attack used is phishing, this method allows attackers to gain access to the user’s personal information thought emails that might seem real but will redirect the victim to a fake website in which the user will insert his sensitive information allowing attackers to use it to gain access to his bank accounts.

The detection of fake websites used in the phising method is becoming more and more difficult since the quality of the work developed. Nowadays more and more pishing application are being added to the google play store since they are not filtrated in the revision process.[4]

**RELATED WORK**

**Use of the Hidden Markov Model for fraud detection**
Sunil S. Mhamane e L.M.R.J Lobo created a fraud detection solution using the Hidden Markov Model [5]. This model is created using the user information, assigning each user a spending profile:

The model created in this solution is divided in four steps:

- Identifying each user spending profile
- Identifying each user usage pattern
- Build a sequence using the training data
- Build a training model

The resulting model will define for each client which is the acceptable spending for a particular type of product. This model way trained with regular transactions performed by normal users, which allows the model to detect transactions that are unusual for a particular client.

**Fraud detection by monitoring customer behavior and activities**
Parvinder Singh and Mandeep Singh developed a system to detect fraud on credit card transactions trough the analysis of customers activities and behavior[2]. For each transaction it is calculated a risk value that will later determine whether the transaction is fraudulent or not. For the risk calculating are analyzed the user behavior and physical locations when accessing a banking terminal.

The users behavior is identified by its spending’s using the clustering algorithm k-means.

Between every two transactions it is verified if the user changed locations and if it did the system checks if the distance travelled is possible within the time in which occurred.

**Barclaycard Fraud Detection Module Advanced**
The fraud detection module developed by Barclays [6] is divided in three components which are a module in which specific rules can be determined to block transactions, an additional security layer, the 3-D secure protocol and Blacklist/Greylist.

The rules specification module allows the users to specify the following rules that will be enforced to filter transactions

- Block transactions resulting from specifying countries;
- Define in which countries can the account perform transactions;
- The maximum and minimum amount that can be transferred to other accounts;
- Restrict the number of payments that can be performed in a time frame;
- Restrict the access to the account by IP during a time frame.

The user can also activate the 3-D secure protocol which allows the authentication using biometrics, html passwords or card readers.

The Blacklists will allow the system to block every transaction from accounts that are considered fraudulent. In cases in which it is not clear whether the user is fraudulent or not this will be associated to the Greylist.

**Neural Data Mining for Credit Card Fraud Detection**
R. Brause, T. Langsdorf e M. Hepp [7] showed how it is possible to combine Data Mining techniques with Neural Networks algorithms to obtain better results in fraud detection.
In this work each transaction is considered a tuple in which every attribute is characterized by a symbolic value. Using a database of fraudulent transactions it is possible to combine every transaction in order to obtain rules for fraud detection. For each rule created there is a share, which represents the number of transactions that the rule can detect. A value of confidence is also defined for each rule, which represents the number of false positives that the rule has detected. The symbol * will indicate that the transaction attribute will have no interest in the rule defined.

![Rule generalization tree](image)

**Figure 1. Rule generalization tree [7].**

Using the quantitative values of the transactions like the time of day or the value transferred, it is possible to create a neural network that is trained with both fraud and non-fraud transactions. The final classification of transactions is obtained combining both techniques.

**A Rule-Based and Game-Theoretic Approach to On-Line Credit Card Fraud Detection**

Vishal Vatsa, Shamik Sural e A. K. Majumdar proposed a two-tier fraud detection system with the first layer being a rule engine and the second a theoretical strategic game component [8].

The first layer uses a set of generic rules to classify the transaction as genuine or suspicious while the second layer uses dynamic techniques to predict the next action of the attacker and to calculate the credibility of the client taking into account the fraud model developed. The first layer uses specific rules such as the detection of outliers, detection of break points or types of products purchased. Through the detection of outliers or detection of break points is possible to detect abnormalities if the customer buys something out of the ordinary or buy something in exaggerated amounts.

Each of these rules allows you to assign a suspicious score to each transaction, if it is considered genuine it proceeds normally and otherwise it will enter the second layer of the system. The second layer is considered a strategy game between the attacker and the fraud detection system in which the attacker makes repeated attacks on the system and the latter responds with fraud detection mechanisms, this game is repeated multiple times taking into account that case the attacker fails once he attempts to attack the system more often until he obtains the desired access.

**Pattern Analysis and Fraud Detection Using Hadoop Framework**

S.V. Phulari, Umesh Shantling Lamture, Sumit Villages Madage and Kunal Tirupati Bhandari proposed a Hidden Markov Model to study the profile of each user's spending in the banking system. HMM aims to formulate an expense profile for each user, detect discrepancies in a user's spending patterns over time and in case of anomalies alert the system of a possible fraud.

The process of collecting information and improving current information is done by collecting data from several sources and placing it in a table, taking into account that different sources have different data types or different standards it is necessary to make adjustments to them. After this initial phase is then loaded the data collected in a Hadoop cluster, being distributed by data nodes and allowing the analysis of the same.

Two data mining strategies are considered, one supervised and one unsupervised. In the supervised strategy it is considered that there is an objective variable with known output values, being possible to make predictions of results through the inputs provided, whereas in the unsupervised strategy it is not possible to forecast the possible outputs.

Hadoop allows the processing of unstructured data in several clusters, Map-Reduce operation is then responsible for sending work to be done to several nodes and later to collect and organize the responses of each node so that it is possible to respond in a cohesive way to the imposed queries in the system.

The final evaluation of the model is done by interpreting classification results based on business rules, also taking into account the ability of the model to divide the input data into sets that produce similar results.

**IBM System Z**

The IBM System Z scoring system uses historical data to assign a score to the current transactions and will progressively incorporate these last transactions in the system as a means of increasing performance and with the intention of renewing the information present in the system. Depending on the score and the limits set for the maximum score, the system may reject, accept or place the transaction on hold by making contact with the respective call center.
The analysis module creates scoring models based on currently used business rules, and the second module uses previously created templates to assign each transaction a score.

**SYSTEM ARCHITECTURE**

The BankOnBox Fraud Detector developed system divides its operation into three different modules:

- Loading of historical bank logs;
- Real-time fraud detection;
- BankOnBox Fraud Detector Interface;

There are three existing interconnections to the system as it is possible to observe from Figure 3.

The system obtains the historical banking logs with which it will be possible to obtain information about the users of the banking system. Users of the BankOnBox use the application to perform transactions on the system; these will then be forwarded to the BankOnBox Fraud Detector system so that is possible to classify them in real time as to their level of fraud.

The integration between BankOnBox system and the fraud detection system will be done through calls to Web Services which the detection system makes available, bearing in mind that the format of the requests are the defined. Lastly, there is an interface accessed through a browser in which Back Office users of the BankOnBox application will perform all the maintenance and monitor transactions made by customers.

**SYSTEM DEVELOPED**

### The Data Loading Module

The data loading module is responsible for conducting an ETL process on a history of transactions provided. The processes carried out during this module are as follows:

- Production of respective metrics for each user.
- Detecting possible sequences of fraudulent transactions.
- Creation of the database used by the system.
- Analyze the transactions performed by a user and produce the files "arff" (Attribute-Relation File Format) corresponding to each user, which will later be used in the behavioral component.
Real Time Fraud Detection
This component is responsible for analyzing each transaction received by the BankOnBox application in real time.

The transaction received by the real-time detection module is processed by three components:

Statistical Component
This component classifies transactions received using statistical information obtained during the loading of the logs, in order to detect possible outliers the similarity to the work presented in [8]. Later the system adapts the information with the transactions received by the system in order to be able to adapt to a possible behavioral change of the user.

Deterministic Component
This component uses business rules previously defined by Back Office users to detect fraudulent transactions. If any of the rules defined in this component the user should be blocked immediately.

- Uses a Blacklist / Greylist system to resemble the work presented in [6].
- Block transactions using an IP Blacklist as in the work presented in [6].
- Uses location spoofing detection mechanisms as in the presented work in [2].
- Uses a method of detecting fraudulent patterns that allows Back Office users to specify sequences of fraudulent transactions to be detected when loading the historical data or when processing the transaction in real time.

Behavioral Component
Uses detection methods based on Machine Learning that classify the current transaction using the historical records of a user present in the ".arff" files.

- Carries out classifications on the basis of the behavioral records in the same way as what is done in [5][10].
- Uses two Machine Learning components, one supervised and one unsupervised as shown in [9].

Transaction score
If none of the components immediately block the transaction, a scoring module will operate in order to be able to assess the fraudulent content of the same. This process is used in the works presented in [2] [6] [8] [10].

Decision-making process
After obtaining the final score of the current transaction, it goes through a decision process before of sending a final response to the BankOnBox application with respect to its veracity.
As already mentioned, the system has a Greylist and a Blacklist. The Blacklist is intended to block users from making any transactions while Greylist involves a precautionary process.
A fraudulent user could make several transactions that are fraudulent but the system will not calculate a score high enough so that it is directly placed on Blacklist, and through the use of Greylist there is the ability to monitor possible users fraudulent.
If a user is eventually placed on the Blacklist or performs a transaction that is considered automatically fraudulent the
system will return this information to the BankOnBox application.

**Order of processing of components**

Each time a transaction is received there are two possible cases:
- **Truthful transaction**
  - Score obtained after classification is below the defined value considered as fraudulent
- **Fraudulent transaction**
  - Score obtained after classification is higher than the value defined as fraudulent
  - Detected an outlier value through the statistical component.
  - Detected irregularities in the deterministic component.
    - Falsification of location
    - Fraudulent sequence detection
    - IP considered fraudulent

In order to increase the efficiency of the processing, the modules used must be ordered in a way to avoid redundant steps.

In this way the fraudulent IP detection module should be the first to be made since it will block any transaction immediately without it being necessary to perform any processing or to permanently block a user.

Then the processes of detection of fraudulent sequences and falsification of location should be processed, these can immediately block the user and do not allow the transaction to occur. If there is no apparent fraud in any of these modules, and the transaction is scored and subsequently the decision obtained is sent to the BankOnBox system.

**Interface BankOnBox Fraud Detector**

The front-end of the solution developed is a page accessed through a browser, which is of restricted access and for the purpose of being used only by Back Office users of BankOnBox. The page was developed using Javascript in conjunction with HTML, CSS and JQuery and is responsible for communicating with the server and making the necessary requests through the Web Services defined in a Rest API.

The developed module allows the following functionalities:
- Elaborate information pertaining to each user on the page through graphs and tables.
- Adjust the values used as definitions to perform data loading or to perform the detection of fraud in real time.
- Insert or remove the rules used in the deterministic component.
- Manage general system definitions.
- Query or change the classification assigned to a transaction.
- Allow a previously locked user to re-enter transactions on the system.
EVALUATION RESULTS

To perform the tests in the system the SOAP UI tool[12] was used. This application executes web services request to the fraud detector automatically and sequentially. Simulating the BankOnBox application and getting the Web Service response. All requests are made using the XML format.

Deterministic Component
The tests carried out were aimed at testing the respective functionality of each mechanism and divided into four categories:

- Detecting fraudulent sequences.
  - Historical logs
  - Real time
- Detecting falsification of location or improper access
- Detecting fraudulent IPs
- Detection of previously blocked users

Since the tests were deterministic, it was sufficient to verify that all the components applied respective rules. The applied tests showed the complete functionality of the component.

Statistical Component
The tests applied in this component were intended to demonstrate the fraud detection capability of the system using the statistical values associated with each user, also demonstrating the adaptive capacity of the system regarding behavioral changes from the user.

Test 1
The first test carried out aimed to demonstrate the adaptive capacity of the system before behavioral changes of the user. As a concrete case the user will change his spending profile. A group of 10 transactions were generated, each of which one of these must vary their transfer value between -5% and 20% in relation to the previous transaction. The purpose of this test was to demonstrate the ability of the system to adapt to a spending profile that would tend to increase progressively.

As can be seen from Figure 8 as the transfers are made, the user's spending profile is being updated. All Transactions are classified by the system as non-fraudulent because all values obtained from the calculation of the standard deviation between the present value in the transaction and the average of transfers the user is lower than the maximum value allowed.

Test 2
The second test demonstrates a sequence of 7 transactions in which the last one has a transferred amount that when the standard deviation is calculated, between this value and the average value associated with the transfers of the user exceeds the maximum allowed. The system then blocks the transaction and the user who performed it until it is analyzed by the BankOnBox Back Office.

The main objective of tests 1 and 2 was to demonstrate the decision process used by the statistical component to classify the transactions received. This process uses the metric values of associated with each user that were obtained through the user's historical logs and were updated over time.
Behavioral Component

The tests that were performed made use of the components of Machine Learning, respectively the Supervised and Unsupervised components.

Supervised Component

Each transaction classified by the component in question will be processed by different algorithms like J48, Decision Stump, Decision Table and Part on the basis of the historical records present in the user’s “.arff” file.

In the current test, as training data was used records of a user with some transactions classified as "Fraudulent" that should be detected if the same type of behavior is repeated.

The decision tree resulting from the application of the algorithm J48 is illustrated in the Figure 10 as an example.

Unsupervised Component

In the tests carried out for the Unsupervised Machine Learning Component, the process determines if the transaction to be classified falls in the profile behavior of the user who performed it.

The records provided as training data for this process generated the following decision tree using the algorithm J48:

Then the system tried to classify a transaction with the following attributes:

- UserSpends – medium
- Travels – FALSE
- acessTime – night
- transferValue – high

The results obtained were:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>J48</td>
<td>100.00%</td>
</tr>
<tr>
<td>PART</td>
<td>100.00%</td>
</tr>
<tr>
<td>DecisionTable</td>
<td>100.00%</td>
</tr>
<tr>
<td>DecisionStump</td>
<td>75.00%</td>
</tr>
</tbody>
</table>

The values obtained show a near-maximal proximity between the transaction and the profile corresponding to the user.

Discussion

After analyzing the results obtained in the tests carried out on the components used by the system in detecting fraud, it was possible to demonstrate the following functionalities and the possible interactions between them:

- The system allows Back Office users or banking experts to use their knowledge and produce rules through simple mechanisms that allow the detection of bank fraud.

- Statistic component adjusts their fraud detection mechanism to the current spending profile of the user, taking into account that this one may change over time. This same component can immediately classify transactions as fraudulent if the calculated value for the standard deviation exceeds the maximum allowed. The system allows the value of the deviation standard for each component can be adjusted.

- The behavioral component of the system uses the profiles defined for each user as means of detecting fraud, verifying if each new transaction fits into the profile for the user in question. Each transaction made by a user is added to their historical profile allowing more and more that their profile to transmit knowledge about the behavior of the user.

- Through the Supervised Machine Learning component, it is possible to classify an historical transaction as fraudulent, and to use this knowledge for future classifications. Users of Back Office and the bank's
customer manager have the possibility to change the assigned classification of a transaction.

• The transaction score used by the system makes it possible to detect possible fraud through the combining results from different components.

• The system allows the percentage values assigned to the weight of each component in the scoring component to be changed, which allows the components used to classify a transaction may have different weight for each user.

All the tests performed were based on the comparison of the result obtained from the processing of each functionality and the expected result of the same.

It was not possible to demonstrate the total potentiality of the developed system since there was no possibility of providing historical records with labeled transactions.

CONCLUSIONS

The BankOnBox Fraud Detector system had as its main objective the detection of bank fraud in real time using the information previously obtained through the processing of bank historical logs. This objective has been achieved which allows the BankOnBox system to incorporate this system its functioning. The requirements initially defined were fulfilled, bearing in mind that it is now possible to load the system with the historical logs of a bank and to retrieve information about the users that are used later when detecting real-time fraud. Through processing of historical logs, it is possible to obtain information on each user's spending profile or obtain behavioral records. The real-time processing component will make use of this information in detecting fraud and also incorporates simple mechanisms that allow Back Office users of the system or the financial experts to define rules that allow detection of fraud, such as possible fraudulent sequences or blocking IP considered fraudulent. The Use Cases defined in conjunction with the company Link Consulting were the target of a first prototype of interface allowing the maintenance of the system through it. The evaluation of the system demonstrates the functioning of the different component implemented to possible detect of fraud. The system adapts the user profile to each transaction received and detects possible fraud if it does not fit the established profile for the user. The different fraud detection techniques applied individually are subsequently in such a way that they can transmit another type of information that individually does not would be possible, demonstrating the versatility of the developed system.

Contribution

Through the incorporation of the BankOnBox Fraud Detector System into the application BankOnBox, the security of the BankOnBox increases. In addition to the more well-known techniques such as the detection of fraudulent sequences or the detection of falsification of the locations the system incorporates different techniques of machine learning which contributes so that more system of this type integrates them in its processing.

Future Work

If it is understood that performance is a key factor in the classification of transactions, it will be possible that several instances of the BankOnBox Fraud Detector work in parallel, The currently developed server verifies the existing transactions in the queue of entry and forwards the requests to the BankOnBox Fraud Detector if this one is available for process.

This process will only be possible if mutual exclusion is ensured when checking or changing the information which in the actual version of MongoDB is not possible. In the summer of 2018 MongoDB version 4.0 will be released [11] which will allow mutual exclusion when accessing the documents guaranteeing the integrity of the same and consequently the possibility of performing transaction processing in parallel.

The work developed was presented to a bank manager from BPI with the intention of obtaining some feedback about the components developed and the classification process. The classification of fraud or non-fraud could penalize the system since the detection of a false-positive could be very penalizing in monetary and reputational terms.

As such advised the system should have three types of classification:

• Fraud.
• Possible Fraud.
• Non-Fraud.

The process applied to the deterministic components should be maintained by blocking the user each time one of the defined rules is detected. Instead of blocking the user each time a detection of an outlier value occurs or the transaction get the score needed to be placed on the Blacklist, the BankOnBox Fraud Detector should indicate to the BankOnBox system that it should increase the user's authentication level.

ACKNOWLEDGMENTS

Initially, I would like to thank my family for all the support provided throughout my entire academic course and for always helping me when I needed it most. Then thank my colleagues and friends for the help and sharing of knowledge that allowed me to overcome all the moments of greater pressure. I would also like to thank the entire Financial Services department of Link Consulting for all the sharing of knowledge and help in the development of my work and for all the shared experience that will allow me to become a better professional. Finally, a special thanks to
Prof. José Alves Marques and Tiago Santos without whom the development of this dissertation would not have been possible, through all the advices and for always making me want to learn more.

REFERENCES
1. ACI Worldwide. 2010. Stopping card fraud in its tracks, An industry guide from ACI
7. R. Brause, T. Langsdorf and M. Hepp. 1999. “Neural Data Mining for Credit Card Fraud Detection”, J.W.Goethe-University, Frankfurt
10. IBM. 2013. IBM System Z, RedBooks
12. SmartBear Software (2005), [ONLINE] Available at: https://www.soapui.org/