Fraud Detection within Mobile Money

A mathematical statistics approach

Frida Kappelin and Jimmie Rudvall

Dept. Computer Science & Engineering
Blekinge Institute of Technology
SE–371 79 Karlskrona, Sweden
This thesis is submitted to the Department of Computer Science & Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full-time studies.

Contact Information:
Authors:
Frida Kappelin
E-mail: frkb10@student.bth.se

Jimmie Rudvall
E-mail: jiru10@student.bth.se

External advisor:
Dr. Dejan Baca

University advisor:
Dr. Stefan Axelsson
Dept. Computer Science & Engineering

Dept. Computer Science & Engineering
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden
Internet : www.bth.se/didd
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57
Acknowledgement

We would like to begin with a great thank you to our friend Patrik Eriksson for his fresh pair of eyes into this thesis and also for all helpful input and long discussions.

Next we would also like to give our dear friend John Heiding a great gratitude for proofreading our report, having feedback together with suggestions of improvements and for bringing light into our toughest moments.

Lastly we would like to thank our Stefan Axelsson and Dejan Baca for their support, expertise and scientific guidance through our work.


Abstract

Context. Today it is easy to do banking transaction digitally, both on a computer or by using a mobile phone. As the banking-services increases and gets implemented to multi-platforms it makes it easier for a fraudster to commit financial fraud. This thesis will focus on investigating log-files from a Mobile Money system that makes it possible to do banking transactions with a mobile phone.

Objectives. The objectives in this thesis is to evaluate if it is possible to combine two statistical methods, Benford’s law together with statistical quantiles, to find a statistical way to find fraudsters within a Mobile Money system.

Methods. Rules was extracted from a case study with focus on a Mobile Money system and limits was calculated by using quantiles. A fraud detector was implemented that use these rules together with limits and Benford’s law in order to detect fraud. The fraud detector used the methods both independently and combined. The performance was then evaluated.

Results. The results show that it is possible to use the Benford’s law and statistical quantiles within the studied Mobile Money system. It is also shown that there is only a very small difference when the two methods are combined or not both in detection rate and accuracy/precision.

Conclusions. We conclude that by combining the chosen methods it is possible to get a medium-high true positive rates and very low false positive rates. The most effective method to find fraudsters is by only using quantiles. However, combining Benford’s law with quantiles gives the second best result.

Keywords: Fraud detection, Benford’s law, quantiles, Mobile Money.
# List of Figures

3.1 Benford curve of first digit ........................................ 12  
3.2 Example of Benford curve with fraud ............................. 13  
3.3 Illustration of ROC-curve with extreme points .................. 19  
4.1 Visualization of how often users send money .................... 24  
4.2 Unzoomed ROC-curve ............................................... 30  
4.3 Zoomed in ROC-curve ............................................... 31  
7.1 Frequency plot of how often user is sender in each transaction type 42  
7.2 Frequency plot of how often user is receiver in each transaction type 43  
7.3 Frequency plot of how often a user sends amounts ............... 44  
7.4 Frequency plot of how often a user receives amounts ........... 45
### List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Table with statistics for live-data set</td>
<td>17</td>
</tr>
<tr>
<td>4.1</td>
<td>Limits, 95%-quantile for rule A</td>
<td>25</td>
</tr>
<tr>
<td>4.2</td>
<td>Limits, 95%-quantile for rule C</td>
<td>25</td>
</tr>
<tr>
<td>4.3</td>
<td>Limits, 99%-quantile for rule A</td>
<td>26</td>
</tr>
<tr>
<td>4.4</td>
<td>Limits, 99%-quantile for rule C</td>
<td>26</td>
</tr>
<tr>
<td>4.5</td>
<td>Table with statistics for fraud-data set</td>
<td>27</td>
</tr>
<tr>
<td>4.6</td>
<td>Table of all rules (95%-quantile)</td>
<td>28</td>
</tr>
<tr>
<td>4.7</td>
<td>Table of all rules (99%-quantile)</td>
<td>28</td>
</tr>
<tr>
<td>4.8</td>
<td>Results for each rule’s accuracy and precision</td>
<td>29</td>
</tr>
</tbody>
</table>
List of Algorithms

1 Fraud detector .......................................................... 18
Contents

Abstract ii

1 Introduction 1
  1.1 Background ................................................. 2
  1.2 Research question ........................................... 4

2 Related Work 5
  2.1 Benford’s law ............................................... 5
  2.2 Rules and limits ............................................. 6
  2.3 Big Data .................................................... 7

3 Method 8
  3.1 Case study ................................................ 8
    3.1.1 Case study of Priest attack (Phishing-attack) ....... 9
    3.1.2 Case study of Scooter attack (Grab and run-attack) 10
    3.1.3 Other interesting operation types ................... 11
  3.2 Statistical methods ....................................... 11
    3.2.1 Benford’s law ......................................... 12
    3.2.2 Application of Benford’s law ......................... 13
    3.2.3 Quantiles ............................................... 14
    3.2.4 Application of quantiles ............................. 14
  3.3 Rules ..................................................... 15
    3.3.1 Definition of rules ................................... 15
  3.4 Limits ..................................................... 15
  3.5 Big data .................................................. 16
    3.5.1 Data visualization ...................................... 17
  3.6 Fraud Detector ............................................ 18
  3.7 Performance measurements ................................. 18
    3.7.1 Receiving Operating Characteristics curve ........ 18
    3.7.2 Other measurements .................................. 20

4 Results 21
  4.1 Results of case study ..................................... 21
    4.1.1 Phishing attack - general characteristics .......... 21
Chapter 1

Introduction

From the beginning of time there has been those who somehow tries to circumvent established rules and in the world of finance this is no exception. One way to circumvent rules is to commit fraud, which is defined by Edgar Lopez-Rojas in his licentiate as "...the wrongful or criminal act with the intention of obtaining financial or personal gain" [1]. An example of how to achieve financial gain within the financial sector is something called money laundering.

Money laundering is described by Lopez-Rojas as a complex chain involving placement of illegal funds into a legal financial system together with layering operations that hides the true origin of the funds. The final step is to integrate the funds by involving them in formal and legal activities.

A fairly new problem within the world of finance is phishing, which has become more common since the Internet with E-commerce, online-shopping and the simplicity to do banking transaction online. Phishing is when someone tricks another in order to gain personal information by pretending to be someone or something that they are not, for example an authority. It is not uncommon that payments are involved, which also means that victims may lose money in the process as well. Phishing and exploitation of stolen high privileged users are two types of fraud in the virtual financial world that are going to be discussed and studied in this master thesis.

This research have log-files from a currently running Mobile Money system\(^1\) that will be analyzed in order to find a way to detect fraud. The system is working similar to a banking system with different kinds of operations, like payment, money transfers, deposits and so on. Each operation is logged and contains a lot of information, but the most important information describes what kind operation, sender, receiver, amount and date. These are the parameters that are interesting in the scope of this thesis.

The difference between a Mobile Money system and a banking system lays in the requirements of the users. In a banking system a user is required to have a valid ID together with a social security number. Often you also need to have a stable economy since it is not uncommon, both in richer and poorer regions of the world, that there is some kind of fee when opening and managing an account.

\(^1\)Do banking-operations with a mobile phone.
But in the studied Mobile Money system this is counteracted upon since all you really need is a mobile-phone number. You register your phone-number to a Mobile Money system and then you may send money whenever you like. It is just like sending an SMS with money to another person. The other person is also required to be connected to a Mobile Money system. Personal identification is often considered optional. In countries where you have to travel a long way to a bank, the Mobile Money system is a good solution to keep track of your money in a safe way. The Mobile Money system that has been studied in this thesis is popular in developing countries. Mobile Money systems has revolutionized the situation for the "unbanked", which is those without the proper identification and/or those without sufficient funds for a bank account.[2]

1.1 Background

This section begins with a description of problems and the background of fraud detection and ends with an explanation of frequently used terms when evaluating fraud detection methods performance.

Fraud is an important problem due to its impact on whole economies as well as individuals. Therefore it is just as important to both refine old fraud detection techniques and develop new techniques. In Sweden and many other countries it is required by law that companies within the financial sector must address fraud detection [3]. It is therefore very important to detect and investigate fraud. In practice there are two major approaches to detecting fraud, anomaly and signature detection [4]. When detecting fraud by searching for anomalies the detection system searches for users with a behavior that does not comply with the normal behavior of the majority of users. Signature based systems looks for certain patterns that is predefined as fraud. As long as a user does not follow any pattern for a specific signature of fraud the user is classified as a non-fraudulent user otherwise the user will be classified as a fraudster.

One of the major problems with fraud detection is described by the base-rate fallacy, also known as class imbalance problem. That is, there are typically an overwhelming majority of normal, benign behavior, rather than fraudulent or malicious behavior [5]. This leads to the requirement of having a low rate of false classification and a near-perfect rate of true classification in order to avoid large amounts of non-fraudulent transactions being classified as fraudulent. Otherwise the costs of missed fraudsters and falsely accused users will be too large.

Another common problem in the area of fraud detection that relates to the base-rate fallacy is the amount of data. The data sets are often huge and are growing at a constant pace. As a brief example there are one company in the United Kingdom that has approximately 350 million credit card transactions each year [6]. Let us hypothetically say that 1% of these transactions are fraudulent and every fraudulent transaction’s amount is £1. If these transactions goes unde-
tected and are not being stopped £3.5 million each year will be lost to fraudsters.

In the financial sector there is often sensitive data involved that may violate users privacy when analyzed. Example of such data is name, address or other information that may be used for identifying individuals. This makes it difficult for researchers to conduct their research and experiments with real data from financial systems [7]. One main difficulty within fraud detection that relates to the lack of public data from financial systems is to decide what kind of data is necessary to be able to detect fraud. In this thesis we have the opportunity of working with real data from a fully deployed Mobile Money system. The provider of this data is a company that on request will remain anonymous.

Another problem that makes it harder to achieve decisions with high accuracy is the human’s ability to change pattern. This means that fraudsters constantly changes the way fraud is performed, which is also known as the modus operandi (MO) [8]. This makes it harder to find one universal pattern to look for, but pattern deviation is what makes it possible to find anomalies/fraud. If we can find a normal pattern it is possible to detect if someone deviates from the normal pattern [9].

Below follows a list with terms that is frequently used when evaluating the results of how well a fraud detection method performs.

- **True positive rate (TPR)/sensitivity** - The proportion of positives that are correctly classified [10]

- **False positive rate (FPR)** - The proportion of positives that are incorrectly classified [10]

- **True negative rate/specificity** - The proportion of negatives that are correctly classified [10]

- **False negative rate** - The proportion of negatives that are incorrectly classified [10]

- **ROC-curve** - Visualization of a binary classifier’s performance. Created by plotting TPR and FPR of a classifier [10]

- **Accuracy** - ISO 5725-1 defines accuracy as the closeness of a measurement to the true value[11]

- **Precision** - ISO 5725-1 defines precision as the closeness of agreement among a set of results[11]
Chapter 1. Introduction

1.2 Research question

The research question for this master thesis will be:

- Is it possible to combine the quantile-statistics together with Benford’s law, the law of digits distribution, to find fraud in data from logs within Mobile Money systems?

We intend to perform experiments on our data with injected fraud attacks in order to answer our research question. More detailed information about the proposed methods is available in chapter 3 Method and 7.1 Appendix A, Benford’s law. We will evaluate the performance of both methods when combined and independent.
Chapter 2

Related Work

Since this area is young it does not have that much research, thus this chapter will present the different methods that will be used in this thesis and information on how this methods have been applied in different areas.

None of the reviewed papers have mentioned that they use a data set from a fully deployed system with real transactions from a Mobile Money system between real users. Nor have any reviewed article used Benford’s law within Mobile Money or combining the law with quantiles in order to detect fraud. Since we have access to this kind of data, data from a fully deployed system with real transaction from real users, we hope to be able to give accurate and realistic results regardless of what the results may be.

2.1 Benford’s law

In M.J.Nigrini’s book [12] he describes how to use Benford’s law, the distribution law on how often digits appears in natural numbers, to detect fraud within accounting. To be able to use this law there are certain requirements that needs to be fulfilled, for example the data needs to occur naturally like population in a city. There are also tests that can be used to describe a data set that will be used to identify fraud. The tests that have been used are first-digit-test, which controls how often the first digit appears in a number in a data set. This test can tell if there is an unnatural distribution of the data set. The second-digit-test checks how often the second digit appears and the found information will be passed on to the final test, the first-two-digit-test. This test will tell which amounts starting with the two digits that are the most interesting. More detailed information can be found in 7.1 Appendix A, Benford’s law.

Jasak and Banjanovic-Mehmedovic [13] states in their proceeding that if Benford’s law should be applied on a data set, the data set should comply with the following:

- The data set must describe similar phenomena or the same attribute as amount, length, quantity or some other attribute
- There must be no built-in maximum or minimum values
The data set should not be made up of pre-assigned or set numbers

- The data set should contain more small items than big ones

The data set used for experiments in this thesis follows these prerequisite with one exception, the third bulletin: "The data set should not be made up of pre-assigned or set numbers". The data set used is based on transfers between users for payments etc. Users of the Mobile Money system may send any amount they like, but when paying for groceries, cloths, etc. there is a risk of pre-assigned/psychological numbers are being used. This could mean that Benford’s law are not applicable on the data set, but it is a risk we are willing to take since it is a part of this thesis to test. We also believe the data set being random enough for this method to work due to the size of the data set. If Benford’s law does not work as intended, which is to use the law in order to determine which entries are fraudulent which is not, it could possibly be used as an indicator that fraud exists in a data set. This is also discussed by Jasak and Banjanovic-Menmedovic. We hope in this thesis to be able to use Benford’s law in both auditing as well as confirmation of fraudulent behavior. The proceeding of Curtis A. Smith has been used as inspiration of how to apply Benford’s law [14].

Rosset et al. and M.J. Nigrini both discuss two different ways to detect fraud. We wish to combine the both methods in order to complement the weaknesses of each method and get one improved method. Rules and limits will catch fraudsters that follows a certain pattern and fraudsters that are clever enough to avoid the limits will be caught by Benford’s law, since they are forced to produce unnatural numbers, which fraudsters has a tendency of producing.

To our knowledge there has been no investigation of how well limits and Benford’s law applies within the area of mobile money or how well these methods works together.

2.2 Rules and limits

Rosset et. al. [15] presents a rule-based method to detect fraud within telecommunication. They describes rules as "alarm-setters for suspected fraud", which is the same way rules was used in this thesis. According to the authors there are three criteria that needs to be fulfilled before the requirements for a "good" rule are met. These criteria are:

- High accuracy in cases (=> specificity - most cases found are really fraudulent)
- High coverage of true fraud cases (=> sensitivity - most fraudulent cases are found)
- High coverage of true fraud alerts (=> fraud cases are detected quickly)
Chapter 2. Related Work

The listed criteria was used in this thesis as well together with ROC-curves in order to give a good description and visualization of the performance of the proposed method. By manipulate a well-known existing algorithm to work with thresholds/limits Rosset et. al. created a rule-generator and used this generated rules combined with limits to detect fraud. The idea of detecting rules combined with limits in order to detect fraudulent behavior and/or if someone deviates from a normal and benign behavior is a key component of this thesis proposed method. The usage of rules, limits was proven by the Rosset et. al. to be effective and gave a good accuracy.

2.3 Big Data

Due to the amount of data that is provided for this thesis’s experiment, problems due to large amount of data can not be ignored. A. Rajendra describes in his book [16] Big Data use cases, and lists both fraud detection and log-analytics. The author also also discuss problem with Big Data and some of them are listed below:

- More than 80% of today’s information is unstructured and it is typically too big to manage effectively.
- Since the data may contain personal information it must be secured and at the same time ensure that the data is used correctly in order to protect the users privacy.
- Businesses strive for both more value out of analytics, which means that businesses want the data to be available faster by real-time analytics, and higher user volumes at the same time.

To demonstrate the problem with big data A. Rajendra mentions that in the year 2000 the world had 800,000 petabytes ($10^{15}$ bytes) stored, and by 2020 it is estimated to have grown to be 35 zettabytes ($10^{21}$ bytes of data. The author also mention in his book that social media such as Twitter generates 7+ terabytes (TB) and Facebook 10 TB of data each day.
This chapter will cover the used research methods and their application. First each method that will be used during the implementation of the new fraud detector will be generally explained of how they work. Then each method will be explained how they will be applied in this research.

The data used in the experiments are log files provided by the company’s Mobile Money system. During the experiments two sets of data was available. Both of these sets contains financial transactions similar to any other banking system. The first set contains real transactions from the Mobile Money system. The second set is a subset of the first set but have been injected with fraud. These sets together with the methods described below forms the experiments in this thesis, which will confirm or refute the hypothesis regarding the possibility of using statistical methods from similar areas to detect fraud. The amount of injected fraud will be at a level that correspond to the amount of fraud that the company experience.

To verify that there are no fraudulent transactions within the subset of live data that will be used for true-negative tests, there will be random samples that will be analyzed before use in order to confirm absence of fraudulent transactions. The company also have some basic parameters set on the live data, to detect fraud, and therefore there should only be a very small amount of fraudulent transactions in the live data.

3.1 Case study

M. Berndtsson et. al.[17] defines a case study as "an in-depth exploration of a phenomenon in its natural setting". The case to be explored is not limited to a particular area and examples of areas to study are social behavior of animals in their natural habitat as well as a fully deployed information technology system. The case study in this thesis will be used in order to get a deeper knowledge of the fully deployed Mobile Money system and to identify the characteristics of the two
Chapter 3. Method

scenarios of fraud. These cases were given by the external supervisor [18]1, and is based on his experiences from fraudulent activity in this Mobile Money system. To be able to identify fraudulent behavior with certain characteristics in the studied Mobile Money system these characteristics must somehow be identifiable. There are operation types in the system that may be utilized by users in order to interact with each other or the system. These operation types was used as reflectors of characteristics, that is by looking at how users utilize these operation types it was possible to identify if a user has a fraudulent behavior or not. Which operation types that reflects a certain fraudulent behavior was identified in the case studies.

These characteristics will later on be used in the statistical methods. Section 3.1.1 Case study of Priest attack (Phishing-attack) and 3.1.2 Case study of Scooter attack (Grab and run-attack) describes the cases to be studied in more details. These sections begins with a general description of how the attacks can be performed in any kind of system or environment. Furthermore a more detailed scenario for the studied Mobile Money system will be presented.

3.1.1 Case study of Priest attack (Phishing-attack)

The first scenario given by our external supervisor is a phishing-attack. A phishing-attack is when an attacker claims to be someone or something, like an authority, in order to earn a victim’s trust. If the victim trust the attacker enough he or she may give away sensitive information, pay counterfeit invoices or do anything else that the attackers asks for. An attacker could for example claim to be a priest, or claims they have a problem that they need help with where money plays an important part and asks the victim to send an amount of money to the attacker. Common ways to perform this remote attack is to use email or SMS, but several others way, for example letters, are also possible. Therefore this attack is not limited to be applied within a Mobile Money system. Below follows a more detailed explanation of how the attack is performed in the Mobile Money system that have been studied.

Scenario: The attacker needs to have a Mobile Money account in order to be able to receive money from victims. Since the system supports accounts where no personal identification is required, for example a social security number, the attacker opens a Mobile Money account of this kind. This account will be used when the attacker is trying to receive money from victims. In order to trick a victim the attacker has to counterfeit an SMS that resembles a confirmation of received money. This SMS will be sent to multiple, probably random, victims. The purpose is to make the victim believe that an amount of money has been transferred from the attackers account to the victims account. The attacker then

---

1Baca has a PhD in the area with dissertation on "Developing Secure Software - in an Agile Process". He has experience as a Security Engineer in the industry and works with Mobile Money.
contacts the victims one by one and deceives the victim by explaining that the money has been sent to the wrong account and asks for the money back. In many cases the victims simply sends the amount of money to the attacker without any double check to confirm that the money actually has been received. As soon as the attacker has received money from the victims the attacker withdraws the money from the Mobile Money system to cash by making a cashout operation.

3.1.2 Case study of Scooter attack (Grab and run-attack)

The second case is based on a "grab and run"-attack. A classic version of the attack is when an attacker steal something physically from a victim, for example a wallet or a bag. The items an attacker focus on in a classic grab and run attack are often valuable in itself or contains other valuable items. How the attack is performed may vary a lot. The victims may be chosen at random or by any other reason the attacker finds suitable. If a victim is chosen random the value of what is grabbed will be unknown since a wallet stolen from a stranger may contain anything from no money and upwards. If a victim is chosen by a particular reason it is more likely that the attacker knows the value of what is to be grabbed. An attacker may have seen the victim’s wallet filled with a lot of money or the attacker may know how valuable something is to the victim and will try to get a ransom from the victim in order to get the item back.

In the Mobile Money system that have been studied there are some users, called a mobile money agent or just an agent, who has higher privileges than the ordinary users. These agents will be the victims in this attack and has been chosen for a reason by the attacker, their mobile phone. The valuable item for an attacker to steal is not the mobile-phone itself, rather the high privileged account. An agent with high privileges acts like a smaller bank with the possibilities to transfer, deposit and withdraw money within the Mobile Money system. The agents are the link between users and the Mobile Money system. Agents usually have a decent amount of money to disposal inside the Mobile Money system, since users will deposit cash to be transferred virtually. In order to interact with the Mobile Money system an agent is logged on to a Mobile Money-service by using a mobile-phone with an account with high privileges. If an attacker may access the agent’s mobile-phone and/or the high privileged account the attacker will easily be able to steal or move around money. In order to be able to steal or move around money in peace the attacker runs off with the mobile-phone, hence a grab and run attack. This attack is not limited to be applied in Mobile Money systems.

Scenario: In order to access an agents mobile-phone and the high privileged account an attacker approach the agent and asks for help with a transaction. Before a transaction can be made the agent has to log on to the Mobile Money system and then ask the attacker for an amount of money together with a number
to send the money to. The attacker states an invalid number as receiver of the money. When the agent tries to send money to the invalid number the transaction will not be completed and an error message stating "invalid number" will be shown. After a few tries the attacker offers to fill in the number since the attacker may remember the number more correctly that way. When the attacker receives the mobile-phone the agent is still logged on to the Mobile Money system with a high privileged account. The attacker then grabs the mobile-phone and run off, maybe on a scooter, to a safe location. The attacker will then use the agent’s mobile-phone with the high privileged account in order to transfer money from the agent’s money buffer to an account that the attacker owns which then is withdrawn.

3.1.3 Other interesting operation types
In the studied Mobile Money system there are other operation types that was identified as interesting since they makes it possible for fraudsters to get money out of the system. Therefore, these operation types were used as a complement when identifying fraudsters.

3.2 Statistical methods
The reason to use statistical methods was a request from the company with the Mobile Money system. They wanted an easy system for fraud detection without complex machine learning algorithms, such as neural networks, which will not confuse their customers. After some research it was concluded that statistical methods has a tendency to give better results compared with machine learning algorithms.

The first statistical method to use in this thesis is Benford’s law. This law is used to identify anomalies in a set of numbers. Benford’s law is often used in accounting and since this law is not applied in Mobile Money system with many small transactions, this was a good argument to use for this experiment.

The second statistical method to use is quantiles. Quantiles are used in order to find a confidence interval for values/numbers with a certain probability. This method identifies limits used when checking if rules, soon to be defined, was broken or not.

Below follows a more detailed description of the two statistical methods and how they was applied in this thesis.
3.2.1 Benford’s law

Benford’s law is used to define the frequency of digits in each position of a number for naturally occurring numbers. Formula 3.1 describes the probability, $P$, for each first digit, $d = \{1, 2, ..., 9\}$.

$$P(d) = \log_{10}(1 + \frac{1}{d})$$

(3.1)

For example, the probability that the digit 1 is used as first digit in a number is 30.10% [19]. Which corresponds to the result given by the formula 3.1.

The law only works with numbers that occur naturally, such as population numbers, death rates or other number that is not constructed by the human. Number such as zip-codes or personal-numbers are examples of numbers that are constructed by the human and will not follow the distribution. The set should not have any built in maximum and minimum values[12]. These requirements makes it possible to use this distribution law on financial fraud, since the amount in the transactions that are manipulated by the fraudster will not follow the natural number frequency. See chapter 7.1, Appendix A, Benford’s law, to get more detailed information about the requirements for Benford’s law.

![Benford's law graph](image.png)

Figure 3.1: A Benford curve illustrating the distribution of first digit together with each digit’s frequency.
As mentioned in section 3.2 Statistical methods, Benford’s law was used in this thesis to test if it works to detect fraud in a Mobile Money system, since Benford’s law only have been applied within accounting.

3.2.2 Application of Benford’s law

This method was implemented in several steps using scripts written in Bash and the programming-language named R [20], that is specialized in graphs and statistical calculations with the capacity of handle big data sets. The environment used for coding in R has been RStudio [21], were the output is forwarded to the fraud detector and used to filter the output from RStudio into a result containing possible fraudsters. The first-order-test, explained in 7.1, Appendix A, Benford’s law, was implemented in R together with a package [22] which is equivalent to a library, that is specialized to calculate Benford’s law.

To be able to use Benfords’s law all money amounts involved in transactions had to be sorted out, which was done by parsing the log files with a Bash-script. All log entries with a specific operation type, these was identified during the case study, was categorized based on case and put into different files with the operation-type as filename. Furthermore the amounts of each file was extracted and used as an input to an R-script.

Each file containing amounts for each operation type were then used as an input to check if the amounts aligned with Benford’s law. To test if the amounts aligned with Benford’s law there is a test which can be run in R to check if actual value for the first-two-digits in a number are exceed the expected value, called Zscore-test, see 7.1, Appendix A, Benford’s law. In this case the first two digits in a number that exceed the expected value were saved and passed on to next
step when identifying fraudsters using Benford’s law.

This step filtered out all users with amounts that started with the first-two-digits that the Zscore-test gave. The result was then saved in two separate files, based on if the user was a sender or a receiver. Based on previous step the users was counted in how many times they sent or received a specific amount of money.

Since previous step produced a set of users that only occurred once, the users was sorted out based on the limits, explained in section 3.4 Limits, to only get users that exceeded these limits. The files now contained users based on operation type and if the amount was related to a sender or a receiver. These files were then passed on to the next step, the fraud detector.

3.2.3 Quantiles

Quantiles are used when describing what value a certain percentage exceeds. Claes Jogréus [23] defines the number $x_p$ that solves the equation

$$F_X(x_p) = 1 - \frac{p}{3.2}$$

to be the $p$-quantile.

A brief example is when salary statistics state that the 25%-quantile (also known as the first quantile) is 19000 SEK. This means that 25% of the employees has a salary below 19000 SEK and 75% has a salary above 19000 SEK [23].

In this thesis quantiles was used in order to find a confidence interval for how many times a user is sending and receiving money, and the sent and received amount range with a high probability. The quantiles that was used in the experiments are the 95%-quantile and the 99%-quantile. Two quantiles was tested in order to prove the hypothesis that a higher quantile will give better results. The results of these quantiles was used when deciding when a user deviate from a normal and benign behavior. A user deviates from a normal and benign behavior when rules are broken, see 3.3, Rules. In order to know if a rule is broken the upper and lower limits of the quantiles was used. If a rule specific limit was exceeded the rule was considered broken.

3.2.4 Application of quantiles

The goal of using quantiles was to be able to specify what a normal and benign behavior is with a high probability. Due to the problems with the base rate-fallacy, see 1.1 Background for more information, a high probability was needed. The quantiles used was the 95%-quantile and the 99%-quantile. The decision to test two quantiles was based on the hypothesis that a higher quantile will prove to be better than a lower.
3.3 Rules

Oxford's dictionary of English defines a rule as "a statement of what may, must or must not be done in a particular situation or when playing a game" [24]. This means that one or multiple rules could be used in order to tell if something follows a normal and benign behavior or not.

For example, a behavior is defined as benign if the amount of money that is sent is smaller than 100 and bigger than 0. A user will be classified as a fraudster if the amount 150 is sent since the rule, benign users sends an amount between 0 and 100, has been broken. That is the user deviates from a normal and benign behavior if one or multiple rules are broken.

Rules were used in this thesis in order to tell if a user follows a normal and benign behavior or not. To define the rules that were used the conclusions from the case studies has been combined together with limits defined by statistical methods, see 3.2 Statistical methods.

3.3.1 Definition of rules

In the case study, each case had specific benign behavior that a fraudster could violate, behavior A and behavior B. A rule is a collection of limits that defines if a certain behavior is violated. In order to construct rules that reveals if a user starts to either deviate from a normal and benign behavior or has a fraudulent behavior from the beginning following answers had to be answered:

- What characteristics are found in each type of attack?
- What is the average behavior of known benign users?

3.4 Limits

Limits are used together with the rules resulting from the case studies as described in 3.3.1 Definition of rules in order to know when a rule is broken. Since a rule is related to a predefined normal and benign behavior a broken rule means a deviation from that behavior, thus a broken rule means a fraudulent behavior.

To know what limits to use in each of the cases that was studied the upper and lower limits of quantiles was used, see section 3.2.3, Quantiles for more information about quantiles.
3.5 Big data

Working with data that constantly is growing, also known as Big Data, could be a big problem. As can be derived from the word Big Data could be defined as extremely large data sets. These extremely large data sets may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions.

As A. Rajendra stated when giving examples of areas involving Big Data in his book [16] fraud detection and log-analytics are two areas working with Big Data on a regular basis. The two sets of data used in this thesis are log-files and to be able to detect fraud the log-files must be analyzed. These log-files are also constantly growing, hence the log-files used are Big Data. Each log entry is describing a user’s interaction with the system or between users interaction with each other via the system. An example is when a user transfer money to another user.

The first data set contains data from the Mobile Money system that is considered normal and benign and the second data set contains both normal and benign data and fraudulent data that has been injected by the external supervisor [18]. The authors of this thesis had no knowledge of how much or where this data has been injected in order to get more accurate results from the detection method until after the experiments was completed. The injected data is based on the external supervisors experience and knowledge from the area of fraudulent activity in the given Mobile Money system.

In order to find limits for the rules found during the case study the log data had to be analyzed. To make the data searchable the database MongoDB [25] was used. Due to MongoDB’s flexible schema, in contradiction to SQL, no tables had to be predetermined before data insertion. This and the fact that MongoDB inserts data fast (about 6.5 million log entries in 30 min) is why MongoDB was chosen.

The following table, table 3.1, shows the most important information related to the data set used in this thesis. This data set was both visualized and used when limits for rules were calculated. The operation types in the data set are explained in section 4.1.4, Operation types.
### Table 3.1: Table with statistics for live-data set

<table>
<thead>
<tr>
<th>Description</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table name</td>
<td>Live data</td>
</tr>
<tr>
<td>Time span</td>
<td>25 hours</td>
</tr>
<tr>
<td>Number of entries</td>
<td>6 516 298</td>
</tr>
<tr>
<td>Number of unique users</td>
<td>1 523 476</td>
</tr>
<tr>
<td>Number of cash_out</td>
<td>231 951</td>
</tr>
<tr>
<td>Number of cash_in</td>
<td>256 826</td>
</tr>
<tr>
<td>Number of transfer</td>
<td>99 016</td>
</tr>
<tr>
<td>Number of voucher_to</td>
<td>5 740</td>
</tr>
<tr>
<td>Number of voucher_from</td>
<td>5 083</td>
</tr>
<tr>
<td>Number of other</td>
<td>4 394 206</td>
</tr>
</tbody>
</table>

#### 3.5.1 Data visualization

When data is visualized in a good way it gives the possibility to find patterns and relationships. Bad visualization of data could lead to confusion and is misleading. In this thesis data was visualized in order to get an understanding of the data and roughly estimate potential limits. In an attempt to avoid a bad visualization only data that was assumed to be useful when finding limits for rules regarding behavior A and C, from the case study, was visualized. The data to visualize was extracted with Bash-scripts and graphics for the visualization was made in R, the programming language for statistical computing and graphics. The data that was used in the visualizationinksc was:

- Frequency, how many times something has occurred
- Amounts
- Operation types, see section 4.1.4, *Operation types*
- Number of times user is receiver respectively sender

In order to get the data needed two Bash scripts, both scripts consisted of combinations of grep, sed and Awk commands, was used. The first script simply parsed each log entry and checked every unique user ID on the sender and receiver tag in the available data set and counted the occurrence of each user ID in each position. The second script parsed each log entry in the available data set and counted how many times an amount is associated with each unique user ID.

R was then used to visualize the extracted data. The visualization can be found in the section 4.3, *Data visualization*, where it will be explain in further detail. The graphs used for visualization of the data was used in order to visually confirm potential limits.
3.6 Fraud Detector

To be able to test the defined rules and limits a fraud detector was implemented. The output of the fraud detector gave all the users that broke the rules and limits. The fraud detector was implemented in Bash and followed the pseudo-code below:

**Algorithm 1 Fraud detector**

1: **procedure** DETECTFRAUD(quantile, timeSpan, logsPath)
2:     if quantile = 95 then
3:         limits ← limits for 95%-quantile*timeSpan
4:     else
5:         limits ← limits for 99%-quantile*timeSpan
6:     records ← readRecords(logsPath)
7:     for all record in records do
8:         if records = transactionRecord then
9:             isFraud ← checkIfFraud(record, rule, limits)
10:        if isFraud = true then
11:            alarm(record)

3.7 Performance measurements

This section describes the performance measurements used when evaluating the fraud detector’s performance.

3.7.1 Receiving Operating Characteristics curve

When analyzing the rules a Receiving Operating Characteristics curve, also known as ROC-curve, has been used. ROC-curves are useful when organizing and visualizing performance of classifiers of a wide range of areas and fraud detection is one of them. Within fraud detection ROC-curves can be used as a performance measurement to indicate how well the detection system detects fraud. The X-axis represents the false-positive rate (or false alarm rate) and the Y-axis represents the true-positive rate.

As seen in figure 3.3 there are four points of interest in a ROC-curve, (0,0), (1,0), (0,1) and (1,1). The point (0,0), bottom left corner, means that there are no false alarms, but it also means that the classifier do not find any fraudsters. In contrast to (0,0) the point (1,1) means that the classifier will detect all fraudulent behavior, but will also classify all non-fraudulent behavior as fraudulent. The points (1,0) are the extreme behavior of the false positive rate, which means that the classifier do not find any fraudsters and classifies all non-fraudsters as fraudsters. This performance is not desirable. The desirable performance is
the point (0,1). This represents a perfect classifier that detects all fraudulent behavior and has no false alarms. The diagonal line represented by \( y=x \) is equal to randomly guessing if a behavior is fraudulent or not and could be compared to flipping a coin in order to decide the outcome [26]. An illustration of a ROC-curve with the four extreme points can be found in figure 3.3.

Figure 3.3: Illustration of ROC-curve with extreme points
Chapter 3. Method

The first step to create a ROC-curve was to calculate the true positive rate and the false positive rate. False positive rate describes the proportion of all the positive results that is incorrectly, which is the users that have been classified as a fraudster but actually are not. True positive rate describes the proportion of all positive classifications that have been correctly classified as positive, which is the users that are fraudsters and have been classified as a fraudster. The formulas used were [26]:

\[
FPR = \frac{FP}{FP + TN} \quad (3.3)
\]

\[
TPR = \frac{TP}{TP + FN} \quad (3.4)
\]

The second step is to create the curves. This was made in the programming language R. Code for this is available in Appendix B, R-code.

3.7.2 Other measurements

Other measurements used when measuring the performance of the fraud detector is accuracy and precision. Accuracy is the proportion of the true results among all results, which is the true positive and true negative results. Precision is the proportion of the correctly predicted positive results among all the positive predicted results, that is the true positive and the false positive results. The following formulas has been used in order to calculate the accuracy and precision [26]:

\[
ACC = \frac{TP + TN}{TP + FP + FN + TN} \quad (3.5)
\]

\[
PREC = \frac{TP}{TP + FP} \quad (3.6)
\]
Chapter 4

Results

4.1 Results of case study

This section begins with listing the results from the scenarios studied in the case study. This is followed by the operation types found to reflect the characteristics used to identify fraudulent behavior in the studied Mobile Money system.

4.1.1 Phishing attack - general characteristics

The following characteristics has been identified for the phishing attack:

- Strong imbalanced relation between number of "advantage taker" and "advantage receiver", since a phisher is mostly receiving advantages/benefits and rarely gives away advantages/benefits.

- Many sporadic relations, since a phisher has contact with many victims but only once.

4.1.2 Grab and run attack - general characteristics

The following characteristics has been identified for the grab and run attack:

- Valuable items are stolen

- Short time span

4.1.3 Characteristics in the studied Mobile Money system

The following characteristics was found when the cases was studied based on the scenarios in the Mobile Money system. In contrast to the phishing attack the focus will be on the victims in the grab and run attack. This is based on the assumption that there will be a great behavior deviation when an attacker exploits the victims’ privileges.
Chapter 4. Results

• Phishers will receive the same amount of money a lot but have low number of transfers to other users
• Victims will be chosen by their access to high privileged accounts
• Mobile phones used by high privileged users are highly valuable for an attacker
• Victims of a grab and run attack will start to send a lot of money to the attacker’s account(s)
• Money earned from fraud must leave the system

The following operation types from the Mobile Money system has been identified as reflectors of the characteristics from the case study:

• Transfer
• Cashout

The following operation types could be used as alternative to a direct cashout operation that a fraudster may utilize in order to get money out of the system:

• Transfer to voucher
• Transfer from voucher

4.1.4 Operation types

Below follows an explanation of the interesting operation types found during the case study.

• Cash in - Deposit money to an account
• Cash out - Withdraw money from an account
• Transfer - Transfer money between accounts
• Transfer to voucher - Withdraw money from an account to a voucher
• Transfer from voucher - Deposit money to an account from a voucher
4.2 Results of rules

Based on the characteristics found in the case study in section 4.1.1, *Phishing attack - general characteristics* and 4.1.2, *Grab and run attack - general characteristics* the rules used when detecting fraud was defined as followed:

- **Rule A:** X number of operation type where a user stands as a sender respectively receiver.
- **Rule B:** Benford’s law. Explained in section 3.2.1, *Benford’s law.*
- **Rule C:** Each user can only send a specific amount with a specific operation type X number of times.

In total there was three rules defined, one for each case that was studied and one for Benford’s law.

4.3 Data visualization

Below is the results of a visualization of the data chosen to be visualized in section 3.5.1, *Data visualization.* There is only one graph in this section, which shows how many times users occur as sender in the different operation types. The rest has been omitted due to the size of the visualizations and can be found in 7.3 Appendix C, *Visualization results.*

In figure 4.1 it is possible to confirm potential limits. For example the operation type transfer should have a limit around 35 number of transactions, thus the frequency approaches 0.
Figure 4.1: Visualization of how often users send money for each operation type
4.4 Results of limits

As seen in section 4.2 Results of rules both rule A and C has an X that is undefined. The rules are not usable if the X’s are unknown. Each rule is applicable on any operation type available in the system. The value of X varies depending on which operation type it is applied on. Below follow tables that describes different limits found for rule A, rule C and each operation type for both the 95%-quantile, table 4.1 and 4.2, and 99%-quantile, table 4.3 and 4.4. These limits were found in the case study after statistics has been applied as described in section 3.2.4, Application of quantiles.

<table>
<thead>
<tr>
<th>Operation type</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer Sender</td>
<td>1.72</td>
</tr>
<tr>
<td>Transfer Receiver</td>
<td>2.36</td>
</tr>
<tr>
<td>Cashout Sender</td>
<td>0.92</td>
</tr>
<tr>
<td>Cashout Receiver</td>
<td>3.8</td>
</tr>
<tr>
<td>Cashin Sender</td>
<td>4.6</td>
</tr>
<tr>
<td>Cashin Receiver</td>
<td>1.52</td>
</tr>
<tr>
<td>Transfer to voucher Sender</td>
<td>86.12</td>
</tr>
<tr>
<td>Transfer to voucher Receiver</td>
<td>114.04</td>
</tr>
<tr>
<td>Transfer from voucher Sender</td>
<td>70.72</td>
</tr>
<tr>
<td>Transfer from voucher Receiver</td>
<td>10.44</td>
</tr>
</tbody>
</table>

Table 4.1: Limits, 95%-quantile for rule A

<table>
<thead>
<tr>
<th>Operation type</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer Sender</td>
<td>1.4</td>
</tr>
<tr>
<td>Transfer Receiver</td>
<td>0.92</td>
</tr>
<tr>
<td>Cashout Sender</td>
<td>0.32</td>
</tr>
<tr>
<td>Cashout Receiver</td>
<td>0.91</td>
</tr>
<tr>
<td>Cashin Sender</td>
<td>1.8</td>
</tr>
<tr>
<td>Cashin Receiver</td>
<td>1.24</td>
</tr>
<tr>
<td>Transfer to voucher Sender</td>
<td>8.56</td>
</tr>
<tr>
<td>Transfer to voucher Receiver</td>
<td>8.6</td>
</tr>
<tr>
<td>Transfer from voucher Sender</td>
<td>8.2</td>
</tr>
<tr>
<td>Transfer from voucher Receiver</td>
<td>61.64</td>
</tr>
</tbody>
</table>

Table 4.2: Limits, 95%-quantile for rule C
### Chapter 4. Results

<table>
<thead>
<tr>
<th>Operation type</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer Sender</td>
<td>1.92</td>
</tr>
<tr>
<td>Transfer Receiver</td>
<td>3.84</td>
</tr>
<tr>
<td>Cashout Sender</td>
<td>1.4</td>
</tr>
<tr>
<td>Cashout Receiver</td>
<td>4.76</td>
</tr>
<tr>
<td>Cashin Sender</td>
<td>6.12</td>
</tr>
<tr>
<td>Cashin Receiver</td>
<td>1.72</td>
</tr>
<tr>
<td>Transfer to voucher Sender</td>
<td>109.04</td>
</tr>
<tr>
<td>Transfer to voucher Receiver</td>
<td>114.84</td>
</tr>
<tr>
<td>Transfer from voucher Sender</td>
<td>94.8</td>
</tr>
<tr>
<td>Transfer from voucher Receiver</td>
<td>94.36</td>
</tr>
</tbody>
</table>

Table 4.3: Limits, 99%-quantile for rule A

<table>
<thead>
<tr>
<th>Operation type</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer Sender</td>
<td>3</td>
</tr>
<tr>
<td>Transfer Receiver</td>
<td>1.4</td>
</tr>
<tr>
<td>Cashout Sender</td>
<td>1.16</td>
</tr>
<tr>
<td>Cashout Receiver</td>
<td>0.32</td>
</tr>
<tr>
<td>Cashin Sender</td>
<td>2.32</td>
</tr>
<tr>
<td>Cashin Receiver</td>
<td>1.24</td>
</tr>
<tr>
<td>Transfer to voucher Sender</td>
<td>12</td>
</tr>
<tr>
<td>Transfer to voucher Receiver</td>
<td>12</td>
</tr>
<tr>
<td>Transfer from voucher Sender</td>
<td>10.36</td>
</tr>
<tr>
<td>Transfer from voucher Receiver</td>
<td>10.44</td>
</tr>
</tbody>
</table>

Table 4.4: Limits, 99%-quantile for rule C
4.5 Fraud injection in a data set

The following table, table 4.5, contains information about the data that was injected with fraud by the external supervisor [18]. The injected data is based on the external supervisors experience and knowledge from the area of fraudulent activity in the given Mobile Money system. In this particular case there was 30 injected entries in the fraud data and all 30 entries were found.

<table>
<thead>
<tr>
<th>Description</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table name</td>
<td>Fraud data</td>
</tr>
<tr>
<td>Time span</td>
<td>1 hour</td>
</tr>
<tr>
<td>Number of entries</td>
<td>106 130</td>
</tr>
<tr>
<td>Number of unique users</td>
<td>84 262</td>
</tr>
<tr>
<td>Number of cash out</td>
<td>18 713</td>
</tr>
<tr>
<td>Number of cash in</td>
<td>18 673</td>
</tr>
<tr>
<td>Number of transfer</td>
<td>7 372</td>
</tr>
<tr>
<td>Number of transfer to voucher</td>
<td>523</td>
</tr>
<tr>
<td>Number of transfer to voucher</td>
<td>400</td>
</tr>
<tr>
<td>Number of other transaction types</td>
<td>60 449</td>
</tr>
</tbody>
</table>

Table 4.5: Table with statistics for fraud-data set

4.6 Result of fraud detector and performance

The following tables, table 4.6 and 4.7, describes the result from the fraud detector. The data set that has been used as input to the fraud detector can be found in table 4.5. The tables describes the different rates for each rule and both for the 95%-quantile and the 99%-quantile. They also describes how many suspect fraudsters that were found for each rule. In total there was 30 injected entries in the fraud data and all 30 entries were found. Suspects and an entry is not equivalent, since one user may be involved in multiple transactions/entities.

The true positive describes how many users that were correctly classified as fraudsters, meanwhile false negative shows how many users that were not classified as fraudsters, while being fraudsters. False positive describes how many users that were classified as a fraudster when they were not and true negative describes how many users that were classified as not fraudsters when they were not fraudster, thus correctly classified.

As mentioned earlier the true and false positive rates are showing the proportions of how many users that have been correctly and incorrectly classified as fraudsters. These rates can also be found in tables 4.6 and 4.7.
### Chapter 4. Results

#### Table 4.6: Table that describe the different rates of all rules (95%-quantile)

<table>
<thead>
<tr>
<th>Rule</th>
<th>True positive</th>
<th>True negative</th>
<th>False positive</th>
<th>False negative</th>
<th>True positive rate</th>
<th>False positive rate</th>
<th>Suspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>3</td>
<td>83 829</td>
<td>429</td>
<td>1</td>
<td>0.75</td>
<td>0.005</td>
<td>433</td>
</tr>
<tr>
<td>B</td>
<td>3</td>
<td>84 158</td>
<td>102</td>
<td>1</td>
<td>0.75</td>
<td>0.0012</td>
<td>106</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>84 139</td>
<td>119</td>
<td>1</td>
<td>0.75</td>
<td>0.0015</td>
<td>123</td>
</tr>
<tr>
<td>AB</td>
<td>3</td>
<td>84 157</td>
<td>101</td>
<td>1</td>
<td>0.75</td>
<td>0.0012</td>
<td>105</td>
</tr>
<tr>
<td>AC</td>
<td>3</td>
<td>84 222</td>
<td>36</td>
<td>1</td>
<td>0.75</td>
<td>0.0004</td>
<td>40</td>
</tr>
<tr>
<td>BC</td>
<td>3</td>
<td>84 232</td>
<td>26</td>
<td>1</td>
<td>0.75</td>
<td>0.0006</td>
<td>30</td>
</tr>
<tr>
<td>ABC</td>
<td>3</td>
<td>84 155</td>
<td>103</td>
<td>1</td>
<td>0.75</td>
<td>0.0013</td>
<td>107</td>
</tr>
</tbody>
</table>

#### Table 4.7: Table that describe the different rates of all rules (99%-quantile)

<table>
<thead>
<tr>
<th>Rule</th>
<th>True positive</th>
<th>True negative</th>
<th>False positive</th>
<th>False negative</th>
<th>True positive rate</th>
<th>False positive rate</th>
<th>Suspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>3</td>
<td>83 829</td>
<td>429</td>
<td>1</td>
<td>0.75</td>
<td>0.005</td>
<td>433</td>
</tr>
<tr>
<td>B</td>
<td>3</td>
<td>84 158</td>
<td>102</td>
<td>1</td>
<td>0.75</td>
<td>0.0012</td>
<td>106</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>84 139</td>
<td>119</td>
<td>1</td>
<td>0.75</td>
<td>0.0015</td>
<td>123</td>
</tr>
<tr>
<td>AB</td>
<td>3</td>
<td>84 157</td>
<td>101</td>
<td>1</td>
<td>0.75</td>
<td>0.0012</td>
<td>105</td>
</tr>
<tr>
<td>AC</td>
<td>3</td>
<td>84 222</td>
<td>36</td>
<td>1</td>
<td>0.75</td>
<td>0.0004</td>
<td>40</td>
</tr>
<tr>
<td>BC</td>
<td>3</td>
<td>84 232</td>
<td>26</td>
<td>1</td>
<td>0.75</td>
<td>0.0006</td>
<td>30</td>
</tr>
<tr>
<td>ABC</td>
<td>3</td>
<td>84 155</td>
<td>103</td>
<td>1</td>
<td>0.75</td>
<td>0.0013</td>
<td>107</td>
</tr>
</tbody>
</table>
Chapter 4. Results

4.6.1 Accuracy and precision

In table 4.8 it is possible to see the accuracy and the precision of each rule and combinations of rules. The aim is to have both the accuracy and the precision to 1.0, which is 100%.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Accuracy</th>
<th>Precision</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.994897</td>
<td>0.006944</td>
</tr>
<tr>
<td>B</td>
<td>0.998801</td>
<td>0.029126</td>
</tr>
<tr>
<td>C</td>
<td>0.998576</td>
<td>0.02459</td>
</tr>
<tr>
<td>AB</td>
<td>0.998789</td>
<td>0.028846</td>
</tr>
<tr>
<td>BC</td>
<td>0.999549</td>
<td>0.075</td>
</tr>
<tr>
<td>ABC</td>
<td>0.99968</td>
<td>0.103448</td>
</tr>
</tbody>
</table>

Table 4.8: Results for each rule’s accuracy and precision

4.6.2 Receiving Operating Characteristics curves

The following curves, figure 4.2 and 4.3, are figures of the ROC-curve created when measuring the performance of the rules used by the implemented fraud detector. Figure 4.2, is a curve showing the axis from 0 to 1 and a line between (0,0) and (1,1). The second figure, 4.3, is a curve that has been zoomed in to make it easier to distinguish the distance between the points. The figures illustrate the the 99%-quantile only since the performance of the two quantiles are considered equivalent.
Figure 4.2: Unzoomed ROC-curve, difficult to distinguish were the results are placed
Figure 4.3: Zoomed in ROC-curve, easier to distinguish the different results
When defining the limits for the rules both the 95%-quantile and the 99%-quantiles was tested in order to determine if a higher quantile gives a better performance than a lower. When looking at the tables 4.6 and 4.7 it is possible to see that the performance between the quantiles are basically the same. The 95%-quantile has one user more in total that is misclassified than the 99%-quantile. This means that the results is nearly the same for both quantiles. The reason for this is because the data set that is examined is the same and therefore will not give a large deviation when comparing the 95%-quantile with the 99%-quantile. Also the percentage point is too small compare to the amount of data.

As shown in the tables 4.6 and 4.7 in section 4.6 Result of fraud detector and performance, the true positive has a medium-high detection rate of 75% for all the rules. In order to be able to determine which rule that is the best the false positive rate will be the determinative part. A value close to zero indicates that fewer users has been misclassified as fraudsters, which is desired.

The combination of rule A and C, also known as rule AC, is the rule with the best detection rate, since it has a false positive rate value of 0.0004%, which is very low and desired. It is also shown that combining the two methods, Benford’s law and quantiles determined limits, is not the best way, but it is still far the worst. An interesting discovery is that rule B and C combined is the second best rule combination, which supports the hypothesis stating that it is possible to combine the chosen methods. Benford’s law has almost the same false positive rate as rule C.

At a glance the overall result gives an indication that it has a good detection rate, since all rules has a very low false positive rate and a medium-high true positive rate. By studying the accuracy and precision for each rule and combination in table 4.2 it is possible to see that the proportion of the true result are close to 1. This is very good since it means that almost 100% of the classifications are correctly classified. The precision on the other hand does not give the same good results. The rule with the best precision is the combination of all three rules and it is slightly above 10%. This means that at best only 10% of all the user that are classified as fraudsters are fraudsters. The other 90% are not fraudsters, which is
Chapter 5. Analysis

not a good result.

When comparing our results to the criteria Rosset et. al. had in their report [15] we conclude that our rules do have a high accuracy and a high sensitivity which matches two out of the three given criteria. The third criteria, "High coverage of true fraud alerts", which aims for a quick detection of fraud cases has not been tested in this thesis due to no real time analysis has been made. Thus no conclusions of this criteria will be presented.

There is a difference in relation between the average activity in the two sets, live-data and fraud-data, that could have affected the result. The users in the live-data has an average activity of 4.3 entries per user while the users in the fraud-data has an average activity of 1.3 entries per user. This means that a user will be allowed about 3.3 more transaction in the live-data. This could affect the result in a way that it is easier to find fraudsters in the fraud-data since the users are not as much active as in the live-data. At the same time the live-data is captured over approximately one day, while the fraud-data is captured over one hour. The time-span difference is something that has been taken into account when setting the limits for the logs to be analyzed, but not the average activity.

As previously mentioned in this thesis working with log-files that is constantly growing, also known as big data, is a problem. It is hard to manage this huge amount of data that often is complex and unstructured. To mitigate this problem a static amount of data was analyzed. As a result of this choice, it is not possible to say how the selected method would work when applied on a constantly growing data set. In this case it means that a fraudster could easily pass thought the amount of information that is stored in this kind of system.

Due to the base rate fallacy there is a very strict requirement of have a high true positive rate and a very low false positive rate on a fraud detector. As shown in the results of the implemented fraud detector the chosen methods gives a very low false positive rate and a medium-high true positive rate. The current true positive rate will not be enough since 25% of all fraudsters will not be found. In big data 25% is simply too much. As a brief example: if there are 100 000 transactions with 100 fraudsters that tries to steal 1000 SEK each, there will be a loss of 25 000 SEK.
In this thesis we have investigated if it possible to combine the quantile-statistics together with Benford’s law, the law of digits distribution, to find fraud in data from logs within Mobile Money systems. This is important since M-commerce is a growing area but little research has been conducted within this area.

After evaluating the results of a case study and an implementation of a fraud detector we will say that it is possible to find fraud by combining quantile-statistics together with Benford’s law, even if that combination does not give the best result. The proposed methods has been proven to have very high accuracy and very low precision, both when used combined and independently. This shows that more research is required since the precision needs to be increased.

Benford’s law does not work that good on its own. But the law is a good complement to the other methods used in this thesis, which has been proven in this thesis when combining the law with limit-based rules. The primary use of the law would then be to tell if a set of data contains fraud rather than identify fraud. Therefore another way to use Benford’s law is to use it like a verifier by checking accounts that occurs in both the set of suspects flagged by Benford’s law and the set of suspects flagged by the limit-based rules.

The quantiles gives a good result by them self, and it is only a very small difference between the 95%-quantile and 99%-quantile with nearly identical performance. It would have been interesting to test even lower quantiles, such as the 75%-quantile, but since it is out of this thesis scope it could be a future work. The most efficient way to find fraudsters is by combining two proposed rules where quantiles were used in order to determine limits for the proposed rules. But since a combination of a rule and Benford’s law is second best the law should not be excluded.

Future work to this experiment could be to add more cases to the Mobile Money system. We had one more case that could been implemented but unfortunately we did not have the time. A short summary of the omitted case was to identify transactions that were split to be able to make a better commission. By adding more cases with belonging rules, another alternative could be to add more rules to the already implemented cases.

Another interesting and more advanced way to detect fraud is to further de-
velop the decision making of the methods in this thesis by taking the users trans-
action history into consideration in the fraud detector. Is it a first-time user (only
registered to perform a phishing-attack) or check if a user’s history is "clean" and
should not get the idea to send huge amount of money in a short time-span (grab
and run attack).
References


Chapter 7

Appendix

7.1 Appendix A, Benford’s law

Below follows the requirements a set of data needs to fulfill to apply to Benford’s law and also how to use Benford’s law.

7.1.1 Requirements

To be able to use Benford’s law there are requirements which the set of numbers needs to fulfill, besides that they need to occur naturally. The mean of the set of numbers must be greater than the median. The skew \(^1\) for the set of numbers must be positive, which means that the peak of the distribution will be to the left with a tail to the right, seen in figure 3.1

M.J. Nigrini concluded in his research, described in his book [12], that the set of data should contain numbers with at least four digits. If the set have numbers with fewer digits, it will give a slightly larger bias at the lower digits. He also concluded that the set of numbers gives a good fit about 3000 entries, to conform Benford’s law, mathematically. Tests with a set fewer then 1000 entries could be run, but it will give a larger deviation from Benford’s law. Tests with a set under 300 entries should not be tested, since they simply can be sorted from smallest to largest.

7.1.2 Conformity

Besides the requirements the set of numbers have to conform to Benford’s law. If one of these tests does not conform to Benford’s law, this could be an indicator that the values has been manipulated.

---

\(^1\)Skew measure the lack of symmetry, that is asymmetry, and checks where the peak is placed in a distribution and decides if the distribution is positive or negative
7.1.3 Z-statistics

Z-statistics is used to check the difference between the expected and the actual values in the first-two digit combinations and how they differ from the expectations of Benford’s law. The Z-score for each digit combination that exceeds a Z-score above 1.96, which means a 5% error rate, indicates that there is a difference between the actual and the expected values.

Z-statistics are sensitive to the excess power problem, which means when working with a large data set, the set could be falsely rejected since the Z-score becomes incorrect. To work around this problem it is easier to ignore the actual numeric value of the Z-statistics and focus on them with the largest values.

7.1.4 Basic digit test

To be able to use Benford’s law to detect anomalies in the data there is basic digit test. This test contains first-digit-test, second-digit-test and a first-two-digit-test and these three tests is called a first-order-test. The first-digit-test checks the frequency of the first digit, the numbers 1 to 9, of a number in a set of numbers. This test is to high level too be determine any abnormal duplications of numbers. However, as M.J.Nigrini mention in his book [12], “the general rule is that a weak fit to Benford’s Law is a flag that the data table contains abnormal duplications and anomalies.”

The second-digit-test checks the frequency of the second digit, the numbers 0 to 9, of a number in a set of numbers. This test is also to high level to determine any abnormal duplications of numbers, since it will show spikes at 0s and 5s because of round numbers, such as 50, 75, 150 and so on. If this test shows a spike at another digit, say 3, then the suggested approach [12] is to go to the first-two digits graph to check which combination that have 3 as the second digit that is causing the spike. When finding the combination causing the spike, select and review a smaller subset containing this combination.

The first-two-digit-test is a more focused test and is used to detect abnormal duplicates of digits and possible biases in the data.
7.2 Appendix B, R-code

Below follows R-code for generating a simple ROC-curve

\[
\texttt{plot}(x=\text{rocValues}[2], y=\text{rocValues}[1], \text{xlim}=\text{range}(0,0.01), \\
\text{ylim}=\text{range}(0,0.8), \text{xlab}="\text{False Positive Rate}" , \\
\text{ylab}="\text{True Positive Rate}" , \\
\text{col}=\text{c("red","blue","green","orange","brown","black","purple")}, \\
\text{pch}=19); \\
\texttt{plot}(x=\text{rocValues}[2], y=\text{rocValues}[1], \text{xlim}=\text{range}(0,1), \\
\text{ylim}=\text{range}(0,1), \text{xlab}="\text{False Positive Rate}" , \\
\text{ylab}="\text{True Positive Rate}" , \\
\text{col}=\text{c("red","blue","green","orange","brown","black","purple")}, \\
\text{pch}=19); \\
\]

\text{rocValues}[2] is a list variable holding every false positive rate for each rule. 
\text{rocValues}[1] is a list variable holding every true positive rate for each rule.
7.3 Appendix C, Visualization results

![Frequency plot of how often user is sender in each transaction type](image)

Figure 7.1
Figure 7.2
Figure 7.3
Figure 7.4

Frequency plot of how often a user receives amounts

- Cash in
- Cash out
- Transfer
- Transfer from voucher
- Transfer to voucher

Number of times vs. Frequency