

FRAUD DETECTION ON REMOTE BANKING: UNUSUAL BEHAVIOR
ON HISTORICAL PATTERN AND CUSTOMER PROFILING



SERHAT ÇAKIR

JANUARY,2020

FRAUD DETECTION ON REMOTE BANKING: UNUSUAL BEHAVIOR
ON HISTORICAL PATTERN AND CUSTOMER PROFILING

BY

SERHAT ÇAKIR

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

IN

DEPARTMENT OF MANAGEMENT INFORMATION SYSTEMS

YEDITEPE UNIVERSITY

JANUARY , 2020

Approval of the Institute of Social Sciences



Prof. M. Fazıl GÜLER

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master



Prof. Avadis Simon Hacınlayan

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Arts



Assoc. Prof. Aşkın DEMİRAĞ

Supervisor

Examining Committee Members

Assoc. Prof. Aşkın DEMİRAĞ- Yeditepe University



Asst. Prof. Aziz TÜTER- Yeditepe University



Prof. Özhan TINGÖY- Marmara University



I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

17/01/2020

Serhat akır

Signature :



ABSTRACT

The goal of this thesis is mentioning about history of informatics crimes and fraud on online banking systems. Additionally, I am going to talk about fraud detection systems, the types of these systems and detection models. Banks use specialized software solutions in order to avoid fraud issues as well as other sector companies. Banks's loses are unpredictably higher than the others which means they need to be consistent, determined, fast and smarter than fraudsters. The thesis is going to talk about the architecture of these systems, how data is evaluated internally and how the output is important for banks. Moreover, I will talk about the customer profiling technique that is a machine learning technique which is more precise and makes output easier to handle. Without that technique, all software solutions would be just collection of rules and became just a 'machine'. However, we need a machine that is smarter than a human. Criminals do not follow rules. Why should we?

Keywords: Fraud, Fraudster, Profiling, Informatics Crime

ÖZET

Bu tezin amacı bilimsel suçlar ve çevrimiçi bankacılıkta yapılan sahtekarlıklara değinmektir. Bununla paralel, özellikle bankaların kullandıkları sahtekarlığı önleme yazılımları, bu yazılım türleri ve kullanılan tespit modelleri hakkında bahsediliyor. Bankalar da diğer şirketler gibi çeşitli sahtekarlıkları engellemek için çeşitli koruma yazılımları kullanmaktadır. Bankalardaki kayıplar diğer şirketlere oranla daha fazla olduğu için sahtekarlardan daha akıllı ve hızlı yazılımlar kullanma ihtiyacı doğmuştur. Bu tez, bu yazılımların ortak yapılarını, datayı nasıl değerlendirdiklerini ve ortaya çıkan çıktının bankalar açısından ne ifade ettiğinden bahsediyor. Bunun yanı sıra, bir makine öğrenme tekniği olan profillendirme tekniğinden bahsediyor. Bu teknik kullanılmadan tüm çözümler insanların yazdığı kurallardan oluşan ve farklı düşüneyen bir makineden başka bir şey olmayacaktır. Bizim ihtiyacımız olan ise tam tersi insan gibi düşüneyen, öğrenebilen ve hatta insandan daha akıllı makineler. Suçlular kurallara uymazken biz neden uyalım ki?

Anahtar Kelimeler: Sahtekarlık, Sahtekar, Profillendirme, Bilimsel Suç

TABLE OF CONTENTS

APPROVAL.....	i
PLAGIARISM.....	ii
ABSTRACT.....	iii
ÖZET.....	iv
CONTENT	v
LIST OF TABLES.....	vii
LIST OF FIGURES.....	vii
1. INTRODUCTION.....	1
2. CYBER CRIME IN REMOTE BANKING.....	1
2.1 Cyber Crime Overview.....	2
2.1.1 The new world with PC and Internet.....	2
2.1.2 Crime before Internet.....	6
2.1.3 History of Cyber Crimes.....	6
2.1.4 Most Famous Cybercrime Types.....	8
2.2 Remote Banking.....	12
2.2.1 Customer Types.....	12
2.2.2 Channel Types.....	13
2.2.3 Transaction types.....	15
2.3 Fraud in Banking.....	22
2.3.1 Fraud Types in Banking.....	23
2.3.1.1 Credit Card Fraud	23
2.3.1.2 Employee Fraud.....	23
2.3.1.3 Application Fraud.....	24
2.3.1.4 Remote Banking Fraud.....	25
3. FRAUD DETECTION & PREVENTION SYSTEMS IN REMOTE BANKING.....	26
3.1 Fraud Detection & Prevention with Internal Systems.....	26
3.1.1 Security Picture and Single Use Pin.....	27
3.1.2 3D Secure.....	27
3.1.3 OTP SMS.....	28
3.1.4 OTP Token.....	28
3.1.5 OTB Mobile.....	28
3.1.6 Mobile Signature.....	29
3.1.7 IP Blocking.....	29
3.2 Fraud Detection & Prevention with External Systems.....	29
3.2.1 Fraud Detection Solutions.....	30
3.2.1.1 Client Database	31
3.2.1.2 Client Web Service	32
3.2.1.3 Solution Database	33
3.2.1.4 Intelligent Engine Server.....	34
3.2.1.5 GUI Application Server.....	36
3.2.2 Types of Fraud Detection Rules	37
3.2.2.1 Monetary.....	39
3.2.2.2 Services.....	41
3.2.2.3 Session.....	42
3.2.2.4 List and References.....	43

3.2.3	Incorporated Methodologies.....	44
3.2.3.1	Supervised Approaches.....	45
3.2.3.2	Unsupervised Approaches.....	45
3.2.4	Interactive Learning.....	46
3.2.4.1	Customer Profiling.....	47
4.	STATISTICAL ANALYSIS.....	56
5.	CONCLUSION.....	67
6.	LIMITATIONS & FUTURE WORK.....	69
	REFERENCES.....	71



LIST OF TABLES

	Page No.
Table 1: Annual Digital Growth Ratios	2
Table 2: Cluster Number-Amount 1	62
Table 3: Cluster Number-Amount 2	63
Table 4: Cluster Number-Amount 3	64
Table 5: Cluster Number-Amount 4	65
Table 6: Cluster Number-Amount 5	66
Table 7: Cluster Number-Amount 6	67

LIST OF FIGURES

	Page No.
Schema 1 : Numbers of Internet Users Increase Since 1995.....	4
Schema 2 : Some Current Digital Numbers	5
Schema 3 : How to Money Laundering Looks Like	11
Schema 4 : Form of Remittance Between Same Customer Different Accounts.....	16
Schema 5 : Form of Remittance Between Different Customer Accounts in Same Bank.....	16
Schema 6: Form of EFT.....	17
Schema 7: Form of WU.....	19
Schema 8: Form of EFT to Name.....	20
Schema 9: Form of Cash to Mobile.....	21
Schema 10: Form of SWIFT.....	22
Schema 11: Web Service Diagram.....	34
Schema 12: Intelligent Server Diagram.....	35
Schema 13: How IES Works	37
Schema 14 : Algorithm Diagram.....	39
Schema 15: Burst in Beneficiary.....	42
Schema 16: Interactive Learning Diagram.....	48
Schema 17: Profiling Periods.....	51
Schema 18: Clustering Types.....	59

Schema 19: Dendrogram.....	60
Schema 20: The Pythagorean Theorem.....	60
Schema 21: Data Sample	62
Schema 22: Cluster Plot 1.....	63
Schema 23: Cluster Plot 2.....	64
Schema 24: Cluster Plot 3.....	65
Schema 25: Cluster Plot 4.....	66
Schema 26: Cluster Plot 5.....	67
Schema 27: Cluster Plot 6.....	68



1. INTRODUCTION

You do not need a gun to rob a bank any more. Now a bank robber's most powerful weapon is a computer and an internet connection. Robbery, theft, pickpocket are the old fashioned crimes even though they are still common in our world. These kind of crimes cost thousands of dollars in best case. Now I am going to talk about the millions of dollars.

“Fraud can be loosely defined as “any behavior by which one person intends to gain a dishonest advantage over another”. In other words, fraud is an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other” (Chakrabarty, 2013, p.2).

Fraud is a million dollar business and it is increasing dramatically with the expansion of modern technology. Although prevention of fraud systems are used in companies, fraudsters also adapts the systems and find alternatives ways. As companies are struggling fraud issue in different ways, it is a priority issue for bank industry. Fraud detection must be performed once fraud is done, means it should be online which makes hard to detection and prevent it. Fraud prevention means stopping fraud at the first place where fraud detection involves identifying fraud as quickly as possible once it has been perpetrated. Banks use internal systems as well as other sector companies. However, these prevention systems are not as enough as stopping fraudsters. Therefore, detection of fraud becomes more important part of the fighting against fraud.

2. CYBER CRIME IN REMOTE BANKING

2.1 CYBER CRIME OVERVIEW

2.1.1 The new world with PC and Internet

“ENIAC, an acronym for Electronic Numerical Integrator and Computer is considered to be the first operational electronic digital computer in the United States, developed by Army Ordnance to compute World War II ballistic firing tables. The first all-electric computing machine was proposed by physicist John Mauchly in 1942 and was completed in 1945” (Beal, 2016, para.1). Before the ENIAC creation, calculating ballistic fire tables was taking 20 hours in manual. It decreased that duration in 15 seconds. The machine’s weight was 30 tons and was covering 167 m² (Bozkurt, 2013).

Computers became popular among people after IBM announced the first personal computers in 1981. With the developing of internet, computers took place in houses for personal use. In 1995, the internet users were just 16m in the world. In just 5 years, the internet users increased to 360m dramatically in the world. According to the research, the internet user in world increased approximately from 16 million to 4.500 billion from 1995 to June 2019 (See Table 1).

Date	Number of Users	% World Population	Information Source
Dec, 1995	16 millions	0.4 %	IDC
Dec. 2016	3,696 millions	49.5 %	Internet World Stats
June, 2017	3,885 millions	51.7 %	Internet World Stats
Dec 2018	4,313 millions	55.6 %	Internet World Stats
Mar 2019	4,383 millions	56.8 %	Internet World Stats
Jun, 2019	4,536 millions	58.8 %	Internet World Stats

Table 1 - *Numbers of Internet Users Increase Since 1995*
 (https://www.internetworldstats.com/emarketing.htm, 2019)

According to the research company “We Are Social”, almost half of the people in the world is using internet (See Schema 1).



Schema 1 - *Some Current Digital Numbers*

(<https://wearesocial.com/uk/blog/2019/10/the-global-state-of-digital-in-october-2019>, 2019)

Additionally, it increased 10% in last year and increasing year by year. It is inevitable to stop this increase while technology is developed in parallel and the way to access this technology is mostly available by internet (See Schema 2).



Schema 2 - *Annual Digital Growth Ratios*

(<https://wearesocial.com/uk/blog/2019/10/the-global-state-of-digital-in-october-2019>, 2019)

We are about to see a new generation of people able to use more technology and with access to much more information than past generation (Leishman, 2013, p.2). Humanity is addictive to internet and it seems that we won't give up to use it until the better and effective technology is invented. Every subject is one click away from people. That is why people do not hesitate to use it without thinking its bad side effects. As every positive look technology, internet also has negative consequences. Internet has many pros such as; unlimited access to information, bridging the culture gap, business, endless entertainment, new connections and so on. On the other hand it has many cons either such as; more dependent world, not secure for children, addiction and so on.

One of the most important negative result of using internet is having difficulties to saving personal information. Everything you are looking for or load onto the internet is becoming traceable and available to handle it for another people. If

you search something about t-shirt, you will be seen another t-shirt company websites everywhere and also you get emails from that websites. Much secure information is put into cyber world, like bank account information and ID numbers. Fraudsters can easily access it and commit fraud.

2.1.2 Crime Before Internet

Humanity and computers meetup goes back to approximately 60 years ago. The cybercrimes attempts started at 1960s by computers appeared and people realized that commit an offense is available by that machines.

Developing of the computer technology, designing new generation computers with smaller size, cheaper machines caused to reveal many computer users. Because people can easily manage this machine, they started to save and share their valuable data via computers. Widespread usage of this devices caused to be formed of new crime techniques. With the developed technology, computers became a crime machine that can harm more than other physical crime activities can.

2.1.3 History of Cyber Crimes

“When computers and networks came into being in the 1990s, hacking was done basically to get more information about the systems. Hackers even competed against one another to win the tag of the best hacker. As a result, many networks were affected; right from the military to commercial organizations. Initially, these hacking attempts were brushed off as mere nuisance as they did not pose a long-term threat. However, with malicious software becoming ubiquitous during the same period, hacking started making networks and systems slow. As hackers became more skillful, they started using their knowledge and expertise to gain benefit by exploiting and

victimizing others” (<https://cyberlawsinindia.wordpress.com/cyber-crimes/>, 2019, para.28).

As Internet usage is growing rapidly, the world is coming closer and becoming a smaller place for its users. However, it has a consequence to create another problem for people who spend many hours in Cyber World – which is cyber-crimes. A crime committed or facilitated via the Internet is a cybercrime

(<http://www.crossdomainsolutions.com/cyber-crime/>, 2011, para.1). Commit an offense over Internet connected activities is common as physical crimes. The crimes had already exist before the invention of internet. By virtue of the world, criminals are more anonymous and freer with virtual tools. Although, law enforcement agencies are trying to solve this issue, it is growing in parallel and many people become victims of cyber-crimes. While technology developing is a continuous activity, criminal people finds another way for commit a crime on the Cyber World (<http://www.crossdomainsolutions.com/cyber-crime/>, 2019).

Cybercrimes had not been known until end of 1960’s. Although it is impossible to exactly know, the first known cyber-crime was happened at 18th of October in 1966 in USA and it was published in a newspaper as ‘Computer specialist was blamed as making fraudulent alterations on accounts’ (Aydin, 1992, p.13).

The cybercrimes on computers and internet that occurred in 1970’s seem relatively basic if we compare them with today’s crimes. Although, computer sabotages, using computers in illegal ways, computer espionages were the crime techniques in that years, it has revolved in parallel to developing of the technology.

2.1.4 Most Famous Cybercrime Types

There are many cybercrime types that have been evolved in time while technology has been evolved in parallel. Each new technology brings risk with its benefits. Cyber Criminals look for this deficient part and penetrate into it. Although specialists find a way to protect people from these activities, they find a new way to commit an offense. The most famous cybercrime are listed below (<http://www.crossdomainsolutions.com/cyber-crime/>, 2019).

a- Hacking

Hacking is a gaining a personal information of people by broking their personal devices. In hacking, the criminal uses different kind of software to penetrate into the personal system and the person may not be aware of his device is being accessed by remote connection.

b- Spam and Phishing

Spamming and phishing are two very common forms of cybercrimes. There is not much techniques that you can control them. Spam is basically unwanted emails and messages. Phishing is a technique where criminals offer a bait so that you take it and give out the information they want. The bait can be about a business proposal, an offer you money with small favor, announcement of a lottery which you have never subscribed.

c- Malvertising

Malvertising is a criminal technique where it works basically clicking at some advertisements on web sites that is infected. Mostly, the websites do not aware of that. Cyber criminals insert that infected advertisements on the websites without the knowledge of websites owners

In other cases, cyber criminals use clean advertisements on websites for a while and replace it with malverts, so neither websites nor users do not suspect that. This techniques is one of the faster way for cybercrime, so websites do not even know they were used as a tool for that cybercrime.

d- Social Engineering

Social engineering is a techniques where the cyber criminals contact you by email or phone. After they gain your confidence, they get the information that they need. This information can be about your password, credit card number, maiden name, or other personal information that can be interest to the cyber criminals.

Recently, we hear this type of crime examples plenty of times in news. Even high educated people are victim of these criminals. From the most uneducated person to educated person, everyone has something to fear. They call randomly generally old people and threat them with the name of police officer. There are many famous people have fell into the trap and lost considerable amount of money.

e- Money Laundering

Money laundering is the criminal activity that has an intention to make the illegal money clear and conceal it from government. This money may come from serious crimes such as drug or terrorist activity money.

The basic money laundering process has three steps:

1- Placement

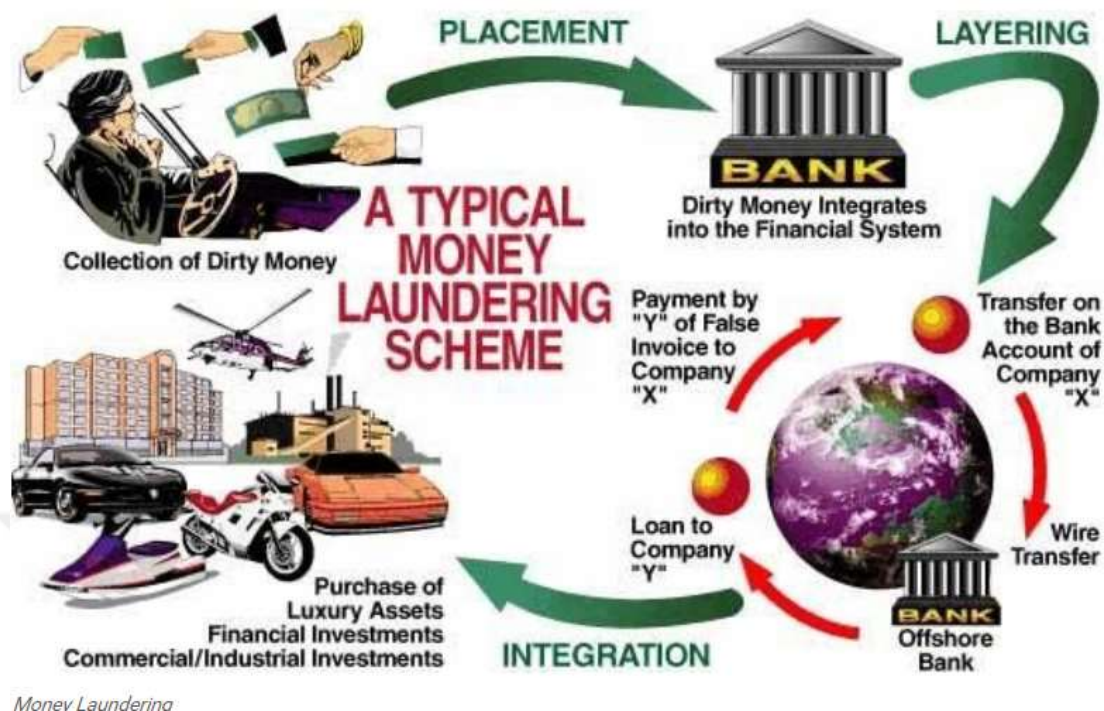
At this stage, launderer puts the dirty money into a bank. This is happening mostly in the form of cash deposit. This is the riskiest stage while large amounts are mostly suspicious in terms of banks. They are responsible to report this kind of high-value transactions.

2- Layering

At this stage, main goal is the sending money with different transactions to change its form and make it difficult to be tracked. Layering consist of many bank-to-bank transfers, swift transfers between different accounts in different countries with different names, making deposits and withdrawals large amount of moneys in accounts, changing currency of money, purchasing high value goods (houses, cars, ...). As a result, this stage is the main one that is all about the making dirty money as hard to follow as possible.

3- Integration

At this stage, the money looks like it is coming from a legal transaction. The criminal is able to use the money in legal way from that time (See Schema 1).



Schema 3 - *How to Money Laundering Looks Like*

(<https://www.jagranjosh.com/general-knowledge/meaning-of-money-laundering-1549620151-1>, 2019)

f- Fraud

“Fraud can loosely be defined as “any behavior by which one person intends to gain a dishonest advantage over another”. In other words, fraud is an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other, either by way of concealment of facts or otherwise” (Chakrabarty, 2013,p.2). Fraud is detected in many ways. Mostly, companies use internal control activities and detection systems to detect and prevent fraud.

Banks are the most important example of the victim of that criminal type. They use some basic internal prevention systems and external detection systems together. Online banking is the widest area for fraudsters for doing crime.

2.2 Remote Banking

Remote banking is an electronic environment that banks provided for customers connect remotely to the bank accounts and make transactions instead of using branches. Invention of banks comes back to need of saving money and taking debt. Banks make it easier to connect two people who do not know each other. People may send money, take a loan, make an insurance, and do similar things via banks.

Banks have opened millions of branches all over the world for their customers in order to make easier to reach the bank and make transactions easily. Customers used to visit branches personally to make transactions before the invention of the internet. With the development of technology banks invented remote banking environment

2.2.1 Customer Types

Most people have been needed to use credit card, transfer money, take a loan or withdraw money in their life. These are bringing to necessity to have an account from a bank. That has a consequence of each type of people became the customers' of banks. Company owner, insurance company, government, association, society, notary are some examples of customer types of banks for all over the world. Mostly banks divide their customer types basically into three types. The common customer types are;

a- Individual Customers

This customer type forms a big percentage of the accounts in banks. The population for this type is just for usual people who can have a low income or high

income. There is no much difference between people for this customer type. Their behaviors are quite similar.

b- Corporate Customers

This customer type is relatively different than individuals in meaning of income. Generally, legal entities, partnerships, notaries and commercial executives form this customer type. The transaction amounts are higher than individuals.

c- Financial Customer

This customer type consist mostly insurance companies, stock exchange funds, The Central Bank, all kind of different banks, tax administrations, social security institutions. Basically, for this customer type, transaction amount could be extremely high and volume also could be high as well.

2.2.2 Channel Types

With the direction of customer demands, banks provided different channels to customer to make the things easier for them. In history, people used to visit branches even for changing their address information. People can withdraw and deposit money, take a loan, pay credit card debit, change password and can do such things easily remotely with different channels.

- Online banking
- Mobile Banking
- Telephone Banking
- ATM

a- Online Banking

Online banking, with other words internet banking, e-banking or virtual banking, is an electronic payment system that provides customers a service for making financial transactions through the website. The online banking system is almost same as branch banking system on the execution of transaction wise. The most important difference is being able to execute the things anywhere internet is available.

b- Mobile Banking

“Mobile banking is the act of making financial transactions on a mobile device (cell phone, tablet, etc.). This activity can be as simple as a bank sending fraud or usage activity to a client’s cell phone or as complex as a client paying bills or sending money abroad” (Chen, 2019, para.1).

c- Telephone Banking

Telephone banking is a service provided by bank or other financial institutions that enables customers to execute different kind of transactions over phone by talking. Although branches are opened for limited hours, telephone banking is open for 24 hours at most institutions with limited amount of transactions.

d- ATM

Automated teller machine is an electronic telecommunications device that enables the customers of a financial institution to execute different kind of transactions without help of a human, branch employee or someone else.

2.2.3 Transaction Types

As banks have different customer types, several transaction types are executed in billions of times a day. Some transactions could be internal which means they are executed within the same bank, some are external which means doing it with other bank accounts, some are done with just address and some are done with just ID. Therefore, all banks have divided transaction type into classes which are easier to handle. The most common transaction type classes of banks are:

a- Account To Account Class

If the transaction is monetary and executed between two accounts, either it is internal or external we can call this class as AccountToAccount. Most of the transactions are executed under this transaction type class. The typical examples of AccountToAccount are Remittance and EFT.

Remittance transaction type is most used one while it is executed within the bank. Banks usually allow customers to make remittance transactions even at midnight. Since the money circulation stays still within the bank, it is easy to control and rather less dangerous in banks perspective. In order to make this transaction, there are 3 options to send the money. The one and easiest one is sending money within the accounts of the same customer. Choosing the own account to send money is the only needed for sending it. The other one is with Account No which needs to be filled both Branch Code and opposite Account No. Another one is with IBAN No which need to be filled just opposite IBAN No. Here are examples of transactions between different accounts of same customer and different accounts of different customers (See Schema 4 and Schema 5).

Schema 4 - *Form of Remittance Between Same Customer Different Accounts*

Schema 5 - *Form of Remittance Between Different Customer Different Accounts*

b- EFT

EFT (electronic fund transfer) is another transaction type which means sending money out of the bank. This type needs to be more investigated more carefully than Remittance since the money is not circulated within the bank which means not

possible to retrieve it in case it is a suspicious activity. Therefore, banks mostly allow to make this transaction within the work hours. There are 2 ways to send the money by EFT. One is again with Account No which needs to be filled, opposite account branch no, city and name and surname. The another one is with IBAN No which needs to be filled both opposite account IBAN No and name and surname (See Schema 6).

EFT to Account Help

Information Entry Approval

Payment Method

☒ From My Current Account ☐ From My Credit Card

Current Account TL	Balance	Flexible Acc. Limit	Available Balance
KOZYATAĞI ATATÜRK CADDESİ TR85 0006 7010 0000 0042 0492 14	100.000.000,00 TL	0,00 TL	100.000.000,00 TL

Recipient Information

Name and Last Name Select a Record from Smart Guide

Transfer Method ☒ IBAN ☐ Account No

IBAN

Transaction Details

Amount 0 , 00 TL

Trx. Date 05/11/2015

Description 0/50

☐ Rent Payment

☐ Add Transaction to Smart Guide ?

Continue

Schema 6 - *Form of EFT*

c- Address Based Payment Class

Banks have provided to their customers different ways to send or receive money. In this transaction type class, the originator or beneficiary doesn't have to have an account from any bank. They can send money with just beneficiary name and country ID. The most common example for this transaction type class is Western

Union which is well known within worldwide. EFT to name, Remittance to Name and Cash to Mobile are the other examples which are known in only Turkish banks.

In Western Union transaction type it is enough to type receiver's name, surname and destination country. It generates a unique code that needs to be sent to receiver. Within ID card or passport and that unique code, receiver can withdraw the money from any bank or institution that has an agreement with Western Union (See Schema 7).

Western Union Send Money Help

Information Entry Approval

Payment Method
Please select an account to complete your transaction.

Sender Information
 Address: Please select
 Mobile Phone: Please select
 There is no cell phone number which allows you to make the transaction. You can record your cell phone number via Yapı Kredi ATMs and branches.

Recipient Information
 Name:
 Last Name:
 Destination Country: Please select
 Destination Currency: Please select

Transaction Details
 Send Amount: 0, 00
 Delivery Option: Please select

Please [click here](#) to display Western Union money transfer customer notification form.

☐ I have read and accepted the Western Union money transfer customer notification form and I approve to share my personal information with Western Union.

Continue

Schema 7 - Form of WU

For EFT to Name and Remittance to Name, it is allowed to send money to just a name that can be withdrawn from the same bank(Remittance to Name) or different bank(Eft to Name) with only selected branches. The recipient can withdraw money easily with ID card or passport (See Schema 8).

The screenshot displays the 'EFT to Name' form interface. At the top, there's a title bar with 'EFT to Name' and a 'Help' icon. Below this is a progress bar with 'Information Entry' (active) and 'Approval'. The form is divided into three main sections: 'Payment Method', 'Recipient Information', and 'Transaction Details'. In the 'Payment Method' section, 'From My Current Account' is selected. Below it, a table shows account details for 'Current Account TL'. The 'Recipient Information' section includes fields for Name and Last Name, Father's Name, Telephone, Address, Bank, and Branch. The 'Transaction Details' section includes fields for Amount, Trx. Date, and Description, along with a checkbox to 'Add Transaction to Smart Guide'. A 'Continue' button is at the bottom right.

Current Account TL	Balance	Flexible Acc. Limit	Available Balance
KOZYATAĞI ATATÜRK CADDESİ TR86 0006 7010 0000 0042 0492 14	100.000.000,00 TL	0,00 TL	100.000.000,00 TL

Schema 8 - Form of EFT to Name

For the other addressed based class transaction type is Cash to Mobile. Here is again there is no need to be an obligation to be customer of the bank which one the money was sent from. There is need to go any ATM branch of the sender bank. Then without card, entering ID no, the own mobile phone, the amount of money and the unique code that mobile phone generates sufficient information to withdraw money (See Schema 9).

Cash to Mobile Help

Information Entry Approval

Payment Method

Current Account TL	Balance	Flexible Acc. Limit	Available Balance
KOZYATAGI ATATURK CADDESİ TR86 0006 7010 0000 0042 0492 14	100.000.000,00 TL	0,00 TL	100.000.000,00 TL

Recipient Information

Mobile Phone Select a Record from Smart Guide

Name and Last Name

Transaction Details

Amount , TL ?

☐ Rent Payment

☐ Add Transaction to Smart Guide ?

Continue

Schema 9 - *Form of Cash to Mobile*

d- Wire Fields Class

This transaction type class is more like Account To Account class with the sending money procedures. The most important difference from other types is this can be only available with foreign currency. The only example of that class can be given as SWIFT transaction type. In this transaction type, receiver should have an account on the same bank or another bank. There are 3 options to send the money over SWIFT. The first one is with IBAN No which needs to be filled out opposite account IBAN No, name and surname. The second option is entering SWIFT code of the receiver bank. Another one is Country Details options which needs to be filled with Country name, bank name, opposite account no, name and surname (See Schema 10).

The screenshot displays the 'SWIFT Transfer' interface, which is divided into two main tabs: 'Information Entry' (active) and 'Approval'. The 'Information Entry' tab contains several sections:

- Payment Method:** A dropdown menu with the placeholder text 'Please select an account to complete your transaction.' and a blue arrow icon.
- Bank Information:** A section with a 'Transaction Method' row containing three radio buttons: 'IBAN' (selected), 'SWIFT Code', and 'Country Details'.
- Recipient Information:** A section with three input fields: 'Name Surname / Title', 'IBAN', and 'Address' (with a '0/100' character count).
- Transaction Details:** A section with multiple fields:
 - 'Amount': A numeric input field showing '0' and '00'.
 - 'Trx. Date': A date picker showing '05/11/2015'.
 - 'Correspondent Charge': Radio buttons for 'SHA' (selected), 'OUR', and a '?' icon.
 - 'Transaction Type': A dropdown menu with 'Please Select' as the current selection.
 - 'Description': A text input field with a '0/140' character count.

At the bottom of the 'Transaction Details' section, there is an information icon and a link: 'Please [click here](#) to display SWIFT approval text.' Below this is a blue button with a checkmark icon and the text 'I have read and accepted the SWIFT approval text.'

Schema 10 - *Form of SWIFT*

e- Info Change Class

This class consist transaction types which are not based on monetary transaction, only based on customer information changes. Change of address, change of password, change of email address, change of phone number and change of fax number are most used transaction types under that class. Suspicious activities can be related with that changes.

f- Web session/ Mobile Session Class

This class is also not based on monetary transactions, only keeps the customer information during login process. Suspicious activities can also be related that information where fast and slow logins need to be investigated in banks perspectives.

2.3 Fraud in Banking

Fraud is the use of false representations to gain an unjust advantage (Bolton and Hand, 2002, p.235). Fraud is old as the humanity begun and has unlimited variety of different kind of forms. Moreover, recently with the development of technology, which makes easier our life to communicate and helps increase our spending power, has also provided more ways in which criminals may also commit fraud.

Fraud commonly happens due to financial stress and difficulty which give rise to pressure or motive for one to commit fraud regardless of risk involved. The second reason for one to commit fraud is the opportunity to do so (Sanusi, Rameli and Isa, 2015, p.108). The main goal for fraudsters is having monetary gains. This goal is making banks attractive for their perspective and more fraud-fragile as bulk money is kept in the banks. Fraudsters are more versatile year by year by designing their own ways. Banks's large databases and huge amount of information contain customer's personal and history information. As banking institutions have an activity in a wide range business, fraud could affect to many parties, including employees, employers, shareholders.

Beyond financial losses, fraud has also many negative consequences on institution reputation and customer loyalty. Additionally to these negative effects, the fraud cost is passed on to the customer who is the victim of fraud. Moreover, the individual who is the victim of fraud can has damages as mental, social, psychological and physical damage.

2.3.1 Fraud Types in Banking

There are dozens of ways for an individual to commit bank fraud. Some of them are more complex, and affect more people or institutions. Common types of bank fraud are:

2.3.1.1 Credit Card Fraud

Credit Card Fraud is an using some one else's credit card with the fraudulent purpose to make transactions in order to obtain money.

Credit card fraud happens when customers give their credit card, password information to unfamiliar individuals, when credit cards are stolen or lost, or when card information is copied by criminals. Although credit card fraud incident is about 0.1% of all cards transactions, it has a consequence of huge amount of losses as these kind of fraudulent activities are such large value of transactions. "In 1999, out of 12 billion transactions 10 million of them turned out to be fraudulent. Also, 0.04 % which means 4 out of every 10,000 accounts were fraudulent. Although, unexpectedly increasing of volume and value of the credit card transactions, these proportions stays already same or decreased by the help of precautions that institutions take (Hassibi PhD, 2000, p.151).

2.3.1.2 Employee Fraud

Employee fraud is a fraud once it is committed against the company where employee is working for. Employees are one of an organization's most important assets, but financial loss and reputational damage from employee fraud activities cause a greater threat. Employee fraud is more common and dangerous than most businesses think. In most cases, employee fraud can cause business failure and destroying careers. Misplaced trust, inadequate hiring, and failure of implementing

internal control systems lead to opportunity for employee to commit fraud. Employee fraud is all about the opportunity. As a result, business should take precautions to reduce this opportunity.

Employee fraud can take different forms. Some of these can be seen as trivial by the employees. In many cases, employees will not even consider the fact that they have committed fraud. They ignore that even the gained money is small amount it doesn't change the fact that they have committed fraud. It could be seen as small amount of money, but if all employees within a company do that same act then there may be certain financial results. The other more serious forms of employee fraud can be the following:

- Direct theft of Property
- Sending business information to competitors for personal gain
- Passing customer details to third parties in order to make attacks easier against organization.

2.3.1.3 Application Fraud

Application fraud is a fraud type when a person's account is opened with information is stolen or fake documents. Fraudsters can gather the useful information in order to cheat banks or they can create fake ones.

Normally, fraudsters collect personal information and financial data of innocent people from the documents, pay slips and other sources to commit the application fraud. The information that is collected from all these sources will be imitated or sometimes the details in the documents will be changed for the purpose of

submitting a new credit application. In recent years, internet has become the first place to collect that such information.

2.3.1.4 Remote Banking Fraud

Remote banking serves many benefits to banks and their customers. While the satisfaction of customers are increased, they also provide to financial institutions for lower operating costs. As a summary, remote banking is playing key role for most institutions.

Unfortunately, these remote channels puts the customer accounts in a danger, often across channels. As a result, these different channels cause new channels in proactively identify and preventing this electronic payment fraud.

Banks historically should to fight against deposit account fraud with channel-specific monitoring. However, as fraud continues to rise, these solutions are getting be less effective in a time that requires better account-level detection.

Fraudsters use sophisticated and evolving techniques to target various remote banking channels and leverage information from one channel to attack another. At the same time, banking customers increasingly use multiple channels and demand effective security with faster payments and fewer interruptions. Banks must be able to identify fraud and bridge the gap between fraud prevention and customer satisfaction.

3. FRAUD DETECTION & PREVENTION SYSTEMS IN REMOTE BANKING

Fraud is million dollar of business and increasing dramatically with the developments of technology. It has results like losing billions of dollars worldwide each year, that is why prevention fraud has a critical role for financial institutions. Although prevention technologies are the efficient way to prevent and reduce fraud, fraudsters are adaptive and always find a way to commit a fraud.

“Fraud prevention describes the security measures to avoid unauthorized individuals from initiating transactions on an account for which they are not authorized”(Kovach and Ruggiero , 2011, p.166). In spite of there exist advanced mechanism for fraud prevention for online banking, sometimes it can fail. Fraud detection is formed by identifying such unauthorized activities once the fraud prevention system is failed. Fraud detection is an alive system and must be used continuously, since the system is unaware the fraudster is committing a new kind of fraud.

Methods for the detection of fraud are significant if we are to catch fraudsters once fraud prevention has failed. This situation makes important to know the fraud cases before fraudsters commit it. Statistics and machine learning provide efficient technologies for fraud detection and is used to detect activities for credit card fraud, money laundering, telecommunications fraud, to name but a few.

3.1 FRAUD DETECTION & PREVENTION WITH INTERNAL SYSTEMS

We should start from distinguishing between fraud prevention and fraud detection. Fraud prevention describes measures to stop fraud from occurring in the first place (Bolton and Hand,2002, p.235). These includes fluorescent fibers,

watermarks, holographs on banknotes, personel identification numbers for bankcards, Internet security systems for credit card transactions, passwords on computer and telephone bank accounts. I am going to give some prevention examples for some Turkish Banks Remote systems.

3.1.1 Security Picture and Single Use Pin

After the system is activated, it will show different pictures and ask you to choose one of them. The picture will be the user's own "Security Picture.

The user will see the Security Picture each time the password is entered on to Internet/Mobile Banking. This application has been developed to protect customers from fake websites. The picture will not be seen on fake website and by the help of that it will prevent to make transaction on that website.

While providing extra security in your Internet/Mobile Banking logins, Şifrematik also provides speed and convenience in your Mobile Banking logins with the "Mobile Banking" step that appears in its menu.

Internet Banking first login and registration transactions:

When you run the application , the PIN code will be asked. After entered the PIN code, press Continue, and click the "Generate PIN" option in the menu.

Enter the PIN number that will appear on the message on mobile phone then confirm the Security Picture.

3.1.2 3D Secure

Dimensiol Security System which allows you secure shopping via internet.

With 3D Secure, the information flow between customer, the bank and the workplace is provided by passwords and keys during internet shopping. The customer who make the shopping is responsible to just entering 3D password that comes up to mobile

phone via sms. System will work with the guarantees by "Verified By VISA" for VISA cards and "SecureCode" for Master Cards.

3.1.3 OTP SMS

OTP SMS is a system to send to mobile phone one time password for login to internet banking and make the money transfer and payment operations. No one can use this one time password for the second time.

3.1.4 OTP Token

OTP Token is a portable device that creates one time passwords for login the internet banking and transaction signing.

OTP token creates two stage security while you enter one time password generated by this token after you enter your User ID and password.

If OTP Token is lost, you can cancel it by telephone call and request a new one immediately.

3.1.5 OTB Mobile

OTP Mobile is One-Time Password that is a software operating via the mobile phone. There is two stage security for your login and transaction approval at Internal Banking. You can use the t passwords that the mobile phone generates in addition to static password with OTB Mobile for login the internet banking and making transaction. These passwords can not be used twice from any one.

3.1.6 Mobile Signature

By using Mobile Signature, you can easily log on to Internet Banking and quickly perform your transactions. The places where Mobile Signature is used are listed below:

Mobile Signature is a service that enables you to conveniently obtain and use the electronic certificate which stands for your identity card in the electronic environment and Mobile Signature serves as the equivalent of handwritten signature in electronic environments and can be used via GSM SIM cards.

If you wish, you can log on to Internet Banking by using electronic signature.

3.1.7 IP Blocking

User's country that connected to system , internet provider, computer's IP can be saved to the system. Accessing to Internet banking can be blocked in case user connects the system from another country then it was saved before.

3.2 FRAUD DETECTION & PREVENTION WITH EXTERNAL SYSTEMS

Talking to employees of international companies, the answers are mostly same 'Our internal systems are perfect, there is not way for fraud here'. Internal control implies a system of well designed processes for the purpose of preventing fraud.

Are internal control systems effective and sufficient as fraud detection systems? Fraud prevention systems are effective systems for preventing basic fraud attempts. Of course, none of these methods are perfect. In contrast, fraud detection systems involves detecting fraud as quickly as possible once it has ben comitted. Fraud detection involves into the game once fraud prevention methods are failed. In

practise, fraud detection systems have to be used continuously where one will be unaware that fraud prevention has failed. We can try to prevent credit card fraud by saving our cards carefully. However, if the card's details are stolen, they we should be able to detect as soon as possible once the fraud is being committed.

Fraud detection is a continuously evolving system. Once it becomes known that once detection method is in place, fraudsters adapt it and find another way. New criminals are also entering the field constantly in the parallel. Most of them won't be aware of the fraud detection models will adopt these strategies where they have been successful in the past in another new criminals. This means earlier detection tools should be applied with latest developments.

The development of new fraud detection techniques is difficult by the fact that new cases come to mind once they are committed. It doesn't smart to describe fraud detection techniques in detailed in the public domain where it gives fraudsters an idea that they need to conceal the crime. All these reasons caused a need to create fraud detection systems which are able to stop fraud attempts once they are detected by bank's internal control systems. I am going to talk about structure of Fraud Detection Systems in details.

3.2.1 Fraud Detection Systems

Fraudsters use sophisticated and complicated techniques to penetrate remote banking channels and use information from one channel to attack another. At the same time, remote banking customers are making various types of transactions with different channels and expect security and faster payments and fewer interruptions. Banks must be able to detect fraud and look after customer satisfaction while doing that process. The economics of customer relationships are changing in fundamental

ways, and companies are facing the need to implement new solutions and strategies that address these changes (Rygielski, Wang and Yen, 2002, p.484). Fraud is an instant crime, and has to be detected and prevented instantly, real-time. Real-time transaction processing detects fraud attempts while allowing customer to do transactions. This processes is balancing both fraud risk and customer impact. External fraud detection systems are taking crucial role at this point. Lets see the common infrastructure properties of these systems in details.

3.2.1.1 Client Database

All over the world for different kinds of banks , fraud types varies from one place to another. In the same country, different banks have similar data and so do fraud types while customer type is almost same. This makes the needs similar as well and that is how the solutions create their database by collecting common data structure from customers. “Bank's large databases and voluminous information contain customer's information and the history of their transactions. These databases could help them to increase profitability, since they need to use more and better ways for analyzing their customers and increase their profitability” (Zadeh, Faraahi and Mastali, 2011, p.458).

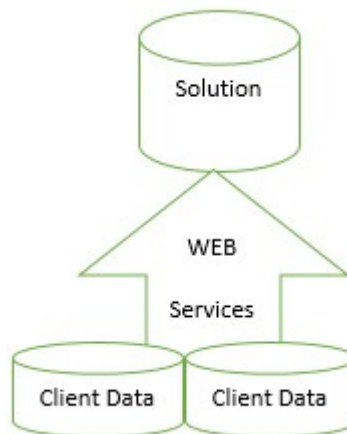
A bank customer can has either 1 account or 1000 accounts like big companies, Mercedes, Mc Donalds. Each account can behave differently and need to be investigated separately. Because of that reason each customer has to have an unique key as Party_Key and each account has an unique key as Account_Key which is specified by the bank itself. That causes a consequence that one Party can have more than one account. These numbers are unique numbers and can not be repeated on another customer or account. The example of other information fields of customers

are Account_Name , Account_Address, Account_Mobile_Phone_Number, Account_Birth_Date, etc.

3.2.1.2 Client Web Service

Banks have web services that are able to transmit transactions real time.

“A web service is a service offered by an electronic device to another electronic device, communicating with each other via the World Wide Web. In a Web service, Web technology such as HTTP, originally designed for human-to-machine communication, is utilized for machine-to-machine communication, more specifically for transferring machine readable file formats such as XML and JSON” (Semule, 2017, para.1). Web services get needed data from the bank database and distribute them into different transaction type-classes and then map fields with solution database fields. As I mentioned in previous subjects, there are different transaction type and classes in Bank X’s Remote Banking Web Service which are AccountToAccount, Address Based Payment, Wire Fields, Info Change Fields and Web/Mobile Login Sessions . The transactions that come from the bank internal DB is divided into these classes in the web service in first place. Then each field in that transaction types are mapped with the same fields that exist in the solution WSDL (Web Services Description Language) (See Schema 11).



Schema 11 - *Web Service Diagram*

3.2.1.3 Solution Database

The customer data that comes from bank's internal system via web service, is populated into solution staging database. Most common database brands are Oracle and SQL. Though they have plenty of similarities, there are some differences on query language and operation based. The most important difference is the operation system that these systems build on. Since SQL is only work on Windows, Oracle is working on not only Windows, but also UNIX related operating systems such as Linux, Solaris, and FreeBSD which can be also free. That is the main reason that most of the banks choose Oracle Database. Oracle database consist of users which each has one schema that has the same name with the user. A schema is created with proper tables and fields with respect to needs of solution engine server. There are different tables that keeps the customer reference data such as account, party, address, email, phone, card, country or transactional data such as transactions and transfers.

The data from the solution database comes through into the intelligent engine server via appropriate channels. The data is evaluated into that server and export

meaningful outputs for user display screen. Let's deep dive in the Intelligent Engine Server.

3.2.1.4 Intelligent Engine Server

At the heart of the solution platform is the Intelligent Engine Server that is an analytical engine that analyses of high-volume customer data, detects complex suspicious scenarios and behavioral patterns. Rather than setting up a costly data warehouse and executing exhaustive data mining against it, the engine processing is performed in real-time by directly connecting to multiple data sources of varying types.

The IES quickly analyzes defined models and proactively monitors the solutions transactional information flow. Analyzing each transaction only once, the solution identifies elements that may impact the models, flagging transactions according to predefined criteria (See Schema 12).



Schema 12 - *Intelligent Server Diagram*

a- The Methodology

Using innovative algorithms, the IES processor rapidly searches through data, analyses the data for matches against predefined models, and then distributes alerts.

In addition to its ability to “listen” to real-time sources, the IES also handles static data (in repositories and files) and data loaded through batch processing.

b- How Does the IES Work?

Solution’s proprietary process utilizes rapid analysis of massive volumes of data, recognizes non- quantitative patterns, predefined events and statistical deviations, and then delivers actionable messages to the dedicated recipient (person or system) best suited to respond. This is accomplished by:

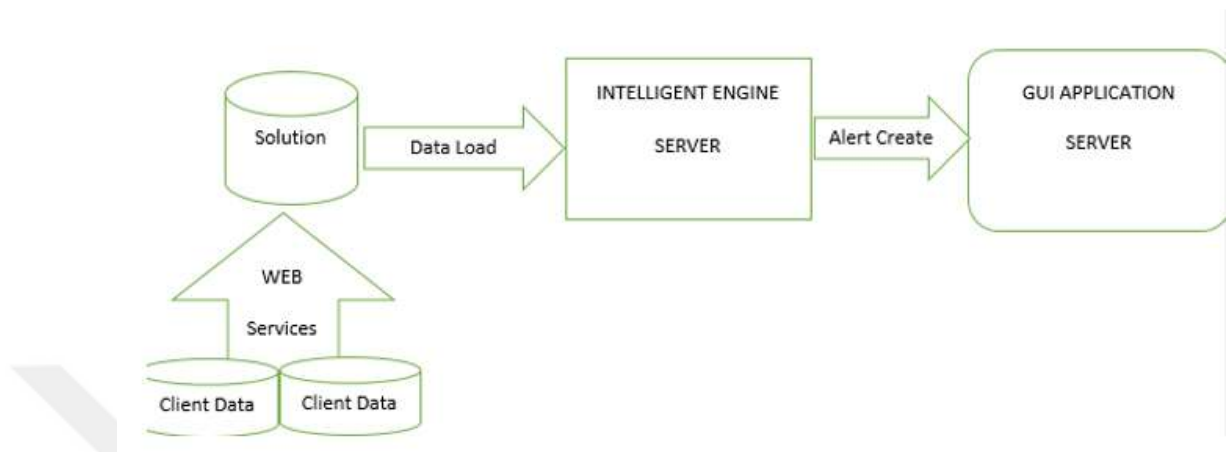
Detection: The Solution platform automatically pre-analyzes various models to understand the parameters that need to be evaluated and the data elements that impact them. It is then able to link to the relevant data sources, processing thousands of records per second to find those that are needed to evaluate the required parameters.

Analysis: Having identified the necessary raw data record, the solution platform evaluates the impact of those records on the various models’ analytical objects. Then the solution platform creates an optimized, multi - dimensional data structure to manage these objects with minimal resources, and can thus process massive volumes of data with very modest infrastructure requirements.

Recognition: Since the solution platform maintains links between the various analytical objects and the models that are based on them, it can quickly test whether a given change in any object has resulted in a change in the status of the model, and thus identify any action that needs to be taken.

Targeting: Should any action be taken, the solution platform delivers an "action item" to the optimal point within the enterprise. The system uses any available

messaging tool or inserts records directly into action queues for downstream systems (See Schema 13).



Schema 13 - *How IES Works*

3.2.1.5 GUI Application Server

GUI Application Server (GAS) is a web-based portal for streamlining investigation and reporting. The GAS controls the organizational workflow for internal review and analysis of the alerts generated by the solution detection application. Analysts, and other designated personnel, receive prioritized and filtered notification of anomalous behavior with supporting case information. Users who wish to gain further context can easily “drill down” into suspicious activity data, find information on related events, and obtain detailed profiles for all accounts and individuals involved.

Depending on the users’ role and level of authority they may reassign, escalate, or process alerts from a personalized list, or a common (departmental) queue. Case Manager Review features enable them to modify the status and score of an alert, to attach notes and other documentation and determine resolutions to alerts. The user can

note and describe the disposition of resolved alerts, and can optionally assign alerts to cases for a more focused review.

The GAS application supports the organizational compliance process for internal review and investigation of suspicious activities. It is a web-based application used by analysts, compliance professionals, managers, administrators and other principals involved in the process.

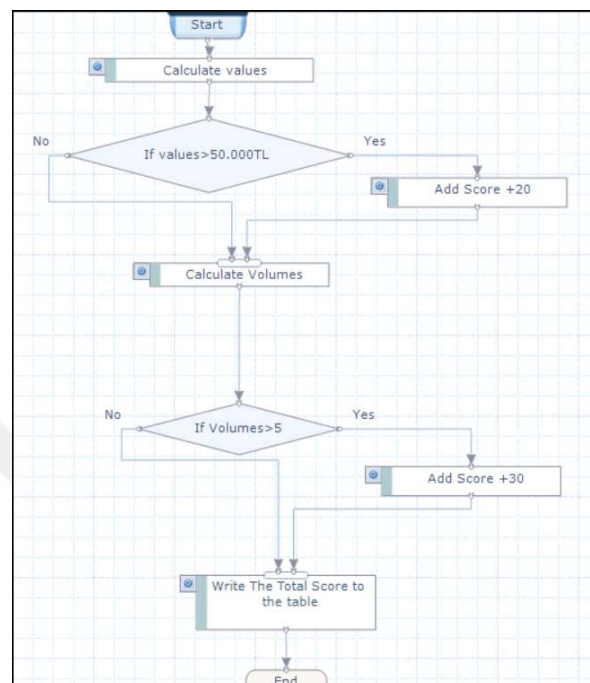
The GAS is built in a modular fashion, enabling each organization to select those modules that fit their needs. Each module can also be presented within the application according to specific users' needs, enabling Management and System Administrators to access modules that are appropriate for their roles, without displaying these modules for all users. The solution receives data from the organization's data sources.

3.2.2 Types of Fraud Detection Rules

The fraud detection solution gets the data from the bank core database and put it into the solution's intelligent engine in order to be evaluated. Transactions are evaluated according to predefined rules that were already created by solution itself by the years of experience of fraud incidents from all over the world. Rules are created with if-else logic, and in case the satisfaction of the demands of the rules, system creates suspicious alerts to be investigated by bank's compliance officers.

Here is an example of a logic of a rule. In this rule; firstly the values of the transactions are calculated. Then, the logic starts to work and it checks whether the values are exceeding 50K or not. If it is, it adds +20 score to the table. Secondly, it checks the volume, in other terms "how many times did it happen". Then, another 'if

logic' calculates the volume and if volume exceeds 5, it adds +30 score to the table
(See Schema 14).



Schema 14 - Algorithm Diagram

Finally, the system adds the scores that is created by the rule's conditions and creates an output to compliance officer screen (GAS). Officer has to investigate the case and immediately decide whether it is a fraudulent activity or not. According to that decision, the transaction may be allowed, blocked or challenged. If there is no sign of the transaction is a fraudulent activity, the officer lets it go (allow). If a customer makes a transaction that can be a fraudulent activity, officer stops (block) the transaction.

We may divide the fraudulent activities into 4 categories. Monetary, service, session and list and references.

3.2.2.1 Monetary

Monetary is a fraudulent activity that is related with only money transactions. Sending or receiving money is the main subject of this type. Common fraudulent models of monetary transactions are following;

- Activity with new payee
- Activity with rounded amounts
- First transaction for customer
- Activity with similar amounts
- Transaction to new foreign country
- Transaction to/from high risk country
- Suspicious amount
- Unusual no email notification
- Multiple Customers Per Payee

In order to deep dive of models, lets explain some of them.

Transaction to/from high risk country

The Transfers to/from High Risk Destinations model monitors fund transfers in order to detect significant transfer activity made from or to a location or entity that is considered high risk. A suspicious source/destination can be:

- A country that refused to cooperate with international regulations (e.g., countries on the High Risk Country List). In the case of such countries it is difficult to monitor movement of transfers within the country
- Transfer to/from High-Risk Financial Services Institutions (FSIs). These may be financial institutions that are not well known by the international

organizations and therefore may not comply with the AML standards (e.g., small private banks in remote locations).

- Any geographical location that is considered high risk, including cities or neighborhoods that are associated with a high degree of criminal activity.

This model is applied to both individual account activity and to activity associated with logical entities. For example:

Funds are transferred from an account during the month of December to an account in Nigeria, which is a country listed on the High Risk Country List of countries. Transfers are made for \$13,000 and then \$20,000. Later, in the same month, a transfer of \$22,000 is made from an account in Myanmar (another country that is on the High Risk Country List) to the account.

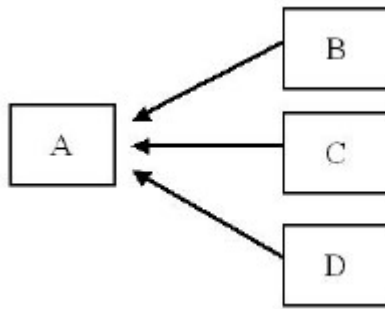
The last transfer triggers an alert by the Transfers to/from High Risk Destinations model, which identifies the three occurrences as suspicious activity. An alert is generated since there are three occurrences during a period of one month. The recurrence of the activity indicates a pattern of transfers to high-risk countries.

Multiple Customers per Payee

This model detects multiple payments to the same beneficiary within a period of time, by different originators. This may indicate that the beneficiary is part of a network of accounts that are engaging in illicit activities. This model works in conjunction with the Burst in Originator model to identify suspicious activity networks.

For example:

For over 5 days, account B makes 2 transfers of \$10,000 each to account A; account C makes 1 transfer of \$20,000 to account A; and account D makes 3 transfers of \$5,000, \$8,000 and \$12,000 to account A. This activity is detected as a burst of transfers to account A, and a Burst in Beneficiary alert is generated (See Schema 15).



Schema 15 - *Burst in Beneficiary*

3.2.2.2 Services

The second type of fraudulent activity is Services. This is subject of non-monetary transactions which is not related money. This is mostly first step of frauds before making money transfer. Common fraudulent models of service transactions are following;

- Recent address change
- Recent email change
- Recent enrollment
- Recent information change
- Recent name change
- Recent phone number change

In order to deep dive of models, lets explain one of them.

Recent phone number change

This model identifies accounts that have just changed the telephone number and made a transaction.

Fraudsters mostly change the recorded telephone number once they hacked the application. By the help of that authentication message will be sent to fraudsters mobile phone once the transaction is executed. For example:

A fraudster has hacked the mobile application password of a client and changed the mobile phone number which was recorded by the client. After then, fraudster immediately made transactions which are suspicious amount. The alert is generated and stopped the transaction.

3.2.2.3 Session

The other type of fraudulent activity is Session. This is mostly first step of frauds before making money transfer. Common fraudulent models of session transactions are following;

- Unusual activity from new device
- Access from old device
- Suspicious activity from same device
- Access from multiple locations
- Implausible/new location
- One time password used
- Multiple challenged logins skipped

3.2.2.4 List and References

The last fraudulent activity type is List and References. This type is related with high risky lists that are released by governments ,other countries or internal experiences. Common fraudulent models of List and References are following;

- High focus bank
- Access from high focus device
- Access from high focus ISP
- Safe Bank
- High focus customer

In order to deep dive of models, lets explain one of them.

High focus customer

Many government regulations, such as the MASAK, require financial institutions to provide higher scrutiny to those customers who have been identified as potential candidates for concern. For example:

- Residents of known terrorist or high risk countries
- Foreign country high officials

This model evaluates the various entities' attributes (KYC) and, based on multiple criteria, identifies entities that have characteristics that may indicate an increased risk of fraud activities.

- This model is designed to identify such characteristics and to calculate a risk score. Financial institutions can flag these customers, so that all their transactions will be especially scrutinized by the solution.

- This model enhances alerts by assigning a higher score to the alert when it detects that an entity with high focus characteristics is involved in the activity. For example:

The customer's Citizenship Country is UK, but Domicile Country is Nigeria. The domicile country of the customer is on the High Risk Country List. This would indicate increased suspicion and would result in enhanced due diligence for this account when detection models are applied.

3.2.3 Incorporated Methodologies

Fraud detection is a non-stopped evolving issue. Whenever it is known by companies, fraudsters will adapt their strategies and constantly applies new criminals. It leads to necessity for fraud detection methods stay as updated. However, it is not that easy where exchange of ideas is a little bit limited among companies. It is impossible to describe fraud detection methods in public, where fraudsters may beat them easily and look for an alternative way. Data sets are not made available and results are often censored, making them difficult to assess. Many fraud detection problems involve huge data sets that are constantly evolving. For example, the credit card company Barclaycard carries approximately 350 million transactions a year in the United Kingdom alone (Bolton and Hand, 2002, p.236).

The Royal Bank of Scotland, which has the largest credit card merchant acquiring business in Europe, carries over a billion transactions a year and AT&T carries around 275 million calls each weekday (Bolton and Hand, 2002, p.236). Processing such data sets for fraudulent transactions requires variety statistical models and efficient algorithms. These values also indicate the potential fraudulent detection and company loses which is critical numbers for them. Statistical tools for fraud

detection are many and varied, since data from different applications can be diverse in both size and type, but there are common themes. Statistical fraud detection methods may be supervised or unsupervised (Jans, Lybaert and Vanhoof, 2007).

3.2.3.1 Supervised Approaches

In supervised methods, samples of both fraudulent and non-fraudulent records are used to construct models which allow one to assign new observations into one of the two classes. Of course, this requires one to be confident about the true classes of the original data used to build the models. It also requires that one has examples of both classes. Furthermore, it can only be used to detect frauds of a type which have previously occurred (Bolton and Hand, 2002). After building a model using the data, new cases can be classified as fraudulent or non-fraudulent. Furthermore, this method is only available to detect fraudulent activities which have been occurred in the past.

3.2.3.2 Unsupervised Approaches

On the other hand, unsupervised methods are not interested in these kind of records that supervised methods are interested in. Unsupervised methods look for accounts, customers that behave unusual from the norm. The aim is modeling a baseline distribution that shows normal distribution and then try to detect unusual behavior from this norm. Divergent records are basic form of nonstandard observation. In these kind of statistical analysis, amount and quality of data is critical in order to help to find the unusual ones.

The analysis should be regarded as alerting us to find real fraud activity among fraudulent ones where it has many accidental error and non-fraud data. By that

way that it can then be investigated in more details. One can think of the objective of the statistical analysis as being to return a suspicion. The higher the score is, then the more unusual is the observation or the more like previously fraudulent values it is. The fact that there are many different ways in which fraud can be perpetrated and many different scenarios in which it can occur means that there are many different ways to compute suspicion scores (Bolton and Hand, 2002).

3.2.4. Interactive learning

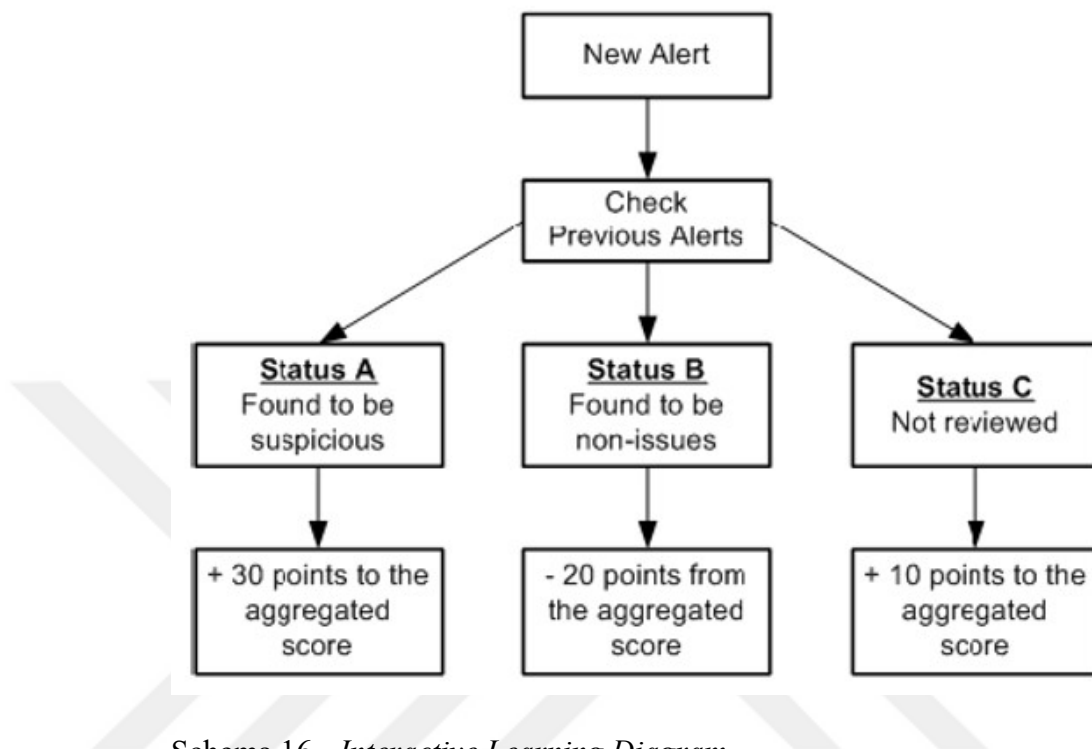
The Interactive Learning mechanism is one of the elements that assist the fraud detection systems to achieve a low false-positive ratio. The models use feedback from system analysts as part of an interactive scoring process that contributes to the prioritizing of future alerts. This learning mechanism analyzes the actions of the users and utilizes this knowledge to enhance its internal analysis algorithms.

In effect, the system becomes more intelligent with time, enhancing its internal algorithms by learning from the users' actions.

This method of learning is based on the statuses of previous alerts. The following demonstrates automatic learning scenarios:

- If previous alerts for the same entity containing the same rule issue were found suspicious, a higher score will be assigned to the new alert.
- If previous alerts for the same entity containing the same rule issue were cleared and identified as non-issues, a lower score will be assigned to the new alert.
- If previous alerts for the same entity containing the same rule issue were not reviewed, a higher score will be assigned to the new alert. Typically,

this score will be lower than in the case of previous suspicious alerts (See Schema 16).



Schema 16 - *Interactive Learning Diagram*

3.2.4.1 Customer Profiling

Profiling is a valuable methodology that enables many solution models to evaluate unusual behavior. Profile data can be collected for different entities over a historical period of interest. For example a core model, dedicated to calculating account profile data, can study the typical activity pattern of each account and maintain behavior profiles on account activities based on specific transactional data elements, over specified periods of time. Ongoing monitored activity can then be compared to the aggregated profile data in order to identify activity that deviates from normal behavior for that entity.

The main goal for fraud detection is being more accurate. I believe that each account's own activity must be followed for better fraud detection. First, fraud

detection has to be event driven rather than time driven. By the help of that way, fraud can be detected once it is happening, not at another fixed time duration which is unrelated to account activity. Second, fraud detection model should have memory and keep history calls account by account. Early calls are less important, but recent calls have to be taken into consideration closely. “Third, fraud detection must be able to learn the calling pattern on an account and adapt to legitimate changes in calling behavior. Fourth, and perhaps most importantly, fraud detection must be self-initializing so that it can be applied to new accounts that do not have enough data for training. The basis of our approach to fraud detection is an account summary, which we call an account signature that is designed to track legitimate calling behavior for an account. An account signature might describe which call durations, times between calls, days of weekend times of day, terminating numbers, and payment methods are likely for the account and which are unlikely for the account”(Cahill, Lambert and Pinheiro, 2000, p.6).

3.2.4.1.1 Profiling Periods

Profiling models combine information available for each transaction belonging to a party with additional information aggregated at the account level, called profiles. Profiles are used mainly to establish patterns of usual behavior for every party in the data. These patterns of behavior are established for time windows of various lengths. The following defines the various timeframes used in the modeling process:

- **History Period** – The time period before the vesting period and does not include the vesting period. This is the period that provides data for profiles.

• **Vesting Period** – The period during which an activity is considered as unknown in terms of fraud occurrence. This means that any activity during this period is not used for constructing the entities' behavioral patterns. This time period spans between the current transaction time and a specified look back period, typically 20 days back.

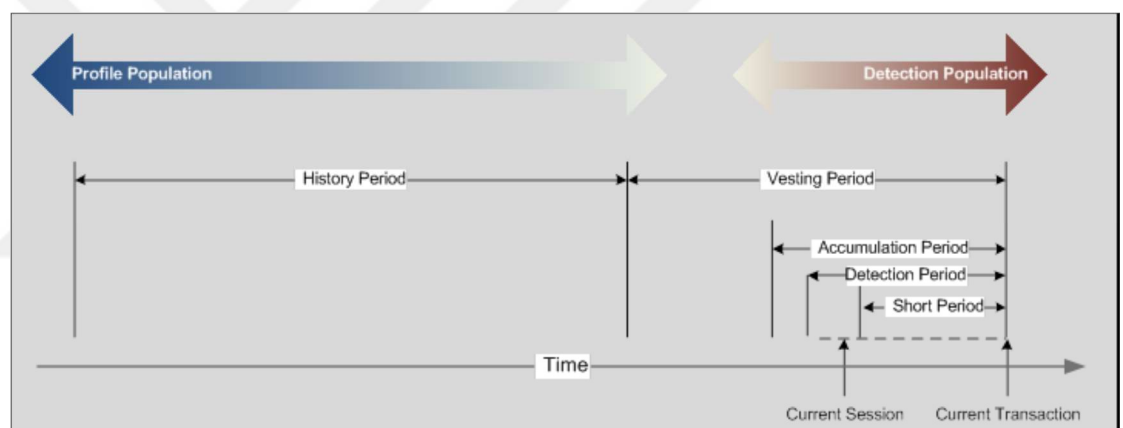
• **Accumulation Period** – The period in which potential fraud could have lately occurred (and may still be occurring). This time period spans between the current transaction time and a specified look back period, typically 5 days back.

• **Short Period** – The time period used by specific key indicators where the impact is calculated over the last few hours of the main entity's activity (typically 2 hours).

• **Detection Period** – The period considered part of the current suspicious fraud and during which detection is performed. By Default, it is set to the last 2 calendar days. This does not have to be the same as the accumulation period, but it cannot be larger than the accumulation period. This is the period that provides a set of all transactions of the main entity and is used primarily for analytics. The corresponding contexts for each transaction risk evaluation by the model are:

- **Profile Population** – The scope of transactions defined for learning an entity's behavioral patterns. An example for this can be: All transactions of the same type as the current transaction, within the History Period.
- **Detection Population** – The scope of transactions used to detect currently occurring fraud (for example, all transactions of the same entity within the accumulation period).

- **Current Session** – The set of transactions included in the party’s current approach to the service. Current session includes all the transactions with the same session ID as the current. For Web, if this field is not available, the session includes all the transactions since the party’s last Session Login transaction. When no Session Login transaction is available in the Accumulation Period, the session includes all the transactions in the Short Period.
- **Current Transaction** – The transaction which triggered the current detection process (See Schema 17).



Schema 17 - *Profiling Periods*

3.2.4.1.2 Structure Of Profiling

The Historical Behavior Profiling core model studies the typical activity pattern of each account and maintains behavior profiles on account activities based on specific transactional data elements, over specified periods of time. They provide the foundation for the detection of unusual activities that may indicate fraud. System checks unusual behavior on historical pattern of customers. Historical pattern is created by profiling that defines usual behavior of customer and helps to distinguish unusual ones. Profiling works used to aggregate statistical information over a period

of time for a certain entity. It creates historical profiles on a periodical basis; daily, weekly, monthly, and quarterly or yearly. It stores sum of amount of transactions, average of amount of transactions, quantity of transactions volume, min, maximum, standard deviation and average amount of this transaction type under a table of a proper database.

Profiling system is also influenced by entity-level historical profiles. For example, a login from a foreign country may appear suspicious in isolation; however, profile information can show a pattern of international travel, reducing the risk of the current transaction. Algorithms are able to combine extremely nuanced or complex sets of indicators, including, looking at historical payees, travel patterns and device usage.

Profiles are created based on historical data that is accumulated over predefined periods and which is retrievable from either transactional data. These profiles are used for evaluating future transactions related to the same entity and deviations from normal behavior patterns.

Profiles that were created based on historical data and updated from previously monitored event data are available to the analytics detection process. The detection process uses these profiles mainly to detect deviations from normal behavior, but can also use them for evaluating current transactions for the same entity.

3.2.4.1.3 Profile Detection Models

Each transaction can be scored by the solution detection analytics based on these key indicators comprising algorithms that evaluate multiple factors. In addition

to scoring, the solution aggregates the transaction data within the profiles, which are used for the evaluation of future transactions related to the same entity

Profiling detection models profile normative customer behavior and then use real-time transaction monitoring and analytics models to detect behavior anomalies indicative of fraud. The basic profile model examples are following:

- **Unusual New Payee Bank**

This key indicator handles situations in which there were transactions of the main entity in the current session to new payee banks (meaning, a financial institution to which the main entity historically never sent payments). In such situations we wish to increase the risk if this activity is considered to be unusual compared to the main entity's normal or expected behavior based on the main entity's historical profile.

- **Unusual New Payee City**

This key indicator checks if the main entity initiated a payment to a new city (meaning, a city to which the main entity historically never sent payments) during the current session, and this activity deviated from expected behavior based on the main entity's historical profile.

- **Unusual New Payee State**

This key indicator checks if the main entity initiated a payment to a new state (meaning, a state to which the main entity historically never sent payments) during the current session, and this activity deviated from expected behavior based on the main entity's historical profile.

- **Unusual No Email Notification**

This key indicator handles situations in which one of the transactions in the current session is initiated with No Email Notification. In such situations we wish to

check the main entity's usual behavior in this aspect (activity with No Email Notification) and increase the risk if such behavior is rare according to the main entity's historical profile.

- **Unusual Transactions to New Foreign Country**

This key indicator is designated to detect situations in which the main entity initiated payments to new payees in foreign countries (meaning, countries to which the main entity historically never sent payments), and this activity deviates from expected behavior based on the main entity's historical profile.

The less frequent this main entity previously (history period) transacted with foreign countries, the higher score this KI should generate. Moreover, the higher the scores the current foreign countries have, the higher the score this KI should generate.

- **Session from New Foreign Country**

This key indicator checks if a non-profiled entity had transactions from new foreign countries during the Vesting Period and specifically during the Accumulation Period. A large number of new foreign countries in a rather short period is abnormal compared to average an entity and may indicate fraudulent behavior, thus the risk is increased.

- **Unusual Activity from New Foreign Country**

This key indicator handles situations in which profiled main entities initiated transactions from new foreign countries during the Accumulation Period. In such situations we wish to increase the risk score since such activity deviates from their usual behavior. However, if the main entity was seen to initiate transactions via

foreign countries in the past, a more moderate risk score can be assigned, according to the number of such countries.

- **Implausible Geo Location**

This key indicator checks if the main entity's current transaction was performed from an unreasonably distant geo-location compared to the geo-location found in another transaction during the Accumulation Period.

Unreasonable geo-location distance is based on the transaction location as calculated from the online sessions

- **Multiple Regions for Non Profiled Party**

This key indicator handles situations in which a non-profiled main entity initiated one or more sessions from multiple new regions (meaning, regions from which the main entity historically never initiated sessions) during the Accumulation Period. In such situations we wish to increase the risk score since such activity is abnormal compared to the average behavior.

- **First Transaction from Aggregator For Party**

This key indicator handles situations in which a profiled main entity initiates a session through an aggregator ISP for the first time during the Accumulation Period. In such situations we need to determine when the first session of this profiled main entity was via an aggregator ISP.

- **Unusual Activity from New Device**

This key indicator handles situations in which a main entity initiates sessions using a New Device during the Accumulation Period. In such situations we wish to increase the risk since this activity deviates from expected behavior based on the main entity's historical profile.

- **Call from New Foreign Country**

This key indicator checks if the non-profiled main entity had sessions from new foreign countries during the Accumulation Period.

When compared to the average, a large number of new foreign countries in a rather short period is abnormal and may indicate fraudulent behavior, thus increased risk.

- **Multiple New Area Codes for Non Profiled**

This key indicator handles situations in which a non-profiled main entity initiated transactions from multiple new area codes during the Accumulation Period. Such situations may indicate fraudulent behavior, thus increased risk.

- **Unusual Activity from Blocked Phone Numbers**

This key indicator handles situations in which profiled main entities initiate transactions from multiple blocked phone numbers during the Accumulation Period. In such situations the risk score would be increased since such activity differs from their usual behavior. However, if the main entity was seen to transact via numerous blocked phone numbers in the past, the risk is increased more moderately.

- **Unusual Activity from Unknown Phone Numbers**

This key indicator handles situations in which profiled main entities initiate transactions from multiple unknown phone numbers during the Accumulation Period. In such situations the risk score would be increased since such activity differs from their usual behavior. However, if the main entity was seen to transact via numerous unknown phone numbers in the past, the risk is increased more moderately.

- **Unusual Activity via Multiple New Area Codes**

This key indicator handles situations in which profiled main entities initiate transactions from multiple new area codes during the Accumulation Period. In such situations the risk score would be increased since such activity differs from their usual behavior. However, if the main entity was seen to transact via numerous distinct area codes in the past, the risk is increased more moderately.

- **Unusual Authentication Method**

This key indicator assigns scores to transactions for profiled main entities in relation to the authentication methods used in calls during the Accumulation Period, where each method is given a score. However, if the main entity was seen to use this authentication method in the past, the risk is increased more moderately.

4. Statistical Analysis

We have a sample of 1042 Bank A's customer accounts, 4215 related transactions with different amounts between the dates 26-12-2017 and 03.01.2019. The bank bought a fraud solution and it started to work between 27th of December 2018 and 3rd of January 2019. Solution generated 2617 alerts which are possible fraudulent activities of these customers. All these transactions were seen as fraudulent just because of the amount of transaction which is equal and higher than 10.000 \$. It means that 2617 transfers out of 3235 have amount over than 10.000 \$. Result says that these 2617 transfers are fraudulent suspicious and need to be investigated.

After the profiling of the customers, system has learned the average transactions amounts of the customers and started to do not evaluate the all customers in just 1 class. Each customer is defined individually by;

- The ratio of transaction amount and transaction average,
- The ratio of spending time on online banking and average spend time

- Transaction week day,
- Transaction type

System now doesn't take only the default threshold for transaction amount and others into consideration anymore. It knows the profiles of each customer and evaluates them regarding that numbers.

At the end of investigations of the compliance officers, 62 alerts out of 2617 were detected as real fraud and were blocked as real time. The result say that 2% of the fraudulent transactions of this sample are real fraud.

The software R was used for statistical computing and graphics. Hierarchical Clustering method was used for clustering transactions by 2.

4.1 Hierarchical Clustering

We will use Hierarchical clustering that is an analyses method that groups similar objects into same groups. At the end, set of clusters are created where each of them are distinct from each other. The objects in same cluster threats almost similar.

In Hierarchical clustering each observation is thought as a separate cluster at the beginning. Then it executes the following until the end.

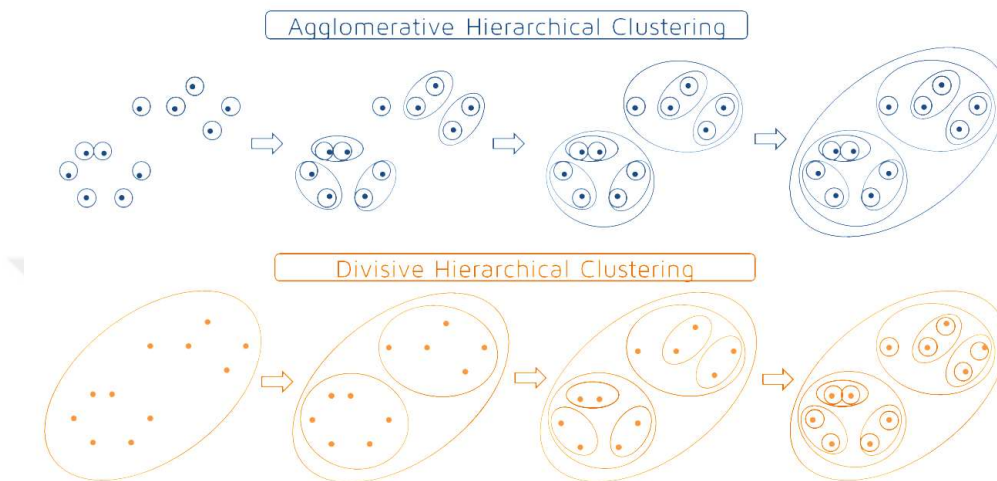
- Identify the two clusters that are similar,
- Merge the two most similar clusters.

There are two main types of hierarchical clustering; Divisive and Agglomerative.

Divisive clustering is clustering type where a single of cluster is divided into similar clusters until there is one cluster for each object. It is totally opposite type of agglomerative clustering type. We used Agglomerative clustering type in that analysis.

4.1.1 Agglomerative Clustering

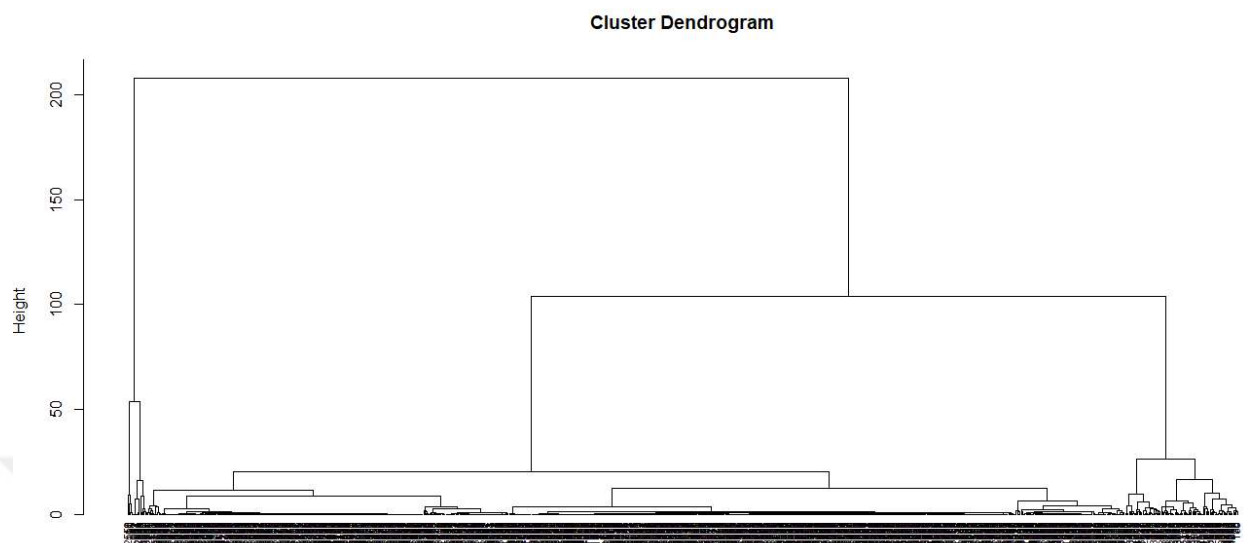
On the contrary of divisive clustering type, agglomerative clustering considers each data as an individual cluster and then combine them each other until all clusters are formed as a single cluster (See Schema 18).



Schema 18 - *Clustering Types* (<https://towardsdatascience.com/https-towardsdatascience-com-hierarchical-clustering-6f3c98c9d0ca>, 2019)

Key operation is the computation of the proximity of two clusters.

A Dendrogram is a tree-like diagram that records the sequences of merges or splits (See Schema 19).

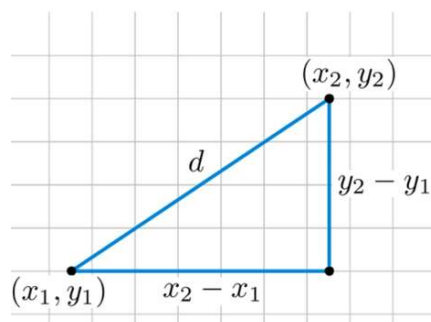


Schema 19 - *Dendrogram*

Euclidean distance calculation while defining the clusters is used at this analysis.

4.1.2 Euclidean distance

The Euclidean distance calculates the length of segment connection two points. It is the most used approach while measuring the distance. The Pythagorean Theorem can be used to calculate the distance between two points. The Euclidean distance between two points is $\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$ (See Schema 20).



Schema 20 - *The Pythagorean Theorem*

Defining the clusters is the matter while calculating the similarity between clusters and combining them. There are different methods while calculating this similarity. MIN, MAX, Group Average, Distance Between Centroids, Ward's Method. Ward's Method is used in that analysis.

4.1.3 Ward's Method

This method works for reducing the sum of squares of distances of each cluster when we merge them. The sum of squares starts from zero and increase when we merge the clusters. This method keeps that sum as small as possible. It is the best method if there is a noise between clusters.

I have divided the data into 2 Clusters for the analysis; fraud suspicious, or not.

Used columns are:

- Transaction_code_sk which represents Remittance, EFT, Swift, Western Union, Credit Card Payment and EFT to Name with codes.
- Ratio_Money which represents the ratio of the amount of transaction and average transaction amount of individual customer
- Ratio_Click which represents the ratio of spending time on online banking and average spend time of individual customer
- Weekday which represents weekdays with codes. (See Schema 21)

	TRANSACTION_CODE_SK	Freq	ratio_money	ratio_click	Day	Week	WeekDay
1	10.816	12	0.0550964200	0.9761905	12	49	2
2	10.827	214	0.3797536000	1.1665413	12	49	2
3	10.741	56	1.7047030000	0.6620690	12	49	2
4	10.766	56	1.3080240000	1.2689655	12	49	2
5	10.826	56	2.8411710000	0.7310345	12	49	2
6	10.711	30	1.3827260000	0.9333333	12	49	2
7	10.800	3	1.0000000000	0.9937500	12	49	2
8	10.827	25	0.9708738000	0.6549232	12	49	2
9	10.691	56	1.7047030000	0.6344828	12	49	2

Schema 21 - *Data Sample*

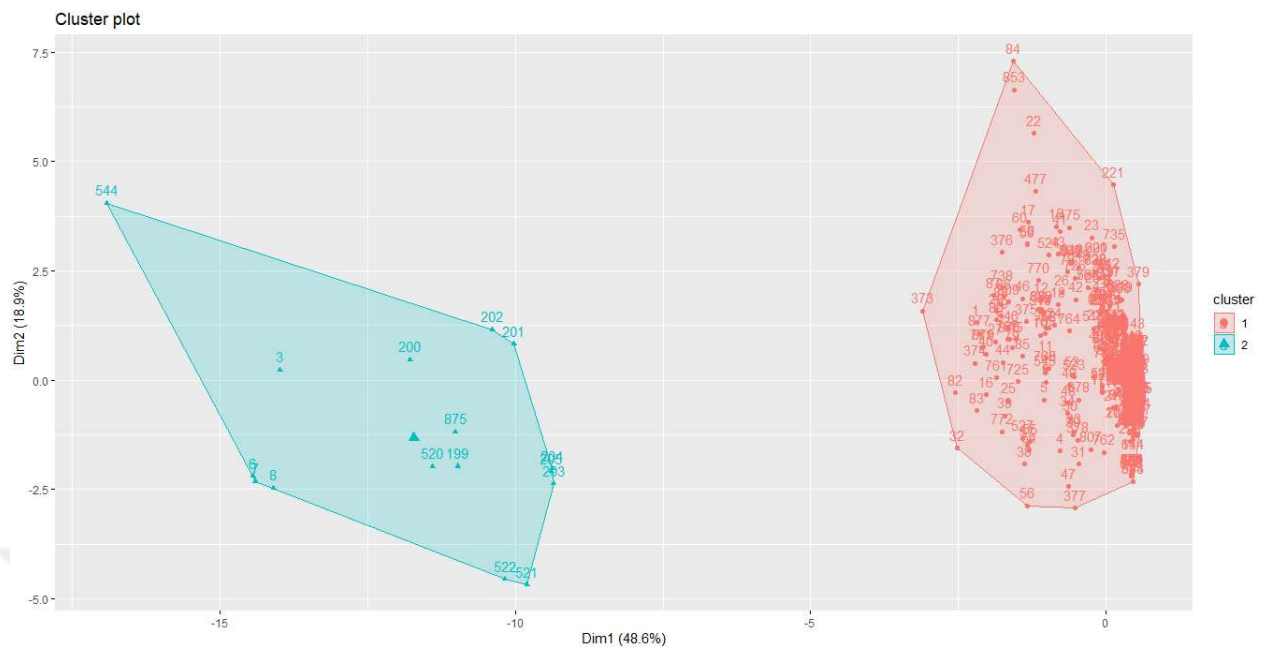
Data frame was grouped base on Transaction_code_sk column and investigated accordingly. The distance between two clusters has been computed based on length of the straight line drawn from one cluster to another. After than hierarchical clustering method is used.

Regarding the first transaction_code_sk (Remittance), there are 894 transactions. Second class (Fraud suspicious) has 16 records where 878 of them belong to the first one (Not suspicious) (See Table 2).

Cluster	N
1	878
2	16

Table 2 - *Cluster Number-Amount 1*

The cluster plot of the clusters is like below (See Schema 22).



Schema 22 - *Cluster Plot 1*

Regarding the second transaction_code_sk (Credit Card Payment), there are 784 transactions. Second class (Fraud suspicious) has 79 records where 705 of them belong to the first one (Not suspicious) (See Table 3).

Cluster	N
1	705
2	79

Table 3 - *Cluster Number-Amount 2*

The cluster plot of the clusters is like below (See Schema 23).



Schema 23 - Cluster Plot 2

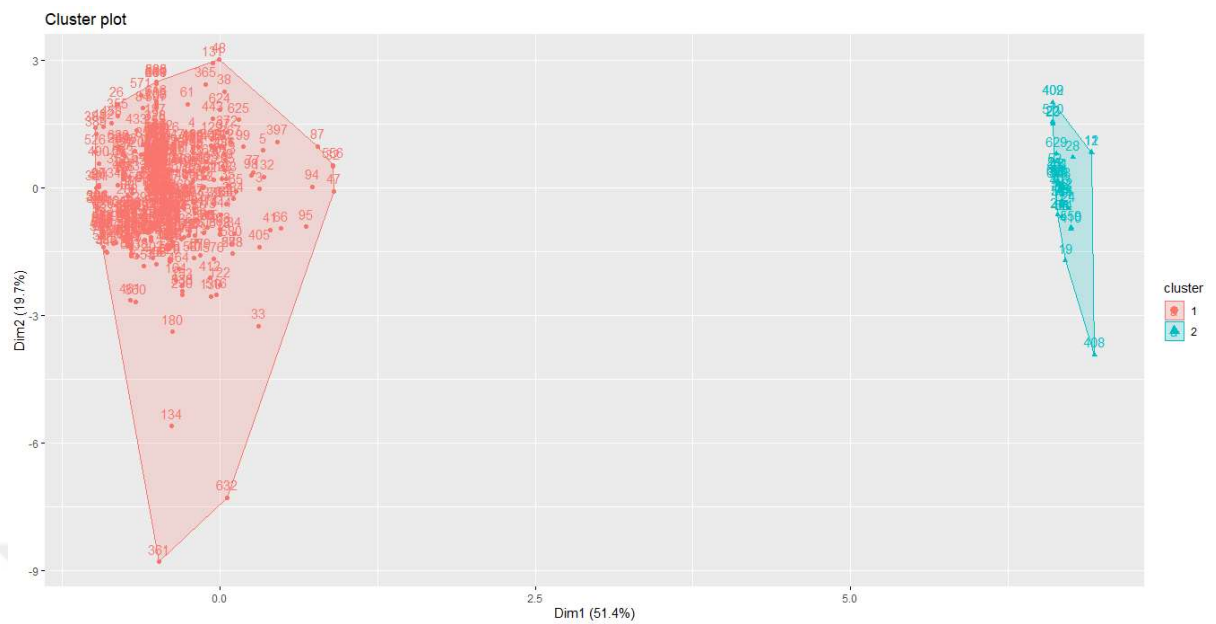
Regarding the third transaction_code_sk (EFT), there are 649 transactions.

Second class (Fraud suspicious) has 41 records where 608 of them belong to the first one (Not suspicious) (See Table 4).

Cluster	N
1	608
2	41

Table 4 - Cluster Number-Amount 3

The cluster plot of the clusters is like below (See Schema 24).



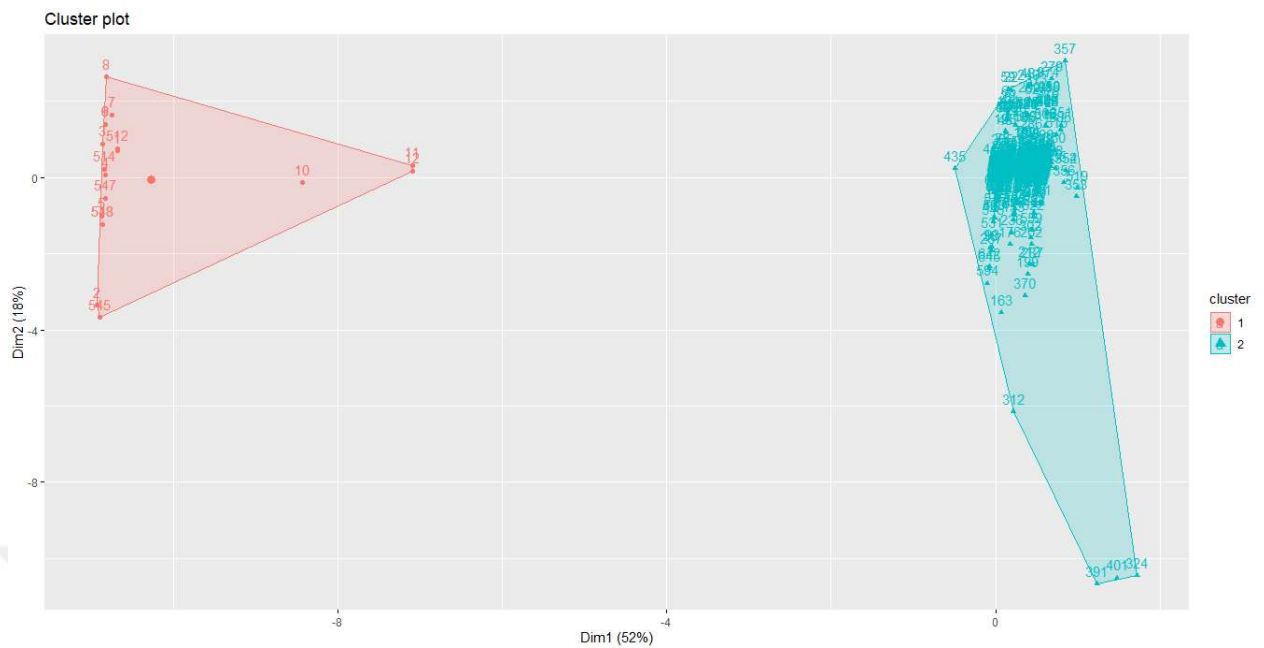
Schema 24 - Cluster Plot 3

Regarding the fourth transaction_code_sk (EFT to Name), there are 648 transactions. First class (Fraud suspicious) has 18 records where 630 of them belong to the second one (Not suspicious) (See Table 5).

Cluster	N
1	18
2	630

Table 5 - Cluster Number-Amount 4

The cluster plot of the clusters is like below (See Schema 25).



Schema 25 - Cluster Plot 4

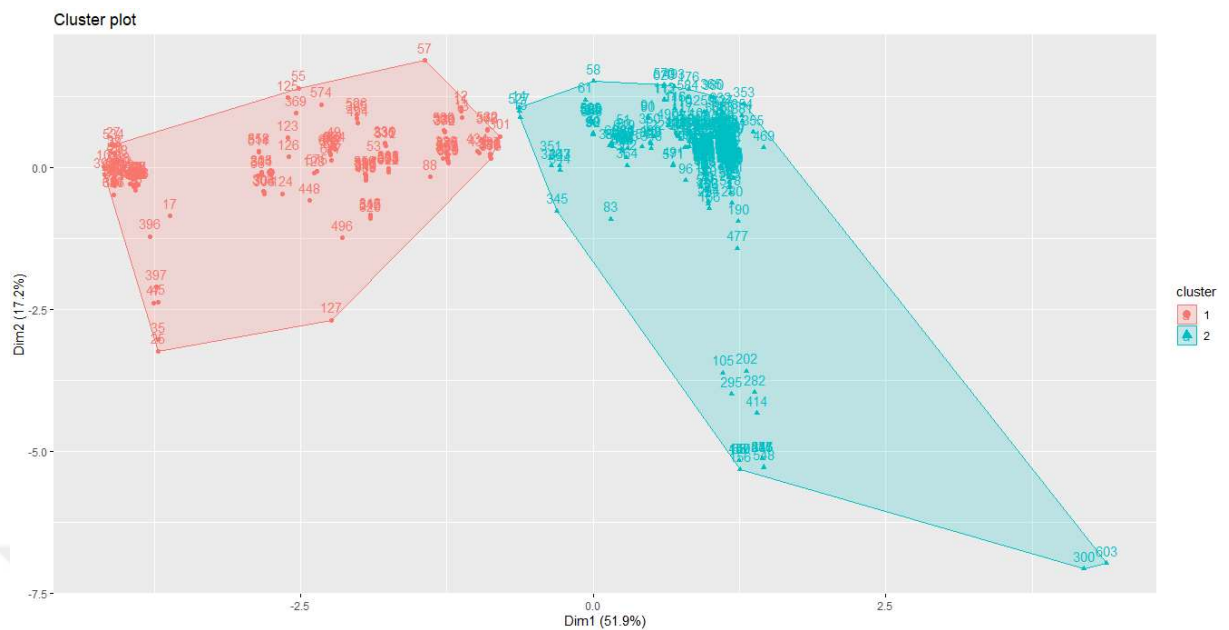
Regarding the fifth transaction_code_sk (WU), there are 632 transactions.

First class (Fraud suspicious) has 163 records where 469 of them belong to the second one (Not suspicious) (See Table 6).

Cluster	N
1	163
2	469

Table 6 - Cluster Number-Amount 5

The cluster plot of the clusters is like below (See Schema 26).



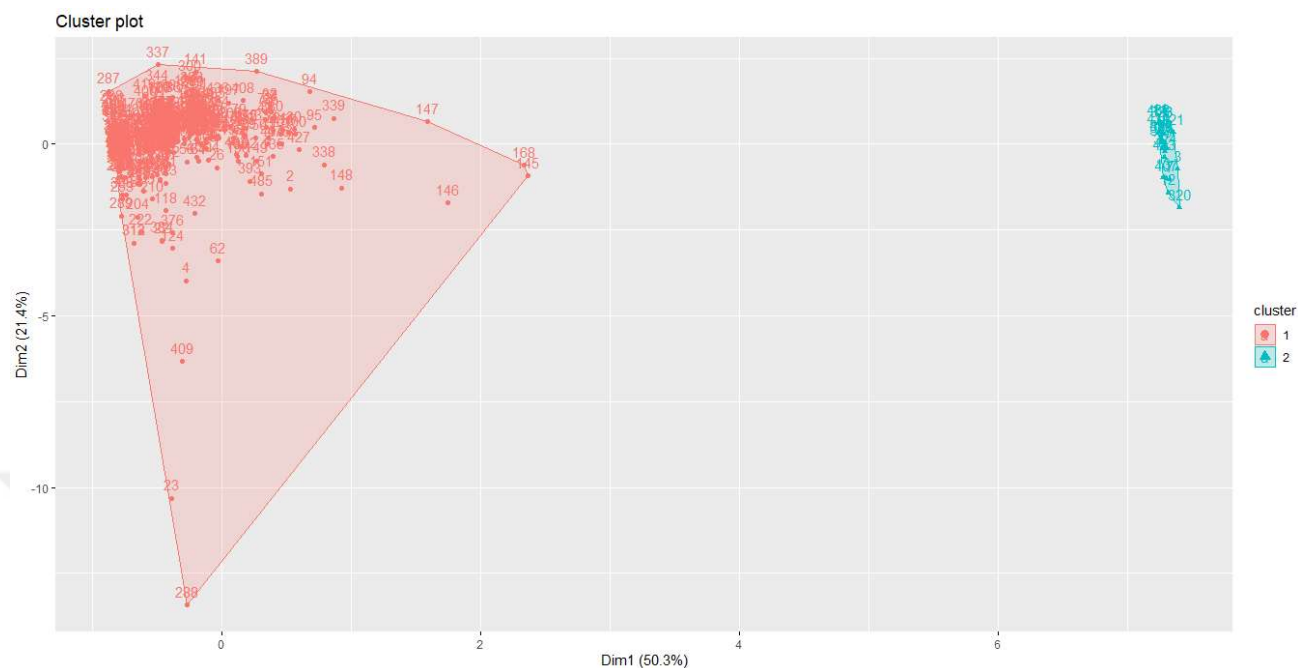
Schema 26 - *Cluster Plot 5*

Regarding the sixth transaction_code_sk (Swift), there are 490 transactions. Second class (Fraud suspicious) has 25 records where 465 of them belong to the first one (Not suspicious) (See Table 7).

Cluster	N
1	465
2	25

Table 7 - *Cluster Number-Amount 6*

The cluster plot of the clusters is like below (See Schema 27)



Schema 27 - Cluster Plot 6

5. CONCLUSION

As a conclusion, “Since the beginning of the invention of internet cybercrime has become one of the most important issue for the cyber world. Branch banking channel distinguishes itself from remote banking channel by face-to-face interaction. The reason branch officer manually matches identity card and person, criminal people mostly use to remote banking channels. Fraud has taken the biggest share of the cake and all focused on it. To establish a better relationship with customers, banks constantly seek ways of differentiating their offerings and developing more appropriate services for distinct market segments” (Hsieh, 2004, p.626). Banks use internal detection and prevention systems as well as external ones.

Fraud catching is a real time work and has to be finalized as soon as possible. Compliance officers are in limited numbers in banks and each officer is limited to

handle specific numbers of alerts. They have to investigate alerts faster than normal speed to handle more alerts which can cause missing the real fraud. Missing fraud doesn't only mean losing money, it also means losing confidence of customers for financial institutions. An important observation on the current state-of-the-art segmentation analysis is the use of past transaction data (Hsieh, 2004, p.626). That is the reason profiling is a key factor while decreasing the number of alerts and increasing the quality of true-positive numbers. In our statistical analysis customers' transactions were compared by their own;

- Executed transaction's codes,
- The ratio of the amount of transaction and average transaction amount of individual customer,
- The ratio of spending time on online banking and average spend time of individual customer and
- Weekday of the transactions executed

We have seen that customers' behaviors' are well classified by the above 4 factors and detected anomalies perfectly. That classification helped to system to create profile of each individual customers. There is a reality that a high value for a customer can be extremely low for another customer and vice versa. As a result, anomalies were extracted from the usual transactions and alerted in acceptable numbers.

If the bank used to profiling technique while creating alerts, they wouldn't have to investigate 2617 alerts. By the help of that technique fraud suspicious alerts number decreased to 342 (around 87% decrease) by sum of clusters which are fraud suspicious. Specialists mostly investigates the cases and creating rules once they are

perpetrated. On the other hand, fraudsters learn the rules and techniques of the banks use and evolve themselves to use different techniques. That weakness of systems makes banks vulnerable against fraudsters. The only way to overcome this issue is being proactive and detecting suspicious acts of people individually in order to stop frauds. Why do we follow the rules while fraudsters do not?

6. LIMITATIONS & FUTURE WORK

I have seen that there are not plenty but enough amount of thesis about the fraud detection. Some of them are about telecommunication, finances, insurance and less of them are about banking environment. Generally, these thesis are just about card fraud detection in online banking. Some thesis struggled with data mining numbers a lot and some struggled on banking terms. There is a thesis which is about putting accounts into groups and evaluates them within those groups. That is the main reason that I was not able to consult to the previous thesis directly about my subject. My thesis is not based on just card fraud, is also be based on other activities of accounts on online banking. It looks for history of account by account to check whether there is any unusual activity or not. It can be calculated as account based or group based.

In the analysis, I have used the limited details of transactions such as transaction type, transaction amount, execution click time, executed week day. For the future researches, it can be used many different details for profiling such as citizenship country, mouse click movements anomaly, geographical location, authentication method of customers. The names of customers can be matched with political exposure people list and black lists which extremely increases the probability

of being fraudster. Moreover, I was able to collect limited amount of customer and transactions. More data can be collected for more specific results.



REFERENCES

- Aydin, E.D. (1992). *Bilişim Suçları ve Hukukuna Giriş*. Türkiye
- Beal, V. (2016). ENIAC - First Computer in the Unites States.
<http://www.webopedia.com/TERM/E/ENIAC.html> (4 September 2019).
- Bolton, R.J and David J. H. (2002). *Statistical Fraud Detection: A Review*.
 Vol. 17, No. 3, 235–255.
- Bozkurt, S. (2013). Bilgisayarın İcadı Ve Tarihi Gelişim Süreci.
<http://www.teknokoliker.com/2013/06/bilgisayar-icadi-gelisim-sureci.html> (7 August 2019).
- Cahill, M.H, D. Lambert, J. C. Pinheiro. (2000), Detecting Fraud in the Real World.1-18.
- Chakrabarty, K.C. (2013). *Fraud in Bank Sector*, K C Chakraborty: Fraud in the banking sector – causes, concerns and cures.1-13.
- Chen, J. (2019). Mobile Banking.
<https://www.investopedia.com/terms/m/mobile-banking.asp> (4 September 2019).
- Cross Domain Solutions. (2019). <http://www.crossdomainsolutions.com/cyber-crime/>. (23 September 2019)
- Cyber Security and Cyber Laws. (2019).
<https://cyberlawsinindia.wordpress.com/cyber-crimes/>. (23 September 2019)
- Frankenfield, J. (2019). Online Banking.
<https://www.investopedia.com/terms/o/onlinebanking.asp> (4 September 2019).
- Jans, M., N. Lybaert and K. Vanhoof. (2007). internal fraud risk reduction: Results of a data mining case study.17-41.
- Hassibi PhD, K. (2000). Detecting Payment Card Fraud with Neural Networks.141-158.
- Hsieh, N.C. (2004), an integrated data mining and behavioral scoring model for analyzing bank customers. 623-633.
- Kemp, S. (2019). The global State of Digital in October 2019,
<https://wearesocial.com/uk/blog/2019/10/the-global-state-of-digital-in-october-2019> (2 November 2019).
- Kovach, S. and W. V. Ruggiero. (2011). Online Banking Fraud Detection Based on Local and Global Behavior. 166-171.
- KPMG. (2013). Global profiles of the fraudster. Holland.
- National crime prevention council. (2012). Cybercrimes. USA
- Rygielski, C., J.Wang and D.C. Yen (2002). Data mining techniques for customer relationship management.483-502.

Sanusi, Z.M., M. N. F. Rameli and Y. M. Isa. (2015). Fraud Schemes in the Banking Institutions: Prevention Measures to Avoid Severe Financial Loss.107-113.

Semule, H. (2017). App Development.
<https://medium.com/testfbpublication/a-web-service-is-a-service-offered-by-an-electronic-device-to-another-electronic-device-337aab00bf25> (17 September 2019).

Singh, H. (2019). What is Money Laundering and how is it done,
<https://www.jagranjosh.com/general-knowledge/meaning-of-money-laundering-1549620151-1> (17 September 2019).

Zadeh, R.B.K, A. Faraahi and A. Mastali. (2011), Profiling bank customers behaviour using cluster analysis for profitability.458-467.

