THE ROLE OF DATA IN THE FIGHT AGAINST PAYMENT FRAUD

A qualitative research of payment fraud prevention in the 2020 century

Lappeenrannan–Lahden teknillinen yliopisto LUT

Bachelor’s Programme in Business Administration, Bachelor’s thesis

2023

Iida Ahola

Examiner: Post-doc Researcher, Jyrki Savolainen

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

LUT Business School

Business Administration

Iida Ahola

The role of data in the fight against payment fraud

A qualitative research of payment fraud prevention in the 2020 century

Bachelor's thesis

2023

38 pages, 3 figures, and 1 appendix

Examiner: Post-doc Researcher Jyrki Savolainen

Keywords: payment fraud prevention, machine learning, data, analytics

This bachelor's thesis focuses on investigating the role of data in payment fraud prevention and discovering the most common machine learning (ML) models for payment fraud detection. The empirical evidence presented in the research was collected through qualitative semi-structured interviews gathered from three (3) people working in fraud prevention in different financial institutions. The empirical research is backed by a theoretical framework, which has been built based on previous literature.

The results show that data plays a significant role in automating payment fraud prevention effectively. The interviews and theoretical framework indicate that supervised ML models are more common in payment fraud prevention than unsupervised models. Supervised ML models can learn to recognize fraud from customers' payment behavior profiles, which can be built based on their previous transactions. For accurate ML models, high-quality training data is needed. Results also show that continuous work on models' performance and the quality of data is required to keep up with the changes in the payment environment. The results of this thesis coincide with the previous literature about the crucial data and most common ML models.

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUT-kauppakorkeakoulu

Kauppatieteet

Iida Ahola

Datan rooli taistelussa maksuvälinepetosta vastaan

Kvalitatiivinen tutkimus maksuvälinepetoksen ehkäisemisestä 2020-luvulla

Kauppatieteiden kandidaatintyö

2023

38 sivua, 3 kuvaa ja 1 liite

Tarkastaja: Tutkijatohtori Jyrki Savolainen

Avainsanat: maksuvälinepetoksen estäminen, koneoppiminen, data, analytiikka

Tämä kandidaatintutkielma keskittyy tutkimaan datan roolia maksuvälinepetosten ehkäisemisessä ja selvittämään käytetyimmät koneoppimismallit maksuvälinepetosten tunnistamisessa. Empiirinen todistusaineisto on kerätty kvalitatiivisin puolistrukturoiduin haastatteluin, joiden kohteena olivat kolme (3) petoksenehkäisemisen parissa työskentelevää ihmistä eri rahoitusalan yhtiöistä. Empiirisen tutkimuksen pohjana on teoreettinen viitekehys, joka on luotu aikaisemman kirjallisuuden pohjalta.

Tulokset viittaavat, että datalla on suuri rooli maksuvälinepetosten ehkäisemisen automatisoinnissa tehokkaasti. Tulokset viittaavat, että ohjatut koneoppimismallit ovat ohjaamattomia malleja suositumpia maksuvälinepetosten ehkäisemisessä. Ohjattujen koneoppimismallien avulla voidaan tunnistaa tehokkaasti petoksia hyödyntäen asiakkaiden maksukäyttäytymisprofiilieja, jotka perustuvat asiakkaiden aikaisempiin maksuihin. Tarkkoihin koneoppimismalleihin tarvitaan korkealaatuista opetusdataa. Tulokset osoittavat myös, että jatkuva mallien suorituskyvystä huolehtiminen ja datan laadun ylläpitäminen on tarpeellista muuttuvassa maksuympäristössä. Tutkielman tulokset ovat yhtenäiset aikaisemman maksuvälinepetosta ja tehokkaita petoksen tunnistamiseen käytettäviä koneoppimismalleja käsittelevän kirjallisuuden kanssa.

ABBREVIATIONS

CNP	Card-not-present
CP	Card present
GDPR	General Data Protection Regulation
KYC	Know your customer
ML	Machine learning
PSD2	Revised Payment Services Directive

Table of contents

Appendices

Figures

1. INTRODUCTION

According to International Criminal Police Organization (Interpol, 2022), online and electronic means of payment have opened new opportunities for criminals to commit payment fraud. Banks and other financial institutions need to readjust their operations and invent alternative practices to recognize and prevent payment fraud as the ways to commit crime change alongside the banking and payment environment. Payment frauds are divided into more traditional card-present frauds (CP) and the now-growing card-not-present frauds (CNP), where a victim holds possession of their payment card while the criminal can make purchases with the card's details to gain financial benefit (Europol 2022).

Traditionally financial crime and fraud detection has been based on rules and static thresholds to recognize suspicious transactions. However, these rule-based manual techniques have become ineffective due to transforming payment landscapes, crime topologies, and characteristics (Kurshan and Shen. 2020). Financial institutions must adapt to changing consumer behavior and criminal activity during the ever-growing digitalization. This thesis studies the role of data and analytics in effective payment fraud recognition and prevention.

1.1 Background

In 2021, 76 percent of adults globally had an account at a bank or other regulated institution compared to 2011's 51 percent, which emerges from World Bank's Findex 2021 research. Online transactions are one of the easiest ways to transfer money between accounts as they can be performed from anywhere with the help of a suitable device, internet, and card or credentials (Khattri and Singh 2018). The data collected in the World Bank’s Findex 2021 research indicates that the COVID-19 pandemic played a role in accelerating the adaption of digital payments, with two-thirds of adults worldwide now making and receiving digital payments.

While the e-commerce industry grows and tools to steal credit card details become more available, the ways to commit fraud also change. According to Karpoff (2021), the COVID-19 pandemic has shaped the markets in a way that will likely increase the incidence of fraud over the next couple of years. During the first four months of the COVID-19 pandemic, uncertainty and fears led to confusion over creditable information, and cyber criminals were there to “help” (Kikerpill and Siibak 2021). This is a prime example of criminals following the changes happening in their victims’ lives to choose the best communication mediums and persuasion tactics. Criminals take advantage of social context and impersonation to gain their victim's trust and make their scams more credible. European Association for Secure Transactions (2022) defines social engineering as psychologically manipulating someone to perform actions or divulge confidential information. To answer these new social engineering schemes, Khattri and Singh (2018) suggest more sophisticated online fraud transaction detection and prevention systems based on various parameters to understand not only static facts but also customers’ behavioral patterns.

Truong, Diep, and Zelinka (2020) think that traditional manual ways of detecting payment fraud are becoming too slow, expensive, and inefficient as the amount of online payment data increases and criminals adapt new techniques to increase the speed and scale of their attacks. They believe that automation helps relocate human resources to the functions where they are most needed. Machine learning (ML), according to Truong et al. (2020), utilizes data to learn and improve itself without explicitly being programmed. Yousefi, Alaghband, and Garibay (2019) divide ML techniques into supervised and unsupervised ones, depending on how much human help they need in their decision-making. They believe that both models can be used for payment fraud detection.

As Chilaka, Chukwudebe, and Bashiru (2019) point out, ML algorithms should continuously improve as fraudsters become more innovative, or the algorithm's performance will eventually fail to meet the designed objectives. These continuous changes in the ways to commit fraud demand continuous research on how to keep detecting and preventing them. Despite various sources stating that the COVID-19 pandemic has severely shaped our consuming habits and ways of payment, there is not much research in the context of payment fraud since the pandemic started in 2020.

1.2 Research objectives & structure

This research investigates the role of data in the payment fraud scene. Data and automation are necessary to keep payment fraud detection effective and efficient. ML models are based on data, and while digitalization keeps thriving, the amounts of data are increasing, which makes it more critical than ever to recognize the crucial data. Besides recognizing the data needed, it is essential to know how to utilize it. The research questions of this thesis are:

Q1: Which data are used to recognize payment fraud and how?

Q2: How can payment fraud be prevented using data, and which are the most applied ML models for payment fraud prevention?

The main objective of this study is to review previous literature on how and why payment fraud prevention should be automated in the 2020 decade. The second research objective is to investigate how payment fraud prevention is organized in financial institutions in the 2020 decade based on empirical research. The final research objective is to think about the challenges in automated payment fraud prevention and what possible future scenarios might lay ahead. All research objectives are supported by the research questions and look at the role of data and analytics in payment fraud prevention, investigating it from different perspectives.

The thesis structure includes theoretical and empirical parts that aim to answer the research questions. The first research question focuses more on the data itself, especially which data is significant in payment fraud recognition. The second research question goes more deeply into the "how" part of question one specifying the most applied ML models, how they are divided into supervised and unsupervised models, what is the base idea behind these methods, and how they help prevent payment fraud.

The theoretical framework views previous literature on the topic and addresses both research questions. Based on previous literature, six supervised and three unsupervised commonly applied ML methods are introduced. In the empirical part, qualitative research is conducted through interviews. Finally, the results of the research are presented, and theoretical and empirical parts are discussed to answer research questions and fulfill set research objectives.

2. THEORETICAL FRAMEWORK

This theoretical framework introduces previous literature on detecting and preventing payment fraud and how the role of data is becoming more critical in this field, creating a basis for the later conducted empirical research. First, the current situation in payment fraud detection is presented, and the process of card-not-present fraud is introduced, starting from means to gain victims' personal information leading to the role of card issuers. Second, the role of data is reviewed, including what kind of data can be utilized and how to recognize and prevent payment fraud. Then, most applied ML methods for payment fraud prevention are introduced, leading to the observation of these methods' advantages and disadvantages.

2.1 Current situation in payment fraud detection

Fraud is expensive for individuals and societies, and the exact costs are difficult to calculate as there are expenses linked to investigating fraud, maintaining operations, and helping the victims that are not included in the official losses. Based on the Nilson Report (2021), in 2020, card issuers and acquirers of ATM and merchant transactions lost $28,58 billion to fraud, out of which 68% was CNP fraud. Furthermore, dollars lost to CNP fraud in 2020 were more than six times higher than in 2019, when the difference to the previous year had already increased four times. The same report shows that the COVID-19 pandemic contributed to the rising trend of card-not-present sales and therefore rising losses to fraud. According to Europol (2022), another reason contributing to the growth in CNP fraud is the effectiveness of measures against the more traditional card-present fraud.

CNP fraud requires that the criminal has a hold of the victim’s credentials or other types of personal information. There are various ways to disclose victims’ private information. Usually, several types of scams are utilized simultaneously to create a sophisticated plot to lure a victim in and gain their trust. According to EAST (2022), social engineering attacks on consumers usually aim to obtain personally identifiable information, which can be used to commit payment fraud or sold on the dark web. The Nilson report (2021) exposed that takeover of legitimate accounts by criminals buying valid credentials on the dark web steadily worsened in 2020. Interpol (2022) stresses that international cooperation is essential in investigating and solving payment fraud, as data can be sold abroad on the dark web.

The FBI lists spoofing and phishing, romance scams, and ransomware as some of their most encountered scams and crimes. Spoofing is a plot where someone convinces the victim that they are interacting with a trusted source by slightly changing an email address, sender's name, phone number, or other information. Phishing is the act of criminals aiming for the victim to disclose their private information, download malicious content, such as ransomware, or send money through spoofing methods that can happen through emails, phone calls, or SMS messages. Ransomware is malicious software that prevents the victim from accessing their computer files, networks, or systems, returning them in exchange for a ransom. In a romance scam, the criminal adopts a fake online identity to gain the victim's trust and affection, creating an illusion of a romantic relationship to manipulate and steal from the victim. (FBI 2022 a, b, c, d)

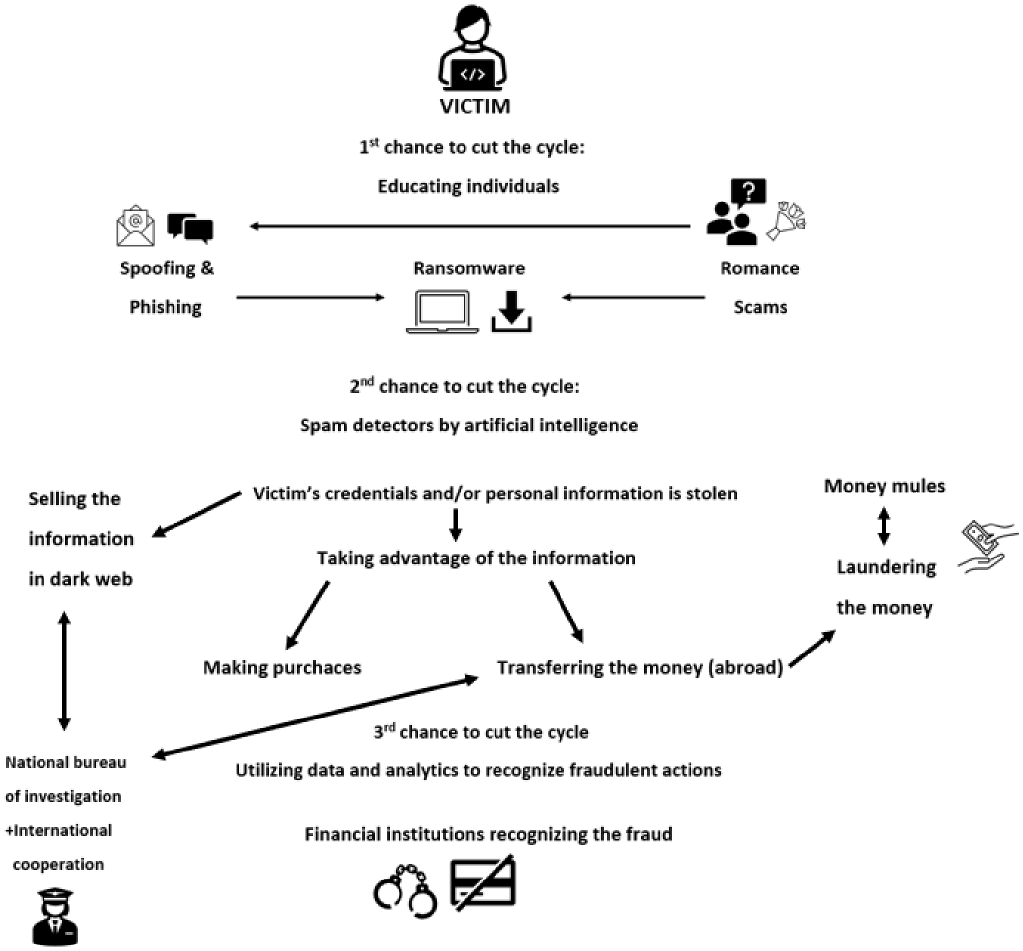
VICTIM
1st chance to cut the cycle:
Educating individuals
Spoofing &
Phishing
Ransomware
Romance
Scams
2nd chance to cut the cycle:
Spam detectors by artificial intelligence
Selling the
information
in dark web
Victim's credentials and/or personal information is stolen
Money mules
Taking advantage of the information
Laundering
the money
Making purchaces
Transferring the money (abroad)
3rd chance to cut the cycle
Utilizing data and analytics to recognize fraudulent actions
National bureau
of investigation
+International
cooperation
Financial institutions recognizing the fraud

Figure 1. Progression of payment fraud

Disclosing a victim's private information usually starts by contacting the victim, for example, by spoofing. Recognizing the threat is essential for cutting the progression of payment fraud in its early stages, as shown in figure 1. Chiew, Yong, and Tan (2018) view relying on user education to prevent phishing as highly insufficient. As a solution, Gangavarapu, Jaidhar, and Chanduka (2020) suggest more dependable unsolicited bulk email filters against phishing and spam, which have become a severe security threat globally due to simplicity in communication. As figure 1 shows, this is the second chance to stop the progression of payment fraud before it has happened. However, if the receiver falls victim to phishing, recognition and prevention of the fraud are on the financial institutions.

The Nilson Report (2021) found that when COVID-19 hit, card issuers were unprepared for the massive increase in CNP transactions, and their fraud risk models were not ready to handle the increased number of first-time CNP authorization requests from valid cardholders. This made benefitting from previously stolen cards easy. The same research established that in 2020, merchants continued to manually review questionable CNP sales, which is both time-consuming and expensive. Truong et al. (2020) see that automation of detecting and responding to threats reduces the work of network security experts, allowing them to focus on new situations instead of consuming time on analyzing common threats. Utilizing data and analytics to recognize fraudulent actions is presented as the third chance to cut the cycle of payment fraud progression in figure 1.

2.2 Data-based recognition of payment fraud

Truong et al. (2020) believe that ML can make payment fraud detection more flexible and adaptable, detecting threats in real-time thanks to its capability to analyze large amounts of data effectively, accurately, and fast. Typically, ML models used in payment fraud recognition utilize an outlier/anomaly detection method, because it is based on finding exceptions from normal behavior. The challenge is recognizing the outlier transactions, which requires defining normal by behavioral profiling cardholders.

Wickramanayake, Geeganage, Ouyang, and Xu (2020) suggest that studying data from past transaction behavior, such as payment frequency and sizes of payments, is an effective way to recognize a legitimate cardholder. They reason that in the short term, legitimate cardholders usually have constant income guiding their spending. The cardholders' different merchants and payment methods offer additional information to define "normal cases." However, they admit that lots of information can be lost due to cardholders using different merchants and payment gateways. Ryman-Tubb, Krause, and Garn (2018) have made the same observation regarding the limited available data to merchants and card issuers separately. Both pieces of research show that merchants' data is limited to transactions occurring at their firm, and card issuers' data is limited to transactions done on their issued cards.

Assessing new fraud detection methods is complex because of the sensitive nature of transaction data. Especially in Europe, the European Union (EU) binds all organizations operating in Europe or with Europeans to follow the EU legislation. The General Data Protection Regulation (GDPR) was put into effect in 2018, and according to European Council (2023), it is “the strongest privacy and security law in the world,” imposing obligations to all organizations across the globe targeting or collecting data related to people in the EU. Another legislation that plays a role in payment fraud prevention is the PSD2 legislation, which according to the European Payments Council (2023), was an answer to the progression of the European economy’s digitalization and new players in the online payments field aiming to reduce the risk of fraud for electronic transactions.

Ryman-Tubb et al. (2018) and Wickramanayake et al. (2020) acknowledge the confidentiality and sensitive nature of data related to payment fraud. Demographic data could be utilized to build an even more detailed profile of the legitimate cardholder adding value to the behavioral profile, but said data is highly confidential. Without real-world transaction data, it is difficult to build models that would work in real-world situations, especially when considering genuine and fraudulent behavior profiles changing over time.

2.3 Machine learning methods for payment fraud detection and prevention

As previously mentioned, ML techniques can be divided into supervised and unsupervised techniques, which can both be used for credit card fraud detection. Reazpour (2019) explains that in supervised methods, a model is trained based on a labeled training dataset divided into classes fraudulent and legitimate. Based on the training, the model can classify new transactions and point out the fraudulent ones. However, they acknowledge that if fraudsters change their patterns to something not classified in the training data, the model cannot label it based on the old observations. In addition to fraudsters changing their patterns, Carcillo, Le Borgne, Caelen, Kessaci, Oblé, and Bontempi (2021) point out that changing customer behavior can also confuse supervised algorithms. These changes can happen, for example, during the holiday season, while traveling, or due to an unexpected change in living situation.

Mehndiratta and Gupta (2019) explain that unsupervised methods do not need training sets with previously labeled data to detect anomalies. Instead, the method sorts data based on patterns, differences, and similarities identifying hidden structures. Yousefi et al. (2019) agree that unsupervised methods' capability to function without training sets makes them an excellent tool for detecting previously unseen types of fraud or applications without prior knowledge.

2.3.1 Supervised algorithms

The most often mentioned supervised ML methods in the previous literature are logistic regression, decision tree, random forest, naïve Bayes, mk-nearest neighbor, and support vector machine (Gamini et al. 2021, Bhanusri et al. 2020, Khatri et al. 2020, Niu et al. 2019, Yousefi et al. 2019). Logistic regression gives a specific percentage indicating the probability of a given outcome as a predictor increases or decreases (Niu et al. 2019). The method is mainly used when there is a chance that a binary classification issue occurs (Khatri et al. 2020). A decision tree utilizes a top-down approach where a root node creates binary splits until specific criteria are met, providing predicted values based on the interior nodes leading to final data. It tends to overfit training data leading to poor performance on previously unseen data. Random forest combines randomized decision trees, making it a versatile method able to be applied to large-scale problems. (Niu et al. 2019) Each tree makes a class prediction, and the class with the most votes becomes the model's prediction. The output is a class selected by most trees. (Gamini et al. 2021) Naïve Bayes calculates the probability of a sample belonging to a particular category (Bhanusri et al. 2020). It can predict multiple classes at once (Khatri et al. 2020). K-nearest neighbor forms a majority vote between the k most similar instances to a given unseen observation defining similarity according to a distance metric between two data points (Niu et al. 2019). Support vector machine creates an optimal boundary between output options (Gamini et al. 2021).

2.3.2 Unsupervised algorithms

Unsupervised ML techniques appear less in the literature related to the topic of this research. Repeatedly mentioned methods include k-means clustering, one class support vector machine, and autoencoder network (Gamini et al. 2021, Niu et al. 2019, Rezapour 2019, Yousefi et al. 2019). K-means clustering divides an unlabeled dataset into k clusters so that each dataset belongs to only one group (Gamini et al. 2021). Although they are simple and easy to implement, they are sensitive to the initial cluster centers making them vulnerable to outliers, which is relevant in the fraud detection context. The parameters and metrics to measure should be chosen appropriately, requiring input from domain experts. (Yousefi et al. 2019) One-class support vector machine is helpful for imbalanced datasets with many cases of regular data and not many cases of outliers (Rezapour 2019). It learns a soft boundary to embrace the regular data instances and learns to identify the abnormalities (Niu et al. 2019). The problem with a one-class support vector machine is its high false positive rate. An Autoencoder network is a branch of neural networks that can be used to learn data in an unsupervised manner. (Rezapour 2019) It learns to map from input to output through a pair of encoding and decoding phases (Niu et al. 2019).

2.3.3 Comparing different machine learning methods

Both supervised and unsupervised techniques have their advantages and disadvantages. Whereas Yousefi et al. (2020) suggest that unsupervised approaches' ability to detect previously unseen types of fraud makes them more potent than supervised approaches, Mehndiratta and Gupta (2019) argue that the unsupervised learning approach is less efficient than the supervised learning approach. Gamini et al. (2021) point out that hybrid models incorporating both supervised and unsupervised ML might be more accurate than either of the methods alone. Because supervised methods learn from past behavior and unsupervised methods detect new types of fraud, they complement each other, especially in the areas lacking in the other method.

Some research has been done to find the best model for payment fraud detection. Finding one best model is impossible because researchers use different criteria when comparing the methods, and usually, different methods do well in different areas. Khatri et al. (2020) have compared different ML methods using sensitivity, precision, and time as their criteria for comparison. Another research (Gamini et al. 2021) used criteria: accuracy, precision, recall, FI score, and specificity. Both papers focused on how well the machine could identify fraudulent actions by measuring the ratio of correctly positively labeled to all positively labeled. Khatri et al. (2020) primarily focused on true positives and how fast the machine could perform. In contrast, Gamini et al. (2021) had more criteria and considered false positives and false negatives by taking the weighted average of both. They also compared the machines based on their true negative rate. Another challenge in comparing the methods is the previously mentioned lack of real-life data in training sets, leading to uncertainty that a method working in a test environment would work in real-life practice.

2.4 Challenges in modern fraud detection methods

As the amount of data grows, outlier detection and ML techniques struggle to build accurate models, and the chance of triggering false alarms grows (Abbassi, El Alaoui & Gahi 2022). False positive is a type of false alarm. It is a transaction that is labeled as fraud but is legitimate. Wallny (2022) thinks that COVID-19 made false positives an even bigger problem making them possibly more expensive than fraud itself because of hidden costs and losing face through the embarrassment of customers, lost revenue of merchants, and administrative costs for card issuers. This is supported by J.P. Morgan’s article (2022) claiming that while actual fraud losses represent an estimated seven percent of the total cost of fraud, false positive losses amount to 19 percent. False positives also affect the accountability of outlier detection and ML tools created to recognize payment fraud.

Another big problem is the class imbalance in data that detects payment fraud. Fraud is relatively rare, and it is not uncommon to find only one fraudulent transaction in 10 000 transactions. These imbalanced data sets, where the distribution of classes is unequal, create challenges for ML techniques used for fraud prevention. Unfortunately, many methods used to predict minority classes in imbalanced data sets accelerate the problem of false positives. (Larson 2020)

3. METHODOLOGY

This research was conducted using qualitative methods to better understand payment fraud prevention in theory and practice. Because the payment fraud environment changes so rapidly, interviews offer current information that the theoretical framework might not be able to provide yet. The COVID-19 pandemic shaped the payment markets and methods, but only a little research has been done on the topic of this thesis since the pandemic started in 2020. Qualitative research supports the research objectives of this thesis, investigating how payment fraud prevention is organized, which challenges are faced, and what the future might look like. Qualitative research can also affirm if the methods mentioned in the literature are genuinely applied in real life.

Empirical research was conducted using semi-structured interview due to its flexibility and ability to address specific research questions simultaneously leaving space for new meanings related to the topic of the study. According to Galletta and Cross (2013), a key benefit of semi-structured interviews is its division between attention to lived experiences and theoretically driven variables of interest creating space for the researcher to ask for clarification if needed. The research and analysis are compared against a framework of pre-existing theories. The theoretical framework of this thesis and the data gathered from the semi-structured interviews were formed and analyzed based on a deductive approach. Content analysis was used to draw insights from the empirical data. Although the research is based on a deductive approach, inductive features also arose during the content analysis.

The interviewees consist of three people working for three different companies. For the privacy of the interviewees and their presented companies, interviewees are named A, B and C. Interviewee A works in a Finnish company in the banking sector. Interviewee B works in an international company providing payment solutions for their customers from both the bank and merchant sides. Interviewee C works in a Finnish financial services group. These interviewees were chosen to gain a holistic view of the field’s current situation from multiple perspectives. Choosing interviewees from different companies that work in slightly different areas contributed to the accountability of this research.

Interviews included twenty pre-written interview questions, which are provided in appendix one. The questions were divided into three categories supporting both research questions: payment fraud prevention, data use in payment fraud prevention, and using ML models for payment fraud prevention. Questions aimed to fulfill the research objectives, asking about the current situation in payment fraud, possible challenges preventing automation, and future scenarios in the upcoming years. These topics were also covered in the theoretical framework. Semi-structured interviews left space for additional questions to arise during the interviews and for discussion about the topic more freely.

The interviews were conducted in November 2022. One of the interviews was held in person, and two of them were held on Microsoft teams. All interviews lasted between 15 and 50 minutes, depending on the answers' width. The interviews were held in Finnish to ensure unproblematic communication. The interview questions were offered for the interviewees to see beforehand to ensure broad answers covering the wanted topics. As the interview questions were not about opinions, attitudes, or beliefs, showing the questions beforehand should not create delimitations for this research. The interviews aimed to learn about the practices and methods used in interviewees' organizations, and pre-seen questions could bring more value on this front.

4. RESULTS AND FINDINGS

This section presents the findings of the interviews conducted in this thesis. The findings of the interviews are analyzed in relation to the findings of the theoretical framework conducted in chapter two. The evidence can be divided into three categories based on the data and research questions to gain a more wholesome view of the research objectives. First, the current situation is described based on the answers to questions regarding data, analytics, and ML are utilized now. Second, challenges are formed and analyzed based on the current situation and interview answers. Finally, future scenarios are created, offering solutions to previous challenges.

4.1 Current situation

The interviewees were asked questions about their organization's current actions to prevent payment fraud and how they utilize data, analytics, and ML in their strategies. Interview questions 1-5 focused on how the companies have organized payment fraud prevention, what actions they are currently taking, and what kind of data they are utilizing. Questions 10 and 11 focused on the type of data utilized for payment fraud prevention dividing it into internal and external data. Lastly, questions 15-18 focused on the technical side of automating fraud prevention, whether it is possible to automate fraud prevention, how ML is utilized in these companies, and which models are being used. This section is divided into three subsections covering actions against payment fraud, effective fraud prevention and relevant data, and ML models used in the companies.

4.1.1 Actions against payment fraud

All interviewees responded that they utilize data, analytics, and ML in fraud prevention, but they also discussed the importance of manual human work. Interviewee A emphasized the importance of human work, saying that machines might not be able to learn or understand things humans can. There was a common understanding that the field is changing fast, new payment methods are introduced, and people's payment behavior is changing. Fraudsters are working hard to develop new schemes, which demands that financial institutions constantly develop new fraud prevention methods and ensure that their systems and models are working correctly. All three companies have their fraud detection and prevention systems working in real-time, which they see as essential to intervene with fraud right when it happens.

Interviewees see that data and analytics are essential in their fraud prevention actions. Interviewee A says that their systems utilize data, analytics, and ML a lot. Their system is based on data and learns from customers' actions. Interviewee B highlights the importance of following models' performance and evaluating it through different metrics. They constantly work with their models' rules and training. This is in sync with Interviewee C's response that highlighted the role of analytics as the base of all their functions.

> "*If we want to develop our perceptiveness, we obviously need to analyze lots of data to create effective rules. Furthermore, if the effectiveness changes over time for certain rules, then we can analyze if it could be improved and if not, is the rule necessary anymore." -Interviewee C*

4.1.2 Effective fraud prevention and relevant data

The interviewees had many examples of data that can be useful for payment fraud prevention. Interviewee A said that when recognizing fraud, everything starts with the need to know the customer. Know your customer (KYC) data can be utilized to create rules for the systems as a base for them to learn how the customers behave and what kind of transactions they make. This is similar to Wickramanayake et al. (2020), stating that behavioral profiling is vital for recognizing outlier transactions. According to Khattri and Singh (2018), knowing customers' behavioral patterns is the key to recognizing more sophisticated fraud cases. An exaggerated example given by interviewee A would be that everything starting from the size of the customer's shoe could be utilized. The better the bank knows its customers and their behavior, the better it can prevent payment fraud.

Interviewee C believes that more specific behavioral data would be significant for fraud prevention in the future. Information regarding the customer's habits when using their device would help recognize who is trying to log into the account. This information could be used to prevent fraud from happening by blocking the fraudsters from logging into the customer's online banking at all. All this is based on effective fraud recognition, which can be automated with the correct technology. Interviewee C's view on payment fraud prevention closely resembled the progression of payment fraud introduced in figure 1, where payment fraud prevention was divided into three stages.

> *"We try to detect fraud when the customer or fraudster is making a transaction. So, transaction data might be the most relevant. An ideal situation would be to detect the fraud already when the fraudster is logging in to our system so the fraud would not take place. Or well the most ideal situation would be that the customer would not trust their credentials to criminals, and no misuse would happen at all."*
> *-Interviewee C*

Because the companies operate in a little bit different areas, there was some division between how much the companies utilize internal and external data. Companies A and C utilize fewer external data than company B because company B does not own the data they utilize. Instead, they process data from their customers. In this sense, they primarily work with external data. Interviewee B listed that they are utilizing, for example, verification data, clearing data, and authentication data. Both A and C say they communicate with other operators about current trends, but regulations and privacy concerns greatly limit this. Even though they think that more open communication between operators would be helpful in fraud prevention, neither company is planning – or even capable of increasing external data in this sense.

Interviewee A mentioned the European Union's fraud risk country lists that they use for internal monitoring as an example of external data that can be utilized. However, they add that if there are thresholds in the models, like blocked countries, the criminals will find their way around them. This again goes back to the importance of continuously working on models' accuracy and performance.

Interviewees agree that the world situation influences fraud. Therefore, it is vital for effective fraud prevention to actively follow their models' performances and accuracy in case there is a need to change rules, add new rules, or train the models against new fraud patterns. Usually, these patterns go in circles, and each cycle has a new twist. These new cases need to be analyzed and investigated to see what could be done better. Sometimes old tricks come up again, but they are not as effective since the banks already have existing prevention methods. Interviewee B states that many people in the field believe they have a common enemy. Sharing information and knowledge about new crime types is important as it is not a way to differentiate from others. Everyone benefits from stopping criminal activity

It is also emphasized that data quality plays a big role in the models' effectiveness. Company B uses different metrics to measure efficiency, including the probability of recognizing and preventing fraud, the number of false positives, and the total losses. Training data is used as the base for models to learn their functions. The data used in the training set needs to be relevant and of good quality for the model to perform as wanted. Interviewee C also emphasizes the importance of banks' independence in rule management to react to changing situations quickly, thus keeping up efficiency and accuracy. They also added that there cannot be too much bureaucracy in the team working on the rules, or effective fraud prevention would be practically impossible.

4.1.3 Technologies and models

All the companies are using some at least partly automated systems for fraud recognition and prevention. A common belief was that the direction is toward more automated fraud prevention by utilizing AI and ML, but the models still need human support. It is crucial to separate recognition and prevention because these parts are automated separately, even though they affect one another. The automation of payment fraud prevention solely depends on how well the transaction can be labeled as fraudulent or legitimate.

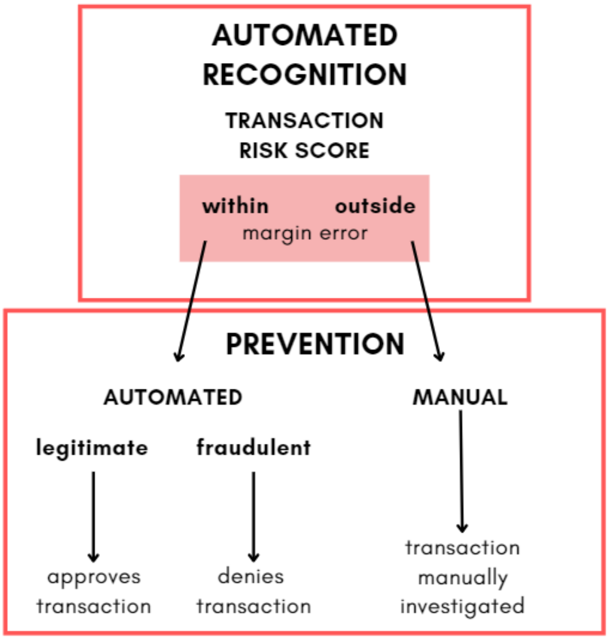

Figure 2: Automating payment fraud recognition and prevention

Interviewee B said that when they receive authorization, they check it against their models and rules, which offer a risk estimate. Depending on the risk score, the transaction can be immediately denied, or it can be manually checked. There is also the option of asking the cardholder if the transaction is legitimate, which can be done through the issuer bank or a two-way communication system. Interviewee C described the same situation. The transaction can be automatically denied if the system can label a transaction as fraudulent 100% sure or with some minor margin error. However, if there is any doubt that a transaction is legitimate or fraudulent, it must be manually investigated.

The process of automating payment fraud recognition and prevention is pictured in figure two. If the recognition of payment fraud is automated, each transaction is given a risk score. The risk score is evaluated against thresholds in the models. If the transaction can be labeled as legitimate or fraudulent and the risk score is within the margin of error, the prevention can also be automated. However, if the risk score is outside the margin error, the transaction needs to be manually investigated to prevent possible fraud.

When asked about ML models used in payment fraud recognition and prevention, interviewee B said that they have some history with Neural Networks but are currently using Gradient Boosting (random forest), which has been working well. Interviewee C also brought up Gradient Boosting (random forest), adding that they also use Naïve Bayes. Both interviewees agreed that their models are supervised. Close to all models brought up in the interviews were included in the theoretical framework’s most mentioned ML models.

The importance of training the models regularly came up repeatedly in the interviews. Constant training is essential for the models’ accuracy, which greatly affects how much the process can be automated. Interviewee C described that after investigating a transaction, they collect datasets where it is marked if a transaction was fraudulent or not. These databases can be used to train the models or discover connections between customers or phenomena by connecting account numbers, IP addresses, countries, et cetera. The quality of data also came up repeatedly. The data quality needs to be high to train effective payment fraud recognition and prevention models that do not cause false alarms.

4.2 Challenges

Some of the interview questions focused on the challenges of data and ML. Some challenges came up in other parts of the interviews as well. Question 6 focused on the kind of data that could be useful for fraud prevention purposes but is not currently used. Question 8 asked about the challenges the interviewees face in their jobs regarding the use of data, and question 19 was about the challenges in interviewees' jobs regarding the use of ML. This section goes through the challenges mentioned in the interviews.

Question six, which asked about possibly valuable data, received divided answers. Interviewee B brought up cryptocurrencies and how money laundering is changing forms. According to interviewee B, crypto merchants have very different risk profiles, creating a need to find an effective way to risk score their services. This topic also came up with interviewee C in question seven while discussing if the type of fraud plays a role in recognizing fraud. They brought up that fraudsters have changed their tactics, especially in investment frauds.

> *"More traditional transactions abroad look quite suspicious, but a customer could legitimately start investing in crypto and usually investments happen in larger amounts as well. The crypto operator cannot directly say if the transactions seem suspicious, and these operators do not have too high interest in preventing this kind of misuse."*
> *-Interviewee C*

Behavioral data was brought up when discussing which kind of data is already helpful. However, interviewee C was adamant that even more specific behavioral data could open new doors to recognizing payment fraud. They primarily focused on behavioral data that could help stop payment fraud from happening before any transactions are even made. Information regarding the device can help in this.

> *"It would be significant if we could somehow automatically conclude who is using the device. Especially in the situation where the device is the customer's own but someone else is using it, for example, by overtaking a mobile phone remotely. ... From the phone, we can theoretically know how the customer holds their phone, what kind of a position, types of movements they make, how long their reaction times, are et cetera. All data related to behavior would be super awesome to be able to use." -Interviewee C*

Interviewees agreed that regulations create many challenges. According to Ryman-Tubb et al. (2018) and Wickramanayake et al. (2020), the data that would be valuable for building the customer's behavioral profile is highly confidential. Another regulation problem concerns transferring data especially connected to using external service providers. Interviewee B says that transferring data is incredibly challenging if any partners are outside Europe. Transaction data can be used to identify people and includes data under the GDPR. All participants need to clearly agree on which data is used and what for.

Interviewee B mentions the difficulties caused by large data masses coming from different sources, while interviewee C emphasized that shaping differently formatted data from various sources into a universal form creates a lot of work. Also, similar to Ryman-Tubb et al. (2018) and Wickramanayake et al. (2020), the interviewees saw the large number of payment methods and merchants challenging for payment fraud recognition. Even for professionals, knowing which data is significant and in which formats it is needed is challenging.

Question 19 asked about the challenges interviewees face regarding ML. This question also received divided answers. Interviewee A brought up the changing criminal behavior, which creates the challenge of systems trying to learn the new patterns fast enough before the pattern changes again. Interviewee B mentioned challenges created by changing or unregular customer behavior, which was also brought up in the theoretical framework by Carcillo et al. (2020). According to interviewee B, some sporadic transactions might differ greatly from the cardholder's usual behavior, for example, due to traveling abroad. The cardholder can suddenly use their card in a way that looks suspicious but is legitimate. In these cases, contacting the customer to verify the transaction can be challenging for various reasons. The customer might not have internet access or be afraid to answer text messages due to the high costs abroad.

Interviewee C focused on the data quality, which was strongly present throughout the interview. They say that if the data is lacking while the model is running, the data can be edited, but the model might not be able to recognize these changes for better performance. Changes to the data can weaken the model's performance. Preparing the model for changes is difficult even if the changes coming in the next six months were known beforehand. New observations can arise during or after the six months, making new updates necessary. Interviewee C reminds us that updates are kind of straightforward for internal models. If the model is external and the creator is from abroad, regulations create enormous challenges for keeping the model effective over time. Truong et al. (2020) believe that automating payment fraud recognition allows the relocation of valuable human workers to more complicated tasks. A model that is not up to date can lead to false positives and wrongly denied transactions creating additional work and abolishing the benefits of automation.

> *"We need to investigate why the transaction was denied, the customer might contact our customer service, customer service contacts someone else, and eventually, it comes back to our table. In these cases, we need to use manual investigation and possibly ask the customer themselves if they made the transaction." -Interviewee C*

4.3 Futuristic approach

Some interview questions were reserved solely to learn about the future of payment fraud prevention. The question about data that could be useful but is not currently in use is connected to the challenges and future of payment fraud prevention. Question nine asked how data-related challenges can be solved and if these solutions are already in use. Questions 12 and 13 asked if the companies plan to increase the use of data and analytics in fraud prevention, with question 13 focusing on external data alone. Question 14 was about utilizing external service providers and new technologies to reach the plans set in the previous two questions. Question 20 asked about ways to utilize ML technology in the future for payment fraud prevention.

Interviewee C phrased well that there is no magic solution to any challenges, only long-term work and development. They describe fraud prevention as an infinite challenge, where solving problems only exposes dozens of new problems to work on. The endlessness of problem-solving related to payment fraud prevention is seconded by interviewee A, whose solution to incorrect or low-quality data is modifying the data to answer the needs better and working on the models and systems. Interviewee C empathizes that a well-done analysis can help create more practical rules for models, which leads to less manual work. However, there is not always time for careful analysis. If too much money goes to criminals too fast, it must be stopped quickly, and analyses are left for later.

Interviewee A says that technology has developed enormously in the past five years, and they believe it will keep developing in the future as well. Changing payment environments, new service providers, and payment methods force banks to keep up with the development. Company A is investing in increasing data and analytics for fraud prevention and has active projects running in this regard.

Interviewee B mentioned interesting aspects of crypto, the dark web, and external operators. The Nilson Report 2021 revealed that buying credentials from the dark web increased in 2020. Interviewee B emphasizes that fraudsters cannot be paid for stolen information, but sometimes free samples that can be used to recognize stolen cards are available on the dark web. Usually, the card number has been masked, but names, addresses, or other information might be left visible. If the BIC is available, the card issuer banks can be recognized. By combining information like the card owner's name and the card's issuer bank, the card owner can be found by fuzzy logic methods. After this, the card can be closed, and the customer can be issued a new one. Interviewee B says that whole datasets would be more helpful, but the stolen cards can be found quite well from samples and available data.

Future scenarios regarding ML models also divided opinions a little. However, the critical point is once again that models need to be worked on, and the models need to be specific. Interviewee B highlights the importance of using the most recent historical data. They have seen an increase in social engineering following the European Union's PSD2 regulation pushing consumers towards strong authentication transactions. Interviewee C says they want to increase the number of different models used. Combining multiple models can lead to the best results, which is supported by Gamini et al. (2021) belief that hybrid models incorporating the best parts from supervised and unsupervised models might be more accurate than either model alone. Interviewee C brings up that other types of transactions besides payment transactions could be given risk scores and utilized for payment fraud prevention.

> *"We do not only want to focus on risk scoring payment transactions but other transactions as well. For example, logins or other non-monetary events like credit applications. Basically, everything that goes on in online banking could be adapted to some sort of a model calculating fraud risk." -Interviewee C*

All interviewees are on common ground regarding data and analytics' role in payment fraud prevention. Everyone thinks that data, analytics, and ML will be utilized more. The ideal situation for all companies would be that the systems would run independently so that no humans would be needed.

4.4 Results analysis

The results of this thesis showed that in vastly changing payment behavior and environment, adapting to new scenarios is vital to prevent money from going to criminal purposes. The results of empirical research mostly supported the theoretical framework built on previous literature, as seen in figure three. All results are in squares, and the results that came up in the interviews are highlighted inside the colored squares.

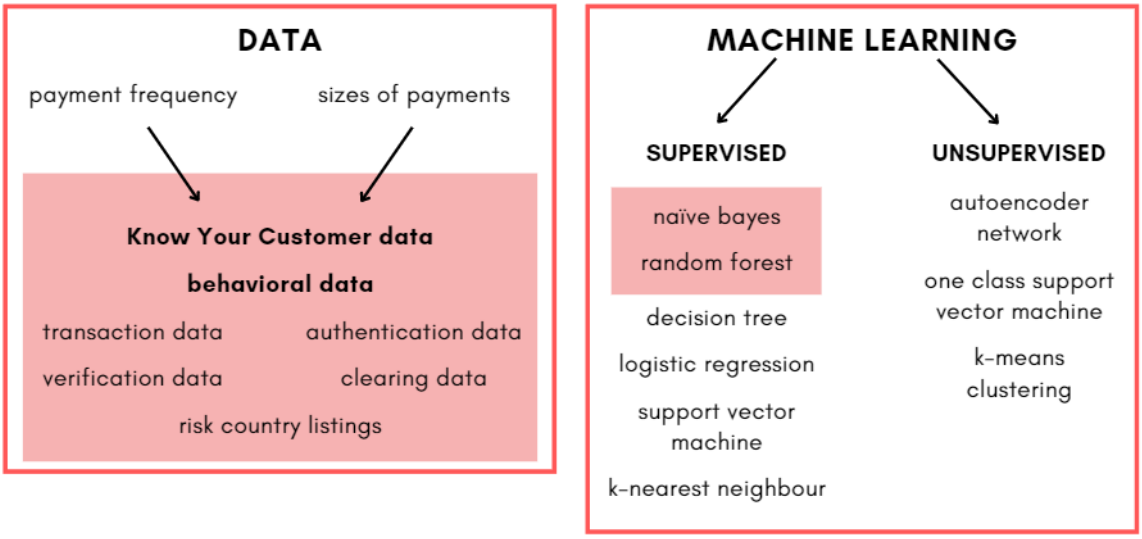

Figure 3: Visualization of the results. Left: Crucial data. Right: Most applied ML models

The research showed that knowing the customer is the base of all payment fraud prevention. A customer's behavioral profile can be built based on various data sources. This can include the frequencies or sizes of payments the customer makes, the devices they use, or even the way they hold their device. Based on data gathered from different transactions, a training data set can be created for a supervised machine learning model to train on.

The empirical study showed that supervised models are more common in real life than unsupervised ones because they are seen as more trustworthy. Unsupervised models are more prone to false positives, which can cause customer damage and additional costs and work for companies, as was mentioned in both the theoretical framework and interviews. However, some literature on the topic supported the view that unsupervised models can better recognize previously unseen fraud cases.

Automating payment fraud prevention and recognition is possible with the correct technologies and constant work toward more accurate models. Training the models came up numerous times in the interviews and theoretical framework, proving its importance. Other frequently coming up topics were the quality of training data and the importance of cooperation between different operators. There were challenges regarding both topics, which should be worked on in the future.

The research also showed that the companies working with payment fraud are keen on increasing automation and the use of data and analytics in the future. Continuous work on the models and data is the key to adapting to new scenarios and preventing money flow for criminal purposes. The interviewees seem aware of the environmental changes and their significance to the field. Their attitudes towards their current situation seemed optimistic despite the need to keep developing in the future.

5. CONCLUSIONS AND DISCUSSION

This thesis aimed to study the role of data and analytics in effective payment fraud recognition and prevention. The objective of this research was to review previous literature on how and why payment fraud prevention should be automated and what the future could look like with a note of how companies are currently organizing their payment fraud. This was declared necessary because despite various sources claiming that the payment fraud environment is drastically changing and the COVID-19 pandemic accelerated the change, there is not much recent research on the topic since 2020. Also, most of the research is quantitative, leaving a gap for qualitative research on the topic.

5.1 Answering the research questions

The interviewees emphasized the importance of separating payment fraud recognition and prevention. This division has been done in the research questions, with the first solely focusing on detecting fraud. The theoretical framework put together some examples of how payment fraud is recognized and which data is significant for this purpose. Interviews complemented this. The theoretical framework and empirical research looked for ways to prevent payment fraud by utilizing data, analytics, and ML models. This subsection focuses on finding the answer to the research questions:

Q1: Which data are used to recognize payment fraud and how?

The key findings of this study showed that data plays a big role in automating payment fraud detection and prevention. ML models can help relocate human resources to tasks they are more needed at, making fraud prevention more cost-efficient and effective. Especially behavioral data of cardholders can be utilized to recognize if a payment transaction is committed by the cardholder themselves or possibly someone else by comparing a transaction to the cardholder’s usual payment behavior. Behavioral data could be utilized even more to recognize and prevent payment fraud before the fraudulent transactions have even happened.

However, due to the sensitive nature of the relevant data, accurate ML models can be challenging to build and keep updated.

This research found that fraudulent transactions can be automatically denied if the systems can label the transactions as legitimate or fraudulent with a small enough margin error. Constant training of models is essential for their accuracy, which is connected to the possibility of automation. Data can be collected from previous fraud investigations and used as a training set for models or to find connections between fraud cases. Data quality plays a big role in how effective the models are. A challenge on this front is the enormous amount of data on the move, which needs to be labeled as essential and nonessential. High-quality training data reduces the number of false alarms.

Q2: How can payment fraud be prevented using data, and which are the most applied ML models for payment fraud prevention?

Six supervised (logistic regression, decision tree, random forest, naïve Bayes, k-nearest neighbor, and support vector machine) and three unsupervised (k-means clustering, one class support vector machine, and autoencoder network) ML models were introduced in chapter two based on how often they came up in previous literature. Finding one best model is difficult due to different comparison criteria and the lack of real-life testing data. Some of the models mentioned in the interviews were included in the six supervised models. The interviewees mentioned neural networks, gradient boosting, random forests, and naïve Bayes.

This research showed that supervised ML models are more common in practice, even though unsupervised models could be better at recognizing previously unseen types of fraud and more fitting for payment fraud prevention. The interviewees rationalized this by emphasizing that false positives, which unsupervised models are more prone to, are the unwanted result. The research proved that false positives create hidden costs and additional workload, abolishing the purpose of automating fraud prevention. The possibility of combining models came up in theoretical and empirical parts, leaving space for more research.

5.2 Verification and validation

The generalizability of the findings of this study is a little poor due to the small take in the empirical research. However, the size of the empirical material (three participants) is relatively good, and interviewees were deliberately chosen from different companies. The results of empirical research and the theoretical framework were similar, suggesting that the research can be generalized quite well. The theoretical framework included scientific articles, recent conference papers, and information from different officials, such as the Federal Bureau of Investigation and the International Criminal Police Organization making the theoretical sources versatile. The vast extent of theoretical sources adds to the accountability of this thesis. Because of the quick changes happening in people's payment behavior, sources used in the theoretical framework were mainly published at the earliest in 2018, aiming to leave out outdated information and build a better understanding of the current situation.

This thesis contributes to research on payment fraud prevention in the 2020 century especially by filling the gap of qualitative research on the topic, offering deeper understanding of real-life practices and challenges. A broader take in the empirical part could give even more understanding of the topic and differences between companies. Choosing participants more dividedly around the globe and from different businesses, for example, the merchant and banking sides could offer even more perspective into the research. Overall, this thesis gives a good understanding of the current situation in payment fraud prevention, challenges in the field, and possible future scenarios.

5.3 Future research

Some challenges brought up in this research were left open. This would include the relation between class imbalance and false positives as well discrepancy between the need for cooperation and the regulations preventing the cooperation. The payment fraud environment is changing quickly; legislation, on the other hand, does not. Legislation needs to be sustainable and future-oriented. Future research could focus on reducing the class imbalance problem without increasing false positives. It came up in this research that different ML models do well in different areas. One option could be combining different ML methods and creating hybrid models.

All in all, more research into the differences between supervised and unsupervised models would help better understand if unsupervised models or hybrid models could be better utilized in payment fraud recognition. Research already shows that unsupervised models could be more potent than supervised approaches. The biggest concern regarding unsupervised models seemed to be the risk of false positives. Clearly, more research into unsupervised models, hybrid models, and false positives is needed.

Several interviews brought up how cryptocurrencies are changing money laundering and payment environments. One question arising from this research is the role of crypto and the dark web in payment fraud schemes right now and in the upcoming years. Both theoretical and empirical research showed that selling credentials on the dark web is increasing, and solutions are needed. This could also be a topic of interest in the future.

REFERENCES

Abbassi, H., El Alaoui, I., & Gahi, Y. (2022). Fraud Detection Techniques in the Big Data Era. Proceedings of the 2nd International Conference on Big Data, Modelling and Machine Learning (BML 2021), pages 161-170

Bhanusri, A., Valli, K. R. S., Jyothi, P., Sai, G. V., & Rohith, R. (2020). Credit card fraud detection using Machine learning algorithms. *Journal of Research in Humanities and Social Science*, *8*(2), 04-11.

Carcillo, F., Le Borgne, Y. A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information sciences*, *557*, 317-331.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1-20.

Chilaka, U. L., Chukwudebe, G. A., & Bashiru, A. (2019). A Review of Credit Card Fraud Detection Techniques in Electronic Finance and Banking. Iconic Research and Engineering Journals, *3*(2), 456-467

European Association for Secure Transactions. Fraud Definitions. 2022. [Online] [Retrieved 2022/10/23] [Available] https://www.association-secure-transactions.eu/industry-information/fraud-definitions/

European Council. 2023. [Online] [Retrieved 2023/01/02] [Available] https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

European Payments Council. 2023. [Online] [Retrieved 2023/01/02] [Available] https://www.europeanpaymentscouncil.eu/node/10606

Europol. 2022. [Online] [Retrieved 2022/10/10] [Available] https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud

Federal Bureau of Investigation (FBI) 2022a. [Online] [Retrieved 2022/10/10] [Available] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes

Federal Bureau of Investigation (FBI) 2022b. [Online] [Retrieved 2022/10/10] [Available] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

Federal Bureau of Investigation (FBI) 2022c. [Online] [Retrieved 2022/10/10] [Available] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

Federal Bureau of Investigation (FBI) 2022d. [Online] [Retrieved 2022/10/10] [Available] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/romance-scams

Galletta, & Cross, W. E. (2013). *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication*. New York University Press. https://doi.org/10.18574/9780814732953

Gamini, P., Yerramsetti, S. T., Darapu, G. D., Pentakoti, V. K., & Vegesena, P. R. (2021). A Review on the Performance Analysis of Supervised and Unsupervised algorithms in Credit Card Fraud Detection. *International Journal of Research in Engineering, Science and Management*, *4*(8), 23-26.

Gangavarapu, T., Jaidhar, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review*, *53*(7), 5019-5081.

Interpol. 2022. [Online] [Retrieved 2022/10/10] [Available] https://www.interpol.int/Crimes/Financial-crime/Payment-card-fraud

Karpoff, J. M. (2021). The future of financial fraud. *Journal of Corporate Finance*, *66*, 101694.

Khattri, V., & Singh, D. K. (2018). Parameters of automated fraud detection techniques during online transactions. *Journal of Financial Crime*, 25(3), 702-720.

Khatri, S., Arora, A., & Agrawal, A. P. (2020). Supervised machine learning algorithms for credit card fraud detection: a comparison. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering*, IEEE. (pp. 680-683).

Kikerpill, K., & Siibak, A. (2021). Mazephishing: The COVID-19 pandemic as credible social context for social engineering attacks. *Trames: A Journal of the Humanities and Social Sciences*, *25*(4), 371-393

Kurshan, E., & Shen, H. (2020). Graph computing for financial crime and fraud detection: Trends, challenges and outlook. *International Journal of Semantic Computing*, *14*(04), 565-589.

Larson, B. J. (2020). False Positive Reduction in Credit Card Fraud Prediction: an Evaluation of Machine Learning Methodology on Imbalanced Data (Doctoral dissertation, Capitol Technology University). 166p.

Mehndiratta, S., & Gupta, M. K. (2019). Credit card fraud detection techniques: a review. *International Journal of Computer Science and Mobile Computing*, *8*(8), 43-49.

Niu, X., Wang, L., & Yang, X. (2019). A comparison study of credit card fraud detection: Supervised versus unsupervised. *arXiv preprint arXiv:1904.10604*.

Rezapour, M. (2019). Anomaly detection using unsupervised methods: credit card fraud case study. *International Journal of Advanced Computer Science and Applications*, *10*(11).

Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence*, *76*, 130-157.

The Nilson Report 2021, Issue 1209 [Online] [Retrieved 2022/12/14] [Available] https://nilsonreport.com/publication_newsletter_archive_issue.php?issue=1209

The World Bank, Global Findex database 2021. [Online] [Retrieved 2022/10/23] [Available] https://www.worldbank.org/en/publication/globalfindex

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry*, *12*(3), 410

Wallny, F. (2022, January). False Positives in Credit Card Fraud Detection: Measurement and Mitigation. In *2022 55th Hawaii International Conference on System Sciences* (pp. 1-10)

Wickramanayake, B., Geeganage, D. K., Ouyang, C., & Xu, Y. (2020). A Survey of Online Card Payment Fraud Detection using Data Mining-based Methods. *arXiv preprint arXiv:2011.14024*.

Yousefi, N., Alaghband, M., & Garibay, I. (2019). A comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection. *arXiv preprint arXiv:1912.02629*.

Appendices

Appendix 1. Interview questions

I MAKSUVÄLINEPETKOSEN EHKÄISEMINEN *(PAYMENT FRAUD PREVENTION)*

Q1: Kuinka maksuvälinepetosten ehkäiseminen on järejestetty organisaatiossanne? / (*How is payment fraud prevention organized in your organization?)*

Q2: Hyödynnättekö tällä hetkellä data, analytiikkaa tai tekoälyä/koneoppimismalleja maksuvälinepetosten ehkäisemiseksi? / (*Are you currently utilizing data, analytics, or AI/ML to prevent payment fraud?)*

Q3: Millaisia työkaluja ja teknologioita käytätte maksuvälinepetosten ehkäisemiseen? (*What kind of tools and technologies do you use for payment fraud prevention?)*

Q4: Millaisia toimia teette juuri nyt maksuvälinepetosten ehkäisemiseksi? (*What actions are you currently taking to prevent payment fraud?)*

II DATAN KÄYTTÖ MAKSUVÄLINEPETOSTEN EHKÄISEMISESSÄ *(DATA USE IN PAYMENT FRAUD PREVENTION)*

Q5: Millaista dataa käytätte maksuvälinepetosten tunnistamiseen? *(What kind of data do you use to recognize payment fraud?)*

Q6: Millainen dataa voisi olla hyödyllistä, muttei ole parhaillaan käytössä? *(What kind of data could be helpful but is not currently used?)*

Q7: Vaikuttaako maksuvälinepetoksen tyyppi siihen millainen data on hyödyllistä? *(Does the way a payment fraud (e.g., phishing, romance scam) is committed affect which data is useful?)*

Q8: Millaisia haasteita työssäsi voi esiintyä tarvittavaan dataan liittyen? (esim. lainsäädäntö ja datan saatavuus) *(What kind of challenges can occur related to the required data in your work? (e.g., related to regulations and accessibility of data))*

Q9: Kuinka nämä ongelmat voidaan ratkaista, käytättekö tämän kaltaisia ratkaisuja jo? (*How can these problems be solved, are you already using these kinds of solutions?)*

Q10: Millaista organisaation sisäistä dataa käytätte petosten ehkäisemisessä? *(What kind of organization internal data do you use for payment fraud prevention?)*

Q11: Hyödynnättekö ulkoista dataa maksuvälinerikosten tunnistamiseksi? Jos kyllä, millaista ulkoista dataa? *(Do you utilize external data to detect payment fraud? If yes, what kind of external data?)*

Q12: Suunnitteleeko organisaatiosi datan ja analytiikan lisäämistä maksuvälinepetosten ehkäisemiseen liittyen? *(Is your organization planning to increase use of data and analytics related to payment fraud prevention?)*

Q13: Suunnitteleeko organisaatiosi ulkoisen datan käytön lisäämistä? *(Is your organization planning to increase use of external data?)*

Q14: Uskotko että uudet teknologiat ja ulkoiset palveluntarjoajat voisivat auttaa tässä? *(Do you think that new technologies and external service providers could help with this?)*

III TEKOÄLYN JA KONEOPPIMISMALLIEN KÄYTTÄMINEN MAKSUVÄLINEPETOSTEN EHKÄISEMISESSÄ *(USING AI AND ML MODELS FOR PAYMENT FRAUD PREVENTION)*

Q15: Voiko maksuvälinepetoksen tunnistamisen ja ehkäisemisen automatisoida? Kuinka yleistä se on organisaatiossanne? *(Can payment fraud recognition and prevention be automated? How common is it in your organization?)*

Q16: Kuinka tekoälyä ja koneoppimista hyödynnetään organisaatiossasi maksuvälinepetosten havaitsemiseen? *(How are artificial intelligence and machine learning utilized currently in your organization to detect payment fraud?)*

Q17: Mitä koneoppimismalleja käytätte maksuvälinepetosten havaitsemiseksi organisaatiossasi? Voitko nimetä muutaman yleisimmän? *(What machine learning methods are used for payment fraud detection in your organization? Can you name a few most used ones?)*

Q18: Ovatko ohjatut vai ohjaamattomat koneoppimismallit yleisempiä, miksi? *(Are supervised or unsupervised learning methods more common, why?)*

Q19: Millaiset haasteet estävät tekoälyn ja koneoppimisen käyttämisen maksuvälinepetosten havaitsemiseksi työssäsi? *(What kind of challenges are preventing the use of AI and ML for payment fraud detection in your work?)*

Q20: Kuinka tekoälyä ja koneoppimismalleja voitaisiin hyödyntää tulevaisuudessa? *(How could AI and ML technology be utilized in the future?)*