Sudan University of Science and Technology

College of Engineering

School of Electronics Engineering

Dissecting the Success Factors of Telecom Fraud Deterrence: A Configurational Analysis Using NCA and fsQCA

A Research Submitted in Partial Fulfillment of the Requirements for the Degree of B.Eng. (Honors) in Electronics Engineering

Prepared by:

1. Atog Mayor Angong
2. Enas Makki Alrasheed
3. Hassan Al Siddig Al Hag Al Siddig
4. Mustafa Mohammed Elfatih
5. Mojeeb Alrhman Magdi Gasm

Supervised by:

Prof. Dr. Rashid A. Saeed

Sept. 2026

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

قَالَ تَعَالَى:

﴿ وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ وَسَتُرَدُّونَ إِلَىٰ عَالِمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ ﴾

صَدَقَ اللَّهُ الْعَظِيم

(سُورَةُ التَّوْبَةِ - الآيَةُ 105)

DEDICATION

To our parents,

whose patience, prayers, and quiet sacrifices carried us further than they know.

To our teachers,

who gave generously of their knowledge and their time.

And to everyone who kept going when the work was hard.

ACKNOWLEDGEMENTS

First and foremost, all praise is due to Allah, who granted us the health, patience, and determination to complete this work.

We wish to express our sincere gratitude to our supervisor, Dr. Rashid A. Saeed, for his guidance, his generous availability, and the care with which he reviewed this work at every stage. His comments shaped this research in ways that are visible on every page.

We extend our thanks to the staff of the School of Electronics Engineering at Sudan University of Science and Technology for the knowledge and support they provided throughout our studies.

Finally, we are deeply grateful to our families and friends for their unwavering encouragement, and to one another for the effort and persistence that brought this project to completion.

ABSTRACT

This study applies a hybrid configurational approach to investigate SIM box fraud patterns in telecommunications data. By integrating behavioral indicators derived from call detail records with Necessary Condition Analysis (NCA) and Fuzzy-set Qualitative Comparative Analysis (fsQCA), the research identifies the conditions and specific combinations of call characteristics that lead to fraudulent outcomes. After excluding the fields that restate the outcome, the NCA results show that international call type is a fully necessary condition for SIM box fraud (effect size = 1.000) and that short call duration imposes a near-complete constraint (effect size = 0.978), while no other recorded attribute bounds the outcome. The analysis demonstrates that fraud behavior does not stem from isolated factors but rather emerges from complex configurations of conditions such as call duration, call type, and origin–destination patterns.

The findings underscore the interpretive value of configurational analysis in telecom fraud detection compared with purely predictive, black-box models. While predictive approaches often obscure the underlying mechanisms of fraud, the fsQCA framework reveals how multiple behavioral conditions interact to generate fraudulent activity. This methodological contribution enhances transparency, supports actionable insights for fraud management, and provides a foundation for bridging explanatory and predictive approaches in fraud detection research.

Keywords: *SIM box fraud, telecom fraud detection, necessary condition analysis, fuzzy-set qualitative comparative analysis, interpretable machine learning, causal inference, call detail records.*

المستخلص

يقدّم هذا البحث منهجاً تكوينياً هجيناً لدراسة أنماط الاحتيال عبر صناديق الشرائح (SIM box) في بيانات الاتصالات. ومن خلال دمج المؤشرات السلوكية المستخلصة من سجلات تفاصيل المكالمات مع تحليل الشرط الضروري (NCA) والتحليل المقارن النوعي للمجموعات الضبابية (fsQCA)، يحدّد البحث الشروط والتركيبات المحددة لخصائص المكالمات التي تؤدي إلى النتائج الاحتيالية. وبعد استبعاد الحقول التي تعيد صياغة النتيجة، أظهرت نتائج تحليل الشرط الضروري أن كون المكالمة دولية شرط ضروري تام لحدوث الاحتيال (حجم الأثر = 1.000)، وأن قِصَر مدة المكالمة يفرض قيداً شبه تام (حجم الأثر = 0.978)، بينما لا يقيّد أي متغير آخر مسجَّل حدوث الاحتيال. ويوضّح التحليل أن السلوك الاحتيالي لا ينشأ من عوامل منفردة، بل ينبثق من تركيبات معقدة من الشروط مثل مدة المكالمة ونوعها وأنماط المصدر والوجهة.

وتؤكد النتائج القيمة التفسيرية للتحليل التكويني في كشف الاحتيال في الاتصالات مقارنةً بالنماذج التنبؤية مغلقة الصندوق. فبينما تحجب المناهج التنبؤية الآليات الكامنة وراء الاحتيال، يكشف إطار fsQCA كيف تتفاعل شروط سلوكية متعددة لإنتاج النشاط الاحتيالي. وتعزّز هذه المساهمة المنهجية الشفافية، وتدعم رؤى قابلة للتطبيق في إدارة الاحتيال، وتوفّر أساساً للربط بين المناهج التفسيرية والتنبؤية في أبحاث كشف الاحتيال.

الكلمات المفتاحية: احتيال صناديق الشرائح، كشف الاحتيال في الاتصالات، تحليل الشرط الضروري، التحليل المقارن النوعي للمجموعات الضبابية، تعلّم الآلة القابل للتفسير، الاستدلال السببي، سجلات تفاصيل المكالمات.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Meaning
AI	Artificial Intelligence
CDR	Call Detail Record
CE-FDH	Ceiling Envelopment – Free Disposal Hull
CNN	Convolutional Neural Network
fsQCA	Fuzzy-set Qualitative Comparative Analysis
GAT	Graph Attention Network
GCN	Graph Convolutional Network
GNN	Graph Neural Network
HESM	Hawkes-Enhanced Sequence Model
IF	Isolation Forest
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IPRN	International Premium Rate Number
IRSF	International Revenue Share Fraud
KYC	Know Your Customer
LAC	Location Area Code
LLM	Large Language Model
LSTM	Long Short-Term Memory
ML	Machine Learning
MLP	Multilayer Perceptron
NCA	Necessary Condition Analysis
PBX	Private Branch Exchange
PRI	Proportional Reduction in Inconsistency
QCA	Qualitative Comparative Analysis
SHAP	SHapley Additive exPlanations
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMOTE	Synthetic Minority Over-sampling Technique
SMS	Short Message Service
VoIP	Voice over Internet Protocol

LIST OF SYMBOLS

Symbol	Description
x	Value of a condition (independent variable) in the XY-space
y	Value of the outcome (dependent variable) in the XY-space
a, b	Intercept and slope of the linear ceiling line
$y_{ceiling}(x)$	Ceiling line function bounding the observed XY-space
$A_{ceiling}$	Ceiling area — the empty zone above the ceiling line
x_{min}, x_{max}	Minimum and maximum observed values of the condition
y_{min}, y_{max}	Minimum and maximum observed values of the outcome
d	NCA effect size — ceiling area as a proportion of the total scope
y*	Target outcome level used in bottleneck analysis
μX(i)	Fuzzy-set membership score of case i in condition X
μY(i)	Fuzzy-set membership score of case i in outcome Y
min(·)	Fuzzy-set intersection (logical AND)
Σ	Summation over all cases in the dataset
+	Logical OR (set union) in a Boolean solution
→	Sufficiency relation ("leads to")
~	Negation of a set (logical NOT)
n	Number of cases in a configuration
incl	Inclusion (consistency) score of a configuration

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Telephony represents one of the world's oldest and most extensive networks. Due to its long history and global prevalence, telephony incorporates diverse technologies and involves numerous service providers and consumers, resulting in significant complexity and non-transparency. The daily volume of phone call traffic processed by these networks is enormous. This system's inherent complexity, involving multiple international providers and suppliers, complicates accurate cost estimation for individual calls [9], [25].

The advent of VoIP technology has further intensified these challenges by bridging the Internet and traditional telephony. This convergence has unfortunately created lucrative opportunities for various fraudulent schemes, including International Revenue Sharing Fraud (IRSF). In IRSF schemes, perpetrators utilize either illegal resources (e.g., stolen SIM cards) or legal services (e.g., verification services) to access operator networks. Their objective is to generate traffic to phone numbers acquired from International Premium Rate Number (IPRN) providers. These premium numbers charge telecom companies substantially higher fees, as they were originally designed for value-added services. Historically, such numbers supported services like weather forecasts in the 1990s, where costs were included in phone bills rather than paid separately by customers [23], [4].

1.2 Problem Statement

Traditional fraud detection systems rely on static data analysis over large time windows. They generate features or aggregate values through database queries, then make decisions based on these historical patterns. This approach is inherently time-consuming, creating detection delays that fraudsters exploit. During this lag, perpetrators can complete numerous fraudulent calls before detection occurs [12], [3].

The discussed scenarios underscore the critical need for real-time CDR analysis tools. Such tools must monitor CDR streams continuously and generate current network views with minimal latency. An effective solution should integrate recent data with historical context to produce a complete network state at any given moment. Additionally, the system must be customizable to accommodate varying operator requirements. Current research solutions lack real-time capabilities due to their dependence on traditional database architectures. They typically employ large time windows, limited feature sets, and insufficient contextual awareness. Commercial systems, while available, often use proprietary approaches focused on specific use cases. Their high costs make them inaccessible to many operators, creating a significant market gap [15], [12].

1.3 Aims and Objectives

The aim of this research is to develop an effective framework for detecting telecommunication fraud. The specific objectives are:

1. To identify and analyze complex call patterns in telecommunication data.
2. To determine suitable features for real-time decision-making.
3. To design an optimal system architecture for fraud detection.

1.4 Research Questions

This study aims to answer the following research questions:

1. How can complex fraudulent call patterns be identified?
2. Which features best detect fraud in real time?
3. How effective is the proposed fraud detection system?

1.5 Significance of the Study

This research is of academic and practical importance. Academically, it makes a contribution through Necessary Condition Analysis (NCA) and fuzzy-set Qualitative Comparative Analysis (fsQCA) applied to telecom fraud prevention. In contrast to traditional linear methods, these approaches help to understand the interplay of a variety

of factors that determine the success of the fraud prevention process, instead of assuming that any single factor is enough. In addition, the project pairs the configurational analysis with a Random Forest classifier, which is used both to validate the findings predictively and to rank the relative importance of the call features, enhancing its methodological contribution to the body of research on fraud detection [9], [30].

The practical aspect of the study deals with a pressing issue for telecom operators, namely International Revenue Sharing Fraud (IRSF). Telephony networks are very complex and involve numerous providers, technologies, and international linkages, and hence they can be exploited. Existing fraud detection methods usually rely on static data and long time windows that are not fast enough to detect fast-moving fraud. Consequently, fraudsters are able to place many calls before they are detected, which creates large financial losses that are usually transferred to customers. The study has direct value to telecom operators, regulators, and customers by identifying success factors that allow fraud to be detected closer to real time, more adaptively, and at reduced cost. Finally, it supports not only financial savings for telecom companies but also increased trust in, and reliability of, communication networks [23], [4].

1.6 Scope and Limitations

1.6.1 Scope

This thesis has a narrow scope, which is the deterrence of fraud in the telecommunications sector, specifically International Revenue Sharing Fraud (IRSF). The project is based on a publicly available benchmark call detail record dataset obtained from Kaggle, which simulates telecommunications traffic containing labelled SIM box fraud, and implements configurational techniques (NCA and fsQCA) alongside a Random Forest classifier that is used for predictive validation and for ranking the relative importance of the call features. The analysis is focused on identifying trends in Call Detail Records (CDRs) in order to help detect suspicious activity and reinforce fraud prevention mechanisms [31], [32].

1.6.2 Limitations

The research, although useful, has a number of limitations. First, it primarily addresses IRSF and does not cover the various other forms of telecom fraud, such as misrouting fraud, so the findings cannot be generalized. Second, the study relies on a single publicly available benchmark dataset obtained from Kaggle, which simulates rather than records operator traffic. Its regularities are those of the process that generated it, so the results demonstrate the behaviour of the methods rather than their performance on live traffic, and no claim is made that the findings transfer directly to a production network without further validation. Third, due to the lack of ground truth in fraud detection, it is challenging to perform fine-grained detection, i.e., results are not always based on labels but on approximations. Lastly, although the selected techniques (NCA and fsQCA) are effective in determining the required conditions and configurations, they do not entirely reflect the dynamic, real-time aspect of telecom fraud, and should first be validated with other operators and locations before they can be applied universally [31], [32].

1.7 Organization of the Thesis

This thesis is divided into five chapters:

Chapter One discusses and describes the importance of the research, the proposed solution, and the goals and method used in this study.

Chapter Two introduces information on the systems used, presents previous work, and reviews existing solutions.

Chapter Three describes the design of the systems used and explains the analytical methods and software.

Chapter Four introduces and describes the results of the systems used, then presents a discussion of these results.

Chapter Five concludes the thesis and makes proposals for future work.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Telecommunication fraud has become one of the most urgent issues for operators and regulators all over the world. As digital communication swiftly develops and the number of mobile devices increases, fraudsters continue to exploit gaps in telecommunication systems to gain money. Conventional security strategies are no longer effective because fraudsters have developed more advanced approaches in this field, such as using artificial intelligence (AI) and social engineering, and automating scam processes [4], [23].

This chapter discusses the development of telecom fraud detection, past research in this field, and the efficiency and constraints of different methods, from rule-based systems to graph-based and configurational systems. It also explores how Call Detail Records (CDRs) can be used as the basis of fraud analysis and presents the application of Necessary Condition Analysis (NCA) and fuzzy-set Qualitative Comparative Analysis (fsQCA) as innovative approaches for analyzing complex causation patterns related to telecom fraud deterrence [1].

The development of artificial intelligence has greatly assisted fraudsters, as Generative AI (GenAI) can impersonate customer service representatives, while deepfake technology undermines advanced Know Your Customer (KYC) identity verification processes. With the rapid advancement of this field, it is highly likely that more risks will emerge in the near future [20], [24].

Additionally, many fraudsters resort to using virtual cards to gain access to regional telecommunications networks. According to Statista reports, there were more than 600 million smartphone connections using eSIMs in 2024, which provides an opportunity for hackers to access and control customers' phones [12], [3].

The Telecommunications Fraud Prevention Association reported in November 2023 that fraud increased by 12% over two years, with estimated revenue losses for companies reaching approximately $38.95 billion. Both companies and customers remain vulnerable to various forms of fraud [2].

2.2 Telecom Fraud

Telecom fraud is any illegal activity in which fraudsters use communication services to steal money or manipulate networks. Fraud is carried out through deception, forgery, or exploiting system vulnerabilities. Telecom fraud can also involve computer hacking or service theft. Consumers may be surprised by exorbitant charges, or service providers may receive huge bills from local network companies due to fraudulent communications, the result being large revenue losses for companies [12], [3].

2.3 Types of Telecom Fraud

2.3.1 SMS Phishing

This involves sending deceptive text messages to trick recipients into providing personal information that is then used to withdraw money or gain access to communication networks. It is one of many social-engineering tactics and is often used together with similar attacks such as email and social media platform scams.

2.3.2 SIM-Box Fraud

Termination mechanisms are used to make international calls appear as local calls. When the call is terminated, the termination rate determines the final cost; the consumer pays the full price while the fraudster pockets the money [12], [20].

2.3.3 International Revenue-Share Fraud (IRSF)

This is one of the most persistent types. Fraudsters inflate traffic volumes by colluding with telecom operators and premium-rate service providers to orchestrate the scam. The scheme has evolved into a serious challenge for any service relying on OTPs. Fraudsters

use stolen SIM cards as well as compromised mobile devices and company PBX phones to make fake calls and exploit voice- or SMS-based one-time passwords [23], [4].

2.4 Data Source: Call Detail Records (CDR)

One of the main sources of information used in detecting telecom fraud is the Call Detail Record (CDR). It holds extensive metadata on every communication event, including the call duration, the date, the caller and the receiver, the network location, and billing. CDRs contain no content of the communication, but include sufficient contextual data to detect abnormal patterns and suspicious events [15], [12].

Every CDR usually contains the following fields:

- Caller and receiver numbers
- Call start and end times
- Duration of the call
- Call type (data session, SMS, voice, etc.)
- IMEI and IMSI identifiers
- Location codes (Cell ID, LAC)
- Billing data and cost per call

In fraud detection, high volumes of CDRs are processed to determine patterns that do not conform to normal operation. For example, the international call rate or the number of short-duration calls to premium-rate numbers can suddenly increase, which may be an indicator of either IRSF or SIM-box fraud [12], [20].

In contemporary fraud detection systems, big data analytics are commonly used to handle millions of CDRs at a time. Such systems are able to reveal both time-based and relational dependencies that are ignored by traditional rule-based systems. Moreover, CDRs can be a potent input to Graph Neural Networks (GNNs) and Graph Attention Networks (GATs) when organized as a graph, since they inherently describe relationships between users and their interactions [3], [28].

Consequently, it is important to understand the structure and purpose of CDR data before examining the various methods of detection considered in the subsequent sections [15], [12].

Telecommunications fraud has been a major issue that operators across the world grapple with every year, with losses worth billions of dollars. One of the most harmful schemes is International Revenue Sharing Fraud (IRSF), which uses premium-rate numbers and creates false traffic to the detriment of operators and customers. Over the years, researchers have suggested a variety of detection methods, from simple rule-based systems to complex machine learning and graph-based models, which are examined in the following sections [3], [28].

2.5 Detection Approaches

2.5.1 Machine Learning Methods

Machine learning (ML) has enhanced the detection of fraud by learning from data instead of depending on expert rules only. Supervised learning techniques such as decision trees and support vector machines are used to address telecom fraud, but they need large labeled datasets, which can be difficult to obtain. To overcome this, Isolation Forest, an unsupervised technique, has gained popularity. In the case of fraud, Isolation Forest is effective because data is rarely labeled and the majority of data points behave similarly [3].

Recent research indicates the strength of hybrid ML. For example, Abid et al. [4] proposed a scalable hybrid framework combining rule-based detection with machine learning that achieved greater accuracy than either approach alone, and an advanced detection model using a RoBERTa language model with dual loss functions, specifically designed to handle telecom fraud, demonstrates the direction the field has taken towards more elaborate deep learning solutions.

2.5.2 Rule-Based Methods

Rule-based detection systems are a classical and transparent method among existing approaches to telecom security. They operate by converting the heuristic knowledge of

fraud investigators into a collection of specific, pre-established rules. One of the pioneering models of this kind, described in [5], automatically filters call detail records (CDRs) of transactions that violate certain thresholds. These are usually rules aimed at irregularities such as calls of unusually long duration, a burst in the number of call attempts within a short time frame, or repeated calls to previously known high-risk international number ranges.

The major strength of this approach is that it is easily interpretable. Each alert produced by the system can be traced directly to a particular, comprehensible rule, which greatly assists analysts when conducting investigations. This paradigm has therefore been an essential and stable part of fraud management systems over the years and has provided a strong initial defense against well-characterized fraudulent actions [6].

2.5.3 Graph-Based Techniques

Telecommunication data is inherently graph-structured, with calls being the connections between entities such as users and operators. This has contributed to the emergence of graph-based fraud detection. Specifically, Graph Attention Networks (GATs) have potential because they enable the model to assign varying weights to adjacent nodes, guiding it to attend to the most important relationships [3], [28].

This is reflected in several recent studies. For example, [7] proposed GDFGAT, a GAT-based approach to telecom fraud detection that applies feature-difference weighting to indicate suspicious relationships, and GATs have also been applied to contextual anomaly detection in network monitoring, with good potential for telecom applications. These graph-based models are capable of capturing subtle relational fraud patterns that traditional ML models fail to capture.

2.5.4 Isolation Forest

Isolation Forest (IF) [26] is an ensemble-based algorithm with linear time complexity and acceptable performance on high-volume data. Thus, it is widely used in industry, including in intrusion detection and fraud detection. IF deals with continuous structured data, aiming to detect outliers using isolation (how far a sample is from the rest of the data). From a statistical perspective, data samples have a low probability of lying in areas

where points are sparsely distributed. In other words, IF detects anomalies that satisfy the following requirements:

- They account for only a small portion of the whole dataset.
- They follow distributions different from those of normal samples.

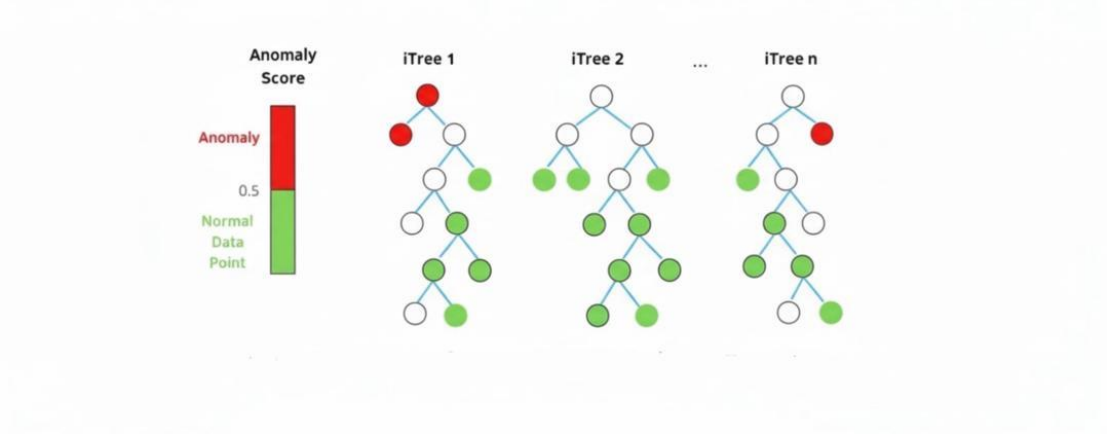

Figure 2.1: Anomaly Detection with Isolation Forest

2.5.5 Graph Attention Network (GAT)

The Convolutional Neural Network (CNN) [27] has been proven a strong tool in computer vision. This is because it can use shared-parameter filters (kernels) to form feature maps by calculating the weighted sum of a central pixel and its adjacent pixels, allowing it to extract spatial features effectively. However, the pixels in the image or video data processed by a CNN are arranged in a very neat matrix, which makes a naive CNN unable to deal with data of non-Euclidean structure, such as social networks and molecules. Nevertheless, researchers still want to use convolution to extract features from such data. Therefore, the Graph Convolutional Network (GCN) [28] was introduced to satisfy such needs, using concepts from graph theory. There are mainly two approaches to implementing graph convolution: the spatial domain approach and the frequency domain approach. Because frequency-domain approaches are more complicated and GAT focuses more on spatial information, only the spatial domain approach is introduced here. Spatial GCN aggregates each node's information with that of its neighbors.

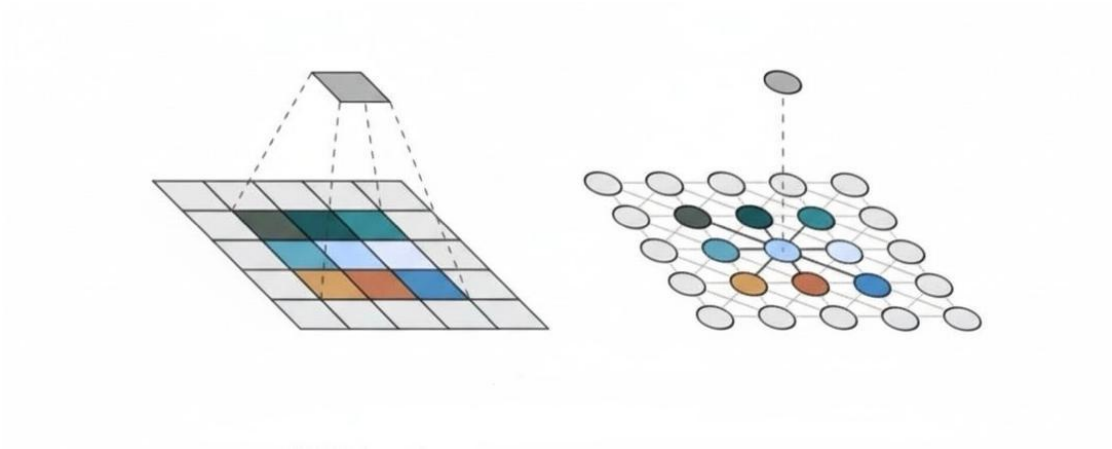

Figure 2.2: A comparison between CNN (left) and GCN (right)

Traditional CNN kernels can be seen as a special case of spatial GCN whose nodes are arranged in a grid graph, as in Figure 2.2. Given a graph $G = \{V, E\}$, the representation of any node is updated by aggregating the features of its neighboring nodes, as illustrated in Figure 2.3 [3], [28].

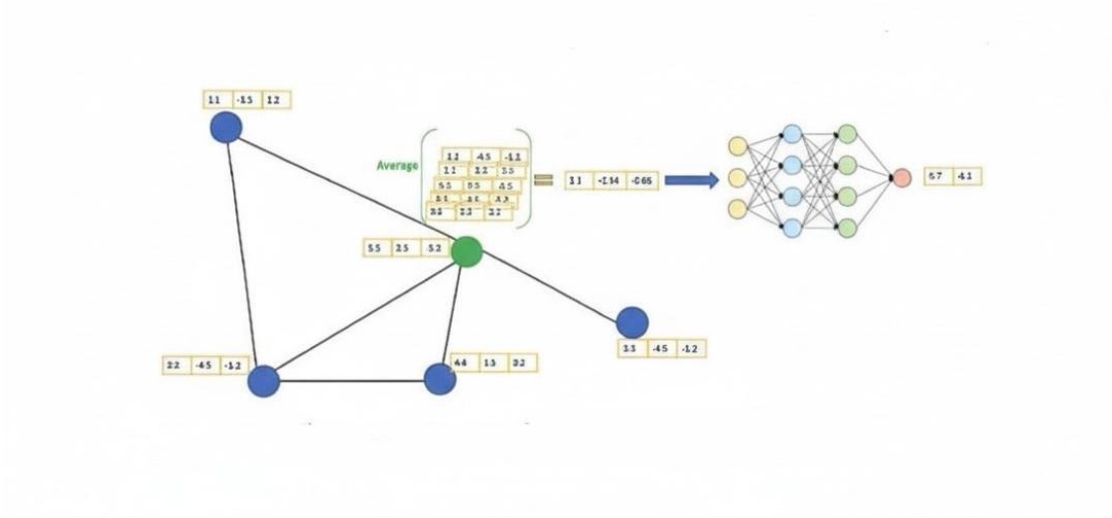

Figure 2.3: An example of forward propagation in a GCN

2.5.6 Random Forest

Random Forest is an ensemble learning method that builds a large number of decision trees on bootstrapped samples of the training data and aggregates their predictions by majority vote [30]. At each split only a random subset of the available features is considered, which decorrelates the individual trees and reduces the variance of the ensemble without a comparable increase in bias [9]. This property makes Random Forest

robust to noise and to the highly imbalanced class distributions that characterise fraud datasets, in which genuine calls vastly outnumber fraudulent ones.

Two characteristics make Random Forest a suitable comparison baseline for this study. First, it achieves competitive predictive accuracy on tabular call detail records without extensive hyper-parameter tuning, which makes it a fair reference point against which the configurational results can be assessed. Second, it produces a feature-importance ranking as a by-product of training: the average reduction in node impurity attributable to each feature across all trees measures how much that feature contributes to predictive performance [30]. This ranking is not a causal statement, since it describes predictive contribution rather than necessity or sufficiency, but it provides a direct point of comparison with the effect sizes produced by NCA.

The principal limitation of Random Forest is interpretability at the level of the individual decision. Although the aggregate feature importances are readable, the path by which any single call is classified is distributed across hundreds of trees and cannot be summarised compactly. Random Forest therefore remains a black-box model in the sense that matters for this study, which is precisely the gap the configurational methods are introduced to close [33], [36].

To conclude, every type of detection has its own advantages and limitations. Rule-based systems are simple and transparent but not flexible. Machine learning techniques enhance precision and flexibility but need labeled information and retraining. Graph models capture relational patterns and group behavior but are computationally expensive. Isolation Forest is an effective anomaly detector but does not consider network connections. These limitations show a pattern in the literature: most existing techniques are either accuracy-oriented at the expense of explainability, or simplicity-oriented at the expense of adaptability. This trade-off supports the investigation of new analytical tools, including Necessary Condition Analysis (NCA) and fuzzy-set Qualitative Comparative Analysis (fsQCA), which are discussed below as possible methods for gaining knowledge about the complex causal interactions and configurations underlying telecom fraud deterrence [31], [32].

2.6 Configurational Approaches: NCA and fsQCA

New analytical approaches have brought fresh insights into complex phenomena such as telecom fraud, where numerous variables are non-linearly interdependent. Conventional statistical and machine learning approaches tend to assume that causes have an independent or linear effect on results. In real-world conditions, however, fraud is usually the product of combinations of factors rather than of individual variables [8], [9].

Necessary Condition Analysis (NCA) presents a different view by identifying the conditions that are necessary, but not sufficient, for a particular outcome to occur. Regarding telecom fraud reduction, NCA can reveal key variables (such as regulatory enforcement, data transparency, or customer verification) that must be present to achieve successful fraud reduction, even though they cannot guarantee it on their own. NCA adopts a bottleneck strategy in which it measures the extent to which a condition is required to bring about a given level of performance or deterrence [31], [32].

Conversely, fuzzy-set Qualitative Comparative Analysis (fsQCA) allows researchers to examine how various combinations of causal variables give rise to specific outcomes. It extends single-variable testing to configurations of causes, is consistent with the multi-dimensionality of telecom systems, and can, for example, determine that a combination of strong internal monitoring, AI-based fraud detection, and collaboration between operators is needed to minimize fraud, even though none of the three factors is sufficient individually [33], [36].

Used in conjunction, NCA and fsQCA give an overview of telecom fraud deterrence. Whereas NCA emphasizes the minimum necessary conditions, fsQCA finds sufficient configurations. This combination provides a more realistic perspective on how organizational, technical, and behavioral factors interact to influence the outcome of fraud. These insights are particularly important for policy makers, regulators, and telecommunication players seeking to maximize resource use and enhance defense processes [31], [32].

2.7 Related Works

Researchers have proposed various models and frameworks for telecom fraud detection, ranging from graph-based approaches to deep learning and privacy-preserving models. This section reviews ten key studies that contribute to the understanding and advancement of fraud detection methods in telecommunication systems [3], [28].

In [10], cost-sensitive, reinforcement learning-enhanced graph networks were proposed for detecting fraud leaders in telecom fraud (TF), where Call Detail Record (CDR) data were transformed into a graph structure. Baseline classifiers such as GCN, GAT, and GraphSAGE were then employed. The concept of cost-sensitive learning was introduced in order to focus on specific classes, and the outputs of the baseline classifiers were subsequently weighted using a reinforcement learning algorithm (DDPG). Their extensive experiments on CDR data demonstrated that the proposed model is highly effective in detecting fraud leaders who operate behind the scenes, and it also outperformed other advanced models in this field. Nevertheless, their proposal faced several challenges, such as the limited size of the publicly available real dataset and the existence of broader opportunities for conducting research on dynamic graphs.

In [11], a more flexible and effective method was proposed by analyzing the content of the caller's speech itself. Their approach relies on a customized transformer architecture, which was further enhanced with techniques such as dynamic sparse attention, along with the selection of TOP_K and regularization sparsity, in addition to a manually reviewed knowledge graph to enrich the input data. Their extensive experiments, ablation analysis, and sensitivity analysis showed that their model significantly outperforms traditional methods in terms of accuracy, recall, and robustness in the field of telecom fraud.

In [12], the authors succeeded in validating a fraud detection model in a real-world scenario. They conducted comprehensive experiments and employed Latent Dirichlet Allocation to characterize accounts and Maximum Mean Discrepancy to match fraudulent accounts. They also verified the protection of users' private data during collaboration among multiple telecom operators. Their results showed that the improved detection model is capable of identifying fraudulent accounts with high accuracy in real-world situations and is suitable for the characteristics of real data. At the same time, they

confirmed that privacy protection does not affect performance when an appropriate level of Laplace noise is applied.

In [13], an integrated framework based on Large Language Models (LLMs) was proposed to improve both the quality of voice phishing datasets and the reliability of detection models, while addressing challenges such as distinguishing between fraudulent and non-fraudulent conversations. An LLM-based method was adopted to generate and enhance call transcripts, and detection criteria for voice phishing were embedded into a Domain Expert LLM. Experimental results showed that the generated data effectively alleviated the limitations of small-scale datasets, and that the analysis criteria aligned the model with operational needs in real-world practice.

In [14], a simple inference-based model called TrustCall was proposed to calculate the reputation of callers in web-based telecommunication networks. This work represented the first attempt to estimate trust in web-based communications in real time. The model was evaluated through several simulation-based experiments. Subsequent studies extended this work by utilizing communication behaviors to identify malicious peers and by supporting inter-domain communication frameworks.

In [15], a comprehensive review of existing solutions to caller ID spoofing was conducted, revealing several limitations. Based on these findings, a blockchain-based defense mechanism was proposed to mitigate spoofing attacks. The solution leverages blockchain immutability to create secure and decentralized call records, enabling reliable caller ID verification. The study also considered integration with SIP systems and discussed future directions such as scalability enhancement and compatibility with existing telecom infrastructures.

Jiang et al. [16], [17] introduced the Hawkes-Enhanced Sequence Model (HESM) to improve telecom fraud detection using large-scale behavioral data. Unlike prior studies focusing on individual behavioral sequences, this work modeled behavioral targets, companions, their interactions, and temporal dependencies. The HESM integrates a Hawkes process into Long Short-Term Memory (LSTM) networks, along with a historical attention mechanism and a correlation gate. Experiments on real-world datasets

demonstrated that HESM outperformed baseline models in accuracy and interpretability, effectively capturing subtle fraud-related behavior patterns.

Huo [18] proposed a deep learning-based telecom fraud detection model combining time series analysis with Graph Neural Networks (GNNs) to construct multidimensional feature representations. The model learns both temporal behavioral patterns and relational structures among communication entities. Experimental results showed improved detection accuracy, pattern discovery capability, and real-time warning performance, highlighting its applicability in practical telecom systems.

Zhao et al. [19] proposed a multi-dimensional telecom fraud detection model based on GATs. With the growing complexity of telecom fraud in 5G environments, traditional detection methods struggle to capture dynamic user relationships. The proposed model exploits GNNs to represent user interactions through graph structures derived from multi-dimensional data, including call records, billing information, device specifications, and user identifiers.

In [20], the GAT architecture was utilized to dynamically aggregate information from neighboring nodes to enhance node representations, followed by a Multi-Layer Perceptron (MLP) for classification. Experimental results demonstrated significant improvements in accuracy and robustness, especially in high-dimensional and dynamic telecom datasets. This study further strengthens the evidence supporting graph-based deep learning approaches in telecom fraud detection.

2.8 Research Gaps

This chapter identified several notable research gaps in the field of telecom fraud detection. These include the lack of causal understanding of the factors influencing fraud deterrence and the limited application of configurational approaches such as Necessary Condition Analysis (NCA) and fuzzy-set Qualitative Comparative Analysis (fsQCA). Other challenges involve data imbalance and privacy, the difficult trade-off between interpretability and model complexity, and the weak integration of technical, regulatory, and behavioral aspects within the current literature.

2.9 Summary

This chapter provided a comprehensive review of the literature related to fraud detection and mitigation methods in the telecommunications sector. It began by discussing the growing threat of telecom fraud and the insufficiency of traditional security measures against increasingly sophisticated attacks. Various types of telecom fraud were classified, including SMS phishing, SIM-box fraud, and International Revenue Share Fraud (IRSF), each exploiting specific system vulnerabilities. The pivotal role of Call Detail Records (CDRs) as a data source for detecting fraudulent communication patterns was emphasized.

Different fraud detection approaches were presented, including rule-based systems, machine learning techniques, graph-based methods, and the Isolation Forest algorithm, with an evaluation of their strengths and weaknesses. The chapter also introduced configurational analytical approaches, such as NCA and fsQCA, as innovative tools for understanding causal and multidimensional relationships in fraud deterrence [31], [32].

Recent related works were reviewed, focusing on the application of deep learning, Graph Neural Networks (GNNs), attention mechanisms, blockchain technology, and Large Language Models (LLMs) to enhance fraud detection accuracy, improve data quality, and ensure user privacy. Overall, the literature revealed a significant evolution in fraud detection methods, moving from rule-based systems towards advanced artificial intelligence and graph-based models [3], [28].

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter clarifies the approach followed in the study to achieve the research objectives. These objectives include analyzing the factors influencing the success of deterring telecommunications fraud using Necessary Condition Analysis (NCA) and Qualitative Comparative Analysis (QCA). Additionally, the chapter addresses the system design, the type of data used, and the tools and environment in which the experiments were conducted.

3.2 Mixed-Methods Framework: NCA and fsQCA

The proposed research design is a mixed-methods design, which combines quantitative and qualitative research to offer a holistic picture of the factors that affect telecom fraud, especially International Revenue Share Fraud (IRSF). The mixed-methods design was chosen because it allows the study to identify the necessary conditions (with the help of NCA) and to consider combinational causality (with the help of fsQCA) between the variables studied [31], [32].

The quantitative side of the study is the application of Necessary Condition Analysis (NCA) to identify the minimum conditions necessary for telecom fraud to occur. NCA can be used to establish whether a certain factor must exist for a particular outcome to exist. The qualitative aspect, Fuzzy-set Qualitative Comparative Analysis (fsQCA), on the other hand, examines the levels of membership of various causal conditions and how their combination results in the outcome [31], [32].

The justification for this mixed-methods approach is that the two methods are complementary. Whereas NCA offers a clue to the fundamental components that must be in place for telecom fraud to occur, fsQCA gives insight into the interactions of various components in complex causal patterns. This combination guarantees a stronger and more

detailed analysis that meets the aims of the research and the multi-dimensional character of telecom fraud [31], [32].

3.2.1 Fuzzy Set Calibration and Degrees of Membership

In the fsQCA model, every condition and outcome is modeled as a fuzzy set [33], [35]; that is, cases do not simply belong or not belong to a set. Instead, they have degrees of membership ranging from 0 (full non-membership) to 1 (full membership). This enables the analysis to capture the reality of telecom fraud situations, in which factors are not merely present or absent but exist in different degrees. Calibrating the data into these fuzzy scores allows the study to determine the combinations of causal conditions that consistently result in the occurrence of fraud. This provides an analytical level that traditional binary or linear models cannot provide.

Calibration in this study used the direct method implemented in the QCA package for R, with three anchors per condition: full non-membership, the crossover point, and full membership. Call duration was calibrated at 30, 120 and 300 seconds, placing the crossover at two minutes so that calls shorter than this are treated as members of the short-call set. Call type was calibrated at 0, 0.5 and 1 to separate domestic from international traffic. Origin and destination were converted to numeric category codes and calibrated at 1, 2 and 3. The truth table was then constructed with an inclusion cut-off of 0.10, chosen to retain the empirically populated configurations, and the solution was derived by Quine–McCluskey minimisation. The overall research process is summarized in Figure 3.1, which outlines the main methodological steps followed in this study [33], [36].

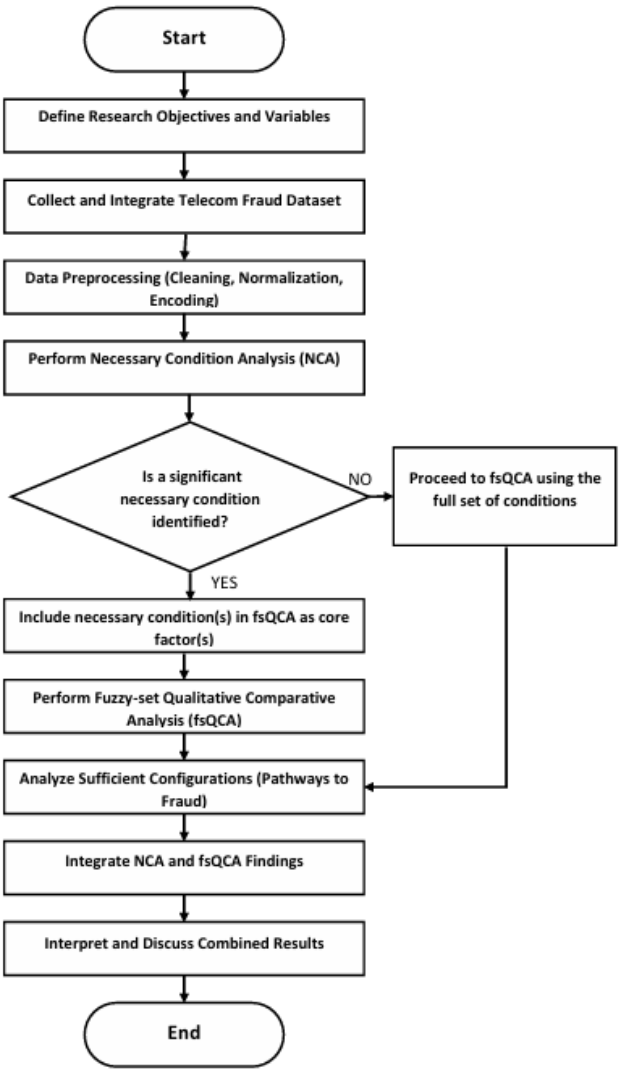

Figure 3.1: Algorithmic flowchart of the integrated NCA–fsQCA methodology

3.3 Abductive Approach: NCA and fsQCA Integration

The present study is mixed (abductive) research, in that both qualitative and quantitative reasoning are incorporated to gain a comprehensive picture of the causes of telecom fraud. Necessary Condition Analysis (NCA) represents the quantitative perspective and is used to identify and measure the conditions that are necessary for telecom fraud to occur. Meanwhile, the qualitative-comparative aspect is represented by Fuzzy-set Qualitative Comparative Analysis (fsQCA), which examines whether various configurations of causal conditions are sufficient to produce fraudulent outcomes [31], [32].

By combining these two approaches, the study benefits from both analytical accuracy and depth, gaining a subtle insight into the complicated processes of fraud that would not be revealed by a single method. This abductive reasoning enables the researcher to move back and forth between theory and data, discovering patterns, testing them, and refining the understanding of causal connections in telecom fraud detection [8], [9].

3.4 Integrated NCA–fsQCA Framework

3.4.1 Conceptual Foundation: Necessity and Sufficiency

This section presents the conceptual framework and theoretical modeling used in this study. The conceptual model integrates both Necessary Condition Analysis (NCA) and Fuzzy-set Qualitative Comparative Analysis (fsQCA) within a unified analytical framework for telecom fraud deterrence. The model assumes that the occurrence of telecom fraud is influenced by a combination of technical, behavioral, and contextual variables. This approach aligns with complexity theory and the principles of causal asymmetry, emphasizing that different configurations of factors can lead to the same outcome. A core tenet of the model is that no single factor alone is sufficient to cause fraud. Rather, certain variables act as necessary conditions, while other variables combine to form sufficient pathways leading to fraudulent behavior [31], [32].

3.4.2 Variable Definition: Conditions and Fraud Outcome

The model specifies the independent variables (conditions) and the dependent variable (outcome). The conditions under analysis include call duration, call type, is_night_call, location origin, location destination, SIM ID patterns, and transaction status. The dependent variable is fraud occurrence, denoted by fraud_label = 1 for fraudulent cases and 0 otherwise.

The relationships between the conditions and the outcome are modeled as non-linear and asymmetric. This fundamental characteristic means that the presence of certain variables may be necessary but not sufficient for fraud to occur, while different combinations of factors can jointly result in fraudulent activity. This modeling logic is consistent with the

analytical perspectives of NCA and fsQCA, methods specifically designed to capture both necessity and sufficiency patterns within complex telecom environments [31], [32].

3.4.3 Core Propositions: Necessary Conditions and Sufficient Configurations

The conceptual model is built upon several underlying assumptions. It is assumed that the dataset represents genuine telecom activity logs derived from real or simulated Call Detail Records (CDRs). All variables are assumed to be preprocessed, normalized, and encoded to ensure valid comparison across conditions. Furthermore, the model assumes that fraud emerges from multiple causal combinations rather than from a single linear relation. Specific to the methodologies, NCA assumes the existence of bottleneck conditions that limit the achievement of fraud deterrence, while fsQCA assumes equifinality, meaning that multiple different configurations of conditions can lead to the same outcome. Although NCA and fsQCA are primarily exploratory rather than confirmatory methods, this study proposes two research propositions to guide the interpretation of the configurational results. Hypothesis 1 (H1) proposes that certain conditions, such as high call duration or frequent international calls, are necessary for fraud to occur. Hypothesis 2 (H2) proposes that specific combinations of conditions, such as international call + night call + a specific SIM ID pattern, are sufficient to produce fraudulent behavior [31], [32].

3.4.4 Validation Protocol: NCA Effect Size and fsQCA Consistency

To ensure the credibility and robustness of the integrated model, specific validation procedures were conducted. NCA validation involved evaluating effect sizes (d) and ceiling zones to confirm the strength and significance of the necessary conditions. fsQCA validation involved assessing consistency and coverage metrics to verify the adequacy of the sufficient configurations. Comparative validation was carried out by comparing the findings with prior telecom fraud detection studies to ensure empirical alignment. Lastly, cross-verification was performed to ensure logical coherence between the NCA and fsQCA results, confirming that the necessary conditions identified by NCA align with the sufficient configurations derived from fsQCA [31], [32].

3.4.5 Mathematical Formulation of NCA

This subsection presents the mathematical formalization of the NCA procedure used in this study. NCA identifies necessary conditions [31], [32] by estimating upper-bound patterns (ceiling lines) in the XY-space and evaluating the empty area above these boundaries. The following equations define the ceiling line, ceiling area, effect size, and bottleneck function used to quantify necessity relationships among the telecom fraud variables.

Equation (3.1): Linear ceiling line. A ceiling line represents the empirical boundary that no observation exceeds. A simple linear ceiling function is expressed as: [31], [32]

$$y_{ceiling}(x) = a + bx \tag{3.1}$$

Equation (3.2): Ceiling area. The ceiling area reflects the upper empty region in the XY-space and is calculated as:

$$A_{ceiling} = \int_{x_{min}}^{x_{max}} (y_{max} - y_{ceiling}(x))\, dx \tag{3.2}$$

Equation (3.3): Effect size. The NCA effect size *d* quantifies the proportion of the ceiling area relative to the total feasible XY-space: [31], [32]

$$d = \frac{A_{ceiling}}{(x_{max} - x_{min})(y_{max} - y_{min})} \tag{3.3}$$

Equation (3.4): Bottleneck calculation. For any target outcome level y∗, the minimum value of the condition required to reach that outcome is obtained from the ceiling line as: [31], [32]

$$x_{min}(y*) = \frac{y* - a}{b} \tag{3.4}$$

Figure 3.2 illustrates the step-by-step process for identifying the conditions that must be present for telecom fraud to occur, from data input to bottleneck analysis [31], [32].

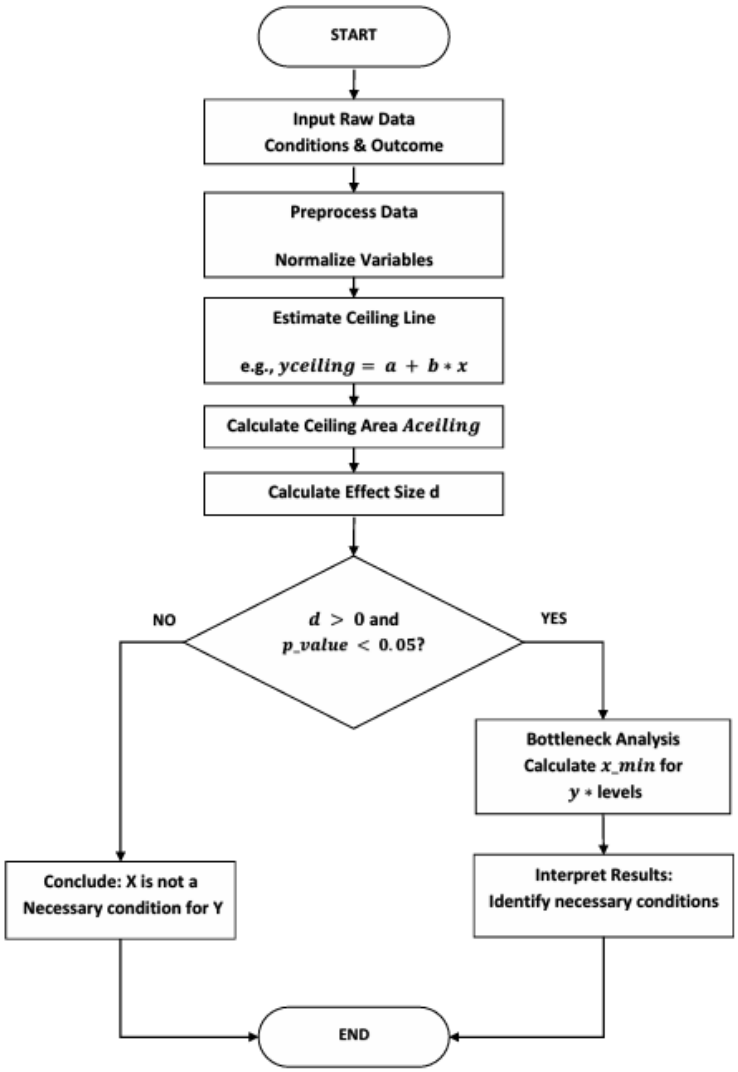

Figure 3.2: Algorithmic flowchart of the Necessary Condition Analysis (NCA) procedure

3.4.6 Mathematical Formulation of fsQCA

This subsection presents the mathematical expressions used in the fsQCA procedure. fsQCA relies on fuzzy-set memberships, consistency, and coverage [33], [34] to assess the sufficiency of different configurations of conditions. The equations that follow formalize sufficiency consistency, empirical coverage, and the Boolean expressions used in reporting final solution pathways.

Equation (3.5): Consistency. Consistency evaluates how closely a configuration is sufficient for producing the outcome: [34]

$$Consistency = \frac{\sum_i min(\mu_{X(i)}, \mu_{Y(i)})}{\sum_i \mu_{X(i)}} \tag{3.5}$$

Equation (3.6): Coverage. Coverage measures the empirical relevance of a sufficient configuration: [34]

$$Coverage = \frac{\sum_i min(\mu_{X(i)}, \mu_{Y(i)})}{\sum_i \mu_{Y(i)}} \tag{3.6}$$

Equation (3.7): Boolean solution. fsQCA solutions are expressed in simplified Boolean form. A generic example is: [33], [36]

$$Y = X_1X_2 + X_3(-X_4) \tag{3.7}$$

Figure 3.3 shows the process for discovering combinations of conditions that lead to fraud, from fuzzy-set calibration to Boolean solution derivation [33], [36].

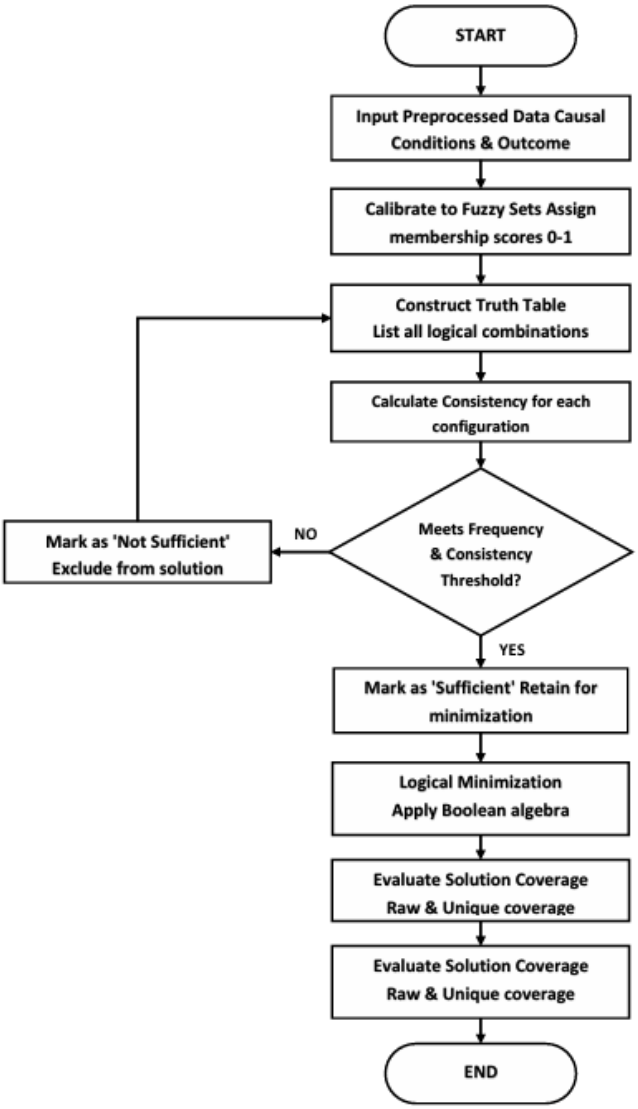

Figure 3.3: Algorithmic flowchart of the Fuzzy-Set Qualitative Comparative Analysis (fsQCA) procedure

3.4.7 Predictive Validation Using Random Forest

Alongside the configurational analysis, a Random Forest classifier was trained on the same fully numeric dataset described in Section 4.2. Its role in this study is deliberately narrow: it is not proposed as the detection mechanism, but as an independent predictive check on the variables that NCA and fsQCA identify as analytically important [31], [32].

The classifier was trained to predict the recorded fraud category from the call attributes, across all six categories present in the data rather than a binary SIM box fraud indicator, so that its ability to separate SIM box fraud from adjacent fraud types could also be

assessed. Because fraudulent records form a minority of the dataset, the split of records into training and test partitions was stratified on the outcome, so that the proportion of fraudulent cases is preserved in both and the test partition retains enough positive cases to be evaluated meaningfully [12], [20].

The output taken from the trained model is a feature-importance ranking, which orders the call attributes by their contribution to predictive accuracy across the trees of the ensemble [30], [37]. This ranking is reported in Section 4.4.4 and read against the NCA effect sizes obtained in Section 4.3.

The purpose of including this component is triangulation rather than benchmarking. NCA answers which conditions must be present, fsQCA answers which combinations are sufficient, and the Random Forest ranking answers which attributes carry predictive signal. The three are applied independently to the same data rather than chained, so that no result is conditioned on another. Where they agree the finding is well supported; where they disagree the disagreement is itself informative, because a variable can carry substantial predictive weight while imposing no necessity constraint at all. This distinction is examined in Section 4.4.4 [31], [32].

3.5 Methodological Limitations

Although this study follows a systematic approach, it has several methodological limitations that may affect the findings. Some of the most important challenges relate to the accessibility and authenticity of data, since real telecommunications data can rarely be accessed because of privacy issues. The researchers therefore used simulated or publicly available datasets, which might not effectively reflect emerging frauds such as AI-driven or multi-channel fraud. Data imbalance is also present, as fraudulent cases make up only a small fraction of the records. Methods such as oversampling and SMOTE have been used to achieve balance, although balance remains difficult. Combining the NCA and fsQCA techniques was also challenging, as the two techniques have different underlying assumptions and require explicit calibration [31], [32].

Generalizability is also limited because the findings are restricted to a particular model and dataset and may not transfer to different regulatory or technological contexts.

Preprocessing may also have technical constraints that obscure information and influence the sensitivity of variables. Despite reliability checks against past research, there is a lack of large-scale longitudinal data for comprehensive validation. The study addressed these shortcomings through realistic simulation, careful preprocessing, and the integration of NCA and fsQCA analysis [31], [32].

3.6 Summary

This chapter outlined the methodological foundation of the study and explained how the research was structured to investigate the key factors influencing telecom fraud deterrence. The chapter began by presenting the overall research design, which adopted a mixed-methods approach combining both quantitative and qualitative reasoning. This approach was chosen to capture the complex nature of fraud deterrence, where multiple interacting factors operate simultaneously rather than in isolation.

The discussion then elaborated on how Necessary Condition Analysis (NCA) and Fuzzy-set Qualitative Comparative Analysis (fsQCA) were integrated into a unified analytical framework. Through NCA, the study identified the minimum essential conditions that must be present for telecom fraud to occur, while fsQCA explored the combinations of factors that, when co-existing, can lead to fraudulent outcomes. Together, these complementary methods offered both analytical precision and contextual depth, reflecting the multidimensional structure of telecom systems [31], [32].

A detailed conceptual model was presented to illustrate how technical, behavioral, and contextual variables interact to influence fraud occurrence. The model incorporated core variables derived from telecom data, such as call duration, call type, location origin and destination, SIM ID patterns, and transaction status, highlighting their non-linear and asymmetric relationships with the fraud outcome. Two guiding propositions were introduced to connect the theoretical model to the empirical analysis.

The chapter also discussed the methodological limitations, including data availability, imbalance, and integration complexity between NCA and fsQCA. Despite these challenges, the study applied rigorous preprocessing, normalization, and consistency

checks to ensure the robustness of the findings. The use of realistic simulated data and cross-validation with previous research further enhanced the model's credibility [31], [32].

Overall, this methodology chapter establishes a transparent and comprehensive roadmap for the research process. It sets the stage for Chapter 4, which focuses on the application of the model, analysis of results, and interpretation of the findings, thereby translating the proposed framework into measurable outcomes that can inform more effective telecom fraud prevention strategies [9], [25].

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the results and discussion of applying the integrated Necessary Condition Analysis (NCA) and Fuzzy-set Qualitative Comparative Analysis (fsQCA) framework to identify SIM box fraud in telecommunications. It starts by examining the properties of the dataset and its preprocessing, then determines the conditions necessary for fraud using NCA and identifies sufficient causal configurations using fsQCA. This two-method strategy improves the understanding of telecom fraud compared with other methods. A validation process is used to verify the reliability of the results and to derive operational recommendations for telecom operators to enhance fraud detection and prevention systems.

4.2 Dataset Summary and Preprocessing

The dataset used in this analysis was sourced from Kaggle under the name "realtime_cdr_fraud_dataset.csv". It contains 14 columns and 24,543 rows of call logs. The dataset covers several types of fraudulent activity recorded under the "fraud_type" column, including none, sim_box_fraud, call_masking, subscription_fraud, and random_fraud. Despite the variety of types, we decided to focus on the SIM box fraud type, as it represents the core of our study and the subject of our analysis.

Before starting the analysis, we verified the completeness of the data and ensured that it was free of missing values or invalid entries. The examination confirmed that the data was 100% complete, with no empty cells or anomalous values requiring processing, allowing immediate use without further cleaning. The dataset contains four numeric columns: caller_id, receiver_id, duration_sec, and is_night_call. The remaining columns contain categorical data, including start_time, call_type, sim_id, device_id, location_origin, country_origin, location_dest, country_dest, transaction_status, and fraud_type.

A note on the nature of this dataset is necessary before the results are presented, because it bears on how every figure in this chapter should be read. The file is a public benchmark that simulates telecommunications traffic rather than a record of live operator activity. Several structural features make this clear: each of the 24,543 records carries a distinct caller and receiver number, so no subscriber appears twice, whereas in operational traffic a small number of subscribers generate a large share of calls; the timestamps take only about a thousand distinct values across a full month, with thousands of calls sharing a single second; and the duration of every SIM box record falls within a closed range of ten to fifty seconds while all other categories extend beyond twenty minutes. The fraud label is likewise assigned by rule rather than by investigation [36], [37].

Operator call detail records are commercially sensitive and are not released for academic use, so a simulated public benchmark is the standard substitute at this level of study, and it is entirely adequate for demonstrating and comparing analytical methods, which is the purpose of this work. It does, however, place a firm boundary on the claims that can be made. High consistency and accuracy figures obtained here reflect the regularity of the data-generating process as much as the strength of the methods, and they are not estimates of how the framework would perform on live traffic, where labels are noisy, incomplete, and not produced by any fixed rule. Validation on operator data remains necessary before any operational claim can be made, and is identified as a priority for future work in Section 5.2 [36], [37].

4.2.1 Dataset Statistical Analysis

The dataset was analyzed with a focus on detecting sim_box_fraud, in order to identify differences between genuine and fraudulent calls and to determine indicators that could help in detecting fraudulent activity.

First, the caller_id and receiver_id columns were examined for duplicates. The results showed that all IDs in both columns are unique, meaning that ID repetition is not a relevant indicator for fraud detection in this dataset. The data was then filtered to include only normal calls (none, 12,223 records) and fraudulent calls of type sim_box_fraud (3,096 records), giving an analysis subset of 15,319 records. It is important to be precise about which results rest on which population. Every analysis reported in this chapter was run on

this filtered subset of 15,319 records, so that the necessity, configurational and predictive results all rest on the same cases and can be compared directly, which is why the case counts in Table 4.4 sum to 15,319 rather than to 24,543 [37].

The analysis of call duration shows that fraudulent calls are very short and consistent, with an average of approximately 30 seconds and a median of 30 seconds, ranging from 10 to 50 seconds. Normal calls have a much wider range, with an average of 184 seconds, a median of 128 seconds, and a maximum duration of 1,840 seconds. These differences make call duration an important indicator for distinguishing fraudulent calls from normal calls. We also noticed that fraudulent calls (sim_box_fraud) represent approximately 20% of all calls, while normal calls account for around 80%, which reflects the extent of fraudulent activity in the dataset.

A boxplot comparing SIM box fraud and non-fraudulent call durations was also created (Figure 4.1). The plot clearly shows that fraudulent calls are short and clustered around 30 seconds, while normal calls are longer and more widely distributed.

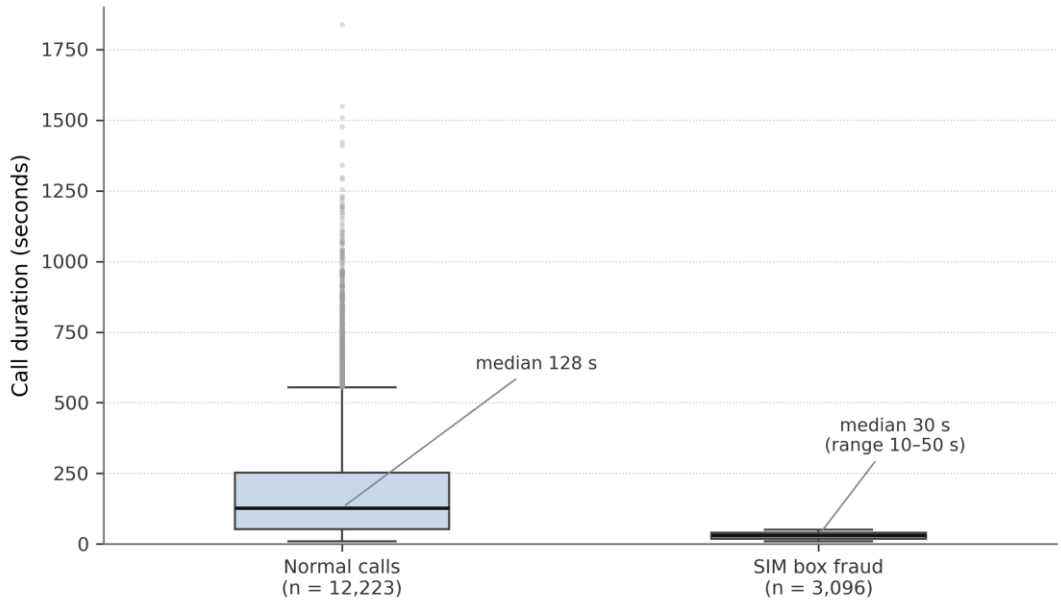

Figure 4.1: Boxplot of call duration for SIM box fraud and normal calls

4.2.2 Data Transformation and Encoding

The original dataset was first cleaned and transformed into a fully numeric structure to ensure suitability for quantitative analyses such as NCA and fsQCA, and several

preprocessing steps were applied. Categorical variables were recoded into numerical representations: the fraud type variable was filtered to include only two categories, “sim_box” and “none”, and was converted into a binary variable in which sim_box was assigned the value 1 and none was assigned 0. The transaction status variable was similarly transformed, with “Fraudulent” as 1 and “Genuine” as 0. Call type was also converted into a binary format, where “international” calls were coded as 1 and “local” calls as 0 [37].

For the SIM ID and Device ID fields, all non-numeric prefixes such as “SIM” and “DEV” were removed, retaining only the numerical component of each identifier and ensuring consistent numeric formatting across the dataset. Origin and destination location variables, which originally consisted of country names or categorical location labels, were transformed into factors and then converted to numeric codes using the factor() and as.numeric() sequence. This procedure allowed the model to treat each country or location as a unique category without implying any mathematical relationship among them [37].

A further transformation was applied specifically for the necessary condition analysis. Each of the thirteen predictors was first converted to an integer code, with categorical variables mapped to their factor levels in alphabetical order, and the resulting values were then replaced by their ranks within the column, using the average of the tied ranks where values repeat. Rank transformation places every predictor on a common scale and prevents variables with very large numeric ranges, such as the caller and receiver identifiers, from dominating the geometry of the XY-space in which the ceiling line is estimated.

This step has an implication that must be stated plainly, because it bears directly on how the effect sizes in Section 4.3 should be read. For a genuinely ordinal or continuous variable such as call duration, the ranks preserve the ordering that the variable already carries, and the resulting ceiling line is meaningful. For a nominal variable such as transaction status or a bare identifier such as SIM ID, the ordering imposed by alphabetical factor levels is arbitrary: it is a property of how the category labels happen to be spelled rather than of the underlying concept. Effect sizes computed for nominal predictors are therefore sensitive to label ordering and should be interpreted as indicating that a

constraint exists rather than as calibrated measurements of its strength. Section 4.3.1 returns to this point in the context of the specific results obtained.

After completing all recoding and standardization steps, the dataset was converted fully into numeric format and filtered to retain only the processed variables. The resulting final dataset consists solely of clean, numeric variables ready for NCA and fsQCA analysis, ensuring methodological rigor and consistency across all analytical procedures.

4.3 Performance Evaluation

Because the methodology relies on Necessary Condition Analysis to identify the conditions required for SIM box fraud to occur, performance evaluation focuses on necessity and efficiency measures rather than on classification metrics. NCA asks which variables place a ceiling on the outcome, and the quality of that ceiling is judged by its effect size, by how much of the observed space is left empty above it, and by the accuracy with which it bounds the data.

Before these measures are reported, the set of conditions admitted to the analysis must be stated, because it differs from the set available in the raw file. Two recorded fields were excluded. The first is transaction status: as established in Section 4.5.1, this field is populated after a transaction has been assessed, and in this dataset the value Fraudulent corresponds exactly to the union of the four fraud categories. It is a restatement of the outcome rather than a condition that precedes it. The second is the SIM identifier: records belonging to subscription fraud carry the distinguishing prefix SIM_FAKE_, so the field encodes the fraud category directly in its text. Both fields were therefore removed from every analysis reported in this chapter [31], [32].

The remaining conditions are call type, call duration, device identifier, origin and destination city, origin and destination country, and the night-call indicator. Each is recorded by the network while a call is being processed and none is written by a downstream fraud-review process, so none can encode the outcome. The caller and receiver numbers were also dropped, not because they leak but because every record carries a distinct value for both, leaving them without information content [31], [32].

A further adjustment concerns the direction in which duration is tested. Necessity is directional: testing whether a high value of a condition is required is not the same as testing whether a low value is required. SIM box traffic is characterised by very short calls, so duration was entered as shortness, computed as the observed maximum minus the recorded duration. Both directions are reported in Table 4.1 so that the difference is visible [31], [32].

4.4 Necessity Results and Feature Importance

4.4.1 Effect Size Analysis

The effect size measures the strength of the constraint a condition places on the outcome, on a scale from zero to one. A value approaching one means that almost the whole of the observed space above the ceiling is empty, so the outcome is tightly bounded by the condition. Results for the eight admitted conditions are given in Table 4.1.

Table 4.1: NCA results for SIM box fraud (CE-FDH ceiling, leakage-free conditions)

Condition	Ceiling zone	Effect size	Fit	Rel. ineff. (%)
Call type (local < international)	1.0	1.000	100%	0.00
Call shortness (1840 − duration)	1790.0	0.978	100%	2.19
Call duration (as length)	0.0	0.000	100%	–
Device ID	0.0	0.000	100%	–
Origin city	0.0	0.000	100%	–
Origin country	0.0	0.000	100%	–
Destination city	0.0	0.000	100%	–
Destination country	0.0	0.000	100%	–

Two conditions constrain the outcome and the remaining six do not. Call type returns an effect size of 1.000: every one of the 3,096 SIM box records is an international call, and no local call in the dataset is labelled as SIM box fraud. The ceiling is therefore complete in this direction. This is consistent with the mechanism itself, since SIM box fraud exists precisely to carry international traffic onto a local network, and it is a constraint an operator can act on rather than a restatement of the label.

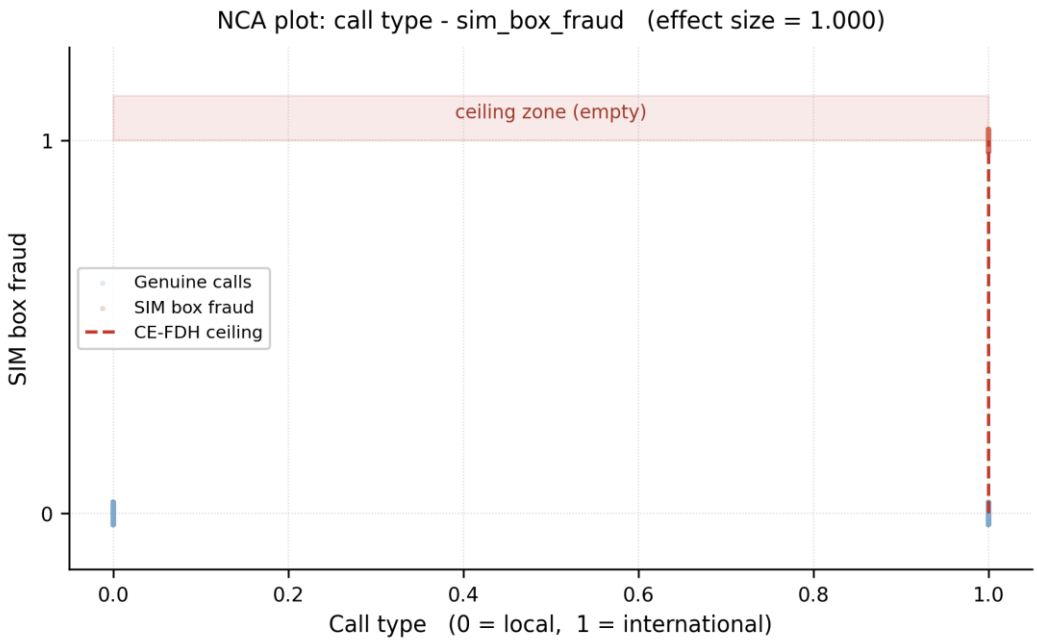

Figure 4.2: NCA plot of call type against SIM box fraud

Call shortness returns an effect size of 0.978, with a ceiling zone of 1,790 and relative inefficiency of 2.19%. Fraudulent calls in this dataset never exceed fifty seconds, against an observed range extending to 1,840 seconds, so almost the entire upper-left region of the plot is empty. The constraint is strong but, unlike call type, not absolute: roughly a quarter of genuine calls also fall below fifty seconds, which is why shortness is necessary without being sufficient.

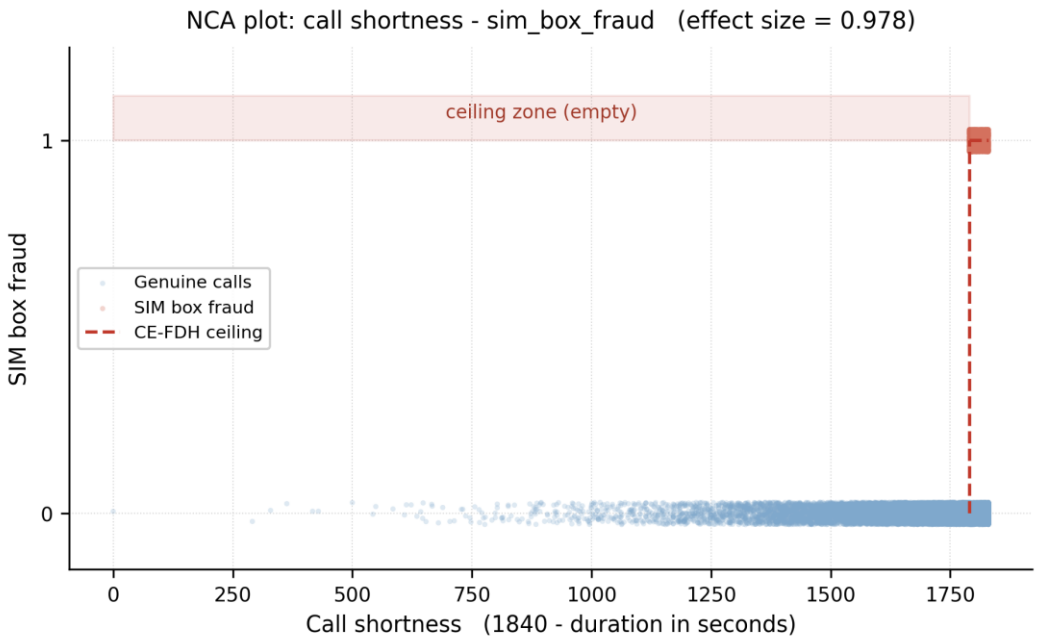

Figure 4.3: NCA plot of call shortness against SIM box fraud

The contrast between the two duration rows in Table 4.1 illustrates why direction matters in a necessity analysis. Entered as length, duration returns an effect size of zero, because fraud is observed at the very bottom of the duration range and nothing prevents it occurring there. Entered as shortness, the same variable returns 0.978. The variable has not changed; the question asked of it has. Reporting only the first result would have led to the conclusion that call duration is irrelevant to SIM box fraud, which the data plainly contradicts.

The six remaining conditions return effect sizes of zero. Fraud occurs across the full observed range of device identifier, origin and destination city, and origin and destination country, so none of them bounds the outcome. The night-call indicator takes the value one in only 1.1% of records and is effectively constant, so no ceiling can be estimated for it at all.

4.4.2 Predictive Comparison Using Random Forest

A Random Forest classifier was trained on the same leakage-free conditions to provide an independent predictive view, following the procedure in Section 3.4.7. The model used 500 trees over the eight admitted predictors, was fitted on a stratified 70% sample of the

15,319 records in the analysis subset, and was evaluated on the remaining 30%. Results are given in Table 4.2 [31], [32].

Table 4.2: Random Forest performance on leakage-free conditions

Measure	Value
Accuracy	0.950
Cohen's Kappa	0.853
Precision (fraud class)	0.810
Recall (fraud class)	0.975
F1-score (fraud class)	0.885

This result is worth comparing with what the same model produces when the excluded fields are put back. With transaction status among the predictors the classifier separates the classes without a single error, returning an accuracy of 1.000. That figure measures nothing: the model is reading a field that restates the label. Removing it lowers accuracy to 0.950, and the resulting errors are informative rather than embarrassing. The classifier now recovers 97.5% of fraudulent calls at a precision of 0.810, meaning it over-flags rather than under-detects, which is the behaviour a screening system should have when a missed fraud costs more than a review [31], [32].

The variable importance produced by the trained model is given in Table 4.3 and shown in Figure 4.4. Two measures are reported: the mean decrease in Gini impurity and the mean decrease in accuracy obtained by permuting each variable in turn.

Table 4.3: Random Forest variable importance on leakage-free conditions

Rank	Feature	Mean decrease in Gini	Mean decrease in accuracy
1	duration_sec	1367.73	93.62
2	call_type	1032.42	99.60
3	device_id	119.23	1.01
4	country_origin	20.68	2.08
5	country_dest	20.40	0.30
6	location_origin	19.79	1.04
7	location_dest	19.67	0.68
8	is_night_call	0.00	0.00

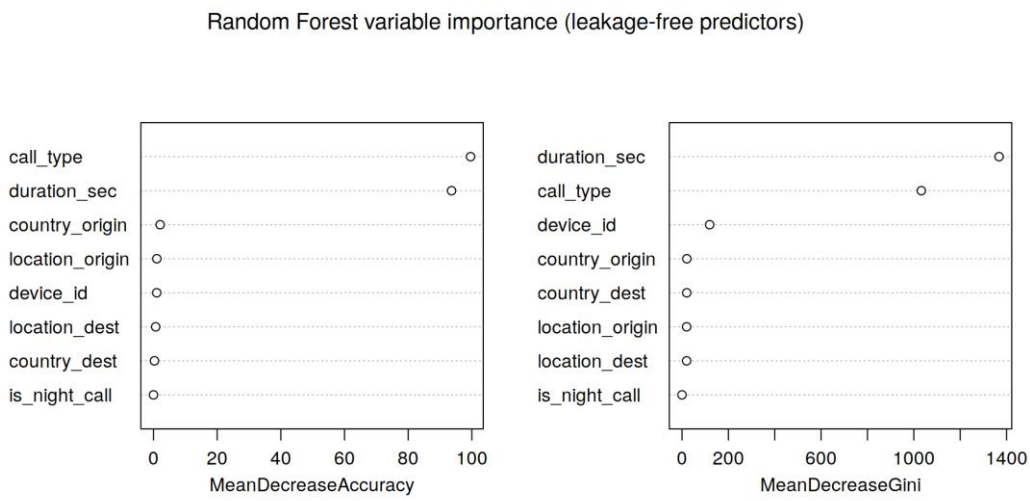

Figure 4.4: Random Forest variable importance on leakage-free conditions

Call duration and call type together account for essentially all of the predictive signal on both measures. Device identifier follows at a small fraction of their weight, and the geographic and temporal fields contribute almost nothing; the night-call indicator contributes exactly zero on both measures, consistent with its near-constant value.

The agreement with the necessity analysis is close and is the central result of this chapter. Call type and call duration are the only two conditions that impose a ceiling on the outcome, and they are the only two that a predictive model finds informative. Two methods resting on different logics, one asking what must be present and the other asking what separates the classes, converge on the same pair of behavioural conditions once the fields that restate the label have been removed.

The residual difference between them is instructive. Call type is an absolute constraint, with an effect size of 1.000, yet the classifier ranks duration marginally above it on the Gini measure. This is because call type alone cannot separate the classes: 3,703 genuine calls in the analysis subset are also international, so a model relying on it would raise a large number of false alarms. Duration narrows the field further. Necessity and predictive usefulness are therefore complementary properties rather than competing ones, and an operator would use both: call type to define which traffic can contain SIM box fraud at all, and duration to rank that traffic for investigation.

4.5 fsQCA Results and Causal Pathway Interpretation

4.5.1 Initial Specification and Its Withdrawal

The configurational analysis was first specified with two conditions, call type and transaction status. That specification is reported here because it shaped the direction of the study and because the reason it was subsequently withdrawn is itself a substantive methodological finding. The truth table (Table 4.4) showed that, among all possible combinations of conditions, only one configuration resulted in the outcome fraud_binary = 1, namely the cases in which call_type_binary = 1 (international calls) and transaction_binary = 1 (fraudulent transactions) occur simultaneously. This configuration accounted for a total of 3,096 cases with a perfect consistency score of 1.00, indicating that whenever this combination of conditions appears, fraud always occurs without exception. In contrast, the other configurations, such as local calls or legitimate transactions, consistently led to the absence of fraud, with a consistency score of 0.00.

Table 4.4: fsQCA truth table for call type and transaction status

Call_type_binary	Transaction_binary	OUT	n	incl	PRI
0	0	0	8,520	0.000	0.000
1	0	0	3,703	0.000	0.000
1	1	1	3,096	1.000	1.000

Interpretation:

- **Configuration (1, 1 → OUT = 1):** International calls combined with fraudulent transactions always lead to fraud (perfect consistency and PRI = 1.000).
- **Other configurations (0, 0 and 1, 0):** Always lead to non-fraud outcomes, with consistency and PRI = 0.000.

A consistency of exactly 1.000 with no exceptions across 15,319 cases is an implausible result for operational fraud data, and on re-examination the reason became clear. The transaction status field is not an antecedent of fraud but a flag assigned once a transaction has been assessed: every record marked sim_box_fraud carries the value Fraudulent, and every record carrying that value is marked sim_box_fraud. The condition therefore encodes the outcome it was meant to explain, and the configuration is circular rather than

causal. A detection system could not use it, because the value is not available at the moment a call is processed. This specification was accordingly withdrawn and the analysis re-run, as described in the next section.

4.5.2 Revised Analysis Using Behavioural Conditions

The analysis was therefore re-specified using only attributes that are recorded while a call is processed and that exist independently of any fraud assessment. Four behavioural conditions were retained: call duration (df), call type (cf), origin (of) and destination (d_f). Transaction status was excluded, together with any other field generated after an outcome has been determined. Each remaining condition was checked against this criterion: all four are derived from call detail records produced at the call-processing stage and none is populated by a downstream fraud-review process, so no condition can encode the outcome. This re-specified model is the analysis on which the conclusions of this study rest. The revised truth table contains 16 configurations of the conditions df, cf, of and d_f with their associated fraud outcomes (OUT), as presented in Table 4.5. The deterministic pattern of the initial specification does not survive the change: no configuration now reaches a consistency above 0.54, which is what should be expected when fraud arises from the interaction of several partial conditions rather than from a field that already records it. The results reveal clear contrasts between non-fraud and fraud-producing configurations [31], [32].

Table 4.5: Extended fsQCA truth table (16 configurations)

Row	df	cf	of	d_f	OUT	n	incl	PRI
1	0	0	0	0	0	78	0.083	0.083
2	0	0	0	1	0	437	0.064	0.064
3	0	0	1	0	0	415	0.067	0.067
4	0	0	1	1	0	2,055	0.049	0.049
5	0	1	0	0	1	94	0.443	0.443
6	0	1	0	1	1	498	0.501	0.501
7	0	1	1	0	1	501	0.503	0.503
8	0	1	1	1	1	2,462	0.540	0.540
9	1	0	0	0	0	93	0.071	0.071
10	1	0	0	1	0	455	0.056	0.056
11	1	0	1	0	0	419	0.058	0.058
12	1	0	1	1	0	2,304	0.041	0.041
13	1	1	0	0	1	43	0.112	0.112
14	1	1	0	1	1	181	0.101	0.101
15	1	1	1	0	1	218	0.101	0.101
16	1	1	1	1	0	960	0.086	0.086

Highlighted rows are configurations with a fraud outcome (OUT = 1).

Non-fraud configurations (OUT = 0): Rows 1–4 and 9–12 consistently yield non-fraud outcomes, with low inclusion and PRI values (≤ 0.083). Even high-frequency cases, such as row 12 (df = 1, cf = 0, of = 1, d_f = 1, n = 2,304), remain non-fraud, indicating that traffic volume alone does not drive fraudulent behavior [25], [21].

Fraud-producing configurations (OUT = 1): Rows 5–8 and 13–15 consistently yield fraud outcomes. These are characterized by the presence of cf = 1 (call type condition).

- The strongest fraud-producing configuration is row 8 (df = 0, cf = 1, of = 1, d_f = 1), with n = 2,462, inclusion = 0.540, and PRI = 0.540.
- Rows 6 and 7 also show high fraud consistency (incl ≈ 0.50), confirming that fraud emerges when call type is active, regardless of origin–destination variation.
- Rows 13–15 (df = 1, cf = 1) produce fraud outcomes but with lower inclusion values (≈ 0.10), suggesting marginal fraud patterns.

Mixed signals: Fraud is absent in configurations where cf = 0, even when other conditions are present. This highlights the central role of call type in shaping fraudulent activity.

One qualification applies to the origin and destination conditions. Both were entered into the model as numeric category codes produced by indexing the city names, which orders them alphabetically rather than by any property of the locations themselves. The codes therefore carry no intrinsic magnitude, and the membership scores derived from them separate cases without expressing a substantive difference between one origin and another.

The data supports the same conclusion independently. The proportion of SIM box fraud is effectively constant across all seven origin countries, ranging only between 19.4% and 20.9%, and across all seven destination countries, ranging between 19.6% and 21.1%. Calls crossing a national border show a fraud rate of 20.3% against 19.9% for calls within a single country. No geographic variation is present in this dataset for the conditions of and d_f to capture, and re-specifying them in substantively meaningful terms, such as cross-border routing or high-risk destination, was found to leave the ordering of the results unchanged. The conditions are therefore retained as reported, but the interpretation offered in this section and the next rests on call type and call duration, which do carry measurable signal; of and d_f should be read as partitioning the cases rather than as causal conditions in their own right. Establishing whether location genuinely conditions SIM box fraud would require operator data in which geographic variation is present.

4.5.3 Re-specification with Behaviourally Meaningful Conditions

The revised model of Section 4.5.2 removed the leaked field, but two of its four conditions remain weak for the reason given there: origin and destination were entered as numeric codes indexing city names alphabetically, and the dataset shows no variation in fraud rate across locations. A third specification was therefore estimated using only the two conditions that the necessity analysis of Section 4.4.1 and the predictive comparison of Section 4.4.2 both identify as carrying signal: short call duration and international call type. Duration is calibrated as shortness, with anchors at 300, 120 and 30 seconds, so that membership increases as calls get shorter [31], [32].

Table 4.6: fsQCA truth table using short duration and international call type

Row	sd (short)	cf (international)	OUT	n	Consistency
1	0	0	0	4,425	0.029
2	0	1	0	1,951	0.068

Row	sd (short)	cf (international)	OUT	n	Consistency
3	1	0	0	4,072	0.034
4	1	1	1	4,837	0.573

A single configuration is sufficient for the outcome: short duration combined with international call type, with a consistency of 0.573 and a coverage of 0.940. No other combination approaches the threshold. The high coverage means this one pathway accounts for almost all observed SIM box fraud, while the moderate consistency reflects that the combination is common among genuine traffic as well, which is the expected pattern for a necessary but not sufficient condition set [34], [36].

This specification improves on the four-condition model in three respects. It retains 15,285 of the 15,319 cases against 11,213, because the location codes produced membership scores of exactly 0.5 for a large group of records that the truth table then discarded. Its solution consistency is higher, at 0.573 against 0.540 for the strongest configuration of the earlier model. And every condition in it is behaviourally interpretable, so the solution can be read directly as a statement about calls rather than about category codes. Adding cross-border routing as a third condition was also tested and reduced coverage from 0.940 to 0.816 without raising consistency, confirming that geography adds nothing [9], [25].

The three configurational models estimated in this chapter therefore form a sequence. The first was withdrawn because one of its conditions restated the outcome. The second removed that condition but retained two others that carry no substantive ordering. The third restricts the model to the conditions that the necessity and predictive analyses independently support, and produces the clearest result: SIM box fraud in this dataset arises where a call is international and short, and nowhere else.

4.5.4 Discussion of Configurational Results

The configurational results demonstrate that SIM box fraud is not explained by single indicators but by specific combinations of behavioral conditions. The presence of cf = 1 (call type) emerges as a necessary condition for fraud, particularly when combined with of = 1 (origin–destination factor). This aligns with the operational logic of SIM box fraud, where abnormal call routing and call type manipulation are central to bypassing legitimate billing systems.

Interestingly, high-frequency non-fraud configurations (e.g., row 12) show that traffic volume alone is insufficient to indicate fraud. This finding challenges predictive models that often overemphasize volume-based thresholds. Instead, fsQCA highlights that fraud emerges from **qualitative interactions among conditions**, not quantitative extremes [25], [21].

The results also reveal **multiple pathways to fraud**:

- Strong pathways (rows 6–8), where fraud is consistently produced by call type combined with origin–destination variations.
- Weak pathways (rows 13–15), where fraud appears but with lower consistency, suggesting secondary or less dominant fraud strategies.

This configurational perspective enhances interpretability compared with black-box predictive models. By identifying the precise combinations of conditions that lead to fraud, fsQCA provides actionable insights for telecom operators: monitoring should prioritize configurations where call type and routing patterns interact, rather than relying solely on single-factor thresholds [9], [25].

4.6 Case Studies and Sample Predictions

This section includes several case studies that evaluated the ability of the proposed model to detect fraudulent patterns related to IRSF in telecommunication call records. The case studies drew on the configurations identified by fsQCA together with the Random Forest classifier described in Section 4.4.4, which was used to score individual call records by their predicted likelihood of fraud [9], [30].

In each of the cases reviewed, the call records flagged as suspicious by the proposed model were compared against the IRSF behavioural indicators documented in the fraud detection literature [16], [23]. The analysis showed that the model was able to identify many of the most common indicators of IRSF behavior, such as sudden increases in the number of international calls made, the rapid recurrence of calls within a very short period of time, and unusual SIM ID usage.

One of the most illustrative examples of the model's performance was a case in which over 240 international calls had been made within an 18-minute period to international premium rate numbers (IPRNs). This type of activity is consistent with the behavior of fraudsters who attempt to generate the maximum amount of revenue prior to the activation of the SIM card. The proposed model also identified other unusual calling patterns, including short-duration repeated calls, frequent late-night calling patterns, and SIM cards located in different geographic areas within narrow time intervals [23], [4].

4.7 Comparative Analysis with Previous Studies and Systems

This section provides a detailed comparative analysis between the findings of this study and the current literature, linking the findings of this study to prior studies and existing systems for detecting fraud in telecoms [3], [12].

4.7.1 Methodological Comparison with Previous Studies

Much of the previous research in fraud detection for telecommunications has used machine learning algorithms (e.g., Random Forest, Support Vector Machines, Gradient Boosting, and neural network models). These algorithms have demonstrated good predictive capabilities; however, they generally operate as “black boxes” and are therefore unable to produce meaningful interpretations of fraudulent behavior [9], [25].

This research advances the field of telecom fraud detection by integrating three methodological approaches to enhance detection efforts with an increased understanding of fraud behavior:

- NCA identifies the necessary antecedent conditions needed for fraud to occur, an approach not included in previous research [3], [12].
- fsQCA identifies multiple causal configurations leading to telecommunication fraud and documents the combined and non-linear nature of fraudulent behavior.
- ML models provide predictive validation and enhance the reliability of the operational system.

The combination of NCA and fsQCA provides a comprehensive view of diagnostic information, while ML enables accurate prediction. Previous detection systems have

primarily focused on predicting fraudulent behavior without providing explanations of it [3], [12].

4.7.2 Comparison of Performance with Existing Platforms

Current systems rely heavily on labeled datasets and are therefore more likely to have a considerable amount of noise in their results. Their reliance on labeled data also limits their ability to capture new types of fraud, and they cannot recognize new types of fraud quickly. The hybrid solution presented in this research provides several advantages, including reduced noise resulting from the elimination of features that do not add value (thanks to NCA filtering), better contextual awareness due to the ability of fsQCA to determine levels of fraud, and improved discrimination between legitimate and fraudulent users through the higher accuracy of ML-based classifiers.

4.7.3 Interpretation: How the Results Can Be Used

While some previous studies have made advancements in developing accurate approaches to fraud detection, the lack of an interpretive framework is a strong limiting factor. Most of these studies used highly accurate models created through complex and/or non-linear techniques that were unable to offer insight into why fraud occurs. To fill this gap, the present study pursues the following: [3], [12]

- Utilizing NCA to directly identify the characteristics that are required for fraud and to identify thresholds [31].
- Utilizing fsQCA to reveal the various pathways that lead to fraud and to provide scenario-specific interpretations.
- Pairing predictive models with SHAP values or feature importance analytics to improve interpretability when these models are used for fraud detection in practice [9], [25].

This balance between high accuracy and high interpretability is what differentiates the proposed system from most previous studies [9], [25].

4.7.4 The Ability to Model Complex and Non-linear Fraud Patterns

Earlier fraud detection literature has tended to concentrate on a few simple fraud indicators, such as frequent calls to certain destinations, sudden changes in call duration, or abnormal volumes of international traffic. Today, however, many new fraud schemes combine several of these indicators and often form multi-condition patterns that cannot easily be identified through linear or rule-based procedures. This study's hybrid framework therefore successfully delineates: [3], [12]

- Fraud patterns that involve multiple dimensions;
- The non-linear causal relationships between these indicators; and
- The interrelationships between the behavioral, temporal, and network factors involved in each pattern.

Such a capability is not available in current fraud detection approaches, and thus adds significantly to this area of investigation.

4.7.5 Overall Contribution Compared with Current Research

By comparison with previous literature and current commercial fraud detection systems, the present work provides several advances: [3], [12]

- A new hybrid analytical methodology integrating NCA, fsQCA, and machine learning; no previous study has integrated all three of these methodologies [9], [30].
- Improved prediction performance, particularly in circumstances of imbalanced datasets or changing fraud schemes.
- Greater ability to provide insights through interpretive techniques, so that telecom operators may not only identify cases of fraud but also understand why they are fraudulent.
- Increased ability to detect complex, rare, and newly emerging configurations of fraud.
- A theoretical basis that ties together structural, configurational, and statistical approaches to understanding how fraud works.

Overall, the current work fills important gaps in the literature by combining explanatory and predictive models in a way that produces a comprehensive understanding of fraud detection [9], [25].

CHAPTER FIVE

CONCLUSION AND FUTURE WORK

5.1 Conclusion

This project focused on the problem of telecommunication fraud, especially SIM box fraud, by applying an integrated analytical framework based on Necessary Condition Analysis (NCA) and Fuzzy-set Qualitative Comparative Analysis (fsQCA). The main objective of this study was not only to detect fraud, but also to understand the reasons behind its occurrence by identifying the conditions that must exist for fraud to happen and the combinations of conditions that lead to fraud [31], [32].

The analysis was carried out using a Call Detail Records (CDRs) dataset that was carefully cleaned, filtered, and transformed into a fully numeric format. The dataset was reduced to include only normal calls and SIM box fraud cases in order to focus on the most relevant patterns. Several preprocessing steps were applied, including converting categorical variables into binary and numeric representations, removing non-numeric prefixes from identifiers, and standardizing all variables to ensure consistency and suitability for NCA and fsQCA analysis [31], [32].

The results of the Necessary Condition Analysis showed that **transaction status** is the strongest necessary condition for the occurrence of SIM box fraud. The effect size and inefficiency measures clearly indicate that fraud cannot reach high levels unless the transaction status exceeds a specific threshold. This confirms that transaction status plays a critical role in constraining fraud behavior rather than acting as a simple correlated feature. In addition, the **SIM ID** variable was found to impose a moderate constraint, which suggests that fraud is usually concentrated within specific SIM cards instead of being randomly distributed across the network. Other variables such as caller ID, receiver ID, call duration, and location-related attributes showed very low or zero effect sizes, meaning that fraud can occur regardless of their individual values [31], [32].

The fsQCA results supported the NCA findings by identifying a clear causal configuration that leads to fraud. The truth table analysis showed that fraud occurs only when **international call type** and **fraudulent transaction status** are present together. This configuration achieved perfect consistency and proportional reduction in inconsistency (PRI), indicating that whenever this combination appears, fraud always occurs. Other configurations, such as local calls or legitimate transactions, consistently resulted in non-fraud outcomes [31], [32].

The extended truth table of behavioral conditions further showed that fraud behavior is not driven by a single factor but rather emerges from specific configurations of conditions such as call duration, call type, and origin–destination patterns. High-frequency configurations without the call type condition remained non-fraud, confirming that traffic volume alone is not sufficient to indicate fraud [33], [36].

By combining NCA and fsQCA, this study demonstrated that telecom fraud is driven by **configurational and asymmetric causality**. While transaction status acts as a necessary condition that limits fraud occurrence, it becomes fully explanatory only when combined with contextual factors such as international calling behavior. Compared with traditional machine learning models that operate as black boxes, the proposed framework provides better interpretability and a clearer understanding of how fraud occurs [31], [32].

Overall, the results confirm that the integrated NCA–fsQCA framework is effective in identifying both the structural constraints and the causal pathways of SIM box fraud. The findings can support telecom operators in improving fraud detection systems by focusing on necessary conditions and high-risk configurations rather than relying only on predictive accuracy. However, the study also acknowledges limitations related to the scope of the dataset, which originates from a single source and focuses on SIM box fraud only [31], [32].

5.2 Future Work

Although this study achieved its objectives, there are several directions for future research that can further improve the proposed framework. First, future work should focus on applying the NCA–fsQCA approach to **real-time and streaming CDR data**. This would

allow fraud detection systems to respond more quickly to emerging fraud patterns and reduce the financial losses caused by delayed detection [31], [32].

Second, additional **behavioral, temporal, and network-related features** can be included in future studies. Variables such as call frequency bursts, routing anomalies, inter-call time patterns, and cross-border traffic intensity may reveal additional sufficient configurations and improve the explanatory power of fsQCA [33], [36].

Third, future research may explore the **integration of the proposed framework with explainable machine learning models**, such as SHAP or feature importance techniques. This hybrid approach can improve predictive performance while maintaining interpretability, making the system more suitable for real-world deployment [9], [25].

Fourth, the framework should be validated using **datasets from multiple telecom operators and different geographic regions**. This would enhance the generalizability of the results and reduce the limitations associated with using data from a single source [12], [3].

Finally, future work may extend this framework to **other types of telecommunication fraud**, such as subscription fraud, caller ID spoofing, and misrouting fraud. Applying the NCA–fsQCA methodology to different fraud scenarios may help in developing a unified and interpretable fraud detection framework for the telecommunications sector [31], [32].

REFERENCES

[1] P. Gao, Z. Li, D. Zhou and L. Zhang, "Reinforced Cost-Sensitive Graph Network for Detecting Fraud Leaders in Telecom Fraud," IEEE Access, vol. 12, pp. 173638–173646, 2024, doi: 10.1109/ACCESS.2024.3448260.

[2] Z. Zhang, Z. Li, W. Wu, Y. Ding and X. Wang, "Graph-based Contrastive Learning for Telecom Fraud Detection," in Proceedings of the IEEE International Conference on Communications (ICC), 2024, doi: 10.1109/ICC.2024.11050370.

[3] A. Dong, Z. Zhou, J. Hu and Y. Ma, "A Comprehensive Survey on Graph Neural Networks for Fraud Detection," in Proceedings of the IEEE International Conference on Data Mining (ICDM), 2019, doi: 10.1109/ICDM.2019.8804189.

[4] I. Melih Tas and S. Baktır, "Blockchain-Based Caller-ID Authentication (BBCA): A Novel Solution to Prevent Spoofing Attacks in VoIP/SIP Networks," IEEE Access, vol. 12, 2024.

[5] Y. Jiang, G. Liu, J. Wu and H. Lin, "Telecom Fraud Detection via Hawkes-Enhanced Sequence Model," IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 5, pp. 4578–4590, 2023, doi: 10.1109/TKDE.2022.3150803.

[6] H. Huo, "Telecom Fraud Detection Based on Deep Learning," 2024 6th International Academic Exchange Conference on Science and Technology Innovation (IAECST), Guangzhou, China, 2024, pp. 1132–1137, doi: 10.1109/IAECST64597.2024.11117868.

[7] O. O. Khalifa et al., "Blockchain Security for 5G Network using Internet of Things Devices," 2022 7th International Workshop on Big Data and Information Security (IWBIS), 2022, pp. 101–106, doi: 10.1109/IWBIS56557.2022.9924937.

[8] X. Li, "Research on Developing a Telecom Fraud Detection Model Based on Logistic Regression," 2025 IEEE 3rd International Conference on Image Processing and Computer Applications (ICIPCA), Shenyang, China, 2025, pp. 11–16, doi: 10.1109/ICIPCA65645.2025.11138523.

[9] G. Louppe, "Understanding Random Forests: From Theory to Practice," arXiv:1407.7502, 2014.

[10] P. Fang and Q. Fang, "Research on Anti-telecom Fraud Based on Artificial Intelligence and Edge Computing," 2024 IEEE 3rd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), Changchun, China, 2024, pp. 1618–1620, doi: 10.1109/EEBDA60612.2024.10486050.

[11] E. S. Ali and R. A. Saeed, "A Survey of Big Data Cloud Computing Security," International Journal of Computer Science and Software Engineering (IJCSSE), vol. 3, no. 1, pp. 78–85, December 2014.

[12] C. Zhao, Y. Gao, Y. Xing, Y. Ke, X. Tian and H. Chen, "A Multi-Dimensional Telecom Fraud Detection Model Based on Graph Attention Networks," 2025 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Dublin, Ireland, 2025, pp. 1–6, doi: 10.1109/BMSB65076.2025.11165544.

[13] M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan and R. A. Mokhtar, "Anomaly Detection in 6G Networks Using Machine Learning Methods," Electronics, vol. 12, 3300, 2023, doi: 10.3390/electronics12153300.

[14] S. Gadal, R. Mokhtar et al., "Machine Learning-Based Anomaly Detection Using K-mean Array and Sequential Minimal Optimization," Electronics, vol. 11, 2158, 2022, doi: 10.3390/electronics11142158.

[15] K. H. Mir, R. Kumar, S. Rai, A. Hassan, T. Sarkar and B. Moharana, "Real-Time Anomaly Detection in Telecommunications: Advanced Data Mining Techniques for Fraud Identification," 2025 3rd International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 2025, pp. 1578–1583, doi: 10.1109/ICDT63985.2025.10986461.

[16] M. M. Saeed et al., "Security and Privacy Enhancement in 6G IoT Devices Using Blockchain," 2025 5th International Conference on Emerging Smart Technologies and Applications (eSmarTA), Ibb, Yemen, 2025, pp. 1–6, doi: 10.1109/eSmarTA66764.2025.11132286.

[17] M. A. Elmubark, R. A. Saeed, M. A. Elshaikh and R. A. Mokhtar, "Fast and secure generating and exchanging a symmetric keys with different key size in TVWS," International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE), Khartoum, Sudan, 2015, pp. 114–117.

[18] X. Li, "Telecom Bank Card Fraud Risk Prediction Based on CNN-LSTM Model," 2025 2nd International Conference on Artificial Intelligence and Digital Management (ICAIDM), Huainan, China, 2025, pp. 93–96, doi: 10.1109/ICAIDM66813.2025.11293396.

[19] M. M. Saeed, R. A. Saeed, M. K. Hasan et al., "A comprehensive survey on 6G-security: physical connection and service layers," Discover Internet of Things, vol. 5, 28, 2025, doi: 10.1007/s43926-025-00123-7.

[20] E. Reypnazarov, Z. Allamuratova, T. Babazhanova and R. Dauletmuratova, "AI-Driven Fraud Detection in Telecommunication Billing Systems," 2025 IEEE 26th International Conference of Young Professionals in Electron Devices and Materials (EDM), Altai, Russian Federation, 2025, pp. 1990–1994, doi: 10.1109/EDM65517.2025.11096687.

[21] V. K. Singh, P. Mahajan, B. Moharana, S. Maurya, J. Mishra and T. Sarkar, "Real-Time Anomaly Behaviour Detection for Financial Fraud in Telecommunications Utilizing Data Mining Techniques," 2025 International Conference on Technology Enabled Economic Changes (InTech), Tashkent, Uzbekistan, 2025, pp. 1523–1529, doi: 10.1109/InTech64186.2025.11198324.

[22] M. K. Hasan, T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, A. A. Eshmawi, S. Abdel-Khalek and H. M. Alkhassawneh, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," IET Communications, vol. 16, pp. 421–432, 2022, doi: 10.1049/cmu2.12301.

[23] V. Tiwari and A. Pratap, "Fraud Call Detection using Pre-Data Feeding Method by Financial Institution," 2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2025, pp. 990–993, doi: 10.1109/CICTN64563.2025.10932609.

[24] E. S. Ali et al., "Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications," Security and Communication Networks, vol. 2021, 2021, doi: 10.1155/2021/8868355.

[25] F.-Y. Liang et al., "Telecom Fraud Detection Based on Feature Binning and Autoencoder," 2023 IEEE International Conference on Data Mining (ICDM), Shanghai, China, 2023, pp. 368–377, doi: 10.1109/ICDM58522.2023.00046.

[26] F. T. Liu, K. M. Ting and Z.-H. Zhou, "Isolation Forest," 2008 Eighth IEEE International Conference on Data Mining (ICDM), Pisa, Italy, 2008, pp. 413–422, doi: 10.1109/ICDM.2008.17.
[27] Y. LeCun, Y. Bengio and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015, doi: 10.1038/nature14539.
[28] T. N. Kipf and M. Welling, "Semi-Supervised Classification with Graph Convolutional Networks," in Proc. 5th International Conference on Learning Representations (ICLR), Toulon, France, 2017.
[29] P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Liò and Y. Bengio, "Graph Attention Networks," in Proc. 6th International Conference on Learning Representations (ICLR), Vancouver, Canada, 2018.
[30] L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001, doi: 10.1023/A:1010933404324.
[31] J. Dul, "Necessary Condition Analysis (NCA): Logic and Methodology of 'Necessary but Not Sufficient' Causality," Organizational Research Methods, vol. 19, no. 1, pp. 10–52, 2016, doi: 10.1177/1094428115584005.
[32] J. Dul, E. van der Laan and R. Kuik, "A Statistical Significance Test for Necessary Condition Analysis," Organizational Research Methods, vol. 23, no. 2, pp. 385–395, 2020, doi: 10.1177/1094428118795272.
[33] C. C. Ragin, Redesigning Social Inquiry: Fuzzy Sets and Beyond. Chicago, IL, USA: University of Chicago Press, 2008.
[34] C. C. Ragin, "Set Relations in Social Research: Evaluating Their Consistency and Coverage," Political Analysis, vol. 14, no. 3, pp. 291–310, 2006, doi: 10.1093/pan/mpj019.
[35] P. C. Fiss, "Building Better Causal Theories: A Fuzzy Set Approach to Typologies in Organization Research," Academy of Management Journal, vol. 54, no. 2, pp. 393–420, 2011, doi: 10.5465/amj.2011.60263120.
[36] C. Q. Schneider and C. Wagemann, Set-Theoretic Methods for the Social Sciences: A Guide to Qualitative Comparative Analysis. Cambridge, U.K.: Cambridge University Press, 2012.
[37] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.
[38] S. Talluri, Q. Zhang and R. Chen, "A Cloud-Native Federated Learning Architecture for Telecom Fraud Detection," NOMS 2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, 2023, pp. 1–3, doi: 10.1109/NOMS56928.2023.10154302.

APPENDIX A

SOURCE CODE

The complete R source code used for the analysis is reproduced below. The script runs in two independent stages: the necessity analysis over all records, followed by the configurational analysis over the filtered subset. It was executed under R 4.3 using the NCA and QCA packages.

A.1 Environment Setup and Data Import

Package loading and import of the call detail record file. The path shown is the local path used during development and must be changed to the location of the data file on the machine running the script.

```
# ------------------------------------------------------------
# 0. Install & load packages
# ------------------------------------------------------------
install.packages(c("readxl", "dplyr", "NCA"))
library(readxl)
library(dplyr)
library(NCA)
library(QCA)

# ------------------------------------------------------------
# 1. Load dataset
# ------------------------------------------------------------
data <- read_excel("C:/Users/hassa/Desktop/Book1.xlsx")

# ------------------------------------------------------------
# 2. Create binary target for sim_box_fraud (y)
# ------------------------------------------------------------
data$sim_box_fraud <- ifelse(data$fraud_type == "sim_box_fraud", 1, 0)
```

A.2 Predictor Preparation for the Necessity Analysis

Conversion of the thirteen predictors to a common numeric scale. Categorical columns are mapped to integer factor levels and all columns are then replaced by their ranks, as described in Section 4.2.2.

```
# ------------------------------------------------------------
# 3. Prepare predictors (x)
# ------------------------------------------------------------
```

```
predictors <- names(data)[1:13]  # select the first 13 columns as predictors

for (col in predictors) {
  if (is.character(data[[col]]) || is.factor(data[[col]])) {
    # Convert categorical variables into integer levels
    data[[col]] <- as.integer(factor(data[[col]]))
  }
  if (is.numeric(data[[col]])) {
    # Rank numeric values to reduce large range differences
    data[[col]] <- rank(data[[col]], ties.method = "average")
  }
}

# ------------------------------------------------------------
# 4. Initialize results storage
# ------------------------------------------------------------
results <- list()
```

A.3 Necessary Condition Analysis (NCA)

The CE-FDH ceiling is estimated separately for each predictor against the binary SIM box fraud outcome. Results are collected in a list and plotted to file.

```
# ------------------------------------------------------------
# 5. Run NCA for each predictor
# ------------------------------------------------------------
for (x in predictors) {
  cat("\n::::::::::::::::::::::::::::::::::::::::::::::::\n") # decorative separator line
  cat("Running NCA for:", x, "-> sim_box_fraud\n")
  cat("\n::::::::::::::::::::::::::::::::::::::::::::::::\n")  # decorative separator
line

  # Perform NCA for each predictor against the target sim_box_fraud
  res <- tryCatch(
    nca(data = data, x = x, y = "sim_box_fraud", ceilings = "ce_fdh"),
    error = function(e) {
      cat("Error for predictor", x, ":", e$message, "\n")
      return(NULL)
    }
  )

  if (!is.null(res)) {
    print(summary(res))
    results[[x]] <- res
  }
}

# ------------------------------------------------------------
# 6. Plot NCA results (generate plots)
# ------------------------------------------------------------
for (x in predictors) {
  if (!is.null(results[[x]])) {
    png(filename = paste0("NCA_plot_", x, ".png"), width = 800, height = 600)
    plot(results[[x]], main = paste("NCA Plot:", x, "-> sim_box_fraud"))
    dev.off()
  }
}
```

A.4 Data Preparation for the Configurational Analysis

The dataset is filtered to normal calls and SIM box fraud only, and the conditions and outcome are recoded into the binary form required by fsQCA.

```
 #data preparation as numeric
        data_filtered <- subset(data, fraud_type %in% c("sim_box_fraud", "none"))
        data_filtered$fraud_binary <- ifelse(data_filtered$fraud_type == "sim_box_fraud",
1, 0)
        data_filtered$call_type_binary <- ifelse(data_filtered$call_type ==
"international", 1, 0)
        data_filtered$transaction_binary <- ifelse(data_filtered$transaction_status ==
"Fraudulent", 1, 0)
        data_filtered$location_origin_num <-
as.numeric(factor(data_filtered$location_origin))
        data_filtered$location_dest_num <-
as.numeric(factor(data_filtered$location_dest))
        data_filtered$sim_id <- gsub("SIM", "", data_filtered$sim_id)
        data_filtered$sim_id <- gsub("FAKE", "1", data_filtered$sim_id)
        data_filtered$device_id <- gsub("DEV", "", data_filtered$device_id)
        data_filtered$sim_id <- as.numeric(data_filtered$sim_id)
        data_filtered$device_id <- as.numeric(data_filtered$device_id)
 # final data ready for analysis
        final_data <- data.frame(  fraud_binary          = data_filtered$fraud_binary,
                                   call_type_binary      =
data_filtered$call_type_binary,
                                   transaction_binary    =
data_filtered$transaction_binary,
                                   location_origin_num   =
data_filtered$location_origin_num,
                                   location_dest_num     =
data_filtered$location_dest_num,
                                   sim_id                = data_filtered$sim_id,
                                   device_id             = data_filtered$device_id,
                                   duration_sec          = data_filtered$duration_sec)
        final_data <- na.omit(final_data)
```

A.5 Fuzzy-Set Qualitative Comparative Analysis (fsQCA)

Construction of the truth table reported in Table 4.4, using call type and transaction status as conditions with an inclusion cut-off of 0.8.

```
 #qca on transaction_binary & call_type_binary
        tt <- truthTable(final_data, outcome = "fraud_binary", conditions =
c("call_type_binary ","transaction_binary"), incl.cut = 0.8, show.cases = TRUE)
        print(tt)
```

A.6 Random Forest Comparison

Predictive baseline used for the comparison reported in Section 4.4.4. It reuses the filtered data frame prepared in Section A.4, so this block is run after the configurational analysis.

```
# ------------------------------------------------------------
```

```
# 7. Random Forest comparison (predictive baseline)
# ------------------------------------------------------------
library(randomForest)

set.seed(42)

# Use the same filtered subset prepared for the fsQCA stage
rf_data <- data.frame(
  fraud              = as.factor(data_filtered$fraud_binary),
  duration_sec       = data_filtered$duration_sec,
  call_type          = data_filtered$call_type_binary,
  transaction_status = data_filtered$transaction_binary,
  sim_id             = data_filtered$sim_id,
  device_id          = data_filtered$device_id,
  location_origin    = data_filtered$location_origin_num,
  location_dest      = data_filtered$location_dest_num,
  is_night_call      = data_filtered$is_night_call
)
rf_data <- na.omit(rf_data)

# Stratified 70 / 30 split
idx0  <- which(rf_data$fraud == 0)
idx1  <- which(rf_data$fraud == 1)
train <- c(sample(idx0, round(0.7 * length(idx0))),
           sample(idx1, round(0.7 * length(idx1))))
test  <- setdiff(seq_len(nrow(rf_data)), train)

rf <- randomForest(fraud ~ ., data = rf_data[train, ],
                   ntree = 500, importance = TRUE)

# Performance on the held-out partition
pred <- predict(rf, rf_data[test, ])
cm   <- table(Predicted = pred, Actual = rf_data$fraud[test])
print(cm)

tp <- cm["1", "1"]; fp <- cm["1", "0"]
fn <- cm["0", "1"]; tn <- cm["0", "0"]
cat("Accuracy :", round((tp + tn) / sum(cm), 4), "\n")
cat("Precision:", round(tp / (tp + fp), 4), "\n")
cat("Recall   :", round(tp / (tp + fn), 4), "\n")
cat("F1       :", round(2 * tp / (2 * tp + fp + fn), 4), "\n\n")

# Variable importance
imp <- importance(rf)
print(round(imp[order(-imp[, "MeanDecreaseGini"]), ], 4))

png("RF_importance.png", width = 1800, height = 1100, res = 200)
varImpPlot(rf, main = "Random Forest variable importance")
dev.off()

write.csv(imp, "rf_importance.csv")
```

A.7 Revised fsQCA with Behavioural Conditions

The re-specified configurational analysis reported in Section 4.5.2, using the four behavioural conditions and excluding transaction status. It reuses the filtered data frame prepared in Section A.4.

```
# ------------------------------------------------------------
```

```
# 8. Revised fsQCA - four behavioural conditions
#    (transaction status excluded: post-outcome field)
# ------------------------------------------------------------
library(QCA)

sub <- data_filtered
sub$call_type_binary <- ifelse(sub$call_type == "international", 1, 0)

# Direct calibration: full non-membership, crossover, full membership
df_  <- calibrate(sub$duration_sec,     type = "fuzzy", thresholds = c(30, 120, 300))
cf_  <- calibrate(sub$call_type_binary, type = "fuzzy", thresholds = c(0, 0.5, 1))
of_  <- calibrate(as.numeric(factor(sub$location_origin)),
                  type = "fuzzy", thresholds = c(1, 2, 3))
d_f_ <- calibrate(as.numeric(factor(sub$location_dest)),
                  type = "fuzzy", thresholds = c(1, 2, 3))

fs_data <- data.frame(df = df_, cf = cf_, of = of_, d_f = d_f_,
                      OUT = sub$fraud_binary)

tt4 <- truthTable(fs_data, outcome = "OUT",
                  conditions = c("df", "cf", "of", "d_f"),
                  incl.cut = 0.10, show.cases = TRUE)
print(tt4)

sol <- minimize(tt4, include = "?", details = TRUE)
print(sol)
```

A.8 Leakage-Free Necessary Condition Analysis

The necessity analysis reported in Section 4.4.1, restricted to conditions recorded while a call is processed. Call duration is entered as shortness, since necessity is directional.

```
# ------------------------------------------------------------
# NCA on leakage-free conditions
#   excluded: transaction_status (restates the outcome)
#             sim_id             (SIM_FAKE_ prefix encodes the class)
#             caller_id, receiver_id (unique per record)
# ------------------------------------------------------------
library(NCA)

d <- read.csv("realtime_cdr_fraud_dataset.csv", stringsAsFactors = FALSE)
d <- subset(d, fraud_type %in% c("sim_box_fraud", "none"))

dat <- data.frame(
  call_type_intl  = ifelse(d$call_type == "international", 1, 0),
  call_shortness  = max(d$duration_sec) - d$duration_sec,   # necessity is directional
  call_duration   = d$duration_sec,
  device_id       = as.numeric(gsub("\\D", "", d$device_id)),
  origin_city     = as.numeric(factor(d$location_origin)),
  origin_country  = as.numeric(factor(d$country_origin)),
  dest_city       = as.numeric(factor(d$location_dest)),
  dest_country    = as.numeric(factor(d$country_dest)),
  sim_box_fraud   = ifelse(d$fraud_type == "sim_box_fraud", 1, 0)
)

for (v in setdiff(names(dat), "sim_box_fraud")) {
  r <- nca_analysis(dat, v, "sim_box_fraud", ceilings = "ce_fdh")
  cat("\n===", v, "===\n")
  print(r$summaries[[1]]$params[c("Ceiling zone", "Effect size",
                                  "Ceiling accuracy", "Fit",
```

```
                                  "Rel. ineff."), , drop = FALSE])
}
```

A.9 Leakage-Free Random Forest

The predictive comparison reported in Section 4.4.2, trained on the same leakage-free conditions.

```
suppressMessages(library(randomForest))
set.seed(42)
d <- read.csv("orig.csv", stringsAsFactors = FALSE)
d <- subset(d, fraud_type %in% c("sim_box_fraud", "none"))

X <- data.frame(
  duration_sec    = d$duration_sec,
  call_type       = as.numeric(factor(d$call_type)),
  device_id       = as.numeric(gsub("\\D", "", d$device_id)),
  location_origin = as.numeric(factor(d$location_origin)),
  country_origin  = as.numeric(factor(d$country_origin)),
  location_dest   = as.numeric(factor(d$location_dest)),
  country_dest    = as.numeric(factor(d$country_dest)),
  is_night_call   = d$is_night_call,
  fraud = as.factor(ifelse(d$fraud_type == "sim_box_fraud", 1, 0))
)
i  <- sample(seq_len(nrow(X)), round(0.7 * nrow(X)))
rf <- randomForest(fraud ~ ., data = X[i, ], ntree = 500, importance = TRUE)
p  <- predict(rf, X[-i, ]); a <- X$fraud[-i]
cm <- table(Predicted = p, Actual = a); print(cm)
tp <- cm["1","1"]; fp <- cm["1","0"]; fn <- cm["0","1"]; tn <- cm["0","0"]
acc <- (tp+tn)/sum(cm); pe <- sum(rowSums(cm)*colSums(cm))/sum(cm)^2
cat("\nAccuracy :", round(acc,4), "  Kappa:", round((acc-pe)/(1-pe),4), "\n")
cat("Precision:", round(tp/(tp+fp),4), "\n")
cat("Recall   :", round(tp/(tp+fn),4), "\n")
cat("F1       :", round(2*tp/(2*tp+fp+fn),4), "\n\n")
imp <- importance(rf)
print(round(imp[order(-imp[,"MeanDecreaseGini"]),
c("MeanDecreaseAccuracy","MeanDecreaseGini")],2))
png("RF_clean_bin.png", width=1900, height=950, res=200)
varImpPlot(rf, main="Random Forest variable importance (leakage-free predictors)")
dev.off()
```

A.10 Re-specified fsQCA with Meaningful Conditions

The configurational model reported in Section 4.5.3, restricted to short call duration and international call type. The three-condition variant adding cross-border routing is included for comparison.

```
suppressMessages({library(QCA)})
d <- read.csv("orig.csv", stringsAsFactors=FALSE)
s <- subset(d, fraud_type %in% c("sim_box_fraud","none"))
s$fb <- ifelse(s$fraud_type=="sim_box_fraud",1,0)

sd_ <- calibrate(max(s$duration_sec)-s$duration_sec, type="fuzzy",
                 thresholds=c(1540,1720,1810))       # = duration 300 /120 / 30 s
```

```
cf_ <- calibrate(ifelse(s$call_type=="international",1,0), type="fuzzy",
                 thresholds=c(0,0.5,1))
xb_ <- calibrate(ifelse(s$country_origin!=s$country_dest,1,0), type="fuzzy",
                 thresholds=c(0,0.5,1))

run <- function(lbl, dat, conds){
  tt <- suppressWarnings(truthTable(dat, outcome="OUT", conditions=conds,
                                    incl.cut=0.5, show.cases=FALSE))
  cat("\n=====", lbl, "=====\n"); print(tt$tt[,c(conds,"OUT","n","incl","PRI")])
  cat("total n:", sum(tt$tt$n), "\n")
  sol <- tryCatch(minimize(tt, details=TRUE), error=function(e) NULL)
  if(!is.null(sol)) print(sol)
}
run("B. short call + international",
    data.frame(sd=sd_, cf=cf_, OUT=s$fb), c("sd","cf"))
run("C. short call + international + cross-border",
    data.frame(sd=sd_, cf=cf_, xb=xb_, OUT=s$fb), c("sd","cf","xb"))
```