Software System for Increasing Security in Telecommunications Networks

Ana-Maria NEGREI[1], Delia-Ioana LEPĂDATU[2], Gabriel PETRICĂ[1]
[1] Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
ana_maria.negrei@stud.etti.upb.ro, gabriel.petrica@upb.ro
[2] Orange Romania

Abstract

The work is based on the design of an automated software tool that provides simulation of traffic events in a telecommunications network and their analysis for the purpose of detecting Wangiri and SMS Bypass frauds. The implemented system allows parameterization of detection and prevention rules for multiple operators, for each type of fraud considered, as well as performing a complex analysis based on them for the purpose of reporting detected fraud cases. The implementation includes technologies such as Spring Boot, Java, Oracle Database, PL/SQL, React and a generative AI model, all integrated into a single architecture. The system is able to suggest measures to minimize the impact of attacks.

Index terms: telecommunications systems, SMS Bypass, SMS fraud, voice fraud, Wangiri

1. Introduction

The telecommunications industry is facing an alarming increase in fraudulent activities, with global losses estimated at $38.95 billion in 2023, a 12% increase from 2021. The rapid expansion of digital communications networks, coupled with the development of 5G technology and the use of sophisticated fraud techniques, has amplified vulnerabilities in the sector, causing significant financial losses for both operators and consumers. Telecom fraud is on the rise, with losses reaching 2.5% of the industry's total revenues. In 2024, the most common types of fraud that generate financial losses and harm to consumers include [1] (fig. 1):

- International Revenue Sharing Fraud (IRSF): estimated losses between $4 billion and $7 billion annually.
- Wangiri fraud: according to the Communications Fraud Control Association (CFCA) [2], Wangiri fraud was among the top five causes of an estimated $2.23 billion loss to the telecom industry.
- Interconnection fraud: the fraudulent manipulation of network traffic, causing annual losses of $3.11 billion.
- Account Takeover (ATO) fraud: the theft of customer identities, causing annual losses of $1.62 billion.

Recent trends indicate a rapid evolution in fraud tactics, with criminals using Artificial Intelligence (AI) and automation. AI-based scams allow fraudsters to carry out automated phishing attacks, identity fraud, and social engineering, making them difficult to detect and prevent.

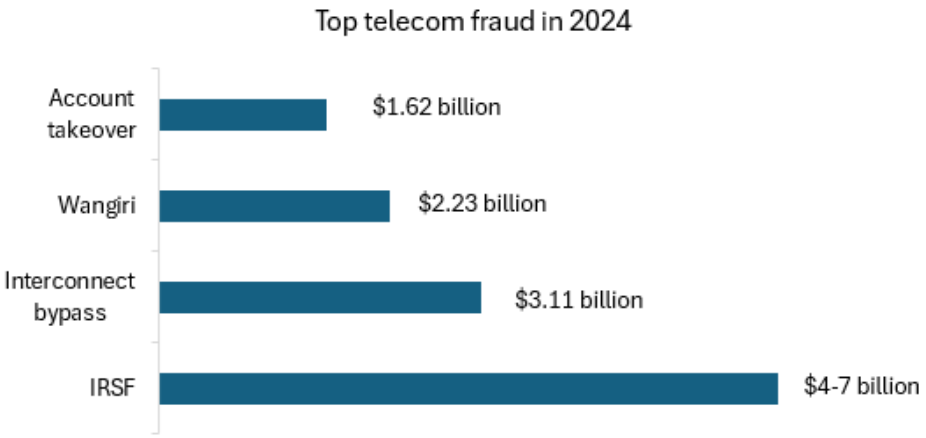

Fig. 1. Highlighting the financial impact of fraud within telecom industry

Smishing attacks in Romania increased significantly in 2023, more than six times compared to the previous year. This type of fraud mainly targets the banking sector (56%), followed by the courier industry (25%) and telecommunications services (15%) [3]. The financial impact of smishing fraud is considerable, as victims are often misled into revealing sensitive banking data or installing malware, leading to unauthorized transactions and direct financial losses. Attackers use fake websites to steal card details or gain access to users' banking applications, resulting in unauthorized access to accounts and financial theft.

In the first months of 2024, 75% of smishing cases involved identity theft by spoofing the sender's name, leading users to believe that the messages came from legitimate companies. This phenomenon affects not only individuals but also companies. Globally, 39% of consumers were the target of at least one SMS fraud attempt in 2023, highlighting the scale of this type of attack. To limit financial damage, authorities and companies emphasize the importance of user awareness and security measures, such as verifying the sender's identity, avoiding accessing suspicious links, and resetting devices if they have been compromised. Despite these efforts, smishing continues to pose a significant financial threat to individuals and organizations in Romania.

2. Fraud in telecommunications networks

Fraud Prevention Systems (FPS) are implemented to detect and mitigate fraudulent behavior using advanced technological solutions. One of the main challenges in combating fraudulent activities lies in the limitations of current infrastructure. Various mechanisms can be used before service provision, such as firewalls, encryption technologies, Subscriber Identity Modules (SIMs) in Private Branch Exchanges (PBXs), PIN codes, software-based security assessments, and customer authentication protocols. Despite their widespread use, the effectiveness of these systems has decreased over time due to the adaptive and evolving nature of attackers. In addition, fraud prevention systems are often perceived as invasive by users and are criticized for their low effectiveness. For example, assigning a security code to SIM cards is a frequently recommended measure; however, this is often neglected, leading to users forgetting the codes. Repeated and failed attempts to enter the correct code can eventually lead to the SIM card being blocked [4].

Fraud Detection Systems (FDS) are a secondary level of defense and are essential when fraudulent actions manage to bypass the implemented prevention mechanisms. These systems play an important role, as they allow for the rapid identification and notification of incidents, through a process known as real-time detection. Unlike prevention systems, which are oriented towards anticipating and blocking potential fraud, fraud detection systems operate through continuous monitoring and automated decision-making.

2.1. SMS fraud

Various types of SMS fraud have existed since the beginning of this service. Examples include SMS Bypass, SMS Malware, SMS Spam, and SMS Phishing. SMS fraud can be mitigated through multiple strategies recommended by fraud management companies, industry forums, academic researchers, and other responsible parties. Telecommunications providers are implementing these strategies, but fraud remains a problem for the industry. To effectively combat SMS fraud, it is essential to investigate the reasons why current fraud reduction methods fail.

a. SMS Spam

Represents fraud in which unsolicited messages are distributed through various electronic communication channels. These messages can be sent by individuals, companies, or even telecommunications operators. A specific form of spam, called "SMS flooding", consists of sending messages to all users connected to an operator's network. Such messages can lead to a breach of user privacy and data loss.

b. SMS Malware

Consists of the use of malicious software, such as viruses, worms and Trojan horses, which are intended to gain unauthorized access to data or services. This type of attack occurs when users unknowingly install infected software, which compromises their data and allows unauthorized messages to be sent to premium rate numbers. Malicious applications or scripts are designed to steal sensitive information, disrupt services, monitor user activities, access confidential data, modify device configurations or generate messages and calls to premium rate numbers without the user's consent.

c. SMS Phishing (Smishing)

It is a method comparable to phishing used in email communications on the Internet. This technique involves the attacker manipulating mobile phone users by sending forged SMS messages, using advanced social engineering practices to mislead and obtain sensitive information.

d. SMS Bypass

This type of fraud has emerged as a direct consequence of the differences in pricing between different message types and transmission routes. Traditionally, SMS messages are classified into two main categories:

- Person-to-Person (P2P): messages exchanged between individual users.
- Application-to-Person (A2P): messages sent by applications or automated systems to users, with the purpose of notifying, alerting, and sending verification codes to users.

SMS Bypass fraud is based on the pricing differences between P2P and A2P messages. While P2P messages are priced at a standard level, A2P messages - mainly used for notifications, alerts or authentication codes - are perceived as having a higher value and, implicitly, are more expensive. Taking advantage of this difference, fraudsters have developed methods to transmit A2P messages using channels intended for P2P traffic, thus bypassing official toll routes. Techniques used include:

- Using specialized equipment that simulates the sending of messages by real users.
- Accessing gray routes, i.e. unauthorized networks that avoid the control and interconnection systems of legitimate operators.
- SIM Box fraud, which involves the use of devices containing multiple SIM cards to locally retransmit international traffic.
- SMS Blasting, i.e. the transmission of many messages through systems that avoid detection and correct billing.

The consequences of SMS Bypass are multiple and affect both telecom operators and communications, as well as end users through:

- Presence of financial losses: operators suffer significant revenue losses due to fraudsters evading legitimate fees.
- Security compromise: users may receive fraudulent or malicious messages, which can lead to the theft of personal or financial information.
- Degradation of service quality: fraudulent traffic can overload networks, affecting the performance and reliability of services for legitimate users.

2.2. Voice fraud

Among the many types of fraud that exist, those that produce the greatest losses globally stand out and which persist despite attempts to combat them by operators.

a. International Revenue Sharing Fraud

IRSF represents one of the most persistent forms of fraud in the telecommunications industry, generating losses of approximately $6.7 billion in 2021, according to CFCA data [2]. Due to the complexity of the mobile network infrastructure and the large number of operators involved, this type of fraud is difficult to eliminate. It is usually orchestrated by organized groups that use illegal connections to initiate a high volume of expensive calls, thus exploiting the roaming capabilities of SIM cards. Within the IRSF, certain scenarios are inspired by the Wangiri fraud model.

b. Interconnection fraud

Interconnection fraud generates annual losses of approximately $3 billion and refers to unethical practices through which certain providers avoid paying mandatory tariffs. They manipulate the routing of calls in the network to benefit from lower costs imposed by the operator of the subscriber receiving the call, costs known in English as “termination rates”.

c. Spoofing

When a call is made to another country or network, it will pass through several telephone operators. The last operator that delivers the call to the person being called charges a termination fee, similar to a commission for taking and delivering the call. This fee is paid by the calling operator to the one receiving the call.

Until 2015, termination rates for calls between European Union member states were dynamic, ranging between €0.01 and €0.15 per minute, depending on each state’s pricing policies. In an effort to harmonise the European telecommunications market and reduce the costs of calls borne by users, EU regulators adopted a measure that would keep the termination rate at a fixed €0.01, similar to a rate applicable to national calls. This regulation, although beneficial for consumers, generated significant revenue losses for telecom operators, as they could no longer charge differentiated rates depending on the origin of the call.

d. Wangiri fraud

Despite their ability to innovate, fraudsters often resort to strategies that have already been tested and proven to be effective and profitable. One of these persistent methods, recognized for the advantages it offers to those who practice it, is Wangiri fraud.

The term “Wangiri” comes from the Japanese language and means “one ring and then hang up”, accurately reflecting the mechanism of the scam: the caller lets the phone ring once, then hangs up. The goal of this technique, classified as a “call back” fraud, is to get users curious or concerned and call them back, usually to International Premium Rate Numbers (IPRN). These return calls generate high costs for users, while the attackers earn revenue. Typically, the calls are made during times when

people are less likely to answer (at night or during business hours), to increase the chance that the call will be returned. The initial costs for the attackers are minimal, as the calls are not charged if they are not answered. Once the user calls back, the fraudsters use various methods - such as automated messages promising prizes or winnings - to keep the user on the call as long as possible. By automating the calls, they can make thousands of calls per minute. Furthermore, it is possible that there are agreements between fraudster groups and premium service providers, with the latter trying to prolong the conversations in order to increase the costs of the call and, implicitly, the joint profits [5].

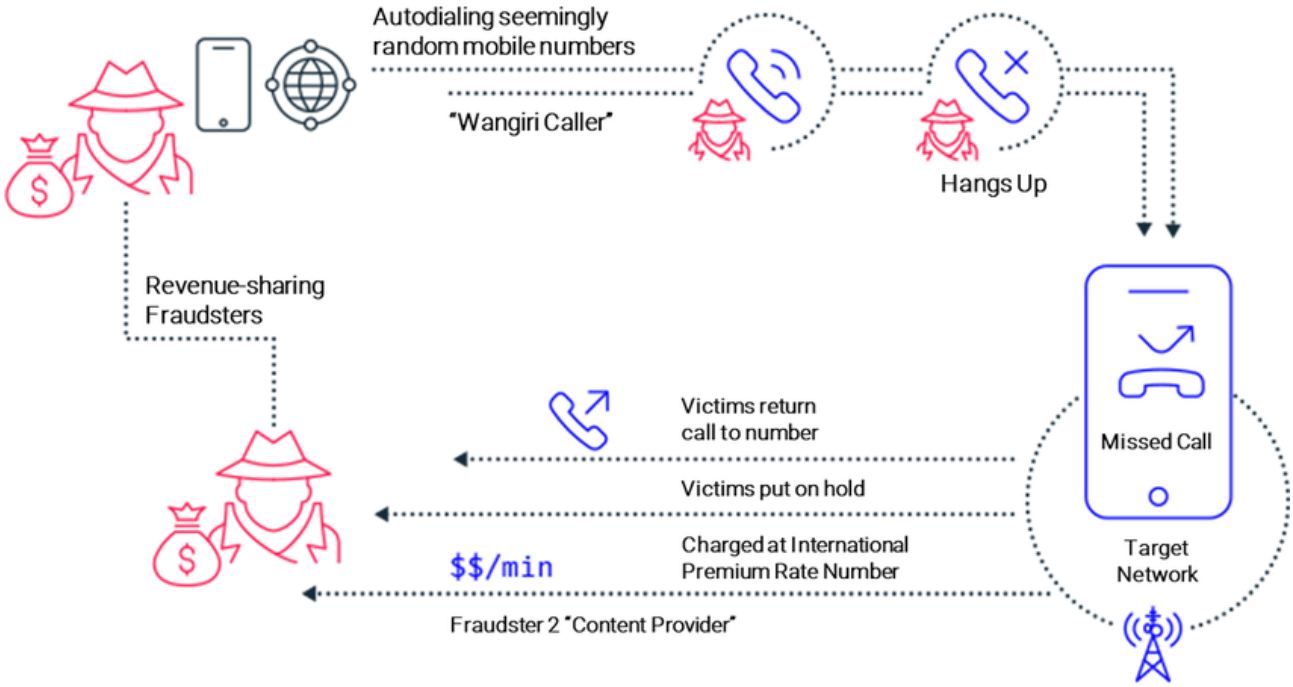

Fig. 2. Wangiri fraud method [6]

In addition to the voice call variant, there is also a form of Wangiri via SMS, in which users receive messages urging them to call back a specific number - usually the wording is urgent or alarming, in order to stimulate an immediate reaction from the victim.

The impact of this type of fraud is twofold: on the one hand, users may have to bear considerable costs, and on the other hand, operators face direct and indirect losses, such as refunding disputed amounts or damaging customer relationships. For this reason, rapid detection and blocking of suspicious calls are essential to protect both the network and users.

3. The designed detection system

In this paper, two of the most widespread and relevant types of fraud in the telecommunications sector are analyzed, selected for practical analysis: Wangiri fraud and SMS Bypass fraud. They were chosen due to their significant impact on both end users and telecommunications operators, as well as their high frequency of occurrence in modern networks.

To better understand the behavior of fraud in telecommunications networks and to evaluate the efficiency of detection mechanisms, the simulation of traffic events is an essential step in this work. Simulation allows the reproduction of fraudulent scenarios under controlled conditions, without affecting real networks and without involving authentic users, thus providing a safe environment for testing and analysis.

The main objective of the simulation is to generate relevant data that mimics real network activity, both under normal conditions (legitimate traffic) and in fraud scenarios. This data is used for:

- Analysis of fraudulent behavior, based on specific traffic patterns.
- Testing of detection algorithms, which are based on identifying anomalies in the structure and frequency of calls or messages.
- Validation of classification and filtering models, used to differentiate fraudulent from legitimate traffic.

Simulation can quickly generate large volumes of data, adapted to different types of attacks, which allows a detailed analysis of how they manifest themselves and the impact they can have on a telecommunications network.

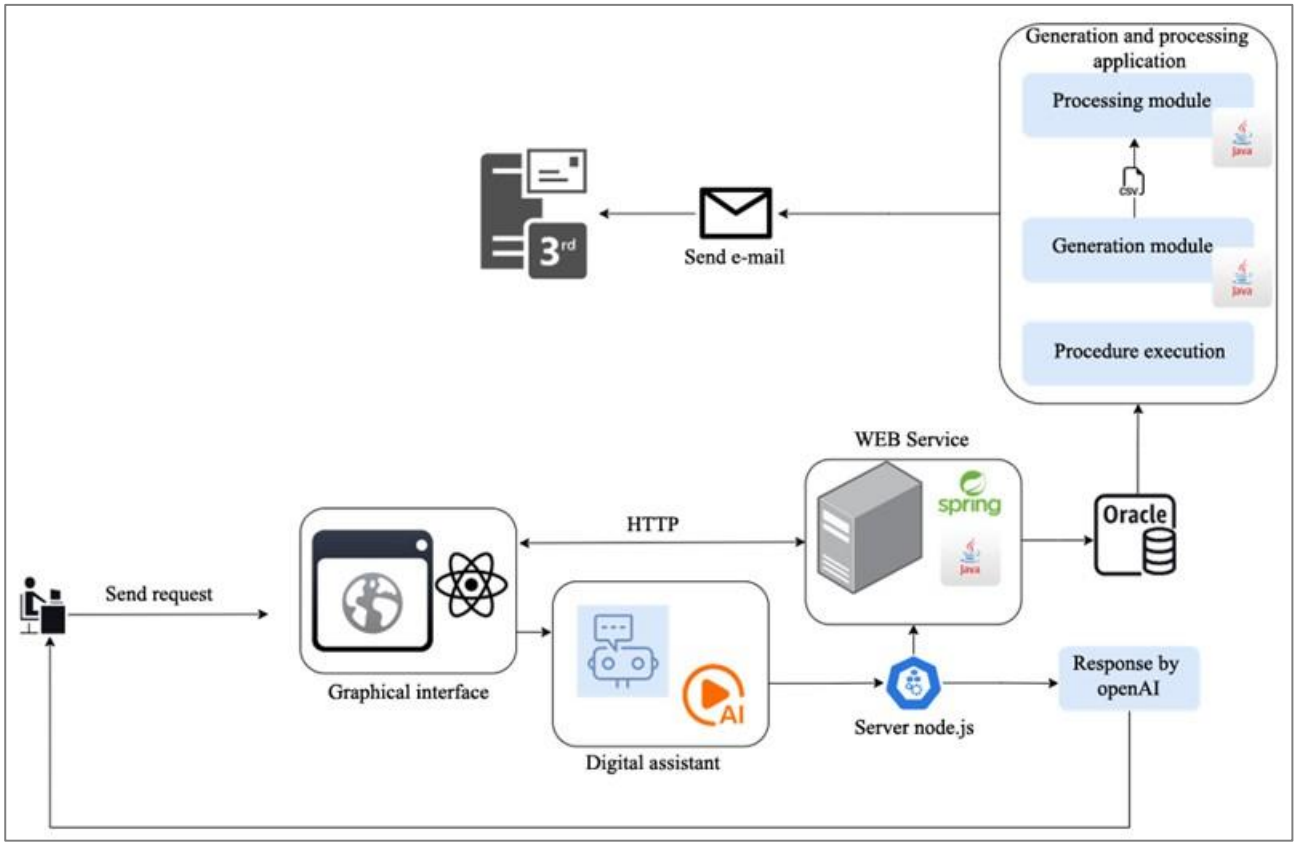

Fig. 3. Architecture of the designed system

In this work, the simulation was performed for two main types of fraud: Wangiri and SMS Bypass. The simulated events were structured to reflect real fraud scenarios as closely as possible:

- Wangiri call simulation is based on the automatic generation of a large number of short-duration events, which appear in the network as missed calls, in a short time interval to many recipients.
- SMS Bypass message simulation is based on the generation of events, imitating the fraudulent use of the infrastructure.

The simulated events are structured in the form of CDR type records, which include information such as calling number, called number, event duration, initiation time, termination time, etc. Both legitimate and fraudulent data events, calls, and messages are also simulated to provide diversity and demonstrate the functionality of data filtering procedures. This data allows for the analysis of network behavior in the presence of fraudulent activities and is the basis for testing detection solutions.

Event Generator

Creates pseudo-random events, but which follow strict rules to maintain data consistency and realism. Thus, each generated event reflects an operationally valid model, and the results can be compared with real traffic. The resulting records are saved as CSV files.

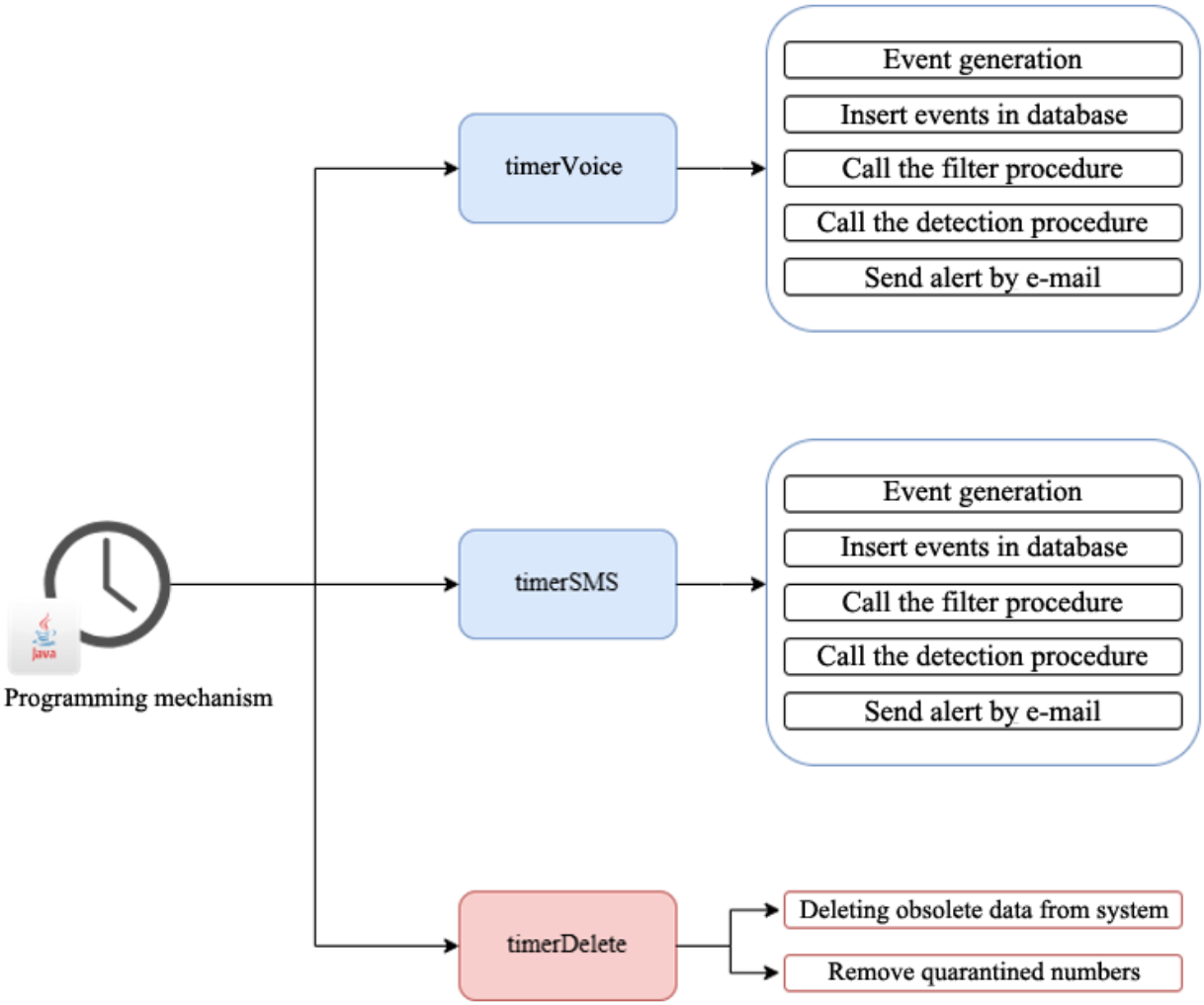

Fig. 4. Event Generator

Database

Contains tables with specific information and attributes. The relational diagram in the database is presented in Fig. 5. Next, I present in detail two of the tables implemented in the database:

detection_rules table

The "detection_rules" table defines the rules used to detect Wangiri fraud. The associated attributes are:

- id_rule - primary key, of type INTEGER, unique identifier of a detection rule.
- id_operator - reference to the operator for which the rule is applied.
- period_of_time - period (expressed in minutes) analyzed to identify fraudulent behavior.
- number_of_events - number of events recorded in the analysis period.
- number_of_distinct_destinations - number of unique destinations called.
- dispersion - degree of dispersion of calls in a certain time interval.

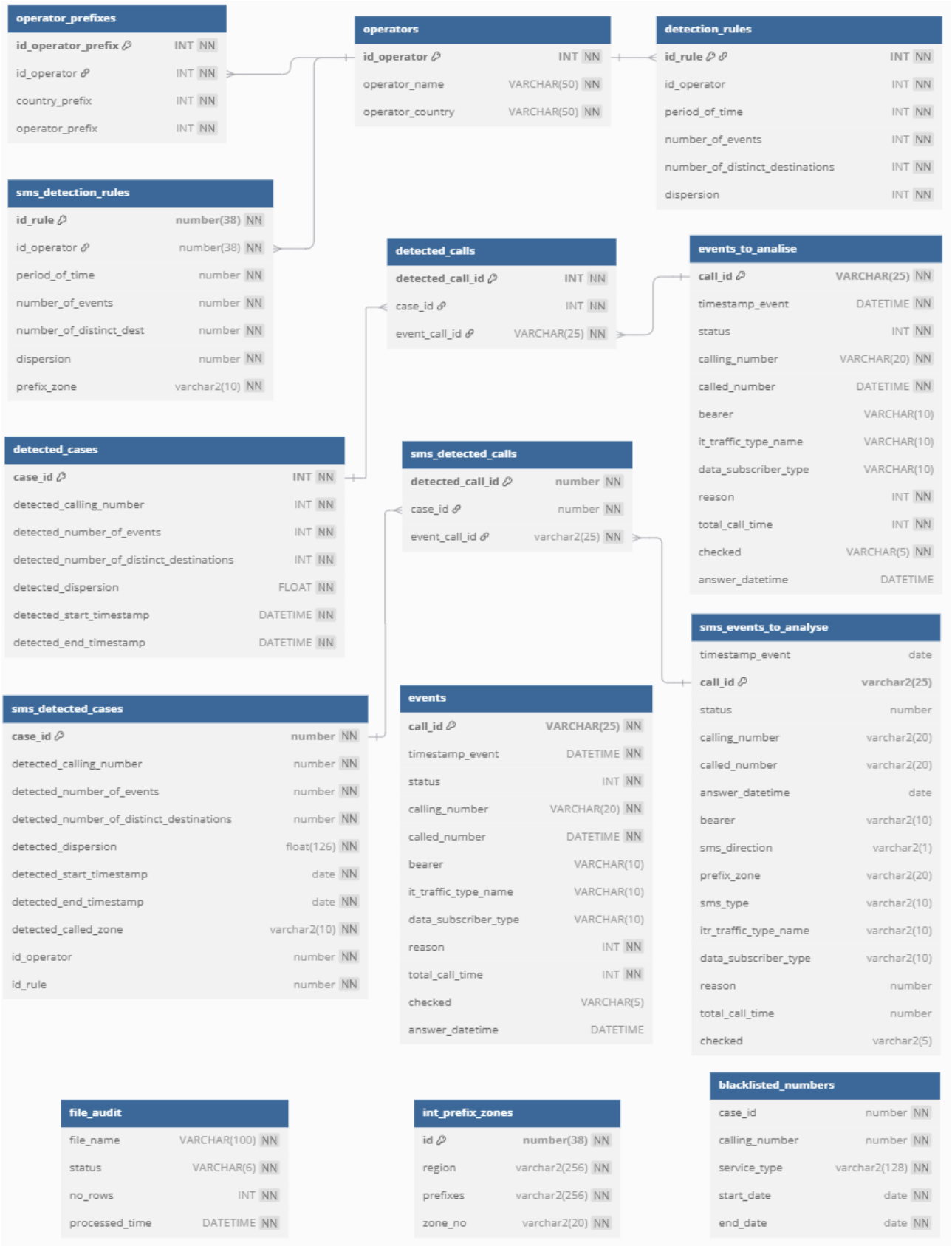

Fig. 5. The database structure

sms_detection_rules table

The "sms_detection_rules" table defines rules applied in the analysis of SMS Bypass fraud. The corresponding attributes are:

- id_rule - primary key, unique identifier of the detection rule.

- id_operator - identifier of the operator to which the rule applies.
- period_of_time - analyzed period (expressed in minutes) to identify fraudulent behavior.
- number_of_events - minimum number of SMSs that trigger the alert.
- number_of_distinct_dest - minimum number of distinct recipients.
- dispersion - dispersion of messages in a given period.
- prefix_zone - international prefix zone where messages are sent.

	ID_RULE	ID_OPERATOR	PERIOD_OF_TIME	NUMBER_OF_EVENTS	NUMBER_OF_DISTINCT_DEST	DISPERSION
1	189	285	20	6	3	0.5
2	3	2	40	10	2	0.2
3	1	1	30	10	2	0.2
4	201	285	50	2	4	0.5

(a)

	ID_RULE	ID_OPER...	PERIOD_OF_TIME	NUMBER_OF_EVENTS	NUMBER_OF_DISTINCT_DEST	DISPERSION	PREFIX_ZONE
1	1	1	10	50	6	0.12	Zone 3
2	2	1	20	30	5	0.16	Zone 2
3	3	1	30	10	3	0.3	Zone 1
4	4	1	60	5	2	0.4	Zone 0

(b)

Fig. 6. The structure of two of the tables implemented in database:
(a) detection_rules and (b) sms_detection_rules

4. Conclusions

The purpose of this work was to design and implement a software system to increase the level of security in telecommunications networks. The system consists of several main components - database, Web service, graphical interface, traffic event generation and execution scheduling application and Artificial Intelligence integration logic. The system's development is based on:

- parameterization of detection and prevention rules for several operators, for each type of fraud considered.
- performing an analysis based on them for the purpose of detecting and reporting detected fraud cases.
- creating the relational model of the database, adding rules for parameterizing operators and for fraud types, defining additional tables for analysis.
- integrating a digital assistant to suggest solutions in natural language to reduce the impact of detected frauds and to provide information from the interface about operators, detected fraud cases, events associated with a fraud case, etc.
- implementation of a processing and generation application that will automate the call of detection procedures and will include two automatic event generators that will facilitate the simulation of fraud traffic for each type of attack and legitimate events.
- graphical interface for viewing and managing detected fraud cases, adding / modifying detection rules and generating statistics in CSV (Comma Separated Values) format.

The central motivation for this work was generated by the need to automate detection and prevention processes, avoiding traditional solutions based on static rules and manual processes. By combining Spring Boot, Oracle Database, React technologies and the generative artificial intelligence model, a system architecture capable of generating, filtering and analyzing traffic data, identifying suspicious patterns and providing real-time assistance to mitigate the impact of fraud was achieved.

The system evaluation demonstrated the effectiveness in identifying fraud patterns, reducing operational response time and providing visualization and interaction tools. The complete integration between data generation, automated processing and digital assistant ensures a fraud fighting platform, where each component contributes to the continuous cycle of detection, alerting and remediation.

References

[1]. Telecom Fraud Analytics: Key Trends 2024, https://dialzara.com/blog/telecom-fraud-analytics-key-trends-2024/.
[2]. CFCA 2021 Global Fraud Loss Survey, Dec 1, 2021, https://cfca.org/document/2021-fraud-loss-survey/.
[3]. R. Dumitrescu, Study: SMS scams up sixfold in Romania in 2023, https://www.romania-insider.com/study-sms-scams-sixfold-romania-2023.
[4]. Fraud Detection and Management for Telecommunication Systems using Artificial Intelligence (AI), https://0d106zzn0-y-https-ieeexplore-ieee-org.z.e-nformation.ro/stamp/stamp.jsp?tp=&arnumber=9951889.
[5]. Arafat, Mais & Qusef, Abdallah & Sammour, George. (2019). Detection of Wangiri Telecommunication Fraud Using Ensemble Learning. 330-335. DOI: 10.1109/JEEIT.2019.8717528.
[6]. Ferreira, Luís & Silva, Leopoldo & Morais, Francisco & Martins, Carlos & Pires, Pedro & Rodrigues, Helena & Cortez, Paulo & Pilastri, André. (2023). International revenue share fraud prediction on the 5G edge using federated learning. Computing. 105. 1-26. DOI: 10.1007/s00607-023-01174-w.