POLITECNICO DI TORINO

Master Degree in Computer Engineering

Master Degree Thesis

Analysis of a multi-channel anti-fraud platform in banking

Supervisors/Advisor
Prof. Alessandro Savino
Dr. Nicoló Maunero

Candidate
Federica Cugnasco

Academic Year 2022-2023

Abstract

Banks are facing fraud attacks every day and in order to minimize their exposure they need to implement the latest anti-fraud technologies. In the banking industry, the costs of fraud incurred cause large damages compared to the lower costs of implementing solutions to prevent attacks.

Checking on banking transactions, such as a withdrawal, wire transfer, or deposit, must take place both in real time, at the time the transaction is created, and in batch, which often falls within a day.

An anti-fraud architecture is a complex system that correlates many components, each based on specific protocols and algorithms, and makes them able to communicate with each other so that transactions can be analyzed both in real time and at a later time. An anti-fraud check consists of many steps, some among them being the extraction of the historical data of the customers involved in the transaction, verification of their presence on any blacklists or whitelists, and a check on the amount of money. Then all the data will be passed to components that will analyze it and produce a risk code. Based on this code, the transaction will be accepted or rejected.

The challenge of an anti-fraud architecture is having to run every possible check, on the user, on accounts, on fraud trends, on background and other checks still, managing to produce a risk index within very few seconds. In fact, the bank not only wants to avoid all fraud but also wants to keep a customer satisfied, performing his transactions without taking up time. Included in this time is latency, which leaves very little time for processing and communication of the other components.

The modules that make up the architecture are chosen based on their performance, cost, and the ease with which they can be introduced into the system and communicate with adjacent modules. Some components use only incoming and outgoing REST API calls, while others expect to send data via a Kafka or MQ queue. Once suitable components have been identified, these must be integrated into it and tested for efficiency and reliability.

Contents

Chapter 1

Introduction

Anti-fraud architectures are widely used in the banking sector to detect fraud attempts and respond promptly to threats. This is because when a bank is subject to fraud, it risks not only a financial loss but also reputational damage, as customers are more likely to switch companies. A robust anti-fraud platform analyzes all transactions involving its customers and must be able, through up-to-date rules, to detect accurately whether it is fraud or not.

The project was focused on introducing improvements within an already functioning anti-fraud banking architecture to avoid not keeping up with new challenges and technologies. An anti-fraud platform must always be evolving, as with the introduction of new types of attacks, fraudsters exploit every flaw to circumvent systems. A modern architecture reviews all transactions, adding historical data about the customer and branches involved to the analysis in order to obtain an accurate risk index.

The first steps were the study of current components and supported protocols, to identify possible connections with additional and better performing modules. Existing rules for processing data regarding online payments and for sharing identified fraud globally were reviewed. Payment Services Directive 2 mandates Multi-factor authentication for users and requires sharing of collected transaction and fraud data. Through sharing, all banks can benefit from the exchanged data and block malicious actors in time.

During the development of the thesis, the modules available on the market were analyzed, and a list with the best modules in terms of efficiency, cost, and ease of integration into the architecture was studied.

Along with the bank, the requirements that the framework needed to support were defined, which covered the speed to analyze a transaction and provide a risk index, the ability to automatically create alerts when the fraud risk index is high, and the ability to add analyst-created rules.

For a period, project management activities were also carried out for the tasks

involved in integrating the new components and implementing the tests in collaboration with the bank. The activities pursued also included managing the budget to buy licenses or modules needed for the architectural upgrade and to talk to various vendors with the scope of exchanging information to identify the necessary components.

Two possible flows were analyzed, one including the service bus and one excluding it. The service bus was later introduced into the architecture to allow for the smooth reception of historical data from the mainframe and real-time transaction data. With the capabilities of this enterprise bus, the data was transformed into the REST API format expected by the orchestrator. MQ queues were introduced to enable the receipt of some historical client data essential for in-depth analysis of the transaction. The orchestrator performs the task of managing an entire operation, providing the calculated risk index and creating a ticket in case of detected fraud. The event monitoring module has also been introduced in the architecture, which through the rules set by the bank's analysts and preset rules allows an optimal selection of the most risky transactions, reducing the workload of anti-fraud experts. the integration of the orchestrator with Security Information and Event Management (SIEM), carried out through REST calls, has been analyzed. The latter connection allows the transaction and its analysis to be saved in the archive, so that it can be used in the future in case the customer is the same or if the conditions fall under the same parameters. Finally, the proper functioning of ticket creation in case of detected fraud was tested: in this way an expert receives the task and analyzes it with a different perspective confirming the result or overturning it.

Toward the end of the thesis development, different types of tests were conducted to make sure that the architecture worked properly with the added components. Both acceptance tests were conducted with the bank to compare the user friendliness of the anti-fraud dashboards and the ability to build appropriate rules for the latest fraud. In addition to these tests, a contribution was made by performing stress tests to learn about the physical limits of the platform and to check that in particular situations the platform continues to work as intended. During these tests it was verified that transactions are analyzed in real time and within 200 ms, in this time it must be included that the event monitoring calculates a risk index and that the anti-fraud system sends a response to the service that generated the request. The transaction data is then sent to the SIEM afterwards, in order to be reused in future analyses.

Structure of the document: Chapter 2 presents an overview of Accenture, the company at which the internship and thesis were conducted to study and enhance a bank's anti-fraud architecture. Throughout the project, analysis and design activities as well as project management activities were carried out in order to achieve the goals established.

While Chapter 3 discusses the European standards related to online transactions, which every bank must comply with. It also shows the different scenarios in which fraud is detected and the distinction between real-time and batch transactions. The last section deals with the most common and recent frauds, analyzing the data used and the method by which they are performed.

Chapter 4 reports on the activities performed during the project and the contributions made to the design of the new version of the anti-fraud platform. Studies were performed on the situation in use prior to the project and on the possibility of smooth integration of components within the architecture.

In Chapter 5, following the implementation, the contribution in terms of work carried out for performance and latency testing is described. It was necessary to verify the compliance with the maximum execution time of a transaction, including the added milliseconds due to the architecture, to check its influence on the daily use of the client.

Chapter 2

Accenture

At the company Accenture S.p.A, I carried out a curricular internship and thesis aimed at deepening my knowledge and techniques regarding the implementation of a new multi-channel anti-fraud platform with learning methodologies and techniques for the design and implementation of complex solutions in IT Security.

Accenture is a multinational company active and focused in the strategic and management consulting industry. The company is firmly in the Fortune 500, the ranking of the world's top 500 multinationals by revenue. The company also performs business process redesign in the areas of finance, accounting, management control, as well as IT consulting. In Fig. 2.1 the logo of Accenture company is shown.

Figure 2.1. Accenture logo [1]

The company consists of 738,000 employees worldwide and is spread over 49 countries, with more than 200 cities in which headquarters and offices have been built. In Italy Accenture has been present for more than 60 years, with offices in Turin, Milan, Rome, Naples and Cagliari and offices scattered throughout the country. In terms of numbers Accenture in Italy has about 20,000 employees and in the last 3 years has averaged 2,500 annual hires. Accenture works for more than 7,000 clients in 120 countries, combining the strength of technology expertise,

functional skills and global delivery capabilities. The company labels the services provided under Strategy and Consulting, Technology, Operations, Industry X, and Accenture Song.

Strategy and Consulting is responsible for always formulating new strategies, reinventing the company to foster its growth and competitiveness. The area is responsible for identifying sustainable options and promoting constant improvement.

The Operations area manages business processes on behalf of clients for some accounting, finance, supply chain, marketing and other operations.

Industry X, on the other hand, is responsible for helping customers reimagine the ways in which their products are designed, renewed and returned through the use of data and technologies such as 5G, AI, IoT and Cloud/Edge.

Song is the area with a focus on creative, media and marketing strategy, campaign and content design and organization.

Technology, the area I entered with the internship, focuses on providing services and solutions ranging from Cloud to application integration and management, software engineering services and data analytics. Accenture is always active in exploring new technologies such as blockchain, 5G, edge computing and Metaverse. Cutting-edge technologies offered by Accenture's many Partners include Adobe, Alibaba, Amazon Web Services, Blue Yonder, Cisco, Dell, SAP, Google, ServiceNow, Microsoft, IBM RedHat, and many others. Technology in turn includes the Cloud part, where new ways to revamp hardware-based IT infrastructures into intelligent, software-defined infrastructures are explored. Data is leveraged more on the cloud, as scalability and agility abilities are leveraged. Another sub-sector, with the spread of the cloud and rapid digitization, is Security. Indeed, attack surfaces and vulnerabilities have increased, which is precisely why continuous study and evolution is needed.

Chapter 3

Background

All banks must adhere to fairly strict regulations on handling customer data and sharing the results of fraud analysis. During the writing of this thesis, studies were conducted on the rules set for sharing the reporting of identified fraud, in order to have a globally updated view and respond to threats immediately. Another requirement to be met for the execution of online transactions is the introduction of Two-Factor authentication to verify the customer. The technologies developed worldwide allow a choice of several alternatives for Multi-Factor authentication without compromising user experience.

It is important for a bank to collect transaction data and to be up to date on fraud trends in order to identify and stop them in time. Each transaction can be analyzed with different criteria depending on whether it is a real-time, for example, an online payment or batch, such as a periodic transfer. The most common attacks that have recently occurred include data breach, in which customers' credentials are made public, credential stuffing, where starting from a data breach a fraudster carries out a brute force attack trying to exploit stolen credentials and access online banking sites. Among the several existing attacks it is common to find also phishing and its variants, in which hackers target a customer or employee and through malicious links try to steal his or her passwords.

3.1 Digital transformations and regulations

As the years have passed and technology has evolved rapidly, banks needed to accelerate their technological transformation. This need has also turned into a duty to comply with the new PSD2 regulations [2] (the 2nd Payment Services Directive), so as to foster wide-ranging innovation in the industry and make payments even more secure.

Payment Services Directive 2 is a regulatory directive aimed at all participating

European countries. Digital leaders outside the payments industry and the immediate European market will also feel the impact, as it will transform the delivery and consumption of digital banking services.

Banking is organized into areas, which include retail banking, to manage services made available to customers, corporate banking, to manage services for business and corporate customers. Also included are payments, investment, and financial services. In each operation related to the previous areas, large amounts of data are involved, in the form of databases containing information about the customer, customer transactions, etc.

PSD2 has been in place since the beginning of 2018 and covers payment services in the internal market. One of the requirements concerns the method of sharing the reporting of bank fraud data: all payment service providers (PSPs) must provide the statistical data to the their competent authorities in aggregate form. The PSD2 articles were introduced to encourage member states to share data collected on fraud for all payment instruments by introducing universal definitions of fraudulent transaction. PSD2 requirements are:

- **Open Banking:** banks are required to share transaction information with third parties (TPPs) to enhance collaboration and services offered to the customer.
- **Strong Customer Authentication:** PSD2 requires banks to strongly authenticate the user to make online payments. The standards adopted are designed to protect the customer and securely authenticate the customer.

To increase customer protection, regulations have mandated the use of more stringent security requirements, such as the introduction of Multifactor Authentication (MFA). MFA is an authentication method that requires users to prove their identity through two factor verification before they can access certain resources or applications. In addition to the basic username and password credentials, additional steps are in fact required to drastically reduce attacks from cyber criminals. Tools developed by various companies to implement Multifactor authentication are based on the following parameters:

- **Location:** geolocation of the user can be useful in recognizing possible attacks and promptly blocking attempts.
- **Possession:** authentication by possession is based on ensuring that the user has a card or badge available to verify his or her identity.
- **Inherence:** Inherence includes authentication by biometric parameters such as fingerprint, face detection and other new techniques, which are being developed and refined all the time.

- **Knowledge:** an example are security questions to which only the real user knows the answers, as they are set directly at user registration. They can range from personal questions to questions about teachers, pets, or locations visited.

Currently, various types of multi-factor authentication have been developed, which differ from each other in the way identity is verified. The latter can be done as an analysis of the user's location, or by his possession of a key or an OTP code. The second authentication factor, along with credentials is requested and verified by a central Identity Provider (IdP). MFA is an essential aspect in safeguarding digital assets.

- **Time-Based One-Time Password (TOTP):** a Time-Based OTP is a code of about 6-8 digits that has a duration ranging from a few seconds to a few minutes. Often these codes are generated through Multi-Factor Authenticator Apps, such as Microsoft Authenticator, DUO or Google Authenticator. The user opens the application from the phone or computer by entering a pin or password, the application begins to generate tokens. The user will take a currently valid code and enter it as a second authentication factor, approving the operation.

- **Email token:** email token involves users receiving codes of about 6-8 digits by email to enter on the authentication page to confirm their identity. If this methodology is used, it is necessary that emails be protected with strong passwords so as to prevent attacks.

- **SMS text message token:** this technology involves registering one's phone number as the first step at the first login, to which codes will then be sent through SMS with each authentication. The user will have to enter this code on the login screen to confirm their identity. The SMS token is one of the least secure as a method of MFA, because it is prone to SIM swapping attacks in which a hacker through social engineering activities convinces the carrier that he has lost or broken the phone, when in truth it was never his.

- **Biometric authentication:** in this case, the second factor is based on the verification of biometric parameters, such as the fingerprint scanned at the first login or facial recognition. it is one of the most secure methods since everyone has his or her own fingerprint, but care must still be taken since the fingerprinting tools may have a lower accuracy and therefore one may match more than one person. However, the probability of this happening is very low, and this methodology allows one to be certain of the person's authentication. If the fingerprint or a biometric parameter should ever be compromised it should absolutely not be used as a Multi-Factor Authentication method again.

- **Hardware security key:** the hardware security key consists mainly of a USB flash drive or personal badge. This type exploits physical recognition, in the possession of the person to be authenticated. Being impossible to hack, this is the second most secure factor , while as a user experience it requires a different action from the usual SMS that users are used to.

- **Security questions:** one way to perform second authentication is to prepare a set of questions that the user will answer with some personal details. it is important that the answers cannot be found through social engineering or even worse from the user's socials. This method is less used in authentication for online payments or logins on banking applications while being used.

- **OTP Over Phone Call:** after the first login in which the personal number to call to authenticate the user is configured, for each transaction that tries to activate the customer will receive a call and upon answering will hear a code between 4 and 8 digits that they must enter on the open payment page.

The benefits of implementing MFA mandated by PSD2 regulations are many, starting with increased protection on online payments, ensuring everyone is who they say they are, reducing costs due to handling detected fraud and improving the user experience without introducing complicated procedures. The following is an excerpt from the document in which Dynamic Linking is requested to be implemented:

- The payer is made aware of the amount of the payment transaction and of the payee [3]. The statement specifies that the details of the transaction, i.e., who the money will go to and how much should always be visible to the customer.

- The authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction [3]. It is good practice to associate each transaction with a universally unique identifier (UUID), so that each unique code is linked to the sum of the transaction and the recipient.

- The authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer [3]. This statement refers to the user's ability to generate a second authentication factor in multiple ways. Once authenticated with the MFA in fact, all other possible codes will be invalid in order to complete the transaction.

- Any change to the amount or the payee results in the invalidation of the authentication code generated [3]. In the event that the transaction sum or

other parameters should change, it is essential that all codes be invalidated and a new authentication requested.

A further requirement of Payment Services Directive 2 reports that all data exchanged between all parties must be encrypted to ensure confidentiality. The introduced and regulated a service that allows banking customers to have a non-banking application, referred to as a Third Parties Provider (TPP), as an intermediary to perform payment transactions. These TPPs can be either Payment Initiation Service Provider (PISP), Account Information Service Provider (AISP) and Card Issuer Credit Provider (CISP). The addition of these intermediate services allows them to perform profiling activity.

The General Data Protection Regulation (GDPR) is a set of rules introduced in 2018 that must be applied by any company that processes data about people in the EU to facilitate the free movement of data and ensure the protection of that data. If a company that does not operate in the EU were to manage the data of people residing in Europe, the GDPR applies to them as well.
Data protection principles are the following:

- **Lawfulness, fairness and transparency:** it is only possible to collect, process, and share Personal Data fairly and lawfully and for specific purposes. The GDPR allows processing of data for specific purposes, such as where the user has given consent to the processing of the data or the processing is necessary for the performance of an agreed activity with the Data Subject (the customer). Consent must be obtained in a valid way, that is, the client must click a flag, which must not be already pre-filled or not highlighted. The GDPR also stipulates that consent can be revoked quickly. Transparency, on the other hand, is required so that the user is aware of how and why their data is being collected. This communication must therefore be placed in a clear and concise manner.

- **Purpose limitation and data minimization:** personal data must be collected only for specific, explicit and legitimate purposes. it is strictly forbidden to use the data for purposes other than those disclosed when it was first obtained, unless the client has been informed of the change.

- **Accuracy:** personal data collected must be up-to-date and accurate. In case of change, this data must be deleted.

- **Storage limitation:** the GDPR requires that personal data be retained only for the period of time necessary to fulfill the stated purpose. Each company must take responsibility for deleting all personal data that is no longer needed.

- **Integrity and confidentiality:** personal Data must be protected by appropriate technical measures against unauthorized data processing, and against

loss, destruction, or damage to the data. new technologies must be implemented to provide protection of personal data from creation to deletion. Confidentiality requires that only those who need to work with that data for a particular purpose have access to it. One point emphasized by the GDPR requires that in the event of a data breach, the Informant Commissioner be promptly notified of the event.

- **Accountability:** in order to follow the regulations, it is required that Data Controllers provide for a Data Protection Officer (DPO) and that Privacy by Design is implemented for each operation or project. Periodic testing is also required to check that the measures are being followed and constant training of the Data Controller.

A final point provides that Automated processing and Automated Decision-Making (ADM) are prohibited when a decision has a significant legal effect on a person, unless explicit consent has been received or processing is essential to the completion of the activity.

Therefore, GDPR is concerned with the protection of personal data in every sector, including banking, while PSD2 aims to make the inclusion of new players and the enhancement of user authentication more flexible.

3.2 Introduction to anti-fraud architectures

A bank's operating perimeter is distinguished between transactions that take place online or by mobile that customers can perform anywhere, transactions performed directly at the counter, and routine internal operations. This section discusses the different types of transactions and the statistics on frequency of their usage.

3.2.1 Banking perimeter

In banking, the perimeter on which the Company operates is divided into three parts based on the platform used to carry out the transaction:

- **Online Banking:** direct channels are those on which most transactions circulate, and volumes are increasing every year. In fact, they include Online Banking and Mobile Banking platforms, which are available to the user wherever they are. Customers have reduced the times they go to the Counter and prefer to conduct transactions from the comfort of home. With the need to provide the user with the ability to carry out transactions that were previously only secured at the Bank even from home through Online Banking, controls and rules to identify possible fraud have had to adapt.

- **Branch:** activities include all transactions performed from the counter or through the Automated Teller Machine (ATM). Branch Banking refers to the wide network of branches made available by the Bank to the customer to provide banking services. The customer goes to the branch to make Domestic and International, SEPA, Urgent, and Circular Transfers and open or manage an account.

- **Internal Banking:** internal Banking includes all management activities carried out within the Bank. Since employees have both knowledge of and access to regulations and structures, it is essential to have rules to protect against internal fraud.

3.2.2 Fraud Trends

The strong technology push has led to the need to support and secure a large number of transactions performed online, making them available anywhere, anytime, but at the same time exposing sensitive data on a global scale and increasing the risks of fraud. Technological prevention, yes, has improved, but hacker attacks never stop and are constantly expanding, exploiting every possible vulnerability. They often target customers and employees of a bank or business with a website on which assets can be purchased with attacks designed to obtain customer credentials or sensitive data. Fraud has evolved keeping pace with the latest technologies and consumer habits: with the rise of online shopping and the increase in the spread of information on social media, hackers are spoiled for choice for their attacks.

In Fig. 3.1 is presented a diagram of the major attacks in recent years.

This year's report [4] shows that over £1.2 billion was stolen through fraud in 2022, a reduction of eight per cent compared to 2021. Within that overall figure, unauthorised fraud losses were £726.9 million (down less than one per cent) and APP fraud losses were £485.2 million (down 17 per cent). Protections such as Strong Customer Authentication (SCA) and Confirmation of Payee are having an impact, but too much money is still getting into the hands of criminals [5].

In Fig. 3.2 it is showed an increase in card fraud, along with online and ATM frauds.

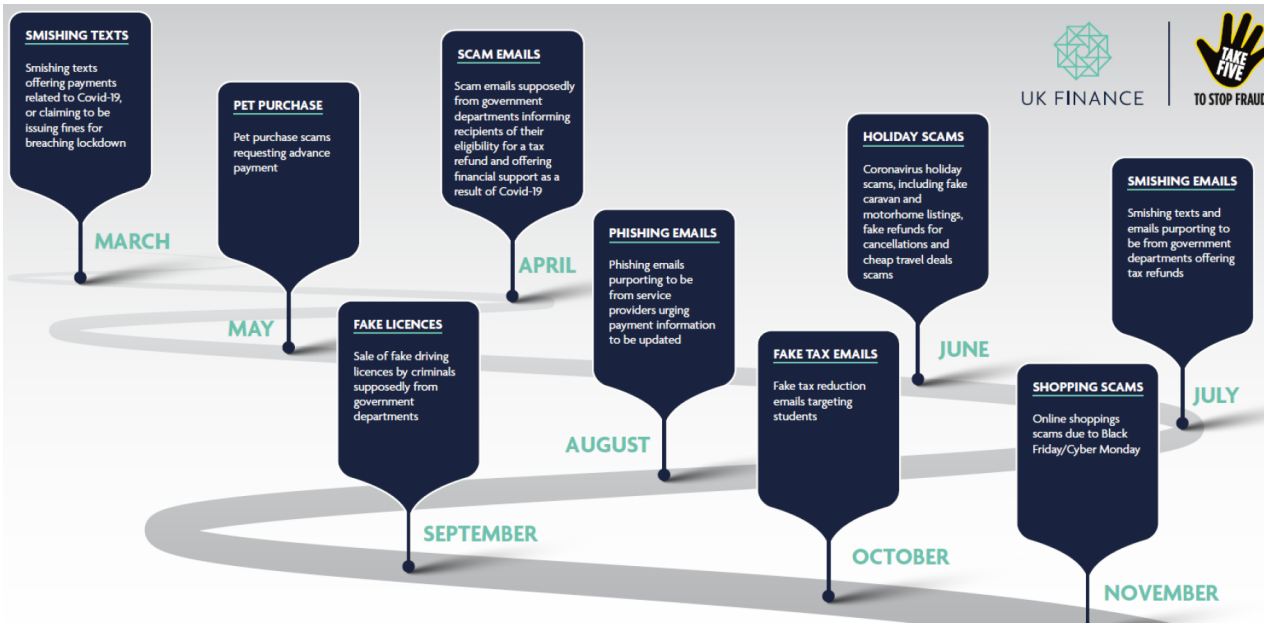

Figure 3.1. Bank Fraud Attacks recently [4]

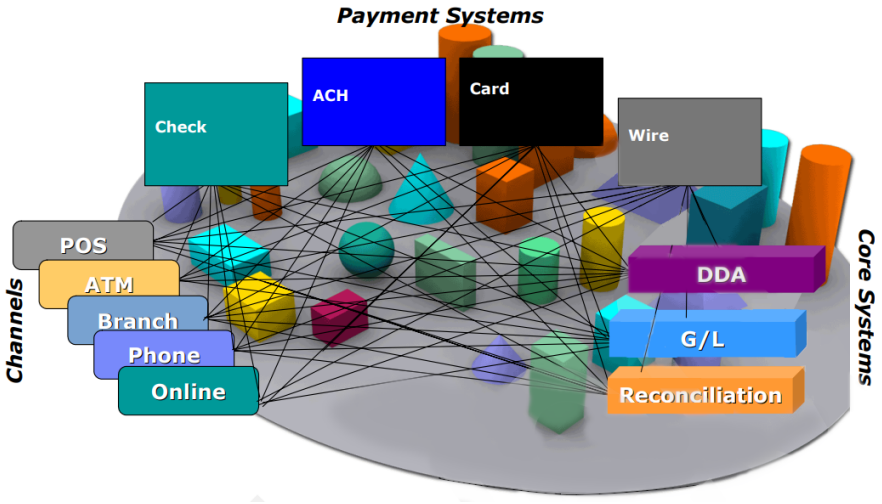

Figure 3.2. Major bank fraud attacks [6]

Online payments frauds are increasing and the most targeted platforms include direct channels and mobile transactions.

3.2.3 Real time e near real time

Having to analyze all the transactions processed by a banking system, the analysis can be reduced to three types based on the time required for processing and the amount of data:

- **Real-time:** the transaction requested by the customer requires an immediate response. In cases such as an ATM withdrawal or a transfer requested at the counter, it is crucial that the system performs the processing immediately. Real-time can also be used for streaming data, where given the continuous input, continuous processing is required.
- **Near real-time data:** this type is often referred to operations that do not require a response in a few seconds, but it is acceptable to produce a result within a few minutes. Near real-time is used in conjunction with CEP, or Complex Event Processing, whose scope is to collect data from numerous sources and detect recurring patterns for threats or fraud. This method is used to continuously monitor operations performed and enriched with inherent data so that the organization can detect problems and act accordingly immediately.
- **Batch:** batch processing consists of processing large volumes of data, collected at the time of each transaction and stored on databases. This type requires different tools for input, processing and output. For input, in fact, with each transaction analyzed by event monitoring, a data set is sent to SIEM to be entered into the logs. During batch analysis, a tool with large computational and large volume handling capabilities is required, while as output, in case of suspected fraud, the SIEM will generate a direct request to the incident management service sending the transaction data, event ID and a timestamp.

Real-time analysis is fast and does not require large amounts of data to run, while it requires a timely response and is an expensive solution, as it requires high performance hardware. Batch analysis, on the other hand, is more accurate, as it has a large dataset and does not require a response in seconds, but the output still needs to be checked by analysts. In banking, it is necessary to have operations oversight at every level, real-time, near or batch. Combining analytics helps identify fraud trends and be able to take immediate action.

3.2.4 Bank channels

As the massive use of cell phones, tablets and computers has increased, the banking sector has also had to adapt by expanding its scope. Portals have been created through which a user can check his balance, make transfers and manage his

account. Recently, smartphone applications have also been introduced, through which a user can perform the same transactions that he previously had to do at a teller or at an ATM.

Banks currently implement an omnichannel system through which they provide customers with a seamless banking experience, offering baning service through the various channels: mobile banking, online banking, physical branches and call-center. According to a Statcounter study, from 2021 to 2022 the market share of mobile users was 60%, while 38% were customers via computer, clearly indicating the need to expand and fortify online and mobile channels.

With online banking, customers receive more timely responses, which increases their satisfaction and makes them continue to rely on the bank to manage their finances. At the same time, the cost of running branches is reduced, while the cost of maintaining the infrastructure is increased.

Attackers seek to exploit weaknesses in payment systems and customer accounts, with the goal of stealing funds without physical interaction. To accomplish these goals, they use a variety of malicious techniques, such as installing malware and phishing scams that can lead to identity theft, theft of credit card data, or unauthorized access to bank accounts. Improving online user identification and enhancing transaction monitoring is critical to catching fraudsters without affecting its customers.

3.3 Attacks and how to protect against them

Banking and real-time transactions have always been the target of many hackers. In Fig. 3.3 the most common threats for online banking are presented.

Based on the perimeter targeted by fraudsters, transactions are exposed to different attacks. Fraud on transactions carried out online is often the result of data breaches and credential stuffing, in which hackers get hold of usernames and passwords and complete the transaction instead of the customer. On the other hand, when fraudsters target internal operations, phishing and social engineering attacks sent directly to employees are more common. The last fraud examined involves the corrupted employee, who will carry out illicit transactions through his credentials which have multiple permissions.

3.3.1 Credential stuffing

The OWASP classified credential stuffing as a brute force attack, i.e., attacks in which hackers use automated software to try all possible combinations and gain possession of an account. Credential stuffing attacks consist of exploiting compromised credentials obtained through a data breach, and using bots or automated scripts to attack and gain possession of an account, known as account takeover

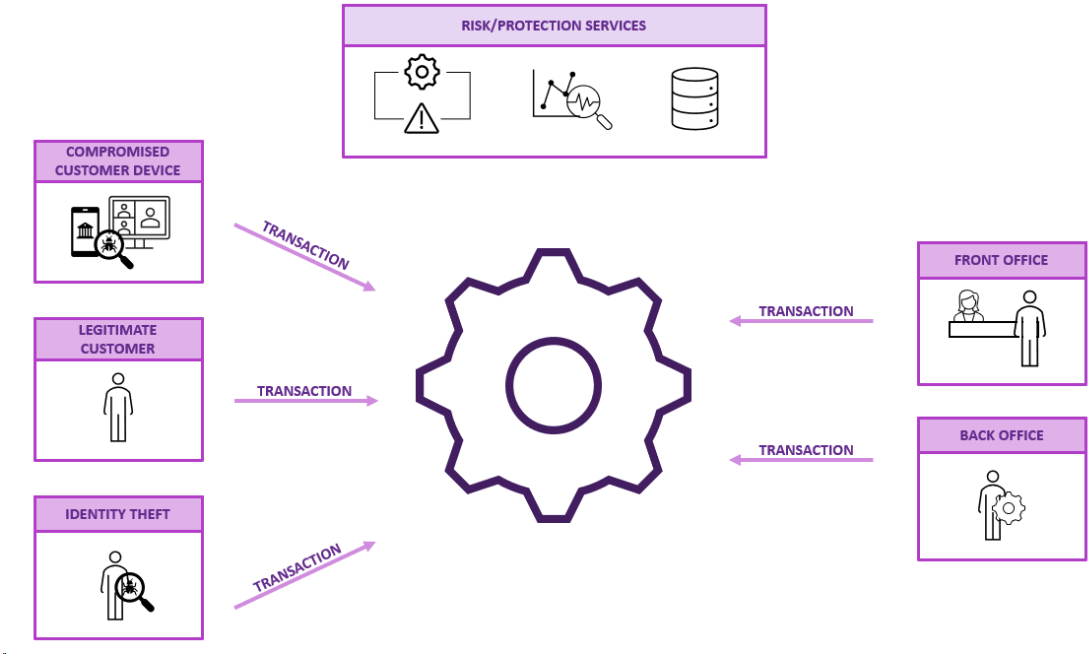

Figure 3.3. Bank fraud transactions background [7]

(ATO). Credential stuffing is based on users' habit of using the same password for different sites to remember it more easily. Hackers use scripts to go through all the credentials obtained through the data breach and try to seize the account. This type of attack has a very low success rate, between 0.1% and 1%, but because the data available is voluminous, there is a pool of vulnerable accounts that makes the attack tempting. The hacker will try various combinations extracted from disclosed accounts and conduct attempts to verify whether the same password is used for social media accounts or bank accounts. An organization to defend against a stuffing credentials attack can run scans on users and check whether the users included in data breaches relate to its customers. The prevention to be used in such cases is to prevent the user from using passwords found in cracking dictionaries and to require a minimum length and the use of special characters. At the same time, restrictions should not be overdone either, because they would bring frustration to the customer and this should be avoided at all costs. Specifically, credential stuffing attacks can be identified by the following techniques:

- **Multi-Factor Authentication (MFA):** the implementation of a second authentication factor is a method that ensures that the user who is currently accessing the service is indeed him or her. The second verification is through a code sent by SMS, an OTP code that the user retrieves from an application

installed on his or her device, using hardware tokens, or authentication using biometric data.

- **Device fingerprinting:** through the integration of modules that perform behavioral fingerprinting, leveraging customer habits and information from the hardware and software used, which combined make the fingerprint left by the customer unique.
- **Rate limiting:** the bank tracks login attempts and in the case of unsuccessful attempts can introduce a progressive delay in the ability to retry login and set custom rate limits for suspicious accounts. Real-time monitoring is also implemented to recognize multiple geolocations, detect unusual IP address changes, identify bots, and by setting maximum request thresholds, greatly reduces the risk of letting compromised accounts act.

3.3.2 Data breach

The largest data breach that occurred in 2022 impacted Flagstar Bank, involving more than 1.5 million consumers, as much of their sensitive information was exposed and compromised. Previously in 2021, Morgan Stanley customers were victims of a data breach. Hackers collected personal data and social security numbers by decrypting the company's files with a decryption key stolen through a vulnerability. Recent studies have calculated an average of 275 days to identify and contain a data breach, which already are small numbers compared to the previous year. To reduce the cost of a data breach by nearly 10 percent, Extended Detection and Response (XDR) rules have been implemented.

3.3.3 Push Payment fraud

This attack also known as APP fraud consists of cyber criminals trying hard to be trusted by victims, who will then give them money by approving transactions with push notifications of second factor authentication and password. These scams are targeted toward elderly people or people who are not confident with new technologies.
A recent attack spread to thousands of Whatsapp chats consisted of a message with the text "Hi Mom, it's me! I broke my phone and had to change my number." In this first step, criminals try to pass themselves off as children/grandchildren or relatives and friends of the victim by saying they lost their phone or with similar excuses. When they receive a response the attackers proceed by asking for money to buy something urgent, such as some medications. At this point, the criminals share a new IBAN to which to deposit money, on which they are ready to empty by buying gift certificates that can no longer be traced.

3.3.4 Phishing and Smishing

Phishing can be executed via phone, email or social media and is intended to induce the victim to download malware or enter credentials on a malicious site. Recent statistics say that 1.2% of emails received are phishing, which corresponds to about 3 billion phishing emails. It has been recorded that 88% of companies are subject to phishing attacks within a year, with an average of $4.90 in breach costs. In the banking sector, the most common phishing attacks are mishing (SMS) and spear-phishing campaigns (fake emails).

Smishing is a cyber-attack that exploits SMS (Short Message Service) and text messages to scam users. The attacks, like email phishing, carry messages in which they demand immediate action from the user, or they will lose access to their bank finances. Hackers emphasize urgency, imposing deadlines within hours, confident that the user, caught up in anxiety and haste will not check some details that reveal precisely the scam. The goal of the attack is to make the user download malicious software, or click on a link that redirects him or her to a fictitious page created specifically to steal credentials. This occurs because hackers gain credibility by developing web pages identical to those of banks or by reproducing the same content and format of SMS messages received from banks. The link is inserted into the body of the email with a hardcoded malicious URL, built via shortURL systems. Many users are more vigilant about the emails they receive and tend to trust SMS more, as the attack developed later.

The steps of smishing attacks are given below:

1. **Target selection:** victims are identified either by buying lists of users obtained from data breaches, or by targeting a specific company.

2. **Message creation:** the SMS must be reconstructed exactly like the original one from the bank, with the addition of malicious links.

3. **Sending SMSs:** spoofing tactics using burner phones or specific software are used to disguise the sender, and the SMS is sent to the list of users.

4. **Attack:** through malicious urls and pages, sensitive data of victims are colleted or in other cases malware is installed on the user's device.

5. **Use of sensitive data:** once collected enough information, the hacker can use that to try selling on the blackmarket, identity theft or perform unauthorized transactions.

Phishing and smishing attacks have a wide range of victims and target both companies and individual users, inserting special details tailored to the case. Below are some of the most common smishing attacks in the banking industry:

- **Bank fraud alerts:** in this attack, the SMS alerts the user to an unauthorized transaction or suspicious activity and incites the victim to click on the link to view the transaction and payment details, directing him or her to resources operated by the hacker. A common message sent by attackers is: "Dear [Bank Name] customer, we have detected unusual activity on your account. Please click on the link to verify your transactions: [malicious link]".

- **Account verification:** the hacker sends a message posing as the bank with an urgent need to verify credentials before the narrow deadline.

- **Tech support:** the victim receives a message in which the hacker enters an incident code and highlights a hardware or software problem with the device in use. By calling the support number, the victim risks not only the loss of credentials, but also giving over remote control of the device to the hacker.

To send e-mails in an automated way, malicious attackers use an e-mail address and lose their tracks. The name that appears as the sender of the message often points to an online VoIP service such as Google Voice, making it impossible for authorities to backtrack them

3.3.5 Banking Trojans

The Threat of Banking Trojans The primary goal of a banking Trojan is to steal login credentials and other sensitive information. This stolen data can be used to take over a user's account on the online banking service, steal money, and potentially perform identity theft and other forms of fraud. Banking Trojans are a popular form of malware because they provide cybercriminals with a direct means of monetizing their attacks.

Banking Trojans are also dangerous because they act as remote access Trojans (RAT) and give an attacker the ability to remotely control the malware installed on an infected system, which can be used to carry out other attacks as well. For example, many banking Trojans are commonly used to drop ransomware as well, enabling cybercriminals to carry out multi-stage attacks once they gain access to an infected computer.

Examples of Banking Trojans Some of the most dangerous and prolific banking Trojans include the following:

- **IcedID:** the IcedID banking Trojan was first discovered in September 2017. The Trojan spreads via mail spam and different malware such as Emotet campaigns and uses a variety of techniques to hide its presence on infected systems.

- **Ramnit:** Ramnit first emerged in 2010 and is a modular Trojan, allowing it to deploy a wide range of capabilities. Its theft of web session information allows it to steal credentials for more than just online banking sites.
- **Hydra:** Hydra is a banking Trojan that targets Android devices and first emerged in 2019. This malware abuses mobile app permissions to gain access to finance credentials.
- **Dridex:** Dridex includes both banking Trojan and botnet functionality and is delivered via spam and exploit kits. This malware uses WebInjects to redirect login attempts to an attacker-controlled server for credential theft.

There are many ways to protect companies from the threats reported above:

- **Employee Training:** banking Trojans typically use trickery to gain access to employee systems. Training employees regarding the threats of phishing, malicious downloads, and other common malware delivery mechanisms can help to mitigate the banking Trojan threat.
- **Email Security:** banking Trojans are commonly delivered via phishing attacks. Email security software can identify malicious links and attachments in emails before they are delivered to the intended recipient's inbox.
- **Endpoint Security:** endpoint security solutions can identify and block Trojans from gaining access to a system or can help to remediate an existing infection.
- **Multi-Factor Authentication (MFA):** banking Trojans are designed to steal login credentials for online financial services. Enabling MFA wherever possible makes these credentials more difficult for an attacker to use by requiring them to steal additional pieces of sensitive information to log in.
- **Credit Freezing:** credit freezing prevents additional accounts or loans to be taken out in a person's name. Freezing credit can help to mitigate the risk of identity theft due to a banking Trojan infection.

Mobile banking malware, in particular, has increased exponentially with the digital banking boom in recent years. According to the Hi-tech Crime Trends 2022/2023 report, 14 Android banking Trojans were detected as active between H2 2021 – H1 2022, and 6 of them were new.

3.3.6 Social Engineering

Social engineering is a technique that hackers use to induce a customer or employee of an organization to share important information about the operation of

internal strategies or to induce the victim to trust and reveal his or her credentials, data that is useful in allowing the criminal to advance within the dorganizational network. The social engineer exploits human error to his or her advantage, and it can take several forms: text message, email, call, or other. In the banking context, the most common social engineering attacks are two: stealing customer credentials through phishing and inducing the client to confirm, through an MFA method, a bank portal access or authorization for a payment.

To counter social engineering, it is necessary to introduce trainings in the company to train employees and warn them of the latest threats. A campaign must also be passed on to customers, to make them participate and reduce risks. Messages such as these are often introduced: "Never give away your passwords, personal data or OTPs to someone who calls." and "If you have to check payment information or confirm an operation, directly access the portal instead of clicking the link."

One distinguishing feature by which a malicious SMS, email or call can be immediately recognized is the haste with which the operation is requested. Indeed, social engineering often exploits the anxiety of the employee/customer by pressuring, for example, "The bank has blocked your account, log in here -link- to unlock it right away."

The most impactful social engineering attack in banking fraud occurred early last year involving Portugal, Spain, Brazil, and other countries in a two-year campaign of attacks. The first step of the attack was to prepare a malicious template to trick customers into entering their banking credentials. The template, as is the practice in email phishing attacks, was exactly the same as the original one in terms of graphics and buttons, while the content was aimed at stealing credentials. Fig. 3.4 depicts that the hackers were able to control each step in the chain, asking the customer for additional information in real-time.

3.3.7 Insiders

Fraud caused by insiders is more common than you might think. This attack occurs when a bank employee decides to hack the system for personal benefit through money and intellectual property theft. The consequences of an insider attack are mainly financial losses and reputational damage. There are two types of insider fraud:

- **Financial fraud schemes.**
- **Confidential data misappropriation.**

Internal fraud is one of the biggest dangers for banks, as employees have in plain sight the vulnerabilities of the system and ways to circumvent it. In 2022 alone, there were 2110 cases of fraud involving an employee. One method of thwarting

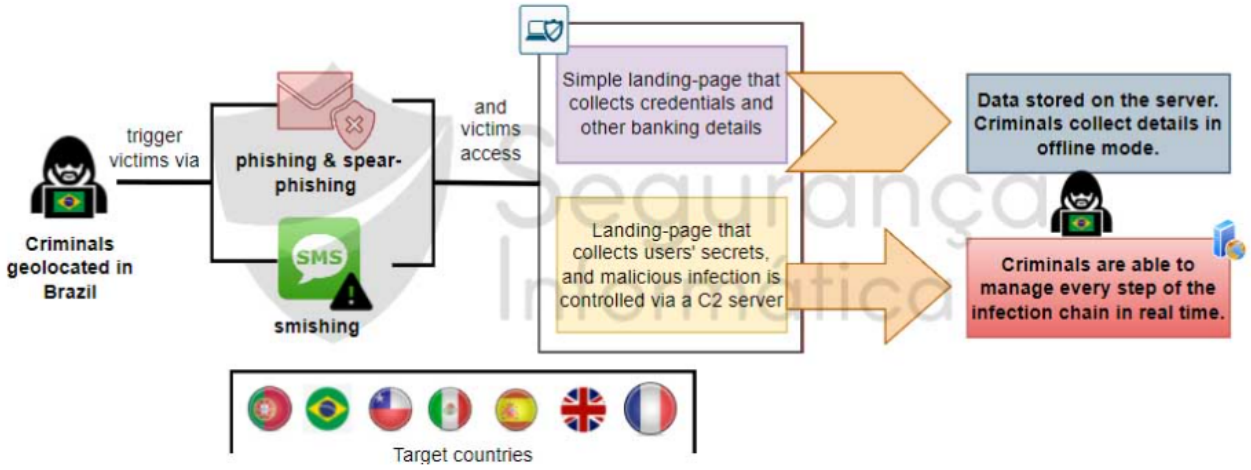

Figure 3.4. Social engineering infection chain [8]

these kinds of attacks is Four eyes: it is a principle for which extra approval is needed in addition to the employee's. Often this rule is associated with an amount of money, beyond which double approval is needed. Because it would be possible for a fraudster to circumvent this check through amounts less than the threshold, controls on cumulative or repeated transactions have been increased. Internal fraud has several types of potential insiders, among which are:

- **Former employees:** by having access to the systems and procedures used within the bank, a previous employee can exploit habits and knowledge to make money as a criminal;
- **Current employees:** an employee who is currently working for the bank has access to numerous resources and could potentially exploit some known bugs internally to obtain money illegally.

Chapter 4

Contribution

This section shows studies of the as-is architecture carried out by examining each component and its functions. Two possible solutions were then designed by checking their feasibility using commercially available products that could be introduced into the platform. The final implementation of the architecture included the introduction of mq queue modules, event monitoring, and service bus.

During the project execution, project management activities were also carried out to monitor the actual integration of the components carried out in collaboration with employees and suppliers.

4.1 Preliminary Activities

The first steps were to study the current state of the client's anti-fraud architecture, which was largely composed of custom applications developed by expert employees. For data collection a lot of information was gathered through scripts created with the COBOL language, while some applications were developed with Java, Python, and C++ languages. Additional information about active customers is sent in real-time via scripts that periodically post modified data to a channel. All this information is collected and passed into the analysis stage to detect fraud.

The second step was to analyze the flow followed during a transaction starting with the customer arriving at the branch or logging on to the bank's website. For each step, the type of data passed, the components involved and the communication protocols implemented were analyzed.

4.1.1 As-is

Initially I was introduced to the different communication methods that underline a generic banking architecture. Any payment and transaction in fact can be

categorized as follows depending on when the data are processed:

- real-time;
- near real-time;
- batch.

The first real-time category encapsulates all transactions such that a response must be received and execution completed in real time, with as little latency as possible. This type applies to any service available at ATMs, since the customer, once requesting a service, is waiting for the outcome right in front of the ATM. Another example is the continuing developments in online and mobile banking: the customer expects to see a balance in real time, be able to make payments online, and manage the card via the app. Both Single Euro Payments Area (SEPA) [9] and Significant Amount Transfers (BIR in Italy) are money transfers that require careful analysis and immediate response in order to proceed with the transaction.

Near real-time transactions require a short response time in terms of minutes, but it is not necessary for them to occur immediately. This type of transaction includes periodic transfers, as they are requested over the counter or online at the bank's website, but they occur with a certain frequency and are not immediate. These transactions can be blocked with a delay margin, so that the customer's historical data can also be better analyzed.

Batch transactions are those that do not require short response time, for example, the database entry of new periodic transfers may take a day to be entered correctly into the system. This type is always used in cases of large volumes of data collected in internal databases for later analysis by more elaborate and slower software.

In Fig. 4.1 possible threats for real-time and batch transactions are presented. In order to better understand the topics touched upon, the procedures that the customer must follow in daily cash withdrawal or card reload operations by cash deposit were examined. The following steps are required to reload a card by cash deposit:

1. Insert the card.
2. Enter the PIN of the card.
3. Press on the "Cash Deposit" button.
4. Insert cash into the cash slot.
5. Finish the operation and withdraw the card.

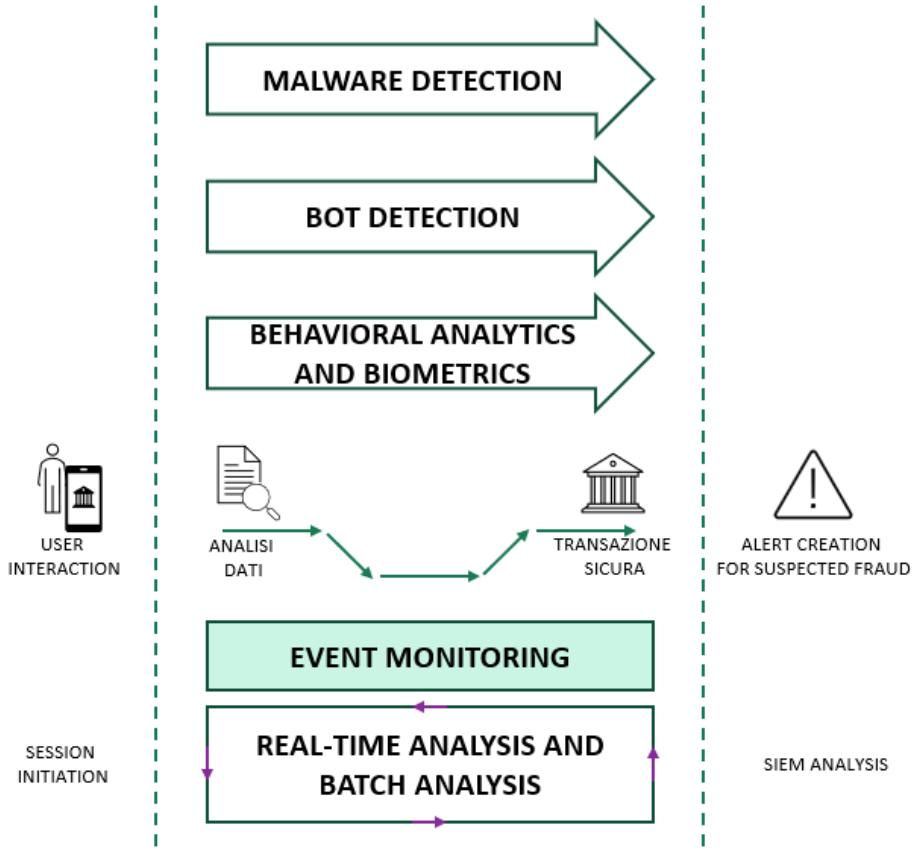

Figure 4.1. Real-time and batch context

Depositing cash on a card may seem harmless at first glance, but behind the transaction there are numerous checks on the card, the customer, and the location where this takes place. First, an analysis of the status of the customer and the card must be performed: the customer's credentials and history of card transactions are checked. A blacklist check is also performed with the card number to avoid allowing transactions on a card already marked for fraud. When one of these checks leads to the determination of fraud, the transaction is blocked and the case with its details is passed to a bank analyst.

During the first month, execution flows were also studied for transactions made at the counter. For example in case of wire transfer the steps are as follows:

1. The operator accesses the application used to manage wire transfers.

2. Enters the type of transfer to be made and some parameters regularly required by the bank.

3. Fills in the form with the necessary data for a wire transfer (name, surname and tax code of the originator, name and surname of the beneficiary, IBAN of the current account beneficiary of the transfer, sum to be transferred and country of destination of the sum, whether in Italy or abroad.

4. The operator at the counter, by pressing a button on the screen, will request a data validity check, which at this stage is limited to a check on the account balance and the applicant's information and will wait for a positive or negative outcome before continuing.

5. At this point the operator will click to perform the transaction, a REST API call will be sent to the infrastructure.

6. The anti-fraud system performs a real-time check on the collected data.

7. The operator will see the operation completed or not after receiving an API Response containing the outcome.

During the creation of a wire transfer, the first check requested by the operator from the banking system database concerns the data entered, i.e., the following conditions are checked: the availability of the customer, that the applicant has not been involved in illegal activities, the amount and frequency requested for the transfer, and finally the country of destination, as each country is characterized by a higher frequency of certain specific frauds.

Many transactions need to be completed in real-time, but behind the individual transaction there is a rather complex flow such that the data passes through many forms, only to return with a successful or unsuccessful response. In fact, the architecture of an anti-fraud system in banking can be divided into several layers: the first layer that includes all data sources and is intended to detect potential fraud attempts and generate related alerts. This level includes web applications that communicate via REST API, such as the web portal through which different types of wire transfers are created, applications that exploit basic message queues such as MQ queues, which are essential to collect large amounts of data and any differences on the data from the previous day, the Service Bus that carries and if necessary transforms information from an application to a module that analyzes it, and the databases, which contain the user master data needed to perform investigations on the validity of transactions. The core of this first block consists of a module that monitors all transactions made in real time, calculates a risk index indicating the probability that the transaction is fraud and returns it to the application to continue with next steps or block the attempt. This component

is called Event Monitoring or Transaction Monitoring, taking its name from its target.

The second layer of an anti-fraud architecture aims to receive and sort alerts of potential fraud received from the previous block and route them to more advanced workflows by opening related cases. During the project, an attempt was made to build a structure with a single case and incident manager so that the results obtained on one channel would be more transparent and could be exploited on the other two channels. In fact, the initial idea proposed a Security Orchestration, Automation and Response, SOAR, as a tool that could replace the execution of repetitive and manual tasks with an automatic flow so as to make the whole process more fluid.

The third block consists of a deep analysis of events and history to improve fraud identification rules and provide a more-accurate score. The analysis of the project led to the identification of a vertical analysis tool with advanced Machine Learning and Artificial Intelligence features: in fact, some vendors of this product claim the ability to improve the analysis.

4.1.2 Feasibility analysis

The project to implement a new multichannel anti-fraud platform was mainly divided into 2 possible solutions, the technical and the strategic. Technical: the solution involves the Service Bus component that collects all the necessary data from the numerous data sources, prepares it as a REST API call to be sent to the Orchestrator. The latter is the component that handles the events received, i.e., sends orders to open tickets in case of fraud, sends the event to the event analyzer, and sends the necessary data to the SIEM and the case manager. Strategic: the solution consists of the same elements as the technical one except for the Service Bus. In fact, in this case all data is collected and processed by the Orchestrator, which in turn sends it back to the SIEM, event analyzer, and case manager.

In Fig. 4.2 it is presented an example of a transaction made at the counter by the customer.

The sequence in fact follows the following steps:

1. The customer requests at the counter to make a wire transfer to a company. The operator at the counter enters the data passed by the customer, such as payee and total amount, into the open Web page that allows the creation of that particular type of wire transfer. When the operator presses enter, a REST API call is sent from the application to the Service Bus.

2. The Service Bus at this point turns over the transaction data to the orchestrator so that the orchestrator can analyze the event from all angles and detect possible fraud.

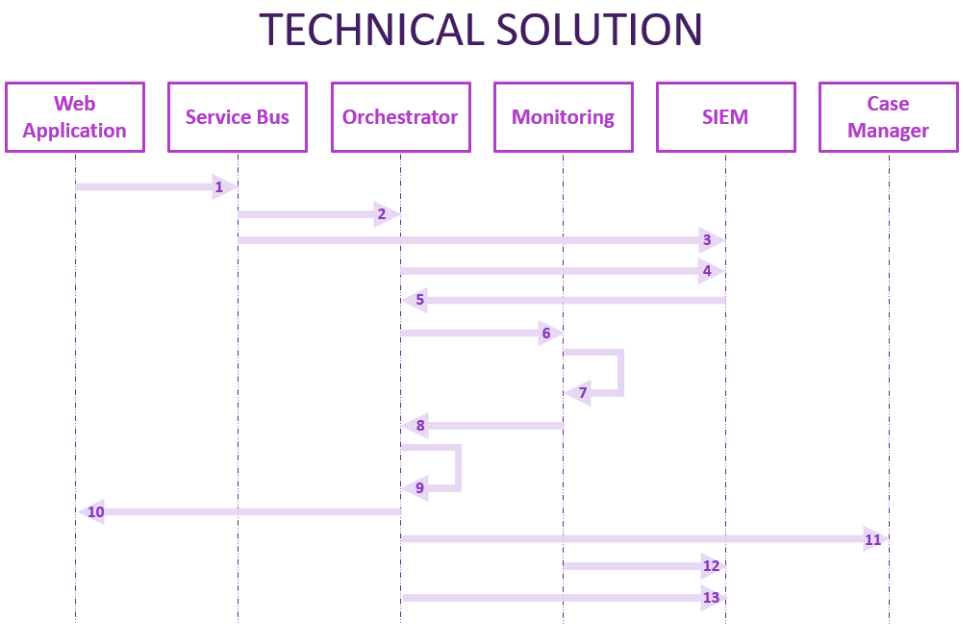

Figure 4.2. Technical Solution

3. The Service Bus at the same time also sends the transaction data to the SIEM to avoid a loss of data.

4. The orchestrator contacts the SIEM, usually with a REST API call, entering the call parameters needed to request the customer's historical and previous transaction data.

5. The SIEM responds to the orchestrator's request by sending the data updated to the user's last synchronization.

6. The orchestrator sends the collected data set to the event monitoring tool for it to perform the appropriate analysis.

7. The event monitor analyzes the received transaction data by merging the historical customer data with the collected real-time transaction data. The analysis leads the module to generate a risk index, which indicates how likely it is that the requested transaction is a fraud or not.

8. Event monitoring sends the calculated risk score to the orchestrator in response.

9. The orchestrator reviews the risk score received and with internal analysis decides whether or not the transaction can continue.

10. The results can be twofold: the orchestrator sends an "Ok," authorizing the transaction to complete, as it does not appear to be a fraud attempt. Or it sends the negative outcome when the fraud risk is high and further investigation is needed.

11. In the case of potential fraud, the orchestrator sends a request to the case manager to open an alert ticket, so that the latter can be assigned to an analyst and confirmed the fraud by human judgment.

12. Event monitoring sends the received data and results to SIEM to enter them into the logs so that they can be accessed in the future.

13. The orchestrator also sends its data to SIEM, which will be stored for future use.

Whereas the strategic solution, without Service Bus involves fewer data passes from one component to another, as it is all handled by the Orchestrator, who decides, with criteria that can be set based on the risk factor, whether it is appropriate to continue the transaction or not.

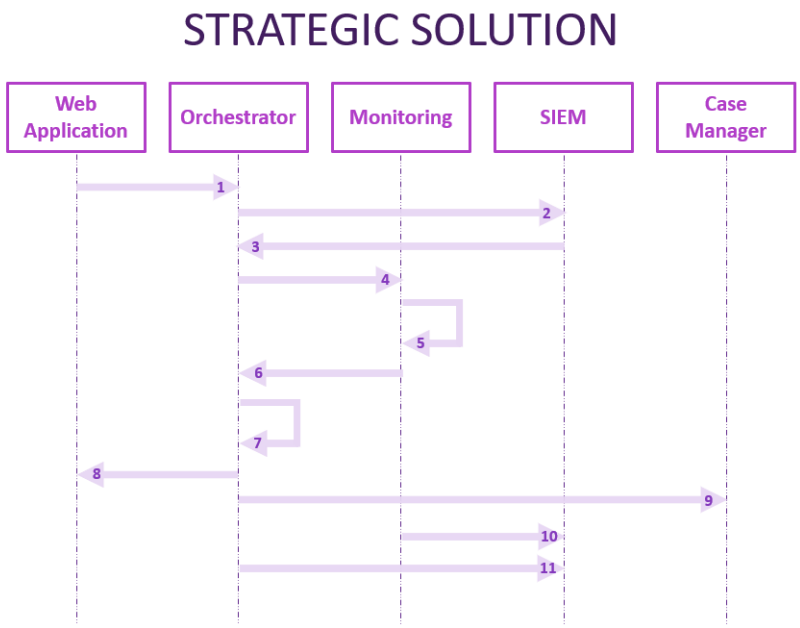

Figure 4.3. Strategic Solution

In Fig. 4.3 the steps of the strategic solution involving the orchestrator are presented.
The steps are listed below:

1. The customer requests at the counter to make a wire transfer to a company. The operator at the counter enters the data passed by the customer, such as payee and total amount, into the open Web page that allows the creation of that particular type of wire transfer. When the operator presses enter, a REST API call is sent from the application to the Orchestrator.

2. The Orchestrator sends a request to the SIEM to receive the history of the customer involved in the transaction.

3. The SIEM responds to the Orchestrator by turning over the collected and updated data about the customer.

4. The orchestrator sends the collected data set to the event monitoring tool for it to perform the appropriate analysis.

5. The event monitoring analyzes the received data of the transaction by merging the historical data about the customer with the collected real-time data of the transaction. The analysis leads the module to generate a risk index, which indicates how likely it is that the requested transaction is a fraud or not.

6. Event monitoring sends the calculated risk score to the orchestrator in response.

7. The orchestrator reviews the risk score received and with internal analysis decides whether or not the transaction can continue.

8. The results can be twofold: the orchestrator sends an "Ok" to the application, authorizing the transaction to complete since it does not appear to be a fraud attempt. Or it sends the negative outcome when the fraud risk is high and further investigation is needed.

9. In the case of potential fraud, the orchestrator sends a request to the case manager to open an alert ticket, so that the latter can be assigned to an analyst and confirmed the fraud by human judgment.

10. The orchestrator sends its data to SIEM, which will be stored for future use.

11. The event monitor also sends the received data and results to the SIEM for inclusion in the logs so that they can be accessed in the future.

4.2 Developed Architecture

The implementation of an Omnichannel structure is adopted so as to have an environment divided into modules through which the entire lifecycle of a transaction can be managed. Some transactions, as mentioned earlier, may require execution in milliseconds, while others such as wire transfers do not require immediate action and can therefore be analyzed with slower, but more reliable tools.

4.2.1 Data Sources

Each transaction requires more data than what is shared at the time it is made by the Client. The first check is where the Client's data is checked, whether there are any active flags related to previous fraud participations, and whether the balance from which the money movement starts is available and reliable. A second check starts for the more in-depth analysis that requires the Client's historical data, i.e., trends on fraud and parameters of some data are also analyzed at this stage.

All information needed to perform fraud checks is sensitive information that is stored by different methods depending on its type and format. Customers' historical data stay on databases and must remain there for years according to current regulations, even if a Customer decides to change banks. Data are saved on Mainframe dataset, i.e., on a file where information is saved separately by record. Data are viewed as groups of records, and unlike a file consisting of a consecutive stream of bytes, record collections can have a maximum size and padding techniques are exploited. Another technique used to store large amounts of data is NAS (Network-Attached Storage), which is a file-level based server. NAS files are accessed through the use of network file-sharing protocols such as NFS (Network File System) or SMB (Server Message Block). The advantages of using a NAS include quick data access and simplified configuration of settings and management by admins, while the disadvantage is the inability to customize hardware components or basic software parts.

4.2.2 MQ queues

Having numerous data sources developed by different vendors and in different languages, a large number of programming languages are used in an anti-fraud architecture. Structured Query Language (SQL) is the most widely used programming language for managing database systems. This language has managed to remain among the best even with the advent of Big Data, as it has excellent efficiency for speed, volume, and variety. SQL organizes data into pages and rows, each with fixed size, often at 8 kilobytes, so when databases are queried, this is done by I/O operations for each page. This organization makes query field operations

significantly faster and quicker. The format by rows helps in the storage and collection of information, in fact by extracting an element you also have its attributes unlike the format by columns. Historical customer data saved on databases are then extracted and processed into XML files, with their data types and mapping between elements and columns.

Messaging queues are a tool for exchanging information between applications, systems, and services by sending and receiving messages. In fact, the name is derived from the two styles used:

- **Messaging:** the two systems communicate with each other via individually sent messages as opposed to the traditional query/response.
- **Queuing:** when one element produces a message it deposits it in the queue and continues the execution of its program, and the second element will pick up the message when it needs it. The sending and receiving of the message may in fact not match when queues are used.

A message queue is a form of asynchronous service-to-service communication used to connect microservices that facilitates their development and deployment because each block is independent and can proceed sencently at its own pace. Fig 4.4 shows a queue implementing a buffer, the size of which is dictated by the need to maintain a few messages or many, in which data is stored temporarily.

Figure 4.4. Message queue scheme [10]

Through the endpoints, Consumer systems connect to the queue and collect messages previously deposited by the Producer.

There are two types of messaging queues:

- **Point-to-point:** point-to-point messaging implies that a message produced by one system can only be received by another application. In this case, the queue name and any queue manager names must be available to implement the queue.

- **Publish/Subscribe:** in the Publish/Subscribe type a Publisher has a queue to which systems, called Subscribers, subscribe in order to receive content sent by the Publisher. Each queue has its own identifier and can have as many Sbscribers, one or none. This mode is used when a piece of information needs to be shared with many systems.

The main advantage of this type of communication is that because messages are stored in queues, the programs receiving the messages need not be running at the time they are sent.

A message is a sequence of bytes consisting of the Producer's data, the sequence and content of which will be processed by the Consumer, and a message descriptor, which identifies the message and notifies it of priority.

The data saved in the Mainframe related to the transfers executed in a day are uploaded to an MQ queue waiting to be extracted by the Enterprise Service Bus and analyzed by the anti-fraud architecture components.

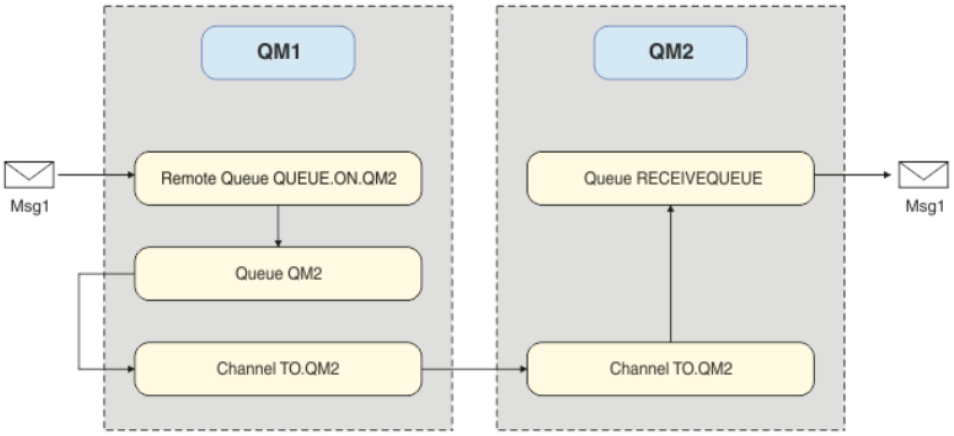

Figure 4.5. MQ Messaging flow [11]

Fig. 4.5 illustrates sending a message from an application on one host via a Queue Manager, which connects to a channel via an identifier. The Consumer Queue Manager on a second host connects to the same channel and collects the data, ready to be processed.

With the introduction of Queue Managers, queues were divided into two types: normal queues and broadcast queues. Transmission queues are those used to manage and possibly deposit messages in transit and directed to other Queue Managers, while normal queues are the standard queues used by two applications to transmit data to each other. To implement messaging queues, a vendor-produced command-line is usually used, on which commands are entered to create, start,

and to check status. Messaging queues provide data definitions via COBOL files, macro in Assembly language, or a command file in C or C++. Messages can be extracted from the queue in three different ways: by using the first-in-first-out (FIFO) method, by using the priority set in the message descriptor, or by pandering to an application that has requested a specific message.
Fig. 4.6 shows a diagram related to Sender-Receiver channels:

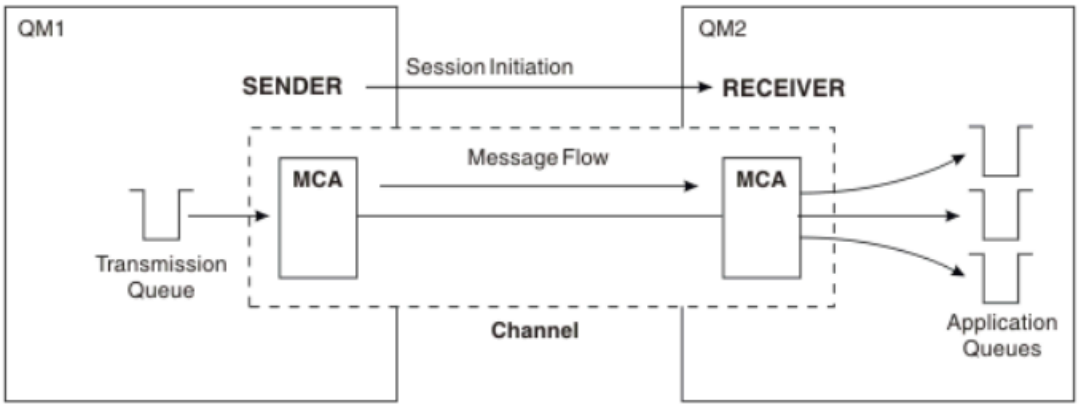

Figure 4.6. Messaging queue: Sender-Receiver [12]

The steps of the Sender-Receiver communication type are:

1. A Sender in one system starts the channel in order to send messages to the other system;
2. The Sender asks the Receiver at the other end of the channel to start and therefore the Sender starts sending messages from its transmission queue to the Receiver;
3. The Receiver puts the messages in the destination queue waiting to be processed.

4.2.3 Enterprise Service Bus

An Enterprise Service Bus (ESB) is a module whose purpose is to connect all the other tools. In fact, the ESB is able to collect information from data sources of different nature, code kafka, Rest API and others, process it and transform it into the format that each module expects. In the context of an anti-fraud architecture composed of a wide variety of data sources and operational modules, the use of a Service Bus capable of converting communication protocols and performing message routing has become necessary. When a client produces a transaction, the

Service Bus passes the data to both the orchestrator and the SIEM so that they have a copy of the original transaction values. In Fig. 4.7 it is presented a standard service bus integration.

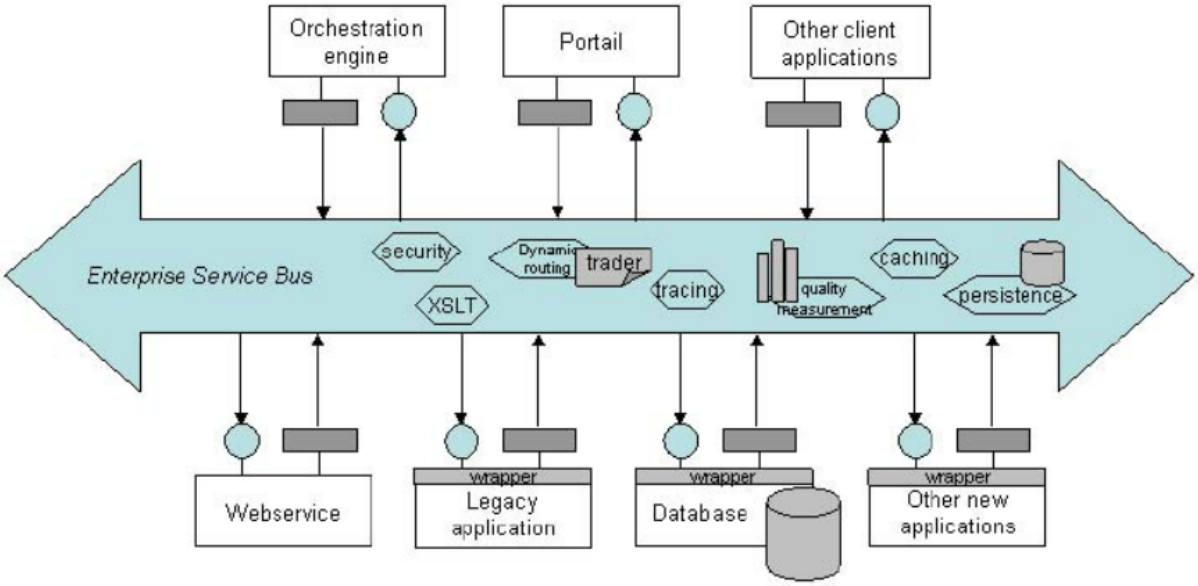

Figure 4.7. Service bus integration [13]

Among the advantages of the Service Bus is the simplicity with which systems are integrated: the program is in fact connected to the Service Bus as a black-box, and the Service Bus takes care of processing the data in the format required by the next component. One disadvantage to consider is the possibility of the Service Bus acting as a bottleneck, both for task management and for upgrades brought to the architecture. Because the Bus is centrally managed, all developments and changes required by each service are queued and activities often fall behind schedule.

4.2.4 Orchestrator

The architecture designed and proposed to the Client includes as the heart of the system an orchestrator, whose task is to manage all the transactions requested in both real-time and batch and to provide a response regarding whether the transaction can be completed or not. In order to arrive at an outcome and thus provide an okay to proceed, the orchestrator is responsible for making requests to the other components (real-time transaction monitoring tool, SIEM, and case manager). This actually sends requests through the necessary protocols and waits

for a response from each module. Once the results of the analysis are received from the components, the orchestrator examines all the data and produces a risk score, from which it deduces whether the transaction is a possible fraud or not. The orchestrator of many vendors in fact relies on the Complex event processing (CEP) method: the method originated in the 1990s with the purpose of identifying special cases, and later fraud, in real time so that action can be taken in time. Following the CEP method, the orchestrator is based on several techniques applied in the banking environment: event filtering, event transformation and aggregation, event extraction, and relationship identification. The orchestrator is the key point of the anti-fraud architecture and must be extremely fast in delivering results. Indeed, the most at-risk transactions are those that occur in real-time, whether it is a card reload or an online payment.

In addition to speed, the orchestrator must have elasticity as a characteristic: in fact, it must be able to work perfectly even under stress, for example, with a large number of transactions carried out in real time. A study conducted by ACI Worldwide predicts an increase in real-time transactions of 63% and estimated that by 2027, a volume of about 512 trillion will be handled. The number of transactions conducted in real-time compared to the total number of all electronic transactions is 28% [14]. This constant evolution and adoption of real-time payments requires increasingly cutting-edge and fast tools, as keeping a customer waiting is every bank's nightmare.

The orchestrator, because it must communicate with many modules, has many communication protocols. The main and most widely used are REST API calls, which are suitable for receiving real-time data. REST APIs, also known as RESTful Application Programming Interfaces, which are a set of protocols and definitions that allow interaction with RESTful Web services. REST calls are often associated with request and response between a consumer and a producer. The HTTP method parameters of a RESTful API HTTP request consist of URIs (uniform resource identifier), metadata, cookies, and more. To have a RESTful API, the following conditions must be valid: the presence of a client-server structure, the communication between them must be stateless, a system composed of security and load-balancer modules. Depending on the vendor, their product focuses more on identity management, fraud detection, or authorization. The Customer must choose the one most relevant to their situation, in this case real-time fraud detection.

Recently Security Risk Management (SRM) vendors have changed their approach, opting to combine the Continuous Adaptive Risk and Trust Assessment (CARTA) method and an orchestration tool. In Fig. 4.8 are presented the main goals of a CARTA orchestrator. In fact, no vendor offers all the required capabilities to deal with fraud through a single end-to-end system. The component playing the role of orchestrator, must have the following capabilities:

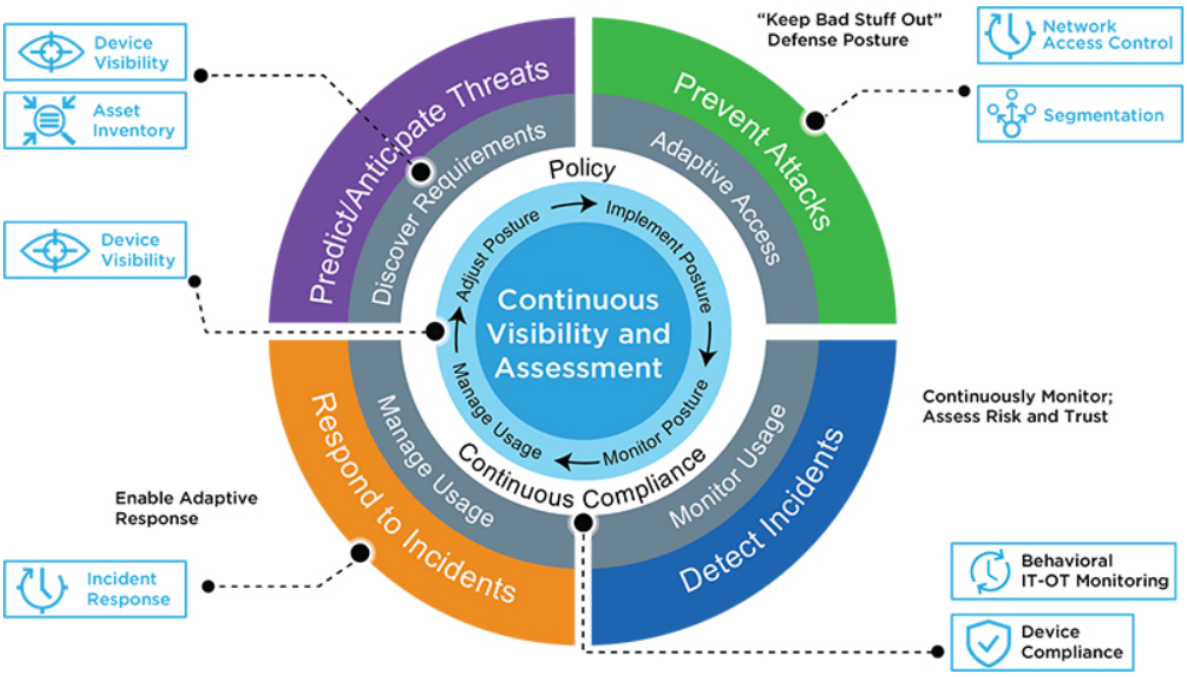

Figure 4.8. Gartner's Architecture and CARTA strategic approach [15]

1. Define risk thresholds based on defined policies and rules for each type of event, obtained through data processing and analysis of anomalous characteristics;

2. Connect all components of an anti-fraud system so that events can be analyzed in real-time and their possibility of fraud determined by exploiting all risk scores calculated by each module;

3. Establish a set of points during the workflow of handling a transaction, so that an in-depth analysis of certain parameters is triggered by the specific components;

4. Define a workflow, detailing each step to be performed in case the analysis detects fraud or not;

5. Provide the ability to smoothly adjust the analysis workflow by changing parameters or adding components to the flow;

Some orchestrators on the market not only deal with event analysis to detect fraud, but also cover the field of identity proofing and authentication, offering

more coverage to the client and simplifying component management. The most modern orchestrators offer tools for creating and managing workflows dynamically: a trained analyst can create an analysis flow for each possible fraud scenario, entering the parameters to focus on and associating specific risk indices.

4.2.5 Risk Assessment Modules

Another essential component of an anti-fraud architecture is the Risk Engine (RE) module, a software that can provide a reliable risk index based on advanced simulations of future behavior in certain areas, ctra including bank fraud detection. A Risk Engine is scalable and very high-performing, qualities that are very useful for analyzing at different levels and from numerous perspectives events. The risk index can be visualized later through the dashboard provided by the Risk Engine, which is always accompanied with Online Analytical Processing(OLAP) software.

A Risk Engine module used to combat fraud on online payments is the transaction analyzer, a generic name for identifying a tool capable of calculating the percentage of risk on each transaction on each line of a banking or commercial service. This module leverages the ability to implement anti-fraud rules and predictive analytics to quickly and accurately provide a response to the many fraud attempts. Once the parameters of the transaction are received, the Risk Engine processes them and compares them with common fraud patterns and saved patterns using neural network technology and produces a risk index with an explanation of what influenced the decision. All transaction data is sent back to the case manager afterwards.

Another module that is expanding because of its efficiency in detecting fraud is the module that analyzes Behavioral biometrics, or behaviors adopted by the consumer. Passwords have been an efficient and trusted method of authenticating users for years, but the concept of Multi-Factor Authentication (MFA) has long been popular because by using a One Time Password (OTP) code or physical biometrics parameters such as facial recognition, user authentication is trusted and the risks of identity theft are dramatically reduced. From Multi-Factor Authentication came the study of modules that can process and analyze behaviometrics, or patterns of user behavior so that government, banking and other events can be analyzed to identify cybercrime. These traits are precisely called patterns because a person tends to always perform certain activities in the same way. For example, the speed at which one types on a computer or pc is a biometric behavior, as are body movements, tone of voice, or the speed at which one scrolls. The advantages of studying biometric behaviors [16] are as follows: with this technology, banks monitor the user's daily activity and compile separate behavioral reports for each individual. Machine Learning is used on this data to equate and distinguish known

traits of the account holder with real-time portal activities. All of these steps reduce the interference caused to the user during a transaction as well as making it more secure. The inner workings of the software are quite complex.

Another example of behavioral biometric integrated without being noticed by the consumer is found in the dynamics of keystrokes: the additional level of security is based how much a user presses the keys while entering his or her password. The authentication system can then perform an additional background check without affecting the user experience. All data collected and processed are stored on secure databases external to the company to avoid data leakage. To study the operation of behavioral biometrics, the method of recognizing the user by input cadence was analyzed.

U.S. Patent Aug. 30, 2016 Sheet 1 of 8 US 9,430,626 B1

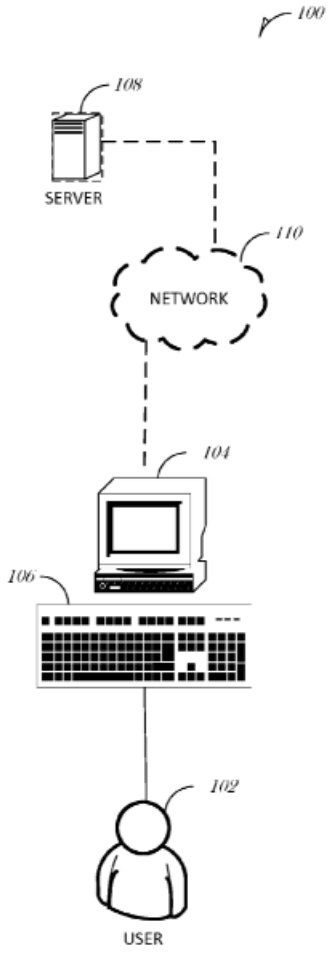

FIG. 1

Figure 4.9. Analysis of input cadence - system [17]

Fig. 4.9 shows a user authentication system by entering a known text in accordance with some formulations. The cadence of the input is saved in the structure shown with the fields of SpecialKeyPosition, KeyDown/KeyPress/KeyUp, Time and the record ID. In Fig. 4.10 is presented the common structure with properties of a user cadence.

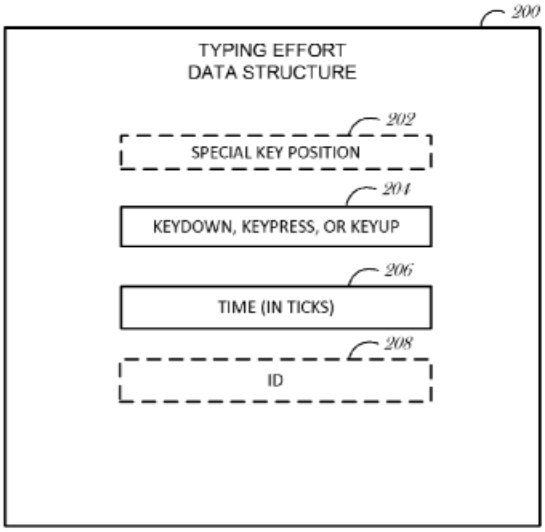

Figure 4.10. Structure of the cadence record [17]

Verification of a user is carried out according to the following steps:

1. The system receives the data from a login including also the user's movement data during the writing of the known input;
2. A statistical summary of the input sample data is computed;
3. Finally, the calculated statistical summary of the input sample data is compared, using geometric and geospatial constructs, with previous input samples stored in the selected user profile. This comparison generates an indication of the probability that the user who typed the input is the one selected [17].

Another feature often made available by vendors as a single package along with Transaction and Event Monitoring is the module that deals with Malware Analysis. Trojans in banking, a type of malware that falls into the Trojan Horse category, focus on the goal of gaining access to a computer by pretending to be legitimate software. For example, a Trojan may be inserted as a malicious attachment in a phishing e-mail or downloaded as part of a fake copy of legitimate software. Once installed on a now-infected computer, banking Trojans can collect online banking login credentials and other sensitive information in a variety of ways.

Some methods include downloading cached credentials from the system and web browsers, monitoring the system's keyboard, searching for passwords stored in the filesystem, and using a keylogger to collect login information when the user browses known websites. Trojans targeting bank accounts are designed to steal a customer's online banking login credentials and use them criminally. Monitoring via Event Monitoring of these accounts for abnormal login attempts identifies with good probability whether a user's account has been compromised by a banking Trojan or through other means. The module leverages threat intelligence methods to compare transactions and performs a check on the signature certificates used in order to detect potential threats.

Device fingerprinting is a method used to associate a device used to make transactions and transfers with a customer. With the spread of online and mobile banking, techniques have had to be developed to create a unique profile of an individual, i.e., his or her fingerprint, by basing the identity on characteristics of the device's software configuration: e.g., browser, operating system, CPU, and plug-ins. The more advanced Device Fingerprint modules are based on algorithms that analyze both software data used by the client and hardware data. Some modules use algorithms to analyze how the GPU renders an image, data that is very difficult for fraudsters to fake. A fingerprinting algorithm is exploited to assimilate the information and create an identifier for the device. Some of the information studied by these algorithms include:

- IP address.
- Header of the HTTP request.
- Font or plugin that the user has installed on their device.
- Screen Resolution.
- Operating System.
- Location and time zone information.
- VPN and browser information.
- Battery information.

Each of these data taken individually does not uniquely identify any device, but considering the set of properties, it is extremely unlikely that there are two devices with the same caretteristics reported above. The device fingerprint is developed by combining both Decision Tree-based and Random Forest-based algorithms.

In Fig. 4.11 it is shown the first step in which data about an instrument is processed. Through a sequence of ifs we arrive at a percentage that indicates how

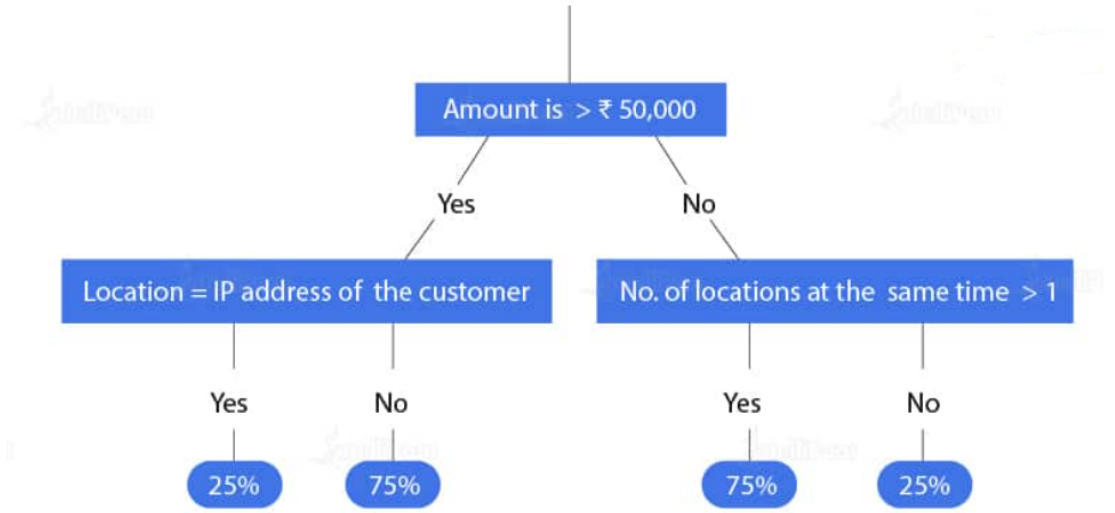

Figure 4.11. Decision tree [18]

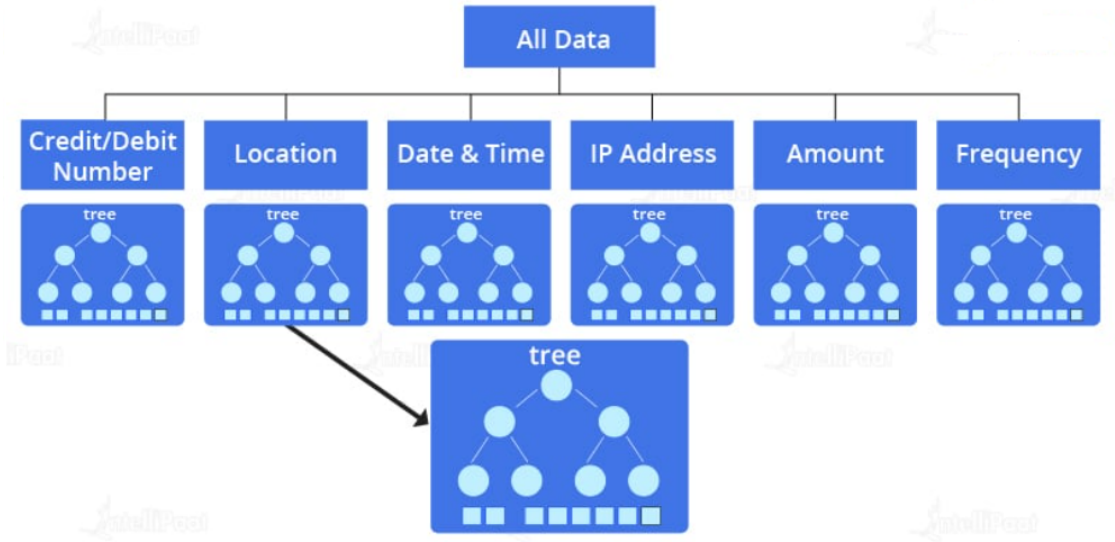

Figure 4.12. Random forest and decisional tree combination [18]

likely this transaction is to be a fraud. As a second step, the Random Forest model is used to combine data and percentages collected from numerous sources. In Fig. 4.12 it is depicted as an example. The diagram below shows the division of the data set into multiple decision trees. The subtrees consist of variables

and the conditions to verify those variables for a transaction. After checking all possible parameters, the subtrees will provide the probabilities that a transaction is "fraudulent" or "non-fraudulent". Based on the combined result, the model will mark the transaction as "fraudulent" or "authentic".

All of these modules are extremely efficient when used in bulk, so that both the fingerprint of the customer's phone or computer and their geographic location and behavior can be compared. Machine Learning must also be leveraged in conjunction, so that you have tools that evolve their methodologies as they monitor transactions.

4.2.6 Security Information and Event Management

The Security Information and Event Management(SIEM) unit is used to aggregate data generated by the security controls and anti-fraud architecture. Possible operations include log file analysis and event correlation, monitoring of intrusion detection alerts mapped to systems, and others. SIEM provides a single, centralized tool for collecting all transactions and alerts. The purpose of the module is to send the request for the creation of an alert in case a past transaction is flagged as fraudulent and likewise provide a robust collection of all processed past events. The main function of a SIEM is the collection of logs: keeping track of all examined data and calculated risk indices, combined with post-mortem analysis helps Event Monitoring modules improve analysis. Analyst-processed alert logs and logs related to each client are also needed so that the modus operandi can be compared. Logs are generally composed of data structures that contain:

- The payee, the applicant and their historical data.
- The type of transaction, total amount, available balance.
- The date and time the request was generated.
- All outline information related to the transaction, such as the activity performed by an IP address, location, and mode.

The strength of these modules is correlation-they are in fact tools that can process large amounts of data together match events from different systems and identify suspicious patterns.

SIEM requires maintenance since as the tools evolve, so must their logs. These modules help enterprise security teams detect anomalies in customer behavior and use Artificial Intelligence (AI) to automate much of the manual processes associated with threat detection and incident response.
A SIEM, regardless of capacity, performs data aggregation, sorting, and consolidation functions. The basic feature set offered by a Security Information and Event Management includes the following:

- **Log Management:** SIEM collects any information useful for post-mortem analysis, receiving data from both on-premises and cloud environments. Event log data from users, endpoints, applications, data sources, cloud workloads, and networks are saved. Some SIEM solutions are integrated with third-party threat intelligence feeds in order to correlate internal security data with previously recognized threat signatures and profiles.

- **Incident monitoring and security alerts:** the module provides the analyst with processing results and analyzed details via a centralized dashboard: this also includes a real-time data visualization so that spikes or special events in monitored activities can be identified.

- **Correlazione e analisi degli eventi:** one of the module's main functions is event correlation, which provides insights to quickly identify and mitigate potential threats to corporate security.

- **Compliance management and reporting:** SIEM is a key part of event analytics as tools are evolving in the market that can work in compliance with regulations governing user privacy. In fact, the modules are developed to be compliant for recent regulations:
  - Payment Card Industry Data Security Standard (PCI-DSS), which deals with the management of sensitive cardholder data, such as expiration date, number and security code.
  - General Data Protection Regulation (GDPR), a regulation imposed by the European Union to achieve compliance with data protection principles and safeguard sensitive user data.

The SIEM module is needed to achieve reduced performance regarding mean time to detection (MTTD) and mean time to response (MTTR) when fraud is detected.

4.2.7 Case management tool

An essential part of the anti-fraud architecture corresponds to the Case Management tool, as all transactions identified as possible fraud are evaluated with it. This tool is used to manage fraud incidents and money laundering. The following practises must be observed for the proper functioning of a case manager:

- Maintain up-to-date policies and process steps to handle possible fraud.

- Provide periodic training for incident analysts so that they are up-to-date on the latest tactics used.

An Event Manager is leveraged to perform the following actions:

- **Respond:** after revealing activities with criminal patterns, a response flow is triggered that differs according to the type of fraud detected. These flows are composed of sequences of actions triggered in cascade or in parallel, which fraud experts can set up as they see fit;

- **Detect:** all tickets generated on a risk basis are sent to an analyst and the outcome is itself recorded, so that it can help future assessments;

- **Investigate:** thanks to new technologies, the Case Management Tool receives the most suspicious transactions, triggering fraud intelligence by running deep queries: in this way, experts will receive the most suspicious transactions, increasingly reducing the margin of error;

- **Discover:** as tools are added to the architecture and new parameters are introduced into the analysis, analyzing patterns to determine criminal activity and setting watchlists for certain events enables early identification of several frauds.

4.3 Project Management Activities

The project initially included revisiting the architecture of a major European bank through in-depth study of new technologies and an analysis of possible evolutions to improve system reliability and accuracy of fraud attack detection. In consulting, it often happens that projects are borrowed according to the client's needs. Off-project activities are included so as to include them in a single process, or projects are scaled down to be adapted to the client's planned expenditure. In my case, the client underwent an internal change such that it reduced the number of activities outsourced to outside consultants and focused more work toward in-house. Thus, there was a change in the project objectives such that strictly technical activities were performed by employees, while on the Accenture side the project was continued with project management activities for an inter-stream coordination of activities. The purpose was to monitor the progress of project activities by having technical knowledge to delve into more complex issues and resolve conflicts and disagreements among the teams in the field in a short time.

The organization envisioned the project manager (PM) as the person responsible for the overall control and success of an individual project from start to finish. The project manager's job is to define project objectives, collect data, schedule activities, and manage resources, costs, and budget. Project managers must possess leadership and communication qualities, as they often supervise teams from

different functional areas that must work together during the project to achieve its goal.

The PM was responsible for monitoring deadlines and keeping track of completed or unfinished tasks and managed the budget entrusted to the project by having pure decision-making power over what licenses to buy, what software to choose, and how much staff to recruit to load hours into it. Of course, to make a decision on which component to choose or whether a product is worth buying or not, he relies on the technical collaborators who bring their expertise to the project. The Project Management Office (PMO) is a group or department that sets and maintains project management standards for a company. The PMO monitors project execution and is responsible for ensuring that projects are delivered on time and on budget.

Sometimes PMOs are external to the company. As more companies with PMOs have achieved returns on investment, the office's popularity has increased. According to the Project Management Institute (PMI), nearly seven out of 10 organizations globally have a PMO.

A PMO generally bases its project management processes with a standard IT industry methodology. Following are some commonly used project management methodologies:

1. **Agile:** The Agile method applies to projects that require speed, flexibility and continuous delivery of product to the customer in short delivery cycles. Agile project management is an iteration-based approach to planning and driving project processes that breaks them down into smaller cycles called sprints or iterations.

2. **Waterfall:** The Waterfall methodology allows greater control to the PMO team during each phase of the project, but is less flexible when the project scope changes.

3. **Scrum:** This term, based on training players in the game of rugby, is part of the Agile framework. Deliverables are due every 30 days. Teams that have struggled with prioritization can improve productivity by switching to Scrum.

4. **Six Sigma:** Six Sigma is a methodology used to improve processes by eliminating what are considered defects, i.e., a product or service that does not conform to specifications.

In Fig. 4.13 illustrates all the steps in a project.

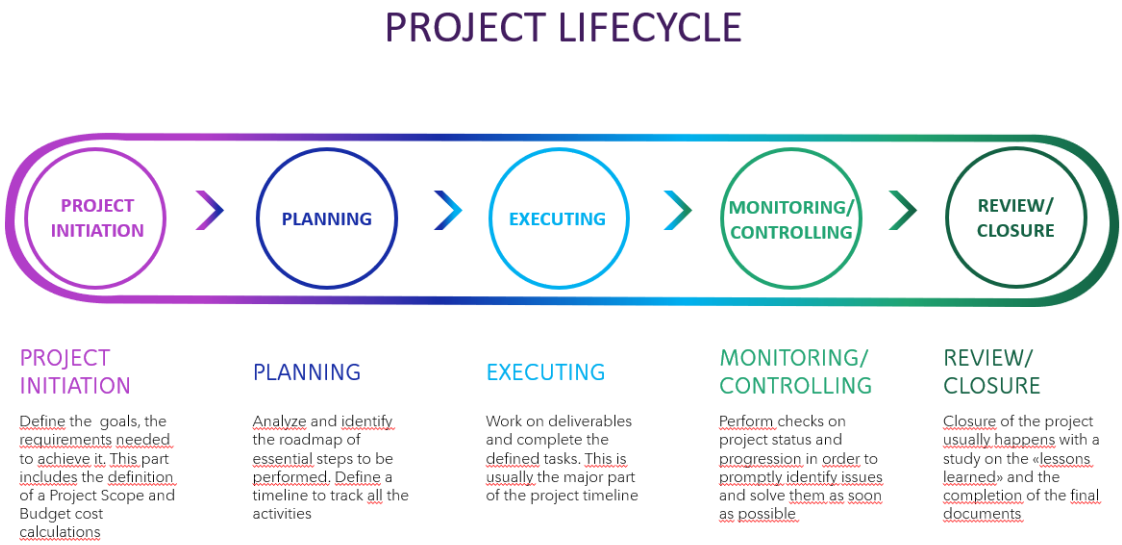

Figure 4.13. Steps of a Project viewed from the PMO point [19]

The cycle of a project viewed from the Project Management side includes an initial initialization part in which all the necessary documentation is gathered, the Project Scope is created, and budgets and costs are broadly defined. This is followed by a planning part, in which a timeline is created with all the macro-activities, which in turn are divided into groups and detailed as to time and cost. There is then an execution phase to which is associated a monitoring phase to keep track of all the tasks and respond quickly to any problems. The last step is closure, where end-of-project documents are drafted and an analysis is made of how much was done, how and in how much time. One of the tasks of the project manager together with the PMO team is to define a Project Scope,which is to determine and document a list of specific project objectives, tasks to be accomplished, costs and deadlines documentation is called a Scope Statement, which establishes project boundaries, responsibilities of each team, members and procedures. A Scope Statement articulates what the project entails so that all stakeholders can understand what it entails. It provides a roadmap for task setting, scheduling, work and budgeting, helps focus team members on common goals and prevents projects from expanding beyond the established vision. A project is expected to evolve along the way. Therefore, the better the project is defined at the outset, the better the team will be able to handle the necessary changes. Being

as precise as possible in defining the scope of the project helps avoid "scope creeps," which are those situations in which certain parts of a project end up requiring more work, time or effort because of poor planning or miscommunication.

Given the size of the project, the original idea was divided into 11 streams, whereby each represented a set of applications to be integrated or a module to be interconnected within the architecture. The first three covered applications used in different European states where the bank has a presence. Some streams each represented a component to be installed in the architecture, while the remainder were concerned with ticket, incident, and log creation and management.

Chapter 5

Requirements testing

In addition to project management activities and supervision of module integration with the architecture, analysis of platform performance and its impact on operations performed by the customer were also carried out. As a major requirement there was indeed the need to comply with a latency of 200 ms: few milliseconds to collect transaction and historical data, calculate the risk index and send a signal to continue or block the transaction in case of fraud. To confirm the result obtained, performance and stress tests were conducted to ensure proper behavior even with a large number of simultaneous transactions.

5.1 Key Performance Indicator

At the beginning of the project, Key Performance Indicators (KPIs) were set jointly with the bank in order to have clear objectives and respect them in the development of the new architecture. The bank, since transaction control operates in direct contact with customers, requested that the entire cycle of checking and approving or blocking the request would take a maximum of 200 milliseconds. One contribution was to check the fulfillment of this point, along with compliance with other less restrictive demands.

In the bank fraud industry, to verify the efficiency of an anti-fraud structure, transactions are divided into two types:

- **False positives:** transactions labeled as false positives are legitimate operations conducted by the right customer in good faith that are blocked because they are suspected to be fraud [20]. It is necessary to keep this type of transaction low because the regular customer will not tolerate well having to repeat the transaction several times because of the controls [21].
- **False negatives:** when a transaction passes all the checks and later turns

out to actually be fraud, it is labeled as false negative. They are a very important factor to consider because the cost to restore the system and reputation following a fraud is very expensive [22].

False positives are a priority parameter as one obviously tries to minimize inconvenience with customers and not create frustration by having to perform the same transaction multiple times. It is crucial to have an architecture that balances the numbers of both types of mishandled transactions. In fact, as a result of unrecognized fraud, the bank loses credibility with customers and thus could also lead to potential clients loss.

Fraud could not be immediately intercepted for several reasons, for example:

- Old anti-fraud infrastructure and/or rules: fraudsters always come up with new methods and try every possible trick, checking whether or not they pass inspection.
- Machine learning systems such as event monitoring are not configured with the proper rules and mistakenly flag transactions as legitimate.

Within the key performance indicators there were a number of requests from the bank, covering the methodology by which transactions were handled, the ability to update the event monitoring rules either manually or automatically, through adaptation based on feedback received from banking professionals. The requests were tracked through a requirement traceability matrix, a document used to mark requirements, related tests, results and issues encountered in performing that point [23]. A summary of common requirements for an anti-fraud architecture is given below:

- **Blocking transactions and creating related alerts in real time:** it is essential for the platform to be able to detect possible fraud on transactions received. In turn, the number of operations blocked and sent for review to experts must not be too high or you risk blocking customer transactions and filling employees with unnecessary work.
- **Usage of historical customer data:** during the operations check, all historical client data must be received through the specialized channels. For a proper study, it is indeed necessary to consult past transactions as well, ranging from the last year to around 5 years.
- **Process transactions automatically:** a fundamental requirement is that the architecture must be able through biometric analysis, historical data, and set rules to recognize fraud with no human intervention required.
- **Review rate:** the percentage of transactions that will have to be manually reviewed for in-depth analysis by human judgment. This factor should be

reduced as much as possible without overdoing it and not detecting major fraud.

- **user-friendly dashboard for bank fraud analysts:** the ability to change alerts by entering analyst opinions and changing the fraud index was requested. In this way, the data of automatically analyzed fraud incorrectly is entered into the system, and this information will come in handy with future checks.
- **Dashboards with trends on corporate fraud and current global trends:** for a broad view of the methods exploited by attackers, it was required to have a dashboard that would allow one to see the results on recent transactions, the values of the parameters most linked to fraud, and a dashboard that would report current scam trends so that they could be compared with internal data.
- **Lists:** the use of whitelists, blacklists and watchlists is essential to maintain a structured database with key fraudsters and their information. These lists need to be updated following a fraud detected with the fraudster's data.
- **Rule customization:** normally anti-fraud tools already have preset rules for analyzing incoming transactions. In particular, event monitoring should also have the ability to add manually created rules via basic formats such as txt or csv.
- **Integration with card management systems:** a request was made to maintain the current direct integration with third-party systems for European and worldwide card management and monitoring.

5.2 Testing Activities

Stress tests are carried out to verify that the architecture functions properly even at full capacity, i.e., with a large number of transactions. Using special scripts and programs, numerous transactions are generated to test the system. As is good practice for any system, through the project, new components were introduced first into the test environment so that their effectiveness could be verified through testing. During the development of the thesis, different types of tests were planned and executed according to the feature that had to be verified. This is because only one type of test is not enough to be able to guarantee that the whole structure will work. Listed below are the types of tests conducted in collaboration with the client, developers, and IT banking analysts [24]:

- **Unit tests:** they are developed to verify the proper execution of tasks in each component. The focus is therefore on the individual module and its

functionality. This type of testing was used for the introduction of the Service bus, to check that the module was able to correctly receive data and change the output format to be sent to another component. These tests were also carried out for Event Monitoring: the correct reception of data and the proper display of transactions on the application dashboard was verified.

- **Integration tests:** this type of test is responsible for verifying proper functioning among all components. The test involves sending dummy transactions and verifying on each module how data is received and how it is sent. During the project, it was reviewed the correct functionality of both the REST API calls between the Service bus and the Orchestrator as well as the MQ queues for transmitting data from the mainframe to the Service bus.

- **Functional tests:** these tests are used to verify that the system output is as expected. While integration tests are primarily about the correct connection between components, functional tests aim to check the output values and make sure that they are as expected. In the event monitoring integration, functional tests were performed by entering precomputed data to verify the risk index calculated by the module.

- **End-to-end tests:** they are used to check the behavior of dashboards of components while they are being used by users. In the antifraud enhancement project, these tests were used to check the graphical implementation of a button that appears to the operator at the counter once the transaction has been analyzed.

- **Acceptance testing:** these tests are conducted together with the client and are used by the client to verify that its requirements and key performance indicators have been met. In conducting the thesis, acceptance tests were conducted with fraud analysts by performing the basic operations of the case management tool. It was seen how the receipt of a possible fraud alert occurs and the possible operations following the receipt of the ticket. Requests included the possibility of collecting tickets by customer ID or by similar amount on the amount.

- **Performance testing:** these evaluate under what conditions the architecture can work properly and identify possible bottlenecks. For this project, performance tests were conducted for event monitoring. The latter by customer request, had to be able to handle a large number of transactions and keep the response under 200 ms. Through scripts, a large number of transactions were generated and sent to the module: event monitoring did not skip any transaction and calculated all risk indices while maintaining an average of 180 ms. During the stress tests, the number of transactions sent at the

same time was continuously increased until the point was reached where the module no longer worked as expected.

Acceptance and end-to-end tests were performed manually, as they required the evaluation of the person who will then have to work with the platform, while other tests were performed in an automated way, through scripts and transactions with pre-filled data. Automated tests are important because they are used to test the limits of the framework, such as finding the maximum number of transactions that can be handled simultaneously.

Following the integration of the Service bus and Event monitoring, fraud control tests were also conducted. The latter require that those performing the tests impersonate fraudsters and carry out their own actions. Fraud control tests should be performed with a high frequency, as fraudsters find a new way around the controls every day [25]. Since the rules set on the modules to detect fraud are critical information, fraud control tests have been carried out by an internal bank team. This type of testing is used to detect shortcomings and remediate them before they explode into large fraud cases, preventing money and reputation loss for the company.

Chapter 6

Conclusions

During the course of the project, in addition to the in-depth study of specific technical methodologies, I had the opportunity to delve into relational aspects both with other team members and with clients and suppliers. In particular, the ways of conducting and formalizing technical meetings were analyzed, so as to identify the subject of discussion quickly and find a solution that brings the participants together. There is also a documentation section in which what was discussed is recorded so that it is available for future meetings. The behavioral aspects related to the various positions in the team, the tasks to be performed and their timelines were also reviewed.

This project was an experience introducing the banking sector with a cybersecurity and anti-fraud orientation. I found the study of the many components in the market very interesting. Each tool had its pros and cons, which were weighed very carefully to derive maximum benefits. Studying the MQ queues in a first step and implementing them within the system led to a lot of information about basic operation that I had not thought of before.

The project management activity was useful for an overview of activities and an understanding of how a project is managed from the ground up. Budget management also brought more insight into how licenses or new components are requested. The most satisfying part was during the execution of the different tests: although some tests were rescheduled with additional changes, it was good to see the platform receiving data correctly and responding to a high number of transactions.

Finally, it was interesting to follow and participate in the dynamics of a team dedicated to a project. The experience was extremely educational and will definitely be used as a basis for future work projects.

Bibliography

[1] Accenture. (2023) Accenture logo. [Online]. Available: https://www.accenture.com/cz-en

[2] F. R. Congiu. (2021) Guidelines on fraud reporting under psd2. [Online]. Available: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

[3] PSD2, "Payment services directive 2 (psd2)," 2018. [Online]. Available: https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/5558

[4] UKFinance, "2023 half year fraud report," 2023. [Online]. Available: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/2023-half-year-fraud-report

[5] U. Finance, "Annual fraud report 2023," 2021. [Online]. Available: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023

[6] J. G. E. R. D. Q. Alex Louwe Kooijmans, Rob Haake. (2009) Enterprise fraud management with aci proactive risk manager on ibm system z. [Online]. Available: https://www.redbooks.ibm.com/redpapers/pdfs/redp4545.pdf

[7] Tibco. (2022) How to detect banking fraud in a constantly evolving cyberspace? [Online]. Available: https://www.tibco.com/reference-center/how-to-detect-banking-fraud-in-a-constantly-evolving-cyberspace

[8] P. Tavares. (2022) Taking the bait: The modus operandi of massive social engineering waves impacting banks in portugal. [Online]. Available: https://seguranca-informatica.pt/taking-the-bait-the-modus-operandi-of-massive-social-engineering-waves-impacting-banks-in-port

[9] E. C. Bank. (2023) Single euro payments area (sepa). [Online]. Available: https://www.ecb.europa.eu/paym/integration/retail/sepa/html/index.en.html

[10] Amazon. (2023) Message queues. [Online]. Available: https://aws.amazon.com/it/message-queue/

[11] IBM. (2023) Ibm mq scenarios. [Online]. Available: https://public.dhe.ibm.com/software/integration/wmq/docs/V9.2/PDFs/mq92.scenarios.pdf

[12] MqSeries. (2002) What is intercommunication? [Online]. Available: http://www.mqseries.net/manuals/intercommunication/csqzae060e.html

[13] C. Herault, P. Lalanda, and E. Adele, "Mediation and enterprise service bus a position paper," 11 2023.

[14] ACI. (2022) Real-time statistics. [Online]. Available: https://www.aciworldwide.com/real-time-payments-report?

[15] Gartner. (2002) Security-risk-management. [Online]. Available: https://www.gartner.com/en/conferences/calendar/security-risk-management

[16] M.Sarfraz, *Recent Advances in Biometrics*. IntechOpen, 2022.

[17] J. D. Rome, "User authentication via known text input cadence," Patent, 2016.

[18] M. Chima. (2022) Fraud detection algorithms using machine learning and ai. [Online]. Available: https://hybridcloudtech.com/fraud-detection-algorithms-using-machine-learning-and-ai/

[19] J. Johansson. (2023) Phases of a project life cycle. [Online]. Available: https://resourceguruapp.com/blog/project-life-cycle

[20] SEON. (2023) False positives. [Online]. Available: https://seon.io/resources/dictionary/false-positives/

[21] I. E. S. S. testing. (2022) How to test fraud detection software and what to expect? [Online]. Available: https://huddle.eurostarsoftwaretesting.com/how-to-test-fraud-detection-software-and-what-to-expect/

[22] SEON. (2023) False negatives. [Online]. Available: https://seon.io/resources/dictionary/false-negatives/

[23] Perforce. (2022) Requirements traceability matrix — everything you need to know. [Online]. Available: https://www.perforce.com/resources/alm/requirements-traceability-matrix#:~:text=A%20requirements%20traceability%20matrix%20is,%2C%20test%20results%2C%20and%20issues.

[24] S. Pittet. (2023) The different types of software testing. [Online]. Available: https://www.atlassian.com/continuous-delivery/software-testing/types-of-software-testing

[25] C. F. P. Centre. (2022) Testing the effectiveness of fraud controls. [Online]. Available: https://www.counterfraud.gov.au/access-tools-and-guidance/testing-effectiveness-fraud-controls