big data and cognitive computing

MDPI

Article

National Payment Switches and the Power of Cognitive Computing against Fintech Fraud

Alessio Faccia

School of Business, University of Birmingham Dubai, Dubai 341799, United Arab Emirates; a.faccia@bham.ac.uk

Abstract: National Payment Switches (NPSs) and International Payment Switches (IPSs), including major players such as SWIFT, Mastercard, and CHIPS, have become vital to the financial infrastructure, facilitating secure and efficient transactions among local financial institutions. Nonetheless, the growing adoption of digital payments has heightened the risk of financial fraud. Consequently, NPSs, under the direct ownership of Central Banks (CBs), are increasingly adopting advanced technologies, such as cognitive computing, to bolster their fraud detection capabilities in their respective countries. This article delves into the role of cognitive computing in detecting financial fraud within NPSs. It examines the advantages of cognitive computing in recognising patterns of fraudulent behaviour and analysing vast amounts of data. Additionally, the study highlights the importance of focusing on how cognitive computing can augment traditional fraud detection methods, such as rule-based systems and data analytics. Nineteen real-world cases from eighteen countries are analysed, exploring the cognitive computing tools employed by NPSs to identify fraudulent transactions. The challenges and limitations of implementing cognitive computing in fraud detection and potential solutions to address these issues are identified. The primary assumption that cognitive computing is crucial for detecting financial fraud in NPSs is substantiated. Its ability to analyse large datasets and pinpoint patterns of fraudulent behaviour proves invaluable for financial institutions seeking to protect themselves against financial fraud in a progressively digital world. The conclusions drawn from the overview of the cases aim to identify best practices, potentially trigger new benchmarking standards, and facilitate the development of integrated cross-border solutions to combat financial fraud on a global scale effectively. The purpose of this research is to examine the role of cognitive computing in detecting financial fraud within NPSs, identify its advantages, challenges and limitations, and provide real-world case examples.

Keywords: national payment switches; cognitive computing; financial fraud; fraud detection; risk management

Citation: Faccia, A. National Payment Switches and the Power of Cognitive Computing against Fintech Fraud. *Big Data Cogn. Comput.* **2023**, *7*, 76. https://doi.org/10.3390/bdcc7020076

Academic Editor: Min Chen

Received: 3 March 2023
Revised: 5 April 2023
Accepted: 13 April 2023
Published: 17 April 2023

1. Introduction

This research aims to examine the role of cognitive computing in detecting financial fraud within National Payment Switches (NPSs) and to identify its advantages, challenges, and limitations in enhancing traditional fraud detection methods. The study also aims to provide real-world examples of how cognitive computing is used in NPSs to identify fraudulent transactions and t practices for implementing cognitive computing in fraud detection. This research aims to integrate solutions to combat financial fraud effectively.

1.1. Payment Switches and Gateways in the Fintech Ecosystem

Payment Switches and Gateways are integral components of payment systems and, more broadly, fintech ecosystems [1,2]. However, they play different roles in enabling and facilitating digital payments. A Payment Switch is a central system connecting multiple banks and financial institutions, allowing them to process and route payment transactions [3]. Payment switches act as intermediaries between banks and financial institutions, facilitating the exchange of payment instructions and settlement of funds. They provide a

centralised infrastructure for payment processing, enabling efficient and secure payment transactions [4]. A Payment Gateway technology platform facilitates online transactions between customers and merchants. Payment gateways enable customers to make online purchases by providing a secure payment processing system that authorises and processes transactions in real time. Payment gateways typically integrate with multiple payment methods, including credit and debit cards, e-wallets, and bank transfers, allowing customers to choose their preferred payment method [5,6].

The main difference between payment switches and payment gateways is the scope of their operations. Payment switches focus on facilitating payment transactions between financial institutions, while payment gateways enable online transactions between customers and merchants. Payment switches operate at a larger scale, handling large volumes of transactions between multiple financial institutions, while payment gateways operate at a smaller scale, facilitating transactions between individual customers and merchants. The importance of payment switches and gateways for fintech ecosystems lies in their ability to enable and facilitate digital payments [7,8]. The rise of fintech has led to an increased demand for digital payment solutions, and payment switches and gateways play a critical role in meeting this demand. They provide the necessary infrastructure and technology to enable secure, efficient, and seamless payment transactions, driving the growth of fintech ecosystems [9]. Furthermore, payment switches and gateways are essential for promoting financial inclusion by making digital payments accessible to a wider range of users, including those who are unbanked or underbanked. They provide a convenient and cost-effective alternative to traditional payment methods, enabling users to transact digitally from anywhere [10].

Given all the above reasons, Payment Switches and Gateways are crucial components of Fintech ecosystems, enabling and facilitating digital payments at different levels. They play complementary roles in providing the necessary infrastructure and technology to support secure, efficient, and seamless payment transactions, driving the growth of fintech and promoting financial inclusion. In general, National Payment Switches (NPSs) have increasingly become an integral part of the financial infrastructure of many countries worldwide, and this trend is reinforcing due to many factors. Central Banks directly control/monitor local payment flows and reduce transaction costs. Most NPSs are owned or directly controlled by the Central Banks [11,12].

These switches provide a secure and efficient way to conduct transactions between financial institutions. The use of national payment switches has increased in recent years due to the rising demand for digital payments. However, with the increased use of digital payments, the risk of financial fraud has also increased. Another reason countries are implementing national payment switches is to reduce the costs associated with using International Payment Switches (IPSs). IPSs charge fees for processing transactions, which can be high, particularly for smaller countries. Countries can reduce these costs and improve their financial independence by implementing NPSs. Implementing NPSs has also led to greater control over the payment system within a country. Indeed, they enable Central Banks to monitor and manage payment transactions within their borders, providing greater security and control [13,14].

There is a research gap in the literature and practice concerning the use of cognitive computing in fraud detection within the fintech industry, particularly regarding the role National and International Payment Switches can play. While cognitive computing has been adopted to some extent, it has not yet been standardised across the industry, leading to varying levels of success and implementation. By conducting an in-depth overview of multiple cases, it may be possible to identify best practices and stimulate the development of new benchmarking standards and integrated cross-border solutions to more effectively prevent and detect fraud in fintech. The outcomes of this research, therefore, target the tfollowing:

- Standardisation of cognitive computing practices can lead to more consistent results in fraud detection, ensuring that financial institutions are better equipped to identify and

prevent fraudulent activities. This standardisation could involve the development of common protocols, algorithms, and data models that facilitate collaboration between different organisations and streamline the deployment of cognitive computing technologies in fraud detection.

- Benchmarking standards, on the other hand, can help financial institutions gauge the effectiveness of their fraud detection systems against industry leaders, thereby encouraging continuous improvement and innovation. These standards may encompass various metrics, such as success rates in detecting fraud, reductions in false positives, and improvements in decision-making speed and accuracy.
- Identifying best practices can provide valuable insights into the most effective methods for implementing cognitive computing in fraud detection. These practices might address challenges such as data privacy and security, integrating cognitive computing with existing systems, and training and upskilling personnel. Financial institutions can learn from their peers by studying cases where cognitive computing has been successfully deployed and adopt proven strategies to bolster their fraud detection efforts.
- Developing integrated cross-border solutions is essential in today's interconnected financial landscape. Fraudsters are increasingly operating across multiple jurisdictions, making it vital for financial institutions to collaborate and share information to combat these threats. By adopting cognitive computing tools and best practices that enable seamless cross-border cooperation, financial institutions can more effectively prevent and detect fraud on a global scale.

1.2. Cognitive Computing, NPSs, and Financial Frauds

Despite the NPSs' benefits, the increasing use of digital payments has also increased financial fraud. Fraudsters are becoming increasingly sophisticated, making it difficult for traditional fraud detection methods to keep pace. It is where cognitive computing comes in. Cognitive computing uses advanced technologies, including artificial intelligence and machine learning, to simulate human thought processes. These technologies enable computers to learn from data and improve their performance over time. In the context of financial fraud detection, cognitive computing can analyse large amounts of data to identify patterns of fraudulent behaviour [15–19].

NPSs can significantly enhance their fraud detection capabilities by implementing cognitive computing. These technologies can identify and flag suspicious transactions, reducing the risk of financial fraud. Furthermore, cognitive computing can also be used to enhance traditional fraud detection methods, such as rule-based systems and data analytics. Several countries have implemented cognitive computing in their national payment switches to detect fraudulent transactions. For example, the Reserve Bank of India has implemented a fraud detection system that uses machine learning algorithms to identify suspicious transactions [20,21].

Similarly, the Central Bank of Nigeria has implemented a fraud detection system that uses artificial intelligence to identify potentially fraudulent transactions. However, implementing cognitive computing in fraud detection is not without its challenges. One of the main challenges is the availability of high-quality data. Cognitive computing algorithms rely on large datasets to learn from, and the quality of these datasets can impact the accuracy of the algorithms. Furthermore, using cognitive computing raises concerns about privacy and data protection [22].

Despite these challenges, the benefits of implementing cognitive computing in fraud detection for NPSs are significant. These technologies can significantly enhance the ability of financial institutions to detect and prevent financial fraud in an increasingly digital world. Therefore, financial institutions must invest in cognitive computing to safeguard against financial fraud and maintain the security and integrity of their payment systems [23].

2. Materials and Methods

Existing relevant literature and case studies are reviewed to investigate the most important techniques of cognitive computing applied by NPSs. It systematically searched relevant academic and industry publications, including journals, conference proceedings, and reports. The search is focused on identifying studies and articles that specifically address the application of cognitive computing in fraud detection for Payment Switches. The review then involved analysing and synthesising the findings from these studies, identifying the most common and effective techniques of cognitive computing used in payment switches, and evaluating their effectiveness in detecting and preventing financial fraud.

The article was then developed using the following research framework (see Table 1 below).

Table 1. Research Framework.

Step	Description
1	Research question: *What are the most important techniques of cognitive computing applied by national and international payment switches in fraud detection?*
2	Literature review: Identify relevant academic and industry publications, including journals, conference proceedings, and reports. Search for studies and articles that specifically address the application of cognitive computing in fraud detection for payment switches. Analyse and synthesise the findings from these studies, if any.
3	Data collection: Collect data on the most common and effective techniques of cognitive computing used in payment switches. Collect data on the effectiveness of these techniques in detecting and preventing financial fraud.
4	Data analysis: Analyse the data collected on the most common and effective techniques of cognitive computing used in payment switches. Analyse the data collected on the effectiveness of these techniques in detecting and preventing financial fraud. Identify patterns and trends in the data.
5	Results and findings: Summarise the most common and effective techniques of cognitive computing used in payment switches. Evaluate the effectiveness of these techniques in detecting and preventing financial fraud. Provide recommendations for payment switches on optimising their use of cognitive computing in fraud detection.
6	Conclusion: Summarise the key findings of the research. Discuss the implications of the findings for payment switches and the wider financial industry. Identify areas for future research.

Given the above-outlined research framework, a suitable qualitative method for this study is thematic analysis [24]. This method allows for identifying, analysing, and reporting patterns or themes within the collected data. The method is flexible and can be used across various data types, including those unstructured, the only consistently available for this research (for confidentiality and know-how reasons, payment switches did not share quantitative data). The process can be broken down into the following steps:

A. Familiarisation with the data by reviewing the literature on cognitive computing in fraud detection for payment switches, including academic publications and industry reports. It provided a foundation for understanding the context and key concepts.
B. Generation of initial codes. The literature review and data collection created a set of initial codes to categorise the information. It included codes related to specific cognitive computing techniques, their effectiveness, or challenges faced in implementation.
C. Search for themes: initial codes review and grouping them into broader themes that capture the essence of the research question.

D. Producing the report: With the themes established, findings are presented by discussing each theme in detail. The most common and effective techniques of cognitive computing used in payment switches are presented. An evaluation of their effectiveness in detecting and preventing financial fraud is performed.
E. Providing recommendations for payment switches on optimising their use of cognitive computing in fraud detection.

3. Findings: Cognitive Computing Tools Adopted by National Payment Switches to Tackle Financial Fraud

This literature review aims to provide an overview of the role of cognitive computing in detecting financial fraud in national payment switches, analysing the benefits, challenges, and limitations of the implementation of cognitive computing in fraud detection, and examining real-world examples of national payment switches that have implemented cognitive computing to detect fraudulent transactions.

Cognitive computing involves using artificial intelligence and machine learning algorithms to analyse data and make informed decisions. In the context of financial fraud detection, cognitive computing can help financial institutions identify fraudulent behaviour patterns and detect fraudulent transactions in real time. By analysing large amounts of data, cognitive computing can enhance traditional fraud detection methods such as rule-based systems and data analytics [25]. One of the key benefits of cognitive computing in fraud detection is its ability to analyse data in real time. It allows financial institutions to detect fraudulent transactions as they occur, enabling them to take immediate action to prevent further losses. Cognitive computing can also help financial institutions to identify patterns of fraudulent behaviour that may not be detectable using traditional fraud detection methods. It can help financial institutions detect and prevent new and emerging types of fraud [26,27].

Implementing cognitive computing in fraud detection requires access to high-quality data to train machine learning algorithms effectively. Financial institutions need to ensure that they have access to data from a wide range of sources, including transaction data, customer data, and external data sources, to maximise the effectiveness of cognitive computing in fraud detection. One of the main challenges associated with implementing cognitive computing in fraud detection is the lack of transparency in machine learning algorithms. Financial institutions must ensure that they clearly understand how machine learning algorithms make decisions to address this challenge. Explainable AI (XAI) techniques can help financial institutions understand the decision-making process of machine learning algorithms [28–30]. Another challenge is the ongoing monitoring and maintenance of machine learning models. Machine learning models must be monitored regularly to ensure they remain accurate and effective in detecting financial fraud. Financial institutions must also ensure they have the resources and expertise to maintain and update machine learning models [31].

3.1. Central Banks and National Payment Switches an Ongoing Collaboration

Central Banks (CBs) play a critical coordinating role in reducing transaction costs and preventing/detecting fraud in the payments ecosystem. They collaborate with local National Payment switches to achieve these objectives. The coordinating role of CBs with local NPSs is crucial in reducing transaction costs and preventing/detecting fraud. This collaboration helps to ensure the safety, efficiency, and soundness of the payments ecosystem, which is essential for the smooth functioning of the economy [32,33].

Many factors support their collaboration: (a) *developing and enforcing standards*: CBs work with NPSs to develop and enforce standards for payment systems. These standards ensure that payment systems are interoperable, secure, and efficient. They also help reduce transaction costs and prevent fraud [34]; (b) *risk management*: CBs work with NPSs to identify and manage payment system risks. They develop and implement risk management frameworks, including fraud prevention and detection measures, to ensure the safety

and soundness of payment systems [35]; (c) *monitoring and supervision*: CBs monitor and supervise NPSs to ensure compliance with regulations and standards. They also conduct regular audits and assessments to identify and address any weaknesses or vulnerabilities in the payment system [36]; (d) *promoting competition*: CBs work with NPSs to promote competition in the payments market. They encourage the entry of new players, which can help reduce transaction costs and improve the quality of services [37]; and (e) *innovation and technology*: CBs work with NPSs to promote innovation and the adoption of new technologies. They encourage the development of new payment systems and services, which can help reduce transaction costs and improve the efficiency and security of payments [38].

3.2. Real-World Examples of Cognitive Computing in Fraud Detection—Data Familiarisation

NPSs are crucial in cognitive computing applications, given their access to real-time monitored Big Data. These systems provide secure and efficient transactions between financial institutions, making them essential to a country's financial infrastructure. NPSs act as the central hub for all financial transactions in a country, facilitating the smooth and seamless transfer of funds between different financial institutions [39]. Moreover, NPSs are responsible for ensuring the security and integrity of financial transactions. With the increasing use of digital payments, the risk of financial fraud has also increased, necessitating the implementation of advanced technologies such as cognitive computing in fraud detection. National payment switches have implemented cognitive computing to enhance their fraud detection capabilities, allowing them to identify patterns of fraudulent behaviour and detect fraudulent transactions in real time [40].

Implementing cognitive computing in fraud detection has enabled NPSs to detect and prevent fraudulent transactions more effectively, safeguarding against financial fraud in an increasingly digital world. By analysing large amounts of data and identifying patterns of fraudulent behaviour, cognitive computing can help national payment switches to enhance their fraud detection capabilities and maintain the security and integrity of financial transactions. Several real-world examples demonstrate the benefits of implementing cognitive computing in national payment switches [41].

The countries were selected based on data availability and information related to using cognitive computing tools to detect financial fraud within National Payment Switches (NPSs). Additionally, the studied countries represent a diverse range of NPSs, reflecting different levels of development, regulatory frameworks, and fraud risks.

3.2.1. ACH (Automated Clearing House) (USA)

The ACH (Automated Clearing House) is the primary National Payment Switch in the United States. It is an electronic payment switch system that facilitates the transfer of funds between bank accounts in the United States. The ACH system is operated by the National Automated Clearing House Association (NACHA), which sets the rules and standards for ACH transactions. The ACH system enables various transactions, including direct deposit, payroll processing, and vendor and consumer payments. Transactions processed through the ACH system typically take one to two business days to settle. The ACH system is an essential component of the US payments ecosystem, processing trillions of dollars in transactions annually.

To prevent and detect financial fraud, ACH uses several cognitive computing tools, including the following:

Risk management and assessment models: The ACH uses machine learning algorithms to analyse transactional data and assess the risk of fraudulent activity. These models can identify unusual or suspicious activity patterns, such as multiple transactions from a single account in a short period or transactions significantly larger than usual. ACH uses advanced risk management tools to monitor and analyse transaction data, identify potential fraud, and prevent fraudulent transactions from being processed. The system uses algorithms to detect anomalies and suspicious transactions and can flag transactions for further investigation [42].

Anomaly detection: ML-powered cognitive computing techniques identify anomalous transactions outside the norm for a particular customer or account. These anomalies can be detected by analysing data points such as transaction amounts, frequencies, and locations [43].

Network analysis: The ACH uses algorithms to analyse the relationships between different accounts and identify potential fraud or money laundering patterns. This type of analysis can help detect complex fraud schemes that involve multiple accounts [44].

User behaviour analysis: Machine learning algorithms can be used to analyse the behaviour of individual users and detect changes or deviations from normal behaviour patterns. It can help identify fraudulent activity, such as account takeovers or unauthorised access to accounts [42].

3.2.2. Bancontact (Belgium)

Bancontact is a Belgian Electronic Payment Switch that allows customers to make payments using their bank accounts. The system was launched in 1989 and has since become one of the most popular payment methods in the country. Bancontact allows customers to make payments directly from their bank accounts, which means they do not need to enter their credit or debit card details when making a purchase. It reduces the risk of fraud and makes the payment process faster and more convenient for customers [45–47].

Bancontact works by linking a customer's bank account to their Bancontact account. When a customer makes a payment, the funds are transferred directly from their bank account to the merchant's account. Customers can make payments using their smartphone, tablet, or computer, and the system is compatible with a wide range of devices and platforms [48]. Bancontact also offers a mobile app that allows customers to make payments using their mobile devices. Bancontact is supported by over 20,000 merchants in Belgium and is accepted at various online and offline retailers, including supermarkets, restaurants, and petrol stations. Bancontact Company owns and operates the system, a joint venture between several major Belgian banks. Bancontact is regulated by the National Bank of Belgium and is subject to strict security standards to ensure the safety and privacy of customer data [49].

To prevent or detect fraud in fintech, Bancontact uses various techniques based on cognitive computing or machine learning. Some of these techniques are as follows:

Machine learning algorithms: Bancontact uses machine learning algorithms to detect patterns and anomalies in transaction data. These algorithms can identify fraudulent transactions by detecting patterns not typical of legitimate transactions [50].

Behavioural biometrics: Bancontact uses behavioural biometrics to authenticate users and detect fraudulent activity. This technique analyses user behaviour patterns such as typing speed, mouse movements, and scrolling patterns to identify suspicious activity [51].

Natural Language Processing (NLP): Bancontact uses NLP to detect and prevent fraud in customer service interactions. NLP can help identify suspicious messages or calls by analysing the language used and flagging potentially fraudulent activity [52].

Network analysis: Bancontact uses network analysis to identify potential fraud by analysing the relationships between different accounts and transactions. It can help detect complex fraud schemes that involve multiple accounts and transactions [53].

Predictive analytics: Bancontact uses predictive analytics to identify potential fraud before it occurs. Predictive analytics can detect potential fraud and alert the relevant parties by analysing past transaction data and identifying patterns [54].

3.2.3. BKM Express (Türkiye)

BKM Express is Türkiye's primary National Payment Switch, operated by the Interbank Card Center of Turkey (BKM). The system enables the processing of a wide range of electronic payments, including credit and debit card transactions, online payments, and mobile payments [55,56]. To prevent and detect financial fraud, BKM Express uses several cognitive computing tools, including the following:

Risk Management: BKM Express uses advanced risk management tools to monitor and analyse transaction data, identify potential fraud, and prevent fraudulent transactions from being processed. The system uses algorithms to detect anomalies and suspicious transactions and can flag transactions for further investigation [57].

Fraud Detection and Prevention: BKM Express uses advanced fraud detection and prevention tools to monitor transactions and identify potential fraud. The system uses algorithms to analyse transaction data, identify unusual patterns or behaviours, and flag potential fraud for further investigation [58].

Biometric Authentication: BKM Express has implemented biometric authentication for mobile payments, which allows users to authorise payments using their fingerprints or other biometric data. Biometric authentication provides a secure and convenient way for users to authorise payments while reducing the risk of fraud [59].

Two-Factor Authentication: BKM Express requires users to provide two-factor authentication for certain transactions, such as adding a new payment card or making a high-value transaction. Two-factor authentication provides an additional layer of security to prevent unauthorised transactions [60].

3.2.4. BPAY (Australia)

It is Australia's primary National Payment Switch, operated by BPAY Group. The system enables the processing of a wide range of electronic payments, including bill payments, government payments, and other transactions. BPAY is Australia's primary National Payment Switch, operated by BPAY Group [61,62]. To prevent and detect financial fraud, BPAY uses several cognitive computing tools, including the following:

Machine learning-based anomaly detection: BPAY uses machine learning algorithms to detect anomalies in transaction data and flag potentially fraudulent transactions for further investigation [63].

Natural language processing (NLP) for customer support: BPAY uses NLP to analyse customer support requests and identify potential fraud attempts. By analysing language patterns and sentiment, NLP can flag potential fraud before it occurs [64].

Data analytics for trend analysis: BPAY uses data analytics to analyse transactional data and identify trends in fraudulent behaviour. It helps the company avoid emerging fraud threats and prevents future attacks [63].

Real-time transaction monitoring: BPAY has implemented real-time monitoring systems that can detect potential fraud attempts as they occur. It allows the company to take immediate action to prevent fraudulent transactions from being processed [64].

3.2.5. China UnionPay (China)

China UnionPay is the primary National Payment Switch in China, operated by China UnionPay Co., Ltd, Shanghai, China. It was established in 2002 as a joint venture between several major Chinese banks, including the Bank of China, Industrial and Commercial Bank of China, China Construction Bank, and Agricultural Bank of China. As a payment switch, China UnionPay provides interbank transaction settlement and payment services for bank card issuers and acquirers in China. It operates a network of ATMs and nationwide point-of-sale (POS) terminals, which accept UnionPay-branded bank cards, including debit and credit cards. China UnionPay is also responsible for regulating and managing the issuance and acceptance of bank cards in China, and it has played a key role in promoting the use of electronic payments in the country. Recently, it has expanded its services beyond China to other countries and regions, including Asia-Pacific, Europe, and North America [65,66]. To prevent and detect financial fraud, China UnionPay uses several cognitive computing tools, including the following:

Advanced data analytics and machine learning: China UnionPay uses advanced data analytics and machine learning techniques to analyse large amounts of real-time transaction data and identify suspicious activity [67].

Fraud detection rules and models: China UnionPay uses a variety of fraud detection rules and models to identify potentially fraudulent transactions. These models are based on statistical analysis and can be updated in real time based on new data [68].

Biometric authentication: China UnionPay has implemented biometric authentication technologies, such as facial recognition and fingerprint scanning, to help prevent fraud by verifying the identity of customers [69].

Tokenisation: China UnionPay uses Tokenisation to protect customer data and prevent fraud. Tokenisation involves replacing sensitive data, such as credit card numbers, with a unique identifier or token, which can be used for transactions without revealing the original data [70].

3.2.6. EBA Clearing (Germany)

EBA Clearing is a provider of pan-European payment infrastructure. It was founded in 1998 by a group of major European banks to facilitate the clearing and settlement of payments across Europe. One of the services EBA Clearing offers is processing SEPA Credit Transfers (SCTs) and SEPA Direct Debits (SDDs) through its pan-European clearing platform, EURO1. EURO1 enables banks to settle transactions in real time in EUR in over 30 countries. In addition to its pan-European services, EBA Clearing operates a national payment switch in Germany called STEP2. STEP2 enables banks to process payments in Germany and other countries using the SCT and SDD schemes. It is connected to other European payment systems, allowing banks to exchange payments with other banks across the continent. As a national payment switch, STEP2 plays a crucial role in Germany's payment industry, facilitating the processing of millions of transactions each day. It also supports the implementation of the Single Euro Payments Area (SEPA), which aims to harmonise payment systems across Europe and make cross-border payments as easy as domestic payments [71,72].

To prevent and detect financial fraud, EBA Clearing uses several cognitive computing tools, including the following:

Risk Management: EBA Clearing uses advanced risk management tools to monitor and analyse transaction data, identify potential fraud, and prevent fraudulent transactions from being processed. The system uses algorithms to detect anomalies and suspicious transactions and can flag transactions for further investigation [73].

Fraud Detection and Prevention: EBA Clearing uses advanced fraud detection and prevention tools to monitor transactions and identify potential fraud. The system uses algorithms to analyse transaction data, identify unusual patterns or behaviours, and flag potential fraud for further investigation [73].

Artificial Intelligence and Machine Learning: EBA Clearing uses artificial intelligence and machine learning to identify and prevent fraudulent transactions. These tools enable the system to analyse large amounts of data, identify patterns and anomalies, and take appropriate action to prevent fraud [72].

3.2.7. EFTPOS (Australia)

EFTPOS stands for Electronic Funds Transfer at Point of Sale, a payment system widely used in Australia. EFTPOS allows customers to pay for goods and services by electronically transferring funds from their bank account to the merchant's bank account at the point of sale. When a customer makes a purchase using EFTPOS, they typically insert their debit or credit card into a card reader or tap their contactless card or mobile device on a terminal [74]. The terminal communicates with the customer's bank, verifying that they have sufficient funds to cover the purchase. Once the transaction is approved, the funds are transferred from the customer's account to the merchants. EFTPOS is widely accepted in Australia and is a popular payment method for consumers and businesses. EFTPOS is typically faster and more secure than traditional paper-based payment methods such as checks. Additionally, EFTPOS transactions are often less expensive for merchants than credit card transactions, making it a more cost-effective option for small businesses [75].

Risk Management: EFTPOS uses advanced risk management tools to monitor and analyse transaction data, identify potential fraud, and prevent fraudulent transactions from being processed. The system uses algorithms to detect anomalies and suspicious transactions and can flag transactions for further investigation [76].

Fraud Detection and Prevention: EFTPOS uses advanced fraud detection and prevention tools to monitor transactions and identify potential fraud. The system uses algorithms to analyse transaction data, identify unusual patterns or behaviours, and flag potential fraud for further investigation [77].

Tokenisation: EFTPOS uses Tokenisation to protect sensitive payment data such as bank accounts and credit card numbers. Tokenisation replaces sensitive data with a unique token, reducing the risk of data breaches and fraud [78].

Two-Factor Authentication: EFTPOS requires users to provide two-factor authentication for certain transactions, such as adding a new payment account or making a high-value transaction. Two-factor authentication provides an additional layer of security to prevent unauthorised transactions [79].

3.2.8. Faster Payments (UK)

Faster Payments is a National Payment Switch in the UK, operated by Faster Payments Scheme Limited. Faster Payments was launched in 2008 by the Faster Payments Scheme Limited (FPSL), a company owned and operated by the major UK banks and building societies. The service is available to customers of most UK banks and building societies and is used for various purposes, including person-to-person payments, bill payments, and online purchases. To make a Faster Payment, customers must provide the recipient's name, sort code, account number, and payment amount [80]. The payment is then processed through the Faster Payments system, which transfers the funds from the sender's bank account to the recipients in seconds. Faster Payments has become an increasingly popular payment method in the UK due to its speed, convenience, and availability. It is particularly useful for urgent payments, such as bill payments or sending money to friends or family in need. Faster Payments are often cheaper than other payment methods, such as wire transfers or international payments [81].

To prevent and detect financial fraud, Faster Payments uses several cognitive computing tools, including the following:

Risk Management: Faster Payments uses advanced risk management tools to monitor and analyse transaction data, identify potential fraud, and prevent fraudulent transactions from being processed. The system uses algorithms to detect anomalies and suspicious transactions and can flag transactions for further investigation [82].

Fraud Detection and Prevention: Faster Payments uses advanced fraud detection and prevention tools to monitor transactions and identify potential fraud. The system uses algorithms to analyse transaction data, identify unusual patterns or behaviours, and flag potential fraud for further investigation [83].

Real-Time Monitoring: Faster Payments provides real-time monitoring of payment transactions, enabling the system to identify and prevent fraudulent transactions [84].

Tokenisation: Faster Payments protects sensitive payment data such as bank accounts and card numbers. Tokenisation replaces sensitive data with a unique token, reducing the risk of data breaches and fraud [85].

3.2.9. Interac (Canada)

Interac is a National Payment Switch in Canada operated by Interac Corp. Interac is a Canadian payment network that facilitates electronic transactions between banks and financial institutions in Canada. Interac allows Canadians to securely and quickly send and receive money, pay bills, and make purchases using their bank accounts. Interac was founded in 1984 as a non-profit organisation by five major Canadian banks: RBC, CIBC, Scotiabank, TD Bank, and Desjardins [86]. Today, Interac is a for-profit company owned by its member financial institutions and has expanded its services to include online and

mobile payments and international money transfers. Interac operates through various payment methods, including Interac Debit, which allows Canadians to make point-of-sale purchases using their debit cards, and Interac e-Transfer, which allows users to send money electronically to other individuals or businesses in Canada using their email address or mobile phone number. Interac is widely used in Canada and is considered one of the country's most secure and reliable payment systems. It is accepted by millions of merchants across Canada and used by millions of Canadians for daily financial transactions. Interac has also expanded its services to include Interac Flash, a contactless payment method, and Interac Online, allowing Canadians to purchase their debit cards online [87]. To prevent and detect financial fraud, Interac uses several cognitive computing tools, including the following:

Risk Management: Interac uses advanced risk management tools to monitor and analyse transaction data, identify potential fraud, and prevent fraudulent transactions from being processed. The system uses algorithms to detect anomalies and suspicious transactions, and it can flag transactions for further investigation [87,88].

Fraud Detection and Prevention: Interac uses advanced fraud detection and prevention tools to monitor transactions and identify potential fraud. The system uses algorithms to analyse transaction data, identify unusual patterns or behaviours, and flag potential fraud for further investigation [89].

Biometric Authentication: Interac has implemented biometric authentication for mobile payments, which allows users to authorise payments using their fingerprints or other biometric data. Biometric authentication provides a secure and convenient way for users to authorise payments while reducing the risk of fraud [90].

Real-Time Monitoring and Alerting: Real-time monitoring and alerting is a security measure that provides real-time notifications of suspicious activity or unusual transactions. Real-time monitoring and alerting can help prevent fraud by enabling quick action to block fraudulent transactions or freeze user accounts. For example, the Interac payment system in Canada provides real-time monitoring and alerting to prevent fraud and protect user accounts [87].

3.2.10. NETS (Singapore)

NETS (Network for Electronic Transfers) is a Singapore-based payment system that provides electronic payment services for consumers and businesses. NETS was founded in 1985 as a joint venture between three local banks: DBS Bank, OCBC Bank, and United Overseas Bank (UOB). NETS allows consumers to make payments for goods and services using their debit cards, credit cards, or stored-value cards. NETS also operates an electronic funds transfer service that lets customers transfer funds between bank accounts in real time. Additionally, NETS provides merchants with various payment solutions, including point-of-sale terminals, online payment gateways, and mobile payment solutions. NETS is widely accepted in Singapore and used by millions of consumers and businesses for daily financial transactions. The company has also expanded its services to include international payments, partnering with major global payment networks such as Mastercard and UnionPay to allow NETS cardholders to make payments overseas. NETS has played an important role in Singapore's transition to a cashless society, with the government promoting electronic payments as part of its Smart Nation initiative. NETS has also been involved in several initiatives to promote financial inclusion, such as providing access to electronic payment services to low-income households and senior citizens [91,92].

Geo-Location: NETS uses geo-location data to monitor the location of users and devices, which can help prevent fraudulent transactions. For example, if a user's mobile device is in a different location from where the payment is being made, the transaction may be flagged as suspicious and blocked [93].

Machine Learning: NETS uses machine learning algorithms to analyse transaction data and identify potential fraud. Machine learning algorithms can quickly and accurately analyse large amounts of data and identify patterns and behaviours that may indicate fraud [94].

Biometric Authentication: NETS has implemented facial and voice recognition for mobile payments besides fingerprint authentication. Biometric authentication provides an additional layer of security by verifying the user's identity before authorising payment [95].

Three-Dimensional Secure: NETS uses 3-D Secure to provide an additional layer of security for online transactions. Notably, 3-D Secure requires users to provide an additional password or code to complete online transactions, which can help prevent fraudulent transactions [96].

3.2.11. NEXI (Italy)

Nexi is one of Italy's leading payment service providers, offering various digital payment solutions for consumers and businesses. NEXI was formed in 2019 following the merger of two major Italian payment companies, Nexi and SIA. NEXI operates a variety of payment solutions, including debit and credit card payments, online payments, and mobile payments. The company also provides point-of-sale terminals to merchants and supports payments through contactless, QR code, and NFC technology. NEXI also provides various value-added services such as loyalty programs and fraud prevention solutions. NEXI is the largest payment technology company in Italy and is used by millions of consumers and businesses for their daily financial transactions. The company has a strong presence in the Italian market, with over 300,000 merchants using its payment solutions. NEXI has also expanded its services to include international payments, partnering with global payment networks such as Visa and Mastercard to enable its customers to make payments overseas. NEXI is committed to promoting financial inclusion in Italy and has launched several initiatives to support underserved communities. For example, the company has partnered with local authorities to provide payment solutions to unbanked communities and has launched a range of financial education programs aimed at improving financial literacy among young people [97]. To prevent and detect financial fraud, Nexi uses several cognitive computing tools, including the following:

Transaction Monitoring: NEXI uses transaction monitoring tools to analyse data and identify potential fraud. The system uses algorithms to analyse real-time transaction data and flag potential fraud for further investigation [98].

Biometric Authentication: NEXI has implemented biometric authentication for mobile payments, which allows users to authorise payments using their fingerprints. Biometric authentication provides a secure and convenient way for users to authorise payments while reducing the risk of fraud [99].

Machine Learning: NEXI uses machine learning algorithms to analyse transaction data and identify patterns or behaviours that may indicate fraud. The system can detect anomalies or unusual behaviour and potentially flag fraud for further investigation [100].

3.2.12. NPCI (India)

For India, the most important National Payment Switches are operated by the National Payments Corporation of India (NPCI). Here are some of the key systems operated by NPCI [101,102]:

- UPI (Unified Payments Interface): UPI is a real-time payment system that enables users to send and receive money using a virtual payment address linked to their bank account. The system has gained widespread adoption in India due to its ease of use and convenience.
- IMPS (Immediate Payment Service): IMPS is a real-time interbank electronic fund transfer system that enables users to transfer money instantly between bank accounts in India.
- RuPay: RuPay is a domestic card payment network that enables users to make payments using debit, credit, and prepaid cards. The system competes with international card networks such as Visa and Mastercard.
- AEPS (Aadhaar Enabled Payment System): AEPS is a payment system that enables users to make payments using their Aadhaar number and biometric authentication.

The system is designed to enable financial inclusion for individuals who do not have access to traditional banking services [103].

UPI Authentication: NPCI uses UPI authentication to ensure secure access to its payment systems. UPI authentication is a two-factor process requiring users to provide a PIN or biometric data to access their accounts or complete transactions. UPI authentication provides an additional layer of security and helps prevent unauthorised access to user accounts [104].

AI-Powered Fraud Detection: NPCI uses artificial intelligence (AI) to detect and prevent fraud in digital transactions. The AI-powered system can analyse transaction data in real time and identify suspicious patterns or behaviour that may indicate fraud. The system can flag potential fraud for further investigation or block fraudulent transactions [105].

Real-Time Monitoring and Alerting: NPCI uses real-time monitoring and alerting to detect and prevent fraud. The system can monitor transactions in real time and flag potential fraud for further investigation or block fraudulent transactions. Real-time monitoring and alerting enable quick action to prevent fraud and protect user accounts [106].

Blockchain Technology: NPCI uses blockchain technology to provide secure and efficient payment services. The blockchain-based payment platform Vajra can facilitate secure and transparent transactions while reducing the risk of fraud. Blockchain technology provides a tamper-proof and decentralised system that can ensure the integrity of transactions and protect user data [107].

3.2.13. NSPK (National System of Payment Cards) (Russia)

NSPK is Russia's primary National Payment Switch, established by the Central Bank of Russia in 2014. NSPK provides a centralised infrastructure for processing electronic payments, including debit and credit card transactions, online payments, and mobile payments. The system operates on the Mir payment network, designed to provide a secure and reliable payment infrastructure for individuals and businesses in Russia. Through advanced security measures and cognitive computing tools, NSPK can prevent and detect financial fraud and protect the integrity of the Russian payments system. However, specific details on the cognitive computing tools used by NSPK to prevent/detect financial frauds are not completely available [108]. The only known used systems are as follows:

Tokenisation: NSPK uses Tokenisation to protect sensitive payment data such as card numbers and other transactional information. Tokenisation replaces the card number with a unique token, which is used to process the transaction without exposing sensitive data. It reduces the risk of data breaches and fraud [109].

Three-Dimensional Secure: NSPK uses the 3D Secure protocol to provide an additional layer of authentication for online transactions. Notably, 3D Secure requires cardholders to provide a password or other form of authentication to complete a transaction, reducing the risk of fraudulent transactions [110].

Fraud Detection and Prevention: NSPK uses advanced fraud detection and prevention tools to monitor transactions and identify potential fraud. The system uses algorithms to analyse transaction data, identify unusual patterns or behaviours, and flag potential fraud for further investigation [111].

Biometric Authentication: NSPK has implemented biometric authentication for mobile payments, which allows users to authorise payments using their fingerprints or other biometric data. Biometric authentication provides a secure and convenient way for users to authorise payments while reducing the risk of fraud [112].

3.2.14. PIX (Brazil)

PIX is Brazil's primary National Payment Switch, operated by the Brazilian Central Bank. The system enables real-time transfers of funds between bank accounts in Brazil, and it handles transactions for a wide range of payment types, including salary payments, loan disbursements, and commercial payments. PIX is a payment switch in Brazil that facilitates instant payments and money transfers between individuals and businesses. The Brazilian

Central Bank manages the system and uses advanced security measures to prevent and detect financial fraud [113]. Here are the cognitive computing tools used by PIX to prevent and detect financial fraud, along with a reference for each:

Machine Learning: PIX uses machine learning algorithms to detect and prevent real-time fraud. The system can analyse transaction data to identify fraud patterns and behaviours and potentially flag fraud for further investigation or block fraudulent transactions [114].

Behavioural Biometrics: PIX uses behavioural biometrics to authenticate users and detect potential fraud. The system can analyse user behaviour, such as typing speed and keystroke dynamics, to identify suspicious activity and prevent unauthorised access to user accounts [115].

Real-Time Monitoring and Alerting: PIX uses real-time monitoring and alerting to detect and prevent fraud. The system can monitor transactions in real time and flag potential fraud for further investigation or block fraudulent transactions. Real-time monitoring and alerting enable quick action to prevent fraud and protect user accounts [116].

3.2.15. SADAD (Saudi Arabia)

SADAD is the primary National Payment Switch in KSA, operated by the Saudi Arabian Monetary Authority (SAMA). The system provides a centralised infrastructure for processing electronic payments, including credit and debit card transactions, online payments, and mobile payments. The SAMA has implemented a machine learning system to detect and prevent fraudulent transactions in the Saudi Arabian Riyal Interbank Express (SARIE) system. The system uses machine learning algorithms to analyse transaction data and identify patterns of fraudulent behaviour. The system has significantly helped the SAMA reduce fraudulent transactions [117]. Here are the cognitive computing tools used by SADAD to prevent and detect financial fraud, along with a reference for each:

Fraud Detection and Prevention: SADAD uses advanced fraud detection and prevention tools to monitor transactions and identify potential fraud. The system can analyse transaction data to identify unusual patterns or behaviours that may indicate fraud and flag potential fraud for further investigation or block fraudulent transactions [118].

Risk-Based Authentication: SADAD uses risk-based authentication to provide an additional layer of security for online transactions. The system can analyse transaction data and user behaviour to assess the risk of a transaction and can require additional authentication for high-risk transactions. It helps prevent unauthorised access to user accounts and reduces the risk of fraud [119].

Tokenisation: SADAD uses Tokenisation to protect sensitive payment data, such as card numbers and other transactional information. Tokenisation replaces the card number with a unique token, which is used to process the transaction without exposing sensitive data. It reduces the risk of data breaches and fraud [120].

3.2.16. SNCE (Sistema Nacional de Compensación Electrónica) (Argentina)

SNCE (Sistema Nacional de Compensación Electrónica) is the primary payment switch in Argentina that facilitates electronic payments and money transfers between individuals and businesses. The Central Bank of Argentina manages the system and uses advanced security measures to prevent and detect financial fraud [121]. Here are the cognitive computing tools used by SNCE to prevent and detect financial fraud, along with a complete reference for each:

Fraud Detection and Prevention: SNCE uses advanced fraud detection and prevention tools to monitor transactions and identify potential fraud. The system can analyse transaction data to identify unusual patterns or behaviours that may indicate fraud and flag potential fraud for further investigation or block fraudulent transactions [121].

Encryption: SNCE uses encryption to protect sensitive payment data such as card numbers and other transactional information. Encryption ensures that the data are secure and cannot be intercepted or accessed by unauthorised parties. It reduces the risk of data breaches and fraud [121].

Biometric Authentication: SNCE has implemented biometric authentication for mobile payments, which allows users to authorise payments using their fingerprints or other biometric data. Biometric authentication provides a secure and convenient way for users to authorise payments while reducing the risk of fraud [121].

Real-time Monitoring and Alerting: SNCE uses real-time monitoring and alerting to detect and prevent fraud. The system can monitor transactions in real time and flag potential fraud for further investigation or block fraudulent transactions. Real-time monitoring and alerting enable quick action to prevent fraud and protect user accounts [121].

3.2.17. SPEI (Sistema de Pagos Electrónicos Interbancarios) (Mexico)

SPEI (Sistema de Pagos Electrónicos Interbancarios) is a real-time electronic payment system in Mexico that allows individuals and businesses to transfer funds between bank accounts. SPEI is operated by the Banco de México, the country's central bank, and is available to customers of most Mexican banks. SPEI is designed to facilitate secure, fast, and efficient electronic transactions and is widely used in Mexico for various purposes, including bill payments, online purchases, and person-to-person payments. To make an SPEI transfer, customers must provide the recipient's bank account number, CLABE (Clave Bancaria Estandarizada), and the payment amount. The funds are transferred instantly and are available in the recipient's account within seconds. SPEI is considered one of Mexico's most reliable and secure payment systems and has been important in promoting financial inclusion. The system has also helped to reduce the use of cash and promote a cashless economy, which has been a key priority for the Mexican government in recent years. SPEI is also used for large-value payments, such as interbank transfers and government payments. The system is linked to other international payment systems, such as SWIFT, allowing for international payments to and from Mexico [122].

To prevent and detect financial fraud, SPEI uses several cognitive computing tools, including the following:

Two-factor authentication: SPEI requires two-factor authentication for all transactions. Users must provide two forms of identification, such as a password and a security token or a biometric authentication method, to complete a transaction. Two-factor authentication is an effective security measure that helps prevent unauthorised access to accounts and fraudulent transactions [123].

Encryption: SPEI uses advanced encryption technology to protect sensitive data, such as account numbers, passwords, and other transactional data, from unauthorised access. Encryption ensures that data transmitted through the system is secure and cannot be intercepted by hackers or other unauthorised parties [124].

Transaction monitoring: SPEI uses advanced transaction monitoring tools to identify potential fraud and prevent fraudulent transactions from being processed. The system uses algorithms to analyse transaction data, identify unusual patterns or behaviours, and flag potential fraud for further investigation [124].

Anomaly detection: SPEI uses anomaly detection algorithms to identify unusual patterns or behaviours that may indicate fraud. These algorithms use machine learning to analyse large amounts of data and identify patterns associated with fraudulent activities. When an anomaly is detected, the system can flag the transaction for further investigation [124].

3.2.18. STET (France)

STET is the primary National Payment Switch in France, operated by STET. The system provides a centralised infrastructure for processing electronic payments, including credit and debit card transactions, online payments, and mobile payments. STET is a payment switch in France that facilitates electronic payments and money transfers between individuals and businesses. Six major French banks manage the system and use advanced security measures to prevent and detect financial fraud [125]. Here are the cognitive computing tools used by STET to prevent and detect financial fraud, along with a reference for each:

Fraud Detection and Prevention: STET uses advanced fraud detection and prevention tools to monitor transactions and identify potential fraud. The system can analyse transaction data to identify unusual patterns or behaviours that may indicate fraud and flag potential fraud for further investigation or block fraudulent transactions [126].

Real-time Monitoring and Alerting: STET uses real-time monitoring and alerting to detect and prevent fraud. The system can monitor transactions in real time and flag potential fraud for further investigation or block fraudulent transactions. Real-time monitoring and alerting enable quick action to prevent fraud and protect user accounts [126].

Biometric Authentication: STET has implemented biometric authentication for mobile payments, which allows users to authorise payments using their fingerprints or other biometric data. Biometric authentication provides a secure and convenient way for users to authorise payments while reducing the risk of fraud [126].

Tokenisation: STET uses Tokenisation to protect sensitive payment data such as card numbers and other transactional information. Tokenisation replaces the card number with a unique token, which is used to process the transaction without exposing sensitive data. It reduces the risk of data breaches and fraud [126].

3.2.19. UAEFTS (UAE Funds Transfer System) (United Arab Emirates)

UAEFTS (United Arab Emirates Funds Transfer System) is a national payment system that facilitates electronic funds transfers between banks in the United Arab Emirates (UAE). UAEFTS was launched in 1995 and is operated by the UAE Central Bank, the country's central bank. UAEFTS is designed to enable secure and efficient electronic transactions and is widely used in the UAE for various purposes, including interbank transfers, bill payments, and online purchases. The system is available to customers of all banks in the UAE and supports both AED (United Arab Emirates Dirham) and foreign currency transactions. To make a UAEFTS transfer, customers must provide the recipient's bank account number, IBAN (International Bank Account Number), and the payment amount. The funds are transferred electronically from the sender's bank account to the recipient's. The transfer typically takes a few hours to process but can be completed in real time if the banks involved have signed up for the system's real-time payment service. UAEFTS is considered one of the UAE's most reliable and secure payment systems and has played an important role in promoting the country's transition to a cashless economy [127,128]. The system has also helped facilitate international trade and commerce, supporting local and cross-border payments.

Top of Form

Bottom of Form

To prevent and detect financial fraud, UAEFTS uses several cognitive computing tools, including the following:

Transaction Monitoring: UAEFTS uses advanced transaction monitoring tools to identify potential fraud and prevent fraudulent transactions from being processed. The system uses algorithms to analyse transaction data, identify unusual patterns or behaviours, and flag potential fraud for further investigation [129].

Risk Assessment: UAEFTS uses risk assessment models to analyse the risk associated with each transaction and customer. By analysing various factors, such as transaction history, customer behaviour, and other variables, UAEFTS can assess the likelihood of fraud and take appropriate action to prevent it [130].

Data Visualisation: UAEFTS uses data visualisation tools to provide its analysts with a clear and concise data representation. By using interactive dashboards and visual data representations, analysts can quickly identify potential fraud and take action to prevent it [131].

3.3. Initial Code Generation

The following step of the thematic analysis methodology involves generating Initial Codes to map the findings with the recurring and non-recurring cognitive computing measures/techniques adopted by the National Payment Switches analysed.

At this stage, all codes are allocated only by following their alphabetic order before being grouped in clusters later on, all codes are matched in Table 2 below.

Table 2. Initial Codification Cognitive Computing Tools used by National Payment Switches worldwide.

3-D Secure	CC-01
Advanced Data Analytics	CC-02
AI-Powered Fraud Detection	CC-03
Anomaly Detection	CC-04
Behavioural Biometrics	CC-05
Biometric Authentication	CC-06
Blockchain Technology	CC-07
Data Analytics for trend analysis	CC-08
Data Visualisation	CC-09
Encryption	CC-10
Fraud Detection Rules and Models	CC-11
Fraud Prevention	CC-12
Geo-Localisation	CC-13
ML Algorithms	CC-14
ML-based Anomaly Detection	CC-15
Network Analysis	CC-16
NLP (Natural Language Processing)	CC-17
Predictive Analytics	CC-18
Real-Time Alerting	CC-19
Real-Time Transaction Monitoring	CC-20
Risk Assessment	CC-21
Risk Management	CC-22
Risk-Based Authentication	CC-23
Tokenisation	CC-24
Two-Factor Authentication	CC-25
UPI Authentication	CC-26
User Behaviour Analysis	CC-27

Table 3 below summarises the findings.

Given the above results, interesting patterns and conclusions can be identified:

Most national payment switches use a combination of risk management, fraud detection and prevention, and authentication measures to secure their systems and prevent financial fraud.

Machine learning and artificial intelligence (AI) are commonly used to detect and prevent fraud across various national payment switches.

Biometric authentication, such as fingerprint or facial recognition, is becoming increasingly popular as a secure and convenient way to authenticate transactions and reduce the risk of fraud.

Table 3. Findings Summary: Cognitive Computing Tools used by National Payment Switches worldwide.

National Payment Switch	Country	Codes	Cognitive Computing Tools Used
ACH	USA	CC-21; CC-22; CC-04, CC-16, CC-27	Risk management and assessment models, Anomaly detection, Network analysis, User behaviour analysis
Bancontact	Belgium	CC-14; CC-05; CC-17; CC-16; CC-18	Machine learning algorithms, Behavioural biometrics, Natural Language Processing (NLP), Network analysis, Predictive analytics
BKM Express	Türkiye	CC-22; CC-11; CC-12; CC-06; CC-25	Risk Management, Fraud Detection and Prevention, Biometric Authentication, Two-Factor Authentication
BPAY	Australia	CC-15; CC-17; CC-08; CC-20	Machine learning-based anomaly detection, Natural language processing (NLP) for customer support, Data analytics for trend analysis, Real-time transaction monitoring
China UnionPay	China	CC-02; CC-11; CC-06; CC-24	Advanced data analytics and machine learning, Fraud detection rules and models, Biometric authentication, Tokenisation
EBA Clearing—STEP2	Germany	CC-22; CC-11; CC-12; CC-03; CC-14	Risk Management, Fraud Detection and Prevention, AI/ML
EFTPOS	Australia	CC-22; CC-11; CC-12; CC-24; CC-25	Risk Management, Fraud Detection and Prevention, Tokenisation, Two-Factor Authentication
Faster Payments	UK	CC-22; CC-11; CC-12; CC-20; CC-24	Risk Management, Fraud Detection and Prevention, Real-Time Monitoring, Tokenisation
Interac	Canada	CC-22; CC-11; CC-12; CC-06; CC-20	Risk Management, Fraud Detection and Prevention, Biometric Authentication, Real-Time Monitoring
NETS	Singapore	CC-13; CC-14; CC-06; CC-01	Geo-Location, Machine Learning, Biometric Authentication, 3-D Secure
Nexi	Italy	CC-20; CC-06; CC-14	Transaction Monitoring, Biometric Authentication, Machine Learning
NPCI	India	CC-26; CC-03; CC-20; CC-07	UPI Authentication, AI-Powered Fraud Detection, Real-Time Monitoring and Alerting, Blockchain Technology
NSPK	Russia	CC-24; CC-01; CC-11; CC-12; CC-06	Tokenisation, 3D Secure, Fraud Detection and Prevention, Biometric Authentication
PIX	Brazil	CC-14; CC05; CC-20	Machine Learning, Behavioural Biometrics, Real-Time Monitoring
SADAD	KSA	CC-11; CC-12; CC-23; CC-24; CC-14	Fraud Detection and Prevention, Risk-Based Authentication, Tokenisation, Machine Learning (SARIE system)
SNCE	Argentina	CC-11; CC-12; CC-10; CC-06; CC-19; CC-20	Fraud Detection and Prevention, Encryption, Biometric Authentication, Real-time Monitoring and Alerting
SPEI	Mexico	CC-25; CC-10; CC-20; CC-04	Two-factor authentication, encryption, transaction monitoring, anomaly detection
STET	France	CC-11; CC-12; CC-19; CC-20; CC-06; CC-24	Fraud Detection and Prevention, Real-time Monitoring and Alerting, Biometric Authentication, Tokenisation
UAEFTS	United Arab Emirates	CC-20; CC-21; CC-09	Transaction Monitoring, Risk Assessment, Data Visualisation

Tokenisation, the process of replacing sensitive data with a unique token, is used by several national payment switches to protect sensitive payment data and reduce the risk of data breaches and fraud.

Real-time monitoring and alerting are essential for detecting and preventing fraud in electronic payment systems. Several national payment switches use this approach to monitor real-time transactions and quickly take action to prevent fraud.

Some national payment switches use natural language processing (NLP) and data analytics to improve customer support and trend analysis.

Different national payment switches use different combinations of cognitive computing tools to secure their systems and prevent fraud, which suggests that there is no one-size-fits-all approach to preventing financial fraud.

In particular, it is possible to observe the frequencies in Table 4.

Table 4. Frequency Cognitive Computing Tools used by National Payment Switches worldwide.

Codes	Freq	Codes	Freq
CC-11 (Fraud Detection Rules and Models)	10	CC-19 (Real-Time Alerting)	2
CC-20 (Real-Time Transaction Monitoring)	10	CC-21 (Risk Assessment)	2
CC-12 (Fraud Prevention)	9	CC-02 (Advanced data analytics)	1
CC-06 (Biometric Authentication)	8	CC-05 (Behavioural Biometrics)	1
CC-14 (ML Algorithms)	6	CC-07 (Blockchain Technology)	1
CC-22 (Risk Management)	6	CC-08 (Data analytics for trend analysis)	1
CC-24 (Tokenisation)	6	CC-09 (Data Visualisation)	1
CC-25 (Two-Factor Authentication)	3	CC-13 (Geo-Localisation)	1
CC-01 (3-D Secure)	2	CC-15 (ML-based Anomaly Detection)	1
CC-03 (AI-Powered Fraud Detection)	2	CC-18 (Predictive analytics)	1
CC-04 (Anomaly detection)	2	CC-23 (Risk-Based Authentication)	1
CC-10 (Encryption)	2	CC-26 (UPI Authentication)	1
CC-16 (Network Analysis)	2	CC-27 (User behaviour analysis)	1
CC-17 (Natural Language Processing (NLP))	2		

The table shows the frequency of various cognitive computing tools used in detecting financial fraud within National Payment Switches (NPSs). It provides valuable insights into the popularity and effectiveness of various cognitive computing tools in detecting financial fraud within NPSs and can be used to guide future research and development in this field. The most popular cognitive computing tools for detecting financial fraud within NPSs, as shown in the table, are CC-11 (Fraud Detection Rules and Models), CC-20 (Real-Time Transaction Monitoring), CC-12 (Fraud Prevention), and CC-06 (Biometric Authentication). The popularity of these tools can be attributed to their effectiveness in detecting and preventing fraud, ease of implementation, and ability to integrate with existing financial infrastructure. For example, Fraud Detection Rules and Models (CC-11) enable NPSs to set up specific rules and models to identify potential fraudulent transactions, while Real-Time Transaction Monitoring (CC-20) allows NPSs to monitor transactions in real time for any suspicious activity. Biometric Authentication (CC-06) is a highly secure method of verifying user identities and can help prevent fraudulent transactions by ensuring that only authorised users can access NPSs.

On the other hand, the least popular cognitive computing tools for detecting financial fraud within NPSs are CC-02 (Advanced data analytics), CC-05 (Behavioural Biometrics), CC-07 (Blockchain Technology), CC-08 (Data analytics for trend analysis), CC-09 (Data Visualisation), CC-13 (Geo-Localisation), CC-15 (ML-based Anomaly Detection), CC-18 (Predictive analytics), CC-23 (Risk-Based Authentication), CC-26 (UPI Authentication), and CC-27 (User behaviour analysis). The lack of popularity of these tools may be due to several factors, including their complexity, high cost of implementation, and the need for an understanding of their potential benefits. For example, advanced data analytics (CC-02) and data analytics for trend analysis (CC-08) require a significant amount of data and expertise to implement and may not be practical for smaller NPSs with limited resources.

Blockchain technology (CC-07) may be perceived as too complex or too early for practical implementation in many NPSs.

3.4. Search for Themes—Codes Grouping

The rationale behind grouping the above tools and techniques into themes is to provide a more structured and comprehensive understanding of the various aspects of fraud detection and prevention in the context of National and International Payment Switches. Each theme represents a distinct area of focus or objective that contributes to the overall goal of safeguarding financial transactions. The groups are as follows:

- Fraud Detection and Prevention (*Tout Court*): This group brings together tools and techniques to identify, monitor, and prevent fraudulent activities in payment systems. These tools help financial institutions detect and respond to potential fraud in real time, thereby reducing the likelihood of financial loss and enhancing the security of transactions. By combining rules and models with advanced detection methods, such as anomaly detection and AI-powered solutions, this group emphasises the proactive aspect of fraud management.
- Authentication and Security: This group's primary objective is to ensure users' authenticity and secure their financial transactions. By utilising various authentication techniques such as biometrics, two-factor authentication, and risk-based authentication, this theme aims to create a secure environment for financial transactions. Encryption and 3-D Secure further strengthen transaction security, making it difficult for malicious actors to compromise sensitive information or impersonate legitimate users.
- Machine Learning and Advanced Analytics: This group leverages machine learning and advanced analytics to enhance fraud detection and prevention capabilities. With the increasing volume and complexity of financial data, these tools play a crucial role in identifying subtle patterns of fraudulent behaviour, making predictions, and adapting to emerging trends. This theme highlights the value of data-driven insights in combating financial fraud by utilising advanced techniques such as natural language processing and user behaviour analysis.
- Risk Management and Assessment: The tools and techniques in this group aim to identify, assess, and manage risks associated with financial transactions. By conducting network analysis, risk assessment, and data analytics for trend analysis, financial institutions can gain a deeper understanding of the potential vulnerabilities in their systems and take appropriate measures to mitigate them. Data visualisation further supports this process by clearly representing risks and trends, enabling informed decision making.
- Data Protection and Privacy: This theme focuses on safeguarding sensitive financial data and ensuring users' privacy. Tokenisation and blockchain technology are key tools in this group that help protect sensitive information from being intercepted or misused. Geo-localisation adds a layer of security by identifying the geographical location of users, which can help detect potential fraud if transactions originate from unexpected or high-risk locations. Overall, this group emphasises the importance of data protection and user privacy in maintaining trust and confidence in the financial system.

3.5. Producing the Report

The digital age has brought about significant advancements in financial technology, with an increasing need for robust security and authentication measures. In order to ensure the authenticity of users and secure financial transactions, five key themes have been identified: Fraud Detection and Prevention (tout court), Authentication and Security, Machine Learning and Advanced Analytics, Risk Management and Assessment, and data protection and privacy. The indicators are reported in Table 5 below, showing that in the observed cases, the most recurring measures adopted by the National Switches observed are those grouped in the "Fraud Detection and Prevention Cluster", namely, Fraud

detection Rules and Models, Fraud Prevention, and Real-Time Transaction Monitoring. These measures highlight the importance of proactive fraud detection and prevention strategies for maintaining security and trust in the financial sector. The most under-processed cluster is the one related to data protection and privacy, which accounts for the lowest number of measures adopted and frequency among NPSs. This fact could be attributed to several factors: lack of awareness: Some NPSs might not fully recognise the importance of data protection and privacy in maintaining trust and security in the financial ecosystem. As a result, they might not prioritise these measures in their security strategies; limited resources: NPSs might face constraints in terms of budget, workforce, or technical expertise, which could limit their ability to implement comprehensive data protection and privacy measures; regulatory environment: the regulatory environment and legal frameworks in some jurisdictions might not mandate or emphasise the need for robust data protection and privacy measures, leading to their under-adoption among NPSs; and complexity: Implementing data protection and privacy measures, such as tokenisation and blockchain technology, can be complex and require specialised expertise. Some NPSs might struggle to navigate these complexities and opt for simpler security measures.

Table 5. Theme Groups for Computing Tools Used by National Payment Switches Worldwide (Own Elaboration).

Codes	Freq	Groups
CC-01 (3-D Secure)	2	Authentication and Security
CC-05 (Behavioural Biometrics)	1	Authentication and Security
CC-06 (Biometric Authentication)	8	Authentication and Security
CC-10 (Encryption)	2	Authentication and Security
CC-23 (Risk-Based Authentication)	1	Authentication and Security
CC-25 (Two-Factor Authentication)	3	Authentication and Security
CC-26 (UPI Authentication)	1	Authentication and Security
CC-07 (Blockchain Technology)	1	Data Protection and Privacy
CC-13 (Geo-Localisation)	1	Data Protection and Privacy
CC-24 (Tokenisation)	6	Data Protection and Privacy
CC-03 (AI-Powered Fraud Detection)	2	Fraud Detection and Prevention
CC-04 (Anomaly detection)	2	Fraud Detection and Prevention
CC-11 (Fraud Detection Rules and Models)	10	Fraud Detection and Prevention
CC-12 (Fraud Prevention)	9	Fraud Detection and Prevention
CC-19 (Real-Time Alerting)	2	Fraud Detection and Prevention
CC-20 (Real-Time Transaction Monitoring)	10	Fraud Detection and Prevention
CC-02 (Advanced data analytics)	1	Machine Learning and Advanced Analytics
CC-14 (ML Algorithms)	6	Machine Learning and Advanced Analytics
CC-15 (ML-based Anomaly Detection)	1	Machine Learning and Advanced Analytics
CC-17 (Natural Language Processing (NLP))	2	Machine Learning and Advanced Analytics
CC-18 (Predictive Analytics)	1	Machine Learning and Advanced Analytics
CC-27 (User behaviour analysis)	1	Machine Learning and Advanced Analytics
CC-08 (Data analytics for trend analysis)	1	Risk Management and Assessment
CC-09 (Data Visualisation)	1	Risk Management and Assessment
CC-16 (Network Analysis)	2	Risk Management and Assessment
CC-21 (Risk Assessment)	2	Risk Management and Assessment
CC-22 (Risk Management)	6	Risk Management and Assessment

4. Discussion and Recommendations

Policy recommendations and collaborations are feasible for National Payment Switches. National Payment Switches could collaborate and share best practices for preventing and detecting financial fraud by sharing information about cognitive computing tools and other security measures and protocols. Collaborating this way could help National Payment Switches stay up to date with the latest security technologies and strategies. NPSs could work together to develop and implement industry standards for payment security. By establishing common standards for security measures, National Payment Switches could ensure that all payments processed through their systems meet a consistent level of security. They could collaborate on research projects to advance the field of payment security by conducting joint research studies or sharing data for analysis. Collaboration could lead to a better understanding of emerging threats and develop new security strategies. NPSs could advocate for government support for payment security initiatives by lobbying for funding for the research and development of new security technologies or advocating for policies that promote the adoption of secure payment technologies. They could provide an extended network to provide training and education for their staff and customers by sharing training materials and best practices or developing joint training programs. It could help ensure that staff and customers have the knowledge and skills needed to prevent and detect financial fraud.

In addition to the policy recommendations and collaborations mentioned, National Payment Switches could also work towards developing a standardised reporting system for fraudulent activities. For example, by developing a uniform set of definitions for fraud, standardising the reporting format, and implementing a centralised database for tracking and analysing fraudulent activities. By sharing this information with other National Payment Switches, they could work together to identify trends and patterns in fraudulent activities, which could lead to the development of new and more effective security measures. Another important area for collaboration is in the field of cybersecurity. National Payment Switches could work together to establish best practices for protecting their systems against cyberattacks, such as sharing information about emerging threats and developing strategies for preventing and responding to cyberattacks.

In particular, it is necessary to consider that among the consequences of underprocessing the data protection and privacy cluster may include increased vulnerability: NPSs with inadequate data protection and privacy measures could be more susceptible to data breaches, identity theft, and other cyberattacks; loss of trust: a failure to protect user data adequately could lead to a loss of trust among consumers and financial institutions, impacting the adoption and usage of these payment systems; regulatory penalties: in regions with stringent data protection and privacy regulations, NPSs that do not comply with the required standards may face fines, penalties, or other legal consequences; and competitive disadvantage: NPSs that do not prioritise data protection and privacy might struggle to compete with more secure alternatives, potentially leading to a loss of market share. In this sense, most of the NPS should focus more on improving their data protection and privacy to meet international standards that might be more stringent than their pairs, especially if they need to engage with international transactions.

Given the analysis of the five key themes in financial technology security, one important recommendation would be to enhance collaboration and information sharing among National Switches and other financial institutions. By fostering a collaborative environment, organisations can pool resources, share best practices, and learn from each other's experiences in implementing effective fraud detection and prevention measures and other security strategies. This collaborative approach can help improve the overall security and resilience of the financial ecosystem by enabling faster identification and response to emerging threats, closing gaps in security measures, and promoting a more comprehensive understanding of the challenges and opportunities in the digital age. Additionally, collaboration can facilitate the development of standardised protocols and guidelines across the industry, further strengthening the security posture of all involved parties.

Finally, National Payment Switches could collaborate with other stakeholders, such as financial institutions (including International Payment Switches), merchants, and consumers, to promote awareness about payment security. The best outcome could be achieved by developing educational campaigns, providing resources for merchants to secure their payment systems, and working with consumers to promote safe payment practices.

5. Conclusions

National Payment Switches (NPSs) are critical in facilitating secure and efficient electronic transactions, essential in today's increasingly digital world. The article highlights the importance of cognitive computing tools in preventing and detecting financial fraud, a significant concern for NPSs. Cognitive computing tools such as machine learning, biometric authentication, real-time monitoring, and transaction monitoring, among others, have helped NPSs stay ahead of emerging threats and maintain the integrity of their payment systems. Collaboration among NPSs can improve payment security by sharing best practices, developing industry standards, conducting joint research, and advocating for government support for payment security initiatives. This article demonstrates the pervasive role cognitive computing plays in securing payment systems and highlights the potential benefits of collaboration among NPSs in safeguarding against fintech fraud. The nineteen cases analysed provide empirical evidence on patterns and common practices adopted by NPSs and contributed to designing coherent and insightful recommendations.

Potential limitations of this article might be related to a limited scope and potentially outdated information. Information on the topic might not be up-to-date, as fintech and cognitive computing are rapidly evolving fields, and some features and applications might not be disclosed for security reasons (the NPSs will waste a competitive advantage against fraudsters if they completely share their techniques).

In terms of future research, additional results can be provided by including the following: success rate of cognitive computing tools: analysing the success rate and the efficiency of cognitive computing tools in detecting and preventing fraudulent transactions across the 19 real-world cases; reduction in false positives: evaluating the reduction in false positives, which can lead to improved customer experience and reduced operational costs for financial institutions; cross-border fraud detection: evaluating the effectiveness of cognitive computing in detecting fraud that spans across multiple jurisdictions and how it can aid in international collaboration against financial crime; regulatory compliance: analysing the impact of cognitive computing on meeting regulatory requirements for financial institutions, such as anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations; integration with existing systems: examining the challenges and opportunities in integrating cognitive computing tools with existing financial infrastructure and the extent of collaboration required between financial institutions, technology providers, and regulators; privacy and security concerns: addressing the potential privacy and security risks associated with using cognitive computing for fraud detection and identifying the best practices for safeguarding customer data; and future trends: identifying emerging trends in cognitive computing and financial fraud detection and predicting how they may shape the future of NPSs and financial institutions in their fight against financial fraud.

In conclusion, this research highlights the critical role of cognitive computing tools in preventing and detecting financial fraud within National Payment Switches (NPSs), and provides insights for future research in evaluating the success rate, cross-border fraud detection, regulatory compliance, integration with existing systems, privacy and security concerns, and emerging trends in this rapidly evolving field.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Putland, P.A.; Hill, J.; Tsapikidis, D. Electronic payment systems. *BT Technol. J.* **1997**, *15*, 32–38. [CrossRef]
2. Omarini, A.E. Fintech and the future of the payment landscape: The mobile wallet ecosystem. A challenge for retail banks? *Int. J. Financ. Res.* **2018**, *9*, 97–116. [CrossRef]
3. Mu, H.L.; Lee, Y.C. How inclusive digital financial services impact user behavior: A case of proximity mobile payment in Korea. *Sustainability* **2021**, *13*, 9567. [CrossRef]
4. Briggs, A.; Brooks, L. Electronic payment systems development in a developing country: The role of institutional arrangements. *Electron. J. Inf. Syst. Dev. Ctries.* **2011**, *49*, 1–16. [CrossRef]
5. Dhobe, S.D.; Tighare, K.K.; Dake, S.S. A review on prevention of fraud in electronic payment gateway using secret code. *Int. J. Res. Eng. Sci. Manag.* **2020**, *3*, 602–606.
6. Lowry, P.B.; Wells, T.M.; Moody, G.D.; Humphreys, S.; Kettles, D. Online payment gateways used to facilitate e-commerce transactions and improve risk management. *Commun. Assoc. Inf. Syst. (CAIS)* **2006**, *17*, 1–48. [CrossRef]
7. Machine Learning for Mobile Network Payment Security Evaluation System. Available online: https://doi.org/10.1002/ett.4226 (accessed on 2 March 2023).
8. Pangestu, A.; Baskoro, R.A. Analysis of the Development of the National Payment Gateway (GPN) as a Symbol of Domestic Retail Transaction Sovereignty in Indonesia. In Proceedings of the 4th International Conference on Economics, Business and Economic Education Science, ICE-BEES 2021, Semarang, Indonesia, 27–28 July 2021; European Alliance for Innovation: Ghent, Belgium, 2022; p. 111.
9. Parlour, C.A.; Rajan, U.; Zhu, H. Fintech disruption, payment data, and bank information. *NBER Work. Pap.* **2019**, *22476*, 1–35.
10. Tay, L.Y.; Tai, H.T.; Tan, G.S. Digital financial inclusion: A gateway to sustainable development. *Heliyon* **2022**, *8*, e09766. [CrossRef]
11. Moreno-Serra, R.; Wagstaff, A. System-wide impacts of hospital payment reforms: Evidence from Central and Eastern Europe and Central Asia. *J. Health Econ.* **2010**, *29*, 585–602. [CrossRef]
12. Adzimatinur, F.; Manalu, V.G. The Effect of islamic financial inclusion on economic growth: A case study of islamic banking in indonesia. *Bp. Int. Res. Crit. Inst. (BIRCI-J.) Humanit. Soc. Sci.* **2021**, *4*, 976–985. [CrossRef]
13. Alkhowaiter, W.A. Digital payment and banking adoption research in Gulf countries: A systematic literature review. *Int. J. Inf. Manag.* **2020**, *53*, 102102. [CrossRef]
14. Nurfahrohim, R.; Aprilianty, F. A study of national payment gateway system in indonesia. In Proceedings of the 4th ICMEM 2019 and the 11th IICIES 2019, Bali, Indonesia, 7–9 August 2019.
15. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny, M.S.H. Application of big data and machine learning in smart grid, and associated security concerns: A review. *IEEE Access* **2019**, *7*, 13960–13988. [CrossRef]
16. Pourhabibi, T.; Ong, K.L.; Kam, B.H.; Boo, Y.L. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decis. Support Syst.* **2020**, *133*, 113303. [CrossRef]
17. Mosteanu, N.R.; Faccia, A. Digital systems and new challenges of financial management–FinTech, XBRL, blockchain and cryptocurrencies. *Qual. Access Success J.* **2020**, *21*, 159–166.
18. Faccia, A.; Al Naqbi, M.Y.K.; Lootah, S.A. Integrated cloud financial accounting cycle: How artificial intelligence, blockchain, and XBRL will change the accounting, fiscal and auditing practices. In Proceedings of the 2019 3rd International Conference on Cloud and Big Data Computing, Oxford, UK, 28–30 August 2019; pp. 31–37.
19. Mosteanu, N.R.; Faccia, A. Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 19. [CrossRef]
20. Ruff, L.; Kauffmann, J.R.; Vandermeulen, R.A.; Montavon, G.; Samek, W.; Kloft, M.; Müller, K.R. A unifying review of deep and shallow anomaly detection. *Proc. IEEE* **2021**, *109*, 756–795. [CrossRef]
21. Zhu, X.; Ao, X.; Qin, Z.; Chang, Y.; Liu, Y.; He, Q.; Li, J. Intelligent financial fraud detection practices in post-pandemic era. *Innovation* **2021**, *2*, 100176. [CrossRef]
22. Farahani, M.S.; Esfahani, A. Opportunities and Challenges of Applying Artificial Intelligence in the Financial Sectors and Startups during the Coronavirus Outbreak. *Int. J. Innov. Manag. Econ. Soc. Sci.* **2022**, *2*, 33–55.
23. Srivastava, K. Paradigm shift in Indian banking industry with special reference to artificial intelligence. *Turk. J. Comput. Math. Educ. (TURCOMAT)* **2021**, *12*, 1623–1629.
24. Tuckett, A.G. Applying thematic analysis theory to practice: A researcher's experience. *Contemp. Nurse* **2005**, *19*, 75–87. [CrossRef]
25. Mhlanga, D. Industry 4.0 in finance: The impact of artificial intelligence (ai) on digital financial inclusion. *Int. J. Financ. Stud.* **2020**, *8*, 45. [CrossRef]
26. Bouzidi, Z.; Amad, M.; Boudries, A. Deep Learning-Based Automated Learning Environment Using Smart Data to Improve Corporate Marketing, Business Strategies, Fraud Detection in Financial Services, and Financial Time Series Forecasting. In *International Conference on Managing Business Through Web Analytics*; Springer International Publishing: Cham, Switzerland, 2022; pp. 353–377.
27. Ololade, B.M.; Salawu, M.K.; Adekanmi, A.D. E-Fraud in Nigerian banks: Why and how? *J. Financ. Risk Manag.* **2020**, *9*, 211–228. [CrossRef]
28. Behera, R.K.; Bala, P.K.; Dhir, A. The emerging role of cognitive computing in healthcare: A systematic literature review. *Int. J. Med. Inform.* **2019**, *129*, 154–166. [CrossRef]

29. Capuano, N.; Fenza, G.; Loia, V.; Stanzione, C. Explainable Artificial Intelligence in CyberSecurity: A Survey. *IEEE Access* **2022**, *10*, 93575–93600. [CrossRef]
30. Pozzar, R.; Hammer, M.J.; Underhill-Blazey, M.; Wright, A.A.; Tulsky, J.A.; Hong, F.; Berry, D.L. Threats of bots and other bad actors to data quality following research participant recruitment through social media: Cross-sectional questionnaire. *J. Med. Internet Res.* **2020**, *22*, e23021. [CrossRef]
31. Capizzi, A.; Distefano, S.; Araújo, L.J.; Mazzara, M.; Ahmad, M.; Bobrov, E. Anomaly detection in devops toolchain. In Proceedings of the Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment: Second International Workshop, DEVOPS 2019, Château de Villebrumier, France, 6–8 May 2019; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 37–51.
32. Auer, R.; Frost, J.; Gambacorta, L.; Monnet, C.; Rice, T.; Shin, H.S. Central bank digital currencies: Motives, economic implications, and the research frontier. *Annu. Rev. Econ.* **2022**, *14*, 697–721. [CrossRef]
33. AL-mamoorey, M.A.; Al-Rubaye, M.M.M. The role of electronic payment systems in Iraq in reducing banking risks: An empirical research on private banks. *Pol. J. Manag. Stud.* **2020**, *21*, 49–59. [CrossRef]
34. Norman, B. Liquidity saving in real-time gross settlement systems: An overview. *J. Paym. Strategy Syst.* **2010**, *4*, 261–276.
35. Fernández-Villaverde, J.; Sanches, D.; Schilling, L.; Uhlig, H. Central bank digital currency: Central banking for all? *Rev. Econ. Dyn.* **2021**, *41*, 225–242. [CrossRef]
36. Schmiedel, H.; Kostova, G.L.; Ruttenberg, W. The social and private costs of retail payment instruments: A European perspective. *ECB Occas. Pap.* **2012**, *137*, 1–49. [CrossRef]
37. Carstens, A. Big Tech in Finance and New Challenges for Public Policy. Keynote address, FT Banking Summit London. 4 December 2018. Available online: https://www.bis.org/speeches/sp181205.htm (accessed on 2 March 2023).
38. Khan, M.A.; Malaika, M. *Central Bank Risk Management, Fintech, and Cybersecurity*; International Monetary Fund: Washington, DC, USA, 2021.
39. Ryman-Tubb, N.F.; Krause, P.; Garn, W. How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Eng. Appl. Artif. Intell.* **2018**, *76*, 130–157. [CrossRef]
40. Sangaiah, A.K.; Goli, A.; Tirkolaee, E.B.; Ranjbar-Bourani, M.; Pandey, H.M.; Zhang, W. Big data-driven cognitive computing system for optimisation of social media analytics. *IEEE Access* **2020**, *8*, 82215–82226. [CrossRef]
41. Raj, S.B.E.; Portia, A.A. Analysis on credit card fraud detection methods. In Proceedings of the 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), Tirunelveli, India, 18–19 March 2011; pp. 152–156.
42. Gutierrez, D.D. ACH Fraud and AI/ML—Much Work to Be Done. 2022. Available online: https://insidebigdata.com/2022/09/19/ach-fraud-and-ai-ml-much-work-to-be-done/ (accessed on 2 March 2023).
43. Goodell, J.W.; Kumar, S.; Lim, W.M.; Pattnaik, D. Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis. *J. Behav. Exp. Financ.* **2021**, *32*, 100577. [CrossRef]
44. Faivusovich, A. Modern Fraud Prevention Playbook Unit21. 2022. Available online: https://www.unit21.ai/resources/fraud-prevention-playbook (accessed on 2 March 2023).
45. Van Droogenbroeck, E.; Van Hove, L. COVID-19 and point-of-sale payments in Belgium: How the older generation also learned to love contactless. *J. Paym. Strategy Syst.* **2022**, *16*, 17–27.
46. Maillard, H.; Vermeulen, J. The Single Euro Payments Area: SEPA. Economic Review. 2006. Available online: https://www.ecb.europa.eu/pub/pdf/other/sepa_brochure_2006en.pdf (accessed on 2 March 2023).
47. Van Hove, L. Electronic money and the network externalities theory: Lessons for real life. *Netnomics* **1999**, *1*, 137–171. [CrossRef]
48. Emerchantpay. Payment Gateway—What Is It and How Does It Work? 2022. Available online: https://www.emerchantpay.com/insights/what-is-a-payment-gateway-and-how-does-it-work/ (accessed on 2 March 2023).
49. Fabcic, D. Strong Customer Authentication in Online Payments Under GDPR and PSD2: A Case of Cumulative Application. In Proceedings of the Privacy and Identity Management: 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Maribor, Slovenia, 21–23 September 2020; Springer International Publishing: Berlin/Heidelberg, Germany, 2021; pp. 78–95, Revised Selected Papers 15.
50. Lone, S.; Harboul, N.; Weltevreden, J. *European E-Commerce Report*; Amsterdam University of Applied Sciences: Amsterdam, The Netherlands, 2021.
51. Wolters, P.T.; Jacobs, B.P. The security of access to accounts under the PSD2. *Comput. Law Secur. Rev.* **2019**, *35*, 29–41. [CrossRef]
52. Lample, G.; Ott, M.; Conneau, A.; Denoyer, L.; Ranzato, M.A. Phrase-based & neural unsupervised machine translation. *arXiv* **2018**, arXiv:1804.07755.
53. Kauffman, R.J.; McAndrews, J.; Wang, Y.M. Opening the "black box" of network externalities in network adoption. *Inf. Syst. Res.* **2000**, *11*, 61–82. [CrossRef]
54. Wu, Z.; Liu, Y. Exploring country differences in the adoption of mobile payment service: The surprising robustness of the UTAUT2 model. *Int. J. Bank Mark.* **2022**, *41*, 237–268. [CrossRef]
55. Aktuğ, S.S. Development of fintech sector in Turkey. *BİLTÜRK J. Econ. Relat. Stud.* **2020**, *2*, 487–499. [CrossRef]
56. Yuksel, B. *Future of Fintech in Turkey in the Absence of Mandatory Open Banking Regulations and the Possible Role of Competition Law*; SSRN: Rochester, NY, USA, 2020.
57. Yazici, M. The impact of COVID-19 on payment systems in Turkey. *Int. J. Inf. Res. Rev.* **2020**, *7*, 6911–6917.

58. Canko, S.; Bruggink, D. The Turkish payment market and its specifics: An interview with Soner Canko. *J. Paym. Strategy Syst.* **2016**, *10*, 230–237.
59. Yeniceler, İ.; Ilgın, H.Ö. New Media and Digital Surveillance Reflections. In Proceedings of the Communication and Technology Congress, Online, 17 April 2019.
60. Alsadi, M.; Mantar, H.A.; Coskun, V.; Ok, K.; Ozdenizci, B. Challenges and Risks of Developing a Payment Facilitator Model. *J. Inf. Secur. Res.* **2016**, *7*, 109–117.
61. Prenzler, T. Detecting and preventing welfare fraud. *Trends Issues Crime Crim. Justice* **2011**, *418*, 1–6.
62. Choo, K.K.R.; Smith, R.G. Criminal exploitation of online systems by organised crime groups. *Asian J. Criminol.* **2008**, *3*, 37–59. [CrossRef]
63. Cao, L. *AI in Finance: A Review*; SSRN: Rochester, NY, USA, 2020.
64. Wewege, L.; Thomsett, M.C. *The Digital Banking Revolution: How Fintech Companies Are Transforming the Retail Banking Industry through Disruptive Financial Innovation*; Walter de Gruyter GmbH & Co KG: Berlin, Germany, 2019.
65. Huang, Z. Is it money laundering: Case study of China UnionPay scandal from the perspective of mutual legal assistance on anti-money laundering. *J. Money Laund. Control* **2015**, *18*, 411–424. [CrossRef]
66. Ghosh, S. Payments Overview-China. Finance Finland. 2018. Available online: https://www.finanssiala.fi/wp-content/uploads/2018/12/Payment20Overview20China.pdf (accessed on 2 March 2023).
67. Henderson, R. Using graph databases to detect financial fraud. *Comput. Fraud Secur.* **2020**, *2020*, 6–10. [CrossRef]
68. Zhou, H.; Chai, H.F.; Qiu, M.L. Fraud detection within bankcard enrollment on mobile device based payment using machine learning. *Front. Inf. Technol. Electron. Eng.* **2018**, *19*, 1537–1545. [CrossRef]
69. Sun, Q.; Tang, T.; Chai, H.; Wu, J.; Chen, Y. Boosting fraud detection in mobile payment with prior knowledge. *Appl. Sci.* **2021**, *11*, 4347. [CrossRef]
70. Sun, Q.; Zhou, Y.; Tang, T. Mobile Payment Innovations in China: China UnionPay's Practice and Experience. In *Business Innovation with New ICT in the Asia-Pacific: Case Studies*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 257–279.
71. Pouwelse, J.; Bruggink, D. Reducing card-not-present fraud using pre-approved transactions. *J. Paym. Strategy Syst.* **2016**, *10*, 50–63.
72. Baba, C.; Batog, C.; Flores, E.; Gracia, B.; Karpowicz, I.; Kopyrski, P.; Xu, X.C. *Fintech in Europe: Promises and Threats*; SSRN: Rochester, NY, USA, 2020.
73. Hassani, B.; Hassani, B.K. *Scenario Analysis in Risk Management*; Springer International Publishing: Cham, Switzerland, 2016.
74. Singh, A.; Rumantir, G.; South, A. Market Segmentation of EFTPOS Retailers. In Proceedings of the Twelfth Australasian Data Mining Conference (AusDM 2014), Brisbane, Australia, 27–28 November 2014; pp. 19–24.
75. Worthington, S. Debit cards and fraud. *Int. J. Bank Mark.* **2009**, *27*, 400–402. [CrossRef]
76. Smith, R.G. *Best Practice in Fraud Prevention*; Australian Institute of Criminology: Canberra, Australia, 1998.
77. Sakharova, I. Payment card fraud: Challenges and solutions. In Proceedings of the 2012 IEEE International Conference on Intelligence and Security Informatics, Washington, DC, USA, 11–14 June 2012; pp. 227–234.
78. Conroy, J. *EMV: Lessons Learned and the US Outlook*; Aite Group, Inc.: Boston, MA, USA, 2012; Available online: https://eft-direct.com/wp-content/uploads/2016/11/Aite_Report_-_EMV_Lessons_Learned_and_the_U.S._Outlook.pdf (accessed on 2 March 2023).
79. Connolly, C. *Australian and Regional Regulatory Responses to the Key Challenges of Consumer Protection in Electronic Commerce (March 2008)*; Galexia: Sydney, Australia, 2008.
80. Balakrishnan, M. Real-time retail payments systems or faster payments: A quick framework for decision making. *J. Paym. Strategy Syst.* **2016**, *10*, 267–278.
81. Natarajan, H.; Balakrishnan, M. Real-time retail payments system or faster payments: Implementation considerations. *J. Paym. Strategy Syst.* **2020**, *14*, 48–60.
82. Weyman, J. Risks in faster payments. In *Retail Payments Risk Forum Working Paper*; Federal Reserve Bank of Atlanta: Atlanta, GA, USA, 2016.
83. Button, M. Fraud investigation and the 'flawed architecture'of counter fraud entities in the United Kingdom. *Int. J. Law Crime Justice* **2011**, *39*, 249–265. [CrossRef]
84. Bech, M.L.; Shimizu, Y.; Wong, P. The quest for speed in payments. In *BIS Quarterly Review March 2017*; SSRN: Rochester, NY, USA, 2017.
85. Hayashi, F. *Faster Payments in the United States: How Can Private Sector Systems Achieve Public Policy Goals? Working Paper*; Federal Reserve Bank of Kansas City: Kansas City, MO, USA, 2015; p. 15-03.
86. Anderson, R.D.; Rivard, B. Antitrust Policy towards EFT Networks: The Canadian experience in the Interac case. *Antitrust LJ* **1999**, *67*, 389.
87. Amin, M. National infrastructures as complex interactive networks. *Automat. Control Complex. Integr. Approach* **2000**, *3*, 263–286.
88. Bansal, H.S.; Taylor, S.F. Investigating interactive effects in the theory of planned behavior in a service-provider switching context. *Psychol. Mark.* **2002**, *19*, 407–425. [CrossRef]
89. Gursoy, M.; Mirafzal, B. Self-security for grid-interactive smart inverters using steady-state reference model. In Proceedings of the 2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL), Cartagena, Colombia, 2–5 November 2021; pp. 1–5.

90. Banerjee, S.P.; Woodard, D.L. Biometric authentication and identification using keystroke dynamics: A survey. *J. Pattern Recognit. Res.* **2012**, *7*, 116–139. [CrossRef]
91. Ng, D. Evolution of digital payments: Early learnings from Singapore's cashless payment drive. *J. Paym. Strategy Syst.* **2018**, *11*, 306–312.
92. Bolt, S.; Emery, D.; Harrigan, P. Fast retail payment systems. In *RBA Bulletin*; Reserve Bank of Australia: Sydney, Australia, 2014; pp. 43–51.
93. Tavani, E. Private Equity, the Powerful Forces Reshaping Capital Markets and the Business Case of Nexi: M&A Activity, IPO and Company Valuation. 2020. Available online: http://tesi.luiss.it/29276/ (accessed on 2 March 2023).
94. Agarwal, S.; Qian, W.; Ren, Y.; Tsai, H.T.; Yeung, B.Y. *The Real Impact of FinTech: Evidence from Mobile Payment Technology*; SSRN: Rochester, NY, USA, 2020.
95. Bhargava, A.; Ubaid, M.; Khan, Y.; Gupta, P.C. Expansion of Unified Payment Interface. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 12491–12499.
96. BusinessWire. Securing Payments in Asia with Latest 3-D Secure Technology. 2022. Available online: https://www.businesswire.com/news/home/20221011006169/en/Securing-payments-in-Asia-with-latest-3-D-Secure-technology (accessed on 2 March 2023).
97. Arditti, L.; Trevisan, M.; Vassio, L.; De Lazzari, A.; Danese, A. User Value in Modern Payment Platforms: A Graph Approach. *arXiv* **2022**, arXiv:2210.11168.
98. Gordon, K. Investment guarantees and political risk insurance: Institutions, incentives and development. In *OECD Investment Policy Perspectives*; OECD: Paris, France, 2008; pp. 95–103.
99. NEXI. Nexi and Biometric Recognition: A Question of Security. 2023. Available online: https://www.nexi.it/en/news.html (accessed on 2 March 2023).
100. Reply. Getting Cloud and ML into the DNA of Nexi. 2023. Available online: https://www.reply.com/data-reply/en/getting-cloud-and-ml-into-the-dna-of-nexi (accessed on 2 March 2023).
101. Cook, W.; Raman, A. *National Payments Corporation of India and the Remaking of Payments in India*; Consultative Group to Assist the Poor Working Paper: Washington, DC, USA, 2019.
102. Dhamija, A.; Dhamija, D. Technological advancements in payments: From cash to digital through unified payments interface (UPI). In *Strategic Human Capital Development and Management in Emerging Economies*; IGI Global: Hershey, PA, USA, 2017; pp. 250–258.
103. Joshi, M. *Digital Payment System: A Feat Forward of India. Research Dimension*; SSRN: Rochester, NY, USA, 2017; ISSN 2249-3867.
104. Gochhwal, R. Unified payment interface—An advancement in payment systems. *Am. J. Ind. Bus. Manag.* **2017**, *7*, 1174–1191. [CrossRef]
105. Dabbeeru, R.; Rao, D.N. *Fintech Applications in Banking and Financial Services Industry in India*; SSRN: Rochester, NY, USA, 2021.
106. Selvaraj, P.; Ragesh, T.V. Innovative approach of a regional rural bank in adopting technology banking and improving service quality leading to better digital banking. *Vinimaya* **2018**, *39*, 22–32.
107. Ahmed, M.R.; Meenakshi, K.; Obaidat, M.S.; Amin, R.; Vijayakumar, P. Blockchain based architecture and solution for secure digital payment system. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
108. Khetagurov, G.V.; Khetagurova, Y.I. National Payment Card System as an Important Factor of Economic Security of Russia. In *International Session on Factors of Regional Extensive Development (FRED 2019)*; Atlantis Press: Paris, France, 2020; pp. 252–255.
109. Khromenkov, G.D. Competitiveness of the Russian market of fintech services in the digital economy. In *Наука и Инновации-современные Концепции*; Financial University: Moscow, Russia, 2019; pp. 15–18.
110. Nedoluga, M.S.; Mustafin, A.N. Payment systems: International payment system mastercard and mir (Russia). In *QUID: Investigación, Ciencia y Tecnología*; IUSH: Medellín, Colombia, 2017; pp. 123–127.
111. Fu, Y.; Yan, Z.; Cao, J.; Koné, O.; Cao, X. An automata based intrusion detection method for internet of things. *Mobile Inf. Syst.* **2017**, *2017*, 1750637. [CrossRef]
112. Almuhaideb, A.M.; Alqudaihi, K.S. Authentication in Wireless Body Area Network: Taxonomy and Open Challenges. *J. Internet Things* **2021**, *3*, 159. [CrossRef]
113. Amaral, G.; Guizzardi, R.; Guizzardi, G.; Mylopoulos, J. Trustworthiness requirements: The pix case study. In Proceedings of the Conceptual Modeling: 40th International Conference, ER 2021, Virtual, 18–21 October 2021; Springer International Publishing: Berlin/Heidelberg, Germany, 2021; pp. 257–267.
114. Gomes, S.L.; Rebouças, E.D.S.; Neto, E.C.; Papa, J.P.; Albuquerque, V.H.D.; Rebouças Filho, P.P.; Tavares, J.M.R. Embedded real-time speed limit sign recognition using image processing and machine learning techniques. *Neural Comput. Appl.* **2017**, *28* (Suppl. 1), 573–584. [CrossRef]
115. Pickens, M.; Porteous, D.; Rotman, S. Banking the Poor via G2P payments. *Focus Note* **2009**, *58*, 1–22.
116. Zhao, L.; Matsuo, I.B.; Salehi, F.; Zhou, Y.; Lee, W.J. Development of a real-time web-based power monitoring system for the substation of petrochemical facilities. *IEEE Trans. Ind. Appl.* **2018**, *55*, 43–50. [CrossRef]
117. Alyabes, A.F.; Alsalloum, O. Factors affecting consumers' perception of electronic payment in Saudi Arabia. *Eur. J. Bus. Manag.* **2018**, *10*, 36–45.
118. Halliday, F. A Curious and Close Liaison: Saudi Arabia's Relations with the United States. In *State, Society and Economy in Saudi Arabia*; Routledge: Abingdon, UK, 2015; pp. 125–147.

119. Authority, S.A.M. *Cyber Security Framework*; Saudi Arabian Monetary Authority: Riyadh, Saudi Arabia, 2017.
120. Kulick, S. Exploiting separation of closed-class categories for arabic Tokenisation and part-of-speech tagging. *ACM Trans. Asian Lang. Inf. Process. (TALIP)* **2011**, *10*, 1–18. [CrossRef]
121. León, M.H. Los servicios de dirimencias como instrumento de resolución de conflictos interbancarios. *CEFLegal. Rev. Práct. Derecho* **2020**, 39–70. [CrossRef]
122. Banco de Mexico. Sistema de Pagos Electrónicos Interbancarios (SPEI). In *Divulgación del Cumplimiento y Adopción de los Principios Para las Infraestructuras del Mercado Financiero*; Banco de Mexico: Mexico City, Mexico, 2016.
123. Banco de Mexico. Information for SPEI® Users. Available online: https://www.banxico.org.mx/services/interbanking-electronic-payme.html (accessed on 2 April 2023).
124. Banco de Mexico. Interbank Electronic Payment System (SPEI). 2016. Available online: https://www.banxico.org.mx/payment-systems/d/%7B90965A55-8F44-7DD2-45CF-2BF1D7C0B75B%7D.pdf (accessed on 2 April 2023).
125. STET. European-Wide Solutions. Available online: https://www.stet.eu/en/payment-solutions/ (accessed on 2 April 2023).
126. IBM. Payment Fraud Prevention at a National Payment Switch. 2019. Available online: https://www.ibm.com/blogs/client-voices/payment-fraud-prevention-national-payment-switch/ (accessed on 2 April 2023).
127. Iman, N. Financial innovations in Islamic countries: The road to perdition or salvation? *J. Islam. Mark.* **2020**, *11*, 1579–1600. [CrossRef]
128. Subramanian, M. Payments in the Middle East and Africa: An overview and review of implications for corporates operating in the region. *J. Paym. Strategy Syst.* **2014**, *8*, 188–205.
129. UAE Central Bank. Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening. 2021. Available online: https://www.centralbank.ae/media/j5shd2lq/amlcft-guidance-for-lfis-on-transaction-monitoring-and-sanctions-screening.pdf (accessed on 2 April 2023).
130. AFP—PNC. Cash and Treasury Management—Country Report UAE. 2023. Available online: https://www.afponline.org/docs/default-source/default-document-library/pdf/cp_afp-uae4ae7354e827d6df1bc1fff00003724d4.pdf?sfvrsn=0 (accessed on 2 April 2023).
131. Bayanat. UAE FTS Statistics 2012–2019. 2020. Available online: https://opendata.fcsc.gov.ae/@central-bank-united-arab-emirates/uae-fts-fund-transfer-system/r/UAE%20FTS%20Statistics%202012-2019 (accessed on 2 April 2023).