International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

The Role of Artificial Intelligence and Technological Advancements in Open Banking: Transformation in the Financial Sector

Nuray İslatince
Anadolu University: Faculty of Business Administration
Eskişehir, Turkey
nislatince@anadolu.edu.tr

Abstract— In the banking sector, efforts to adapt to new technologies play a critical role in the transformation of financial services. While the concept of open banking is at the center of this transformation, the process of banks adapting to these new approaches is influenced by various factors. Firstly, strengthening and developing technological infrastructure is of paramount importance in banks' adaptation to new technologies. This is often a process requiring significant investments and necessitates banks to restructure and modernize their existing systems. Additionally, regulation and compliance processes are also a determining factor in banks' adaptation to new technologies. Compliance with rules set by financial regulators ensures that banks maintain security and compliance standards while utilizing innovative technologies. Collaborating with financial technology companies is another important strategy that enables banks to rapidly adapt to new technologies. These collaborations allow banks to expand their existing services and offer innovative solutions. Furthermore, customer expectations and demands also influence banks' adaptation to new technologies. As demand for digital banking services increases, banks are compelled to invest more in this area. Additionally, security concerns and data privacy measures are important factors that must be considered in banks' adaptation to new technologies. Protecting and securely processing customer data ensures that banks maintain their reliability. Considering all these factors, banks' efforts to adapt to new technologies are a complex process requiring careful planning, investment, and strategic partnerships. However, when managed properly, these efforts enhance banks' competitive advantage and enable them to provide better services to customers.

Keywords- *Open Banking, Artificial Intelligence, APIs, IP Address, NFC Tecnology*

I. INTRODUCTION

Alongside the digital transformation in the banking sector, many concepts are rapidly gaining traction in our daily lives. The concept of Open Banking is one such term and is increasingly gaining popularity. The statement made by Microsoft's co-founder Bill Gates decades ago that "People need banking, not banks." may not have been fully understood at that time. This is due to the perception that while some consider Open Banking as part of the evolution of interaction between customers and financial institutions, others may not see it as revolutionary as expected (Remolina, 2019). The efforts of banks to adapt to new technologies are aimed at responding to changing demands in the financial services sector, developments in the competitive environment, and technological advancements. These efforts are crucial for financial institutions to remain competitive and meet customer needs. One key aspect that explains banks' efforts to adapt to new technologies is the identification of strategies for digitizing and transforming traditional business models. These strategies are designed to enhance customer experience, increase operational efficiency, reduce costs, and gain competitive advantage. Additionally, banks are investing in new technologies such as artificial intelligence and machine learning to enhance data analytics and customer relations. These technologies are used to understand customer behaviors, prevent fraud, provide personalized services, and automate operational processes. Perhaps the most significant aspect is the development of APIs (Application Programming Interfaces) that allow customers to securely share their financial data by embracing the principles of open banking. This will facilitate integration between different financial institutions and provide customers with more options. Furthermore, some banks are focusing on improving payment systems and exploring decentralized financial applications by investing in innovative financial technologies such as blockchain and cryptocurrencies. Parallel to the progress of development and technology, banks are improving digital payment systems and mobile banking applications to enable customers to conduct financial transactions more quickly and easily. This allows customers to access financial services without the need to visit bank branches. In addition to these efforts, banks emphasize the importance of adhering to regulations and compliance requirements while adapting to new technologies. Protecting the privacy and security of customer data is crucial and necessary for financial stability. Successful implementation of these efforts can enhance banks' competitiveness and increase customer satisfaction. Another aspect of development is the inclusion of FinTech companies, which develop innovative technologies and business models challenging traditional banking systems. While FinTech companies specialize in digitizing and optimizing financial services such as payment transactions, lending, investment management, and insurance, banks generally have a wide customer base and financial infrastructure as established organizations with a long history. FinTech firms, which combine financial products and services with technology, have created a new reality in the financial services sector. With the widespread use of the internet, digital channels such as internet banking and mobile banking have become significantly utilized, especially for transactions such as money transfers, bill payments, or account tracking. Particularly, the COVID-19 pandemic

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

experienced globally today has clearly demonstrated the necessity of financial products and services to be accessible without leaving home and even without physical contact with money, proving that it is not a theoretical but a vital need. This new situation, while accelerating the process of change, has shown that beyond internet banking and mobile banking, which provide access to only a specific bank's infrastructure, a more comprehensive service infrastructure is needed to meet customers' needs. Indeed, the structure of open banking, which allows customers to view and transact their financial data simultaneously on a single screen from multiple banks or financial institutions, surpasses internet banking and mobile banking, advancing financial transactions beyond, has attracted the attention of financial regulators in many countries in recent years. Today, the number of conscious bank customers who want to carry out their financial transactions online and closely follow developments in the sector is increasing day by day. It is an undeniable fact that the digital transformation trend is an inevitable reality affecting all industries and reshaping financial services. Many banks have realized the relevance of digitalization to delivering financial services to their customers and have recognized the contribution of changing views on the importance of digital features and data-based finance in the banking sector. Accordingly, it has been anticipated that banks will not disappear, but the way this industry does business will change through open banking. Open banking will initiate a new era in banking services. This will lead to new forms of financial intermediation and enable data-driven finance at the core of banking transactions. This study aims to examine in detail the meaning of different concepts that have rapidly taken place in our daily lives with the digital transformation process in the banking sector in Turkey, how Open Banking emerged, its development worldwide and in Turkey, and the benefits of Open Banking. emphasis has been placed on how the new approach facilitated by APIs (Application Programming Interfaces) focusing on open banking perspective, facilitates customers' secure access to data. In addition, this study has addressed the contributions of technological innovations, especially rapidly evolving technologies such as artificial intelligence, in personalizing the customer experience and accessing financial services from an open banking perspective. Given the fact that it is beneficial to examine how these technologies can be effectively used to understand the advantages provided by open banking and to provide better financial services to customers, research has been conducted.

II. OPEN BANKING

Open banking, also known as "Open Banking" and "Open Bank Data," is a reliable service model that offers customers better banking and financial opportunities through the sharing of financial data with third-party institutions. While there is no technical definition of this approach, the adoption of the open banking model among financial regulators and other stakeholders is increasingly growing. This model provides a consensus among financial institutions and fintech companies regarding the opportunities arising from data sharing and the potential to transform traditional banking. Open banking plays a significant role in supporting reliability and innovation. By offering a system where data sharing occurs entirely with user consent, it prevents the sharing of unwanted data, thereby preserving the privacy of service recipients. Additionally, it promotes competition by increasing transparency in financial products and services, and facilitates easier access to the financial system for customers. This access presents an opportunity for competitive banks, neo-banks, fintech companies, and major technology firms to develop new and innovative financial products and services. Furthermore, it enables traditional banks to enhance customer experience by utilizing large amounts of data or existing infrastructure. The recent COVID-19 pandemic has increased the demand for digital financial services and strengthened trust in these services. The digitization of payments and the ability to provide financial assistance without physical contact have led businesses to lean more towards open banking. Open banking enhances the accounting and cash flow forecasting capabilities of micro, small, and medium-sized enterprises, contributing to the sustainability of their financial performance. Additionally, credit providers can assess credit risk more accurately and offer financing solutions by using data obtained from open banking. Particularly for sectors aiming to increase inclusivity, open banking has the potential to empower consumers and promote financial participation. Open banking reduces the transition costs between traditional banks and fintech companies, encourages innovation, and accelerates the renewal and development of financial products. Among the macro objectives of open banking are the development of new financial products and services, the increase in transparency and competition in the financial sector, the facilitation of financial life, the increase in financial inclusivity, and the improvement of customer experience.

We can evaluate the advantages of open banking under four main headings:

1. Innovation and Progress: Open banking enables financial institutions to develop new ideas rapidly and effectively. Third-party developers can design various financial applications and services using APIs.
2. Customer Experience: Data sharing allows for more personalized and user-friendly services to be offered to customers. This provides customers with a smoother experience when transitioning between different financial institutions.
3. Competitive Environment: Open banking increases competition in the financial sector and allows for better prices and services to be offered. This requires banks to be more innovative in order to increase customer satisfaction and maintain their market share.
4. Future Potential: It is predicted that open banking will appeal to a wider audience in the future. With technological advancements, it is expected that more banks and financial institutions will adopt the open banking model. This will provide customers with a broader range of services and trigger a greater transformation in the financial sector. Additionally, the use of new technologies such as artificial intelligence and blockchain in open banking aims to create a more secure and efficient system.

A. Regulations Regarding Open Banking Worldwide

Many countries around the world adopt legal frameworks and innovative approaches to support the development and acceptance of open banking. Among these approaches, the United Kingdom stands out as one of the most successful examples on a global scale. The model, which was first implemented in the UK and aimed at bringing an innovative touch to the banking sector, enhancing competition, and creating opportunities, was actually discussed and revised in relevant European Union institutions in 2015. In recent years, amid

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

heated Brexit discussions, the UK, especially London, has seen its global leadership in financial technologies being questioned. However, on the other hand, the British government has managed to maintain the country's attractiveness for fintech companies by taking bold yet controlled steps in the field of open banking. The UK Competition and Markets Authority (CMA) first made decisions in 2016 to encourage growth in the sector and accelerate technological innovations in the banking sector.

The Second Payment Services Directive (PSD2) directive laid the foundations for open banking and facilitated the development of a strategy that allows third-party institutions to access and use financial data to enhance user experience. Apart from the PSD2 process, the country brought together the open API structures of nine major banks within the Open Banking Implementation Entity (OBIE) framework, which was licensed by the government, making it the first country in the world to transition to the open banking model. Subsequent decisions were made to implement open banking practices in early 2018, setting targets for securely sharing financial data of individual consumers and SMEs among banks and third parties, with banks being required to clearly inform consumers about these processes. The UK's desire to innovate in the sector and revive opportunities through competition has been the key factor in the emergence of this model. Later, the Open Banking Directive presented by the European Union as PSD2 has contributed to the development of the open banking model by enabling third parties to access financial data and work on improving user experience (Finteo, 2021).

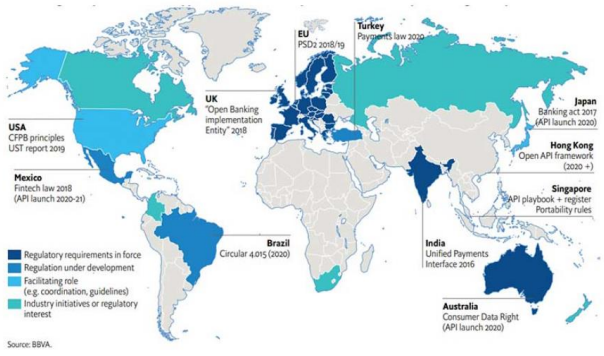


Figure 1. Regulations and maturity level regarding Open Banking worldwide
Source: https://fintechtime.com/2023/07/acik-bankacilik-ve-riskleri-verilerimiz-gercekten-guvende-mi/

Regulatory efforts and maturity levels regarding Open Banking worldwide are illustrated in Figure 1. Turkey stands among the few countries taking action in terms of regulation.

B. Regulations related to Open Banking in Turkey

FinTech regulations in Turkey date back to the early 2010s. With the mandatory introduction of next-generation payment devices in 2012, many FinTech startups began to emerge in this field, and with the issuance of e-money and payment institution licenses in 2015, the number of initiatives in this area rapidly increased. As of December 2022, a total of 74 companies have been licensed.

Figure 1. Milestones In Terms of Fintech Regulations In The Last 3 Years, Source: https://www.cbfo.gov.tr/sites/default/files/docs/2023-03/the-state-of-turkish-fintech-ecosystem-v0.4-compressed.pdf

In the last three years, a series of regulations have been issued specifically to empower FinTech companies, encourage digitalization of banks, and pave the way for open banking. The year 2022 can be considered as the year when the fruits of these regulations began to be harvested. In 2022, successful investments were raised for 46 start-ups. Additionally, other developments in 2022 include:

- Enactment of digital banking regulations,
- Publication of the first version of API principles and rules for payment service data sharing services,
- Granting of the first permit for establishing a digital bank,
- Implementation of the Istanbul Finance Center Law,
- Publication of the "Guide for Evaluating Business Models Offered in the Payment Field in Connection with Payment Service Types",
- Introduction of open banking,
- Inclusion of payment and electronic money institutions in the Fast Transfer System,
- Completion of the first payment transaction on the Digital Turkish Lira Network.

All these developments can be considered as the biggest indicators that Turkey will be much more active in the coming period. With the opening of the Istanbul Finance Center (IFC), it can be expressed that this momentum will be taken to much higher levels (Presidency of the Republic of Turkey Finance Office, 2022).

With the enactment of Law No. 6493 in Turkey in 2013, compliance with the European Union's Payment Services Directive (PSD) has been achieved. In a change made at the end of 2019, payment initiation services (PIS) and account

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

information services (AIS), similar to those covered under PSD2, were incorporated into Turkish law.

The inclusion of PIS and AIS into the law represents a significant step for open banking practices in Turkey, thereby encouraging the emergence of new ventures aiming to provide services in the open banking domain. API sharing is crucial for the development of the open banking ecosystem and the sustainability of services offered by open banking entrepreneurs. On November 12, 2019, an update to Law No. 6493, titled "Regulation on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions," added Payment Initiation Service and consolidated information provision services regarding payment accounts as payment services within the scope of the law. Consequently, these two services are defined as Data Sharing Services in Payment Services (DSSP), referred to as Open Banking Services in the provision of payment services. In line with the regulatory framework, research has been conducted in collaboration with the Central Bank of the Republic of Turkey (TCMB) and the Interbank Card Center (ICC) to determine the implementation strategy of DSSP and detailed technical and operational requirements. Considering Turkey's specific conditions and needs, best global practices have been examined, and a platform enabling low-cost, efficient, and effective data sharing in the payment services field has been designed. In this regard, APIs have been developed and introduced by the ICC using internal resources and technical capabilities, enabling a secure, efficient, effective, low-cost, and innovative business model for open banking in the payment services domain. The Fast and Continuous Transfer (FAST) System, the national QR Code Standard TR QR Code in the Turkish payment ecosystem, the Easy Addressing System facilitating FAST payments using phone numbers, identity numbers, or email addresses instead of IBAN, and the Digital Turkish Lira Collaboration Platform announced by the TCMB on September 15, 2021, together with Data Sharing Services in Payment Services will contribute significantly to the digitalization goals of banks and play a crucial role in achieving Turkey's aim of a fully-fledged digital economy (TCMB, 2022).

In some countries, including Turkey, the "screen scraping" method is used for services provided over the internet, including financial services. In this method, the customer may need to log in to the internet banking system of the bank where they receive services and share their user information with third parties. However, this situation may pose significant security issues such as data security and prevention of fraudulent transactions. The implementation of screen scraping in financial services in Turkey faces obstacles arising from the obligation of secrecy of customer information under Banking Law No. 5411. Even if exceptions to this obligation could be made with these laws, the sharing must be limited to specific purposes and comply with the principle of proportionality.

The "Regulation on Banks' Information Systems and Electronic Banking Services," which came into effect on March 15, 2020, and July 1, 2020, sets out the principles and procedures for electronic banking services and banks' information systems. Additionally, it defines open banking services as electronic banking services, allowing customers or parties acting on behalf of customers to remotely access the financial services offered by the bank and place orders through APIs, web services, and file transfer protocols. Rules similar to PSD2, including robust customer identification, security measures for transactions, monitoring of fraud risks, and informing customers about electronic banking services, have been applied to open banking services in Turkey. However, unlike PSD2, the Regulation imposes obligations only on banks and does not define the obligations of open banking service providers. Another significant innovation introduced by the Regulation is "remote identification." In this way, more opportunities are provided for open banking services, allowing banks to remotely verify the identities of new customers or receive services from another bank that has previously identified such a customer through open banking services. Remote identification will further expand the scope of banking transactions in Turkey by enabling contractual relationships to be established remotely in customer participation processes in recent years.

III. ARTIFICIAL INTELLİGENCE IN OPEN BANKING

Technological advancement is transforming the world, with artificial intelligence emerging as one of the fastest-growing technologies globally. Industries across various domains are embracing artificial intelligence technology, and the banking sector is leading the way in this trend. Artificial intelligence has become a significant factor shaping the future of banking, providing the power of complex data analytics to combat fraudulent transactions and enhance compliance. While artificial intelligence will not replace humans, it will support their work by making processes more efficient and resolving challenges more quickly. Additionally, artificial intelligence helps banks reduce risks and increase customer satisfaction, thereby enhancing their revenues. Today, it is critically important for all banks to integrate artificial intelligence into their strategies. This is because of the intense competition in the banking sector and the constant innovations occurring within it. Since its emergence, artificial intelligence has had a profound transformative impact. This impact has positively affected the operations of businesses in the banking and finance sectors and has changed existing practices. The introduction of artificial intelligence into banking applications and services has made the banking sector more customer-centric and technology-focused. AI-based systems help banks increase productivity, reduce costs, and make decisions based on previously inaccessible information. Moreover, intelligent algorithms can detect fraudulent activities within seconds. A report published by Business Insider indicates that approximately 80% of banks are aware of the potential benefits of artificial intelligence in banking. Another report by McKinsey suggests that the potential of artificial intelligence in banking and finance could reach up to $1 trillion (elvtr, 2023). Furthermore, the potential contribution of artificial intelligence, meaning computers with human-like cognitive abilities, to bank profitability should not be underestimated.

Artificial intelligence has also become a significant area of use in modern digitalization and transformation in open banking activities. This enables computers to acquire and apply information without the intervention of programmers for the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

services provided. At the same time, efforts are being made to develop artificial intelligence for real-time detection and prevention of fraud in online banking and for customer identity verification processes. However, regulatory measures around data privacy and cybersecurity concerns in the future may hinder the use of artificial intelligence in banking. Artificial intelligence technologies can structurally reduce costs in the banking sector by increasing workforce productivity, especially in future open banking activities. Therefore, the rapid implementation of artificial intelligence technologies in the banking sector is important to combat low profitability and to be in a superior competitive structure. Hence, it can be said that banks are generally institutions that early adopt IT opportunities. This is true not only for back-office operations but also for front-end activities such as customer services. For example, one of the oldest IT applications in banking services, automated teller machines (ATMs), has enabled easy and timely access to repetitive services such as cash withdrawal and account balance checks without the need for bank employees. This has not only facilitated easier access to standard banking transactions for customers but also made banks more efficient. As a result, since the installation of the first ATM in London in 1967, it has not taken long for it to become a standard device in bank branches. The liberation of bank employees from routine cash transactions has enabled them to provide other services such as relationship banking and offer various banking services such as credit cards, loans, and investment products. Online banking is the best example of banks adopting new IT applications for customers. Since the late 1990s, the provision of banking services via the internet has increased significantly. Direct or internet banks, with few or no physical branches, have rapidly proliferated. Today, all banks can offer online banking services. Therefore, as banks and customers converge on virtual platforms and an increasing number of people use online services, the dependency on banking branches is gradually decreasing.

Artificial intelligence (AI) in banking is traditionally essential for almost all business lines, from deposit taking to lending and investment banking. Autonomous data management without human intervention offers banks the potential to increase their speed, accuracy, and efficiency. The banking sector in Turkey aims to provide more data-driven and effective services in a competitive industry by embracing and developing this technology. Therefore, in the future, the further integration of AI technologies into the banking sector and the emergence of new opportunities in innovation are expected developments. Many Turkish banks support developments in this field by organizing AI-based bootcamps. Virtual assistants are among the primary examples of AI used in the banking sector in Turkey. For example, Garanti Bank's virtual assistant Ugi is an AI-based model that provides support similar to customer representatives in various areas such as account transactions and currency exchange. Similarly, İş Bankası's AI-based assistant Maxi has features such as providing information on customer account and credit card statuses, reporting payments or past expenses by category when requested, providing information on the current financial situation, and tracking customer debts. Today, many banks have AI-supported virtual assistants, and these assistants continue to improve themselves every day.

In addition to its advantages, attention should be drawn to the potential malicious manipulation of big data in banking, which could be a possible barrier to the use of artificial intelligence. For example, hackers may attempt to influence AI decisions by loading fake data (fake social media accounts, websites, news) into systems. As a result, AI tools may make biased decisions and discriminate against certain individuals, or hackers may take control of AI systems. With AI systems interconnected, malicious problems can become even more pronounced. While artificial intelligence may have relatively high accuracy in detecting cyberattacks and malicious software, continuous oversight and supervision by programmers may be required to address cybersecurity issues. Introducing regulatory sandbox environments, where new AI tools' security is tested in real-world scenarios, could be beneficial in this regard. Some observers argue that artificial intelligence, particularly neural networks, have an opaque reasoning structure and function as a black box. These concerns sometimes arise from the complexity of AI algorithms and humans' inability to visualize and understand these patterns. Compounding the complexity issue is the fact that AI algorithms are updated over time and create more dependencies. AI predictions and decisions can ultimately be very close to those of humans. However, due to the nature of artificial intelligence, it cannot explain its reasoning like humans do. Therefore, when considering the use of AI in banking, decisions should be traceable back completely, even if they are considered reasonable and justifiable. If there is a problem with a decision, it should be clearly identified at which step the error occurred. The entire decision-making process must fully comply with regulatory and supervisory rules and be entirely transparent.

IV. OPEN BANKING AND SECURITY REQUIREMENT

Open banking stands out as a significant component of digital transformation in the financial sector. This approach enables banks to share customer data with third-party service providers, allowing them to offer more innovative and personalized financial services. However, security has become a fundamental concern in this new paradigm. Various approaches such as strong authentication, data encryption, fraud detection, and regulatory compliance are required to ensure security. In this way, open banking platforms can gain the trust of customers and financial institutions and can be successful in a sustainable manner.

The fundamental principle of open banking is based on sharing financial data with third parties to provide better financial services. This practice has liberated financial data, which is highly important and should be kept confidential, from the monopoly of banks. Through user consent, these data have become accessible to third-party service providers. With this compliance, the data have become accessible to FinTech companies. All these financial dynamics are undergoing

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

transformation every day due to the impact of technology. In this transformation, the relationship between financial data and the characteristics of open banking has become crucial. Financial data is crucial for recording, analyzing, and reporting financial transactions for businesses. It has the most significant impact on understanding financial conditions such as income, expenses, debts, and assets. By evaluating these data, both the economic stability of individuals and corporate structures can be determined. The accuracy of financial data directly affects the correctness of the decisions made. Incorrect information can threaten the economic stability of a company. Therefore, in the world of technology, financial data forms the basis of open banking.

In this context, open banking is an approach that enables customers to securely share their financial data between different financial institutions. This approach facilitates financial data sharing through Application Programming Interfaces (APIs). APIs are tools that enable different systems to communicate with each other and form the basic infrastructure of open banking. Open banking allows customers to personalize their financial experiences and easily switch between different financial institutions.

With the proliferation of open banking, concerns about the security of financial data have also increased. Naturally, security measures and policies form the foundation for ensuring the security of open banking platforms. It is critically important for users to be confident that their personal and financial data are secure for the success of open banking services. Therefore, financial institutions and financial technology companies must continually review and update their security measures.

1. Authentication and Authorization: The primary way to ensure security in open banking transactions is to authenticate and authorize users. This process is carried out using strong authentication methods. Various methods can be used to verify users' identities, such as passwords, biometric data, and two-factor authentication. This helps prevent unauthorized access to financial data.

2. Data Encryption: Data encryption techniques are used to ensure the security of financial data. These techniques encrypt data during transmission and storage, ensuring protection against unauthorized access. Particularly during data transfer, encrypting data during transmission enhances security and reduces the risk of data breaches.

3. API Security: The security of APIs used in open banking transactions is of paramount importance. APIs facilitate data exchange between different systems, making their security critical. Various security protocols and standards can be used to ensure the security of APIs. For example, security standards like the OAuth protocol are commonly used to ensure the security of APIs.

4. Penetration Testing and Security Audits: Financial institutions and financial technology companies are required to regularly test and audit the security of their systems. Methods such as penetration testing and security audits are used for this purpose. These tests and audits play an important role in identifying and addressing potential security vulnerabilities.

5. Data Privacy Policies: Protecting data privacy in open banking transactions is crucial. Therefore, financial institutions and financial technology companies should develop privacy policies that explain how they use and store users' data. These policies provide transparency about how users' data is processed and protected, thereby increasing user trust

Especially through APIs, which are fundamental elements of open banking and facilitate data exchange between different financial service providers, sharing financial data can enable the development of innovative services. For example, banks collaborate with customers' consent to share financial data and develop innovative products and services based on them. This creates a suitable environment for customers to better understand their financial situations. However, all these significant developments entail security risks associated with data sharing over time. Misuse of customer data or unauthorized access can threaten financial health. Therefore, strong security measures and strict regulations are necessary in open banking platforms. As FinTech companies grow and evolve, the issue of financial data security increasingly concerns users. It is crucial for users to be confident that their personal and financial data are secure. Thus, the security of financial data is the top priority for the success of innovations in the open banking sector. In this regard, the industry has established a security network as one of its fundamental components. By implementing robust identity verification, data encryption, and authorization features, customer data can be protected. Consequently, when financial service providers achieve customer satisfaction, open banking services succeed. Implementing stringent security measures and data security policies in the open banking domain can enhance customer experience and enable the provision of new services.

A. API (Application Programming Interface)

An API, or Application Programming Interface, is a set of rules or protocols that allows software applications to communicate with each other and exchange data, features, and functionality. APIs facilitate application development by enabling developers to integrate these features from other applications rather than building them from scratch. Additionally, APIs enable application owners to securely and simply provide application data and functionality to internal departments within the organization. Application owners can also share or market this data and functionality to partners or third parties.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

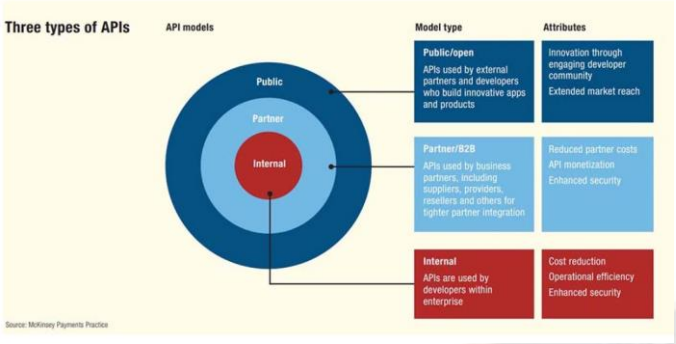


Figure 3. Types and Features of APIs
Source: https://fintechtime.com/2023/07/acik-bankacilik-ve-riskleri-verilerimiz-gercekten-guvende-mi/

Figure 3 illustrates the types and features of APIs in detail.

Today, the majority of APIs are web APIs, which expose an application's data and functionality over the internet. There are four main types of web APIs:

1. Open APIs: These are open-source application programming interfaces accessible using the HTTP protocol. Also referred to as public APIs, they have defined API endpoints and request and response formats.

2. Partner APIs: These APIs connect strategic business partners. Typically, developers access these APIs through a public API developer portal in self-service mode. However, they are required to complete an onboarding process and obtain login credentials to access partner APIs.

3. Internal APIs: These APIs are not visible to external users. They are private APIs and are not accessible to users outside of the company. Internal APIs are designed to enhance productivity and facilitate communication across different internal development teams.

An important point to emphasize is that the low risk arising from stringent control and security measures is one of the key indicators encouraging open banking. The function of open banking is based on the access of third-party financial institutions to bank customers' financial and personal data, which is then used to provide various services. Data sharing typically occurs through Application Programming Interfaces (APIs) and is generally done in three different ways: openly shared data, shared with stakeholders under specific conditions, or used only within the organization.
An attempt has been made to explain how APIs work through an example as the simplest way to understand.

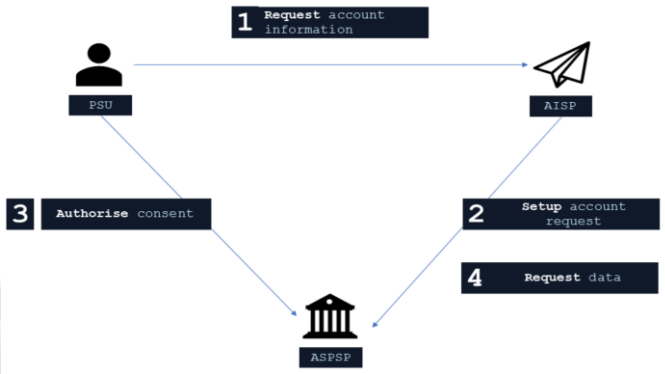


Figure 4. General outline of an account information request and flow using the Account Info APIs.
Source: https://openbankinguk.github.io/read-write-api-site3/v3.1.7/profiles/account-and-transaction-api-profile.html#sequence-diagram

The figüre 4 provides a general outline of an account information request and flow using the Account Info APIs.
Step 1: Account Information Request
This process begins with an account holder granting permission for a Financial Service Provider (FSP) to access their account information.
Step 2: Account Access Authorization Setup
The AISP connects to the ASPSP that serves their account and creates an account access authorization resource. This notifies the ASPSP that an account holder has authorized an AISP to access their account and transaction information. The ASPSP responds with an identifier to the resource (the ConsentId - which is the intent identifier). This step is accomplished by making a POST request to the /account-access-consents endpoint. The account access consent resource will include the following fields, identifying the data approved for access by the account holder with the AISP:
Permissions: A list of approved data sets for access.
Expiry Date: An optional expiration date when the AISP will no longer have access to the PSU's data. Transaction Validity Period - A Start/End date range representing the period during which the AISP can access data. An AISP may act as a data intermediary for other parties, so it's valid for a PSU to have different account access consents with different parameters for the same accounts.
Step 3: Authorization Consent
The AISP requests authorization from the PSU. The ASPSP may accomplish this using a redirection flow or a separate flow. In the redirection flow, the AISP redirects the PSU to the ASPSP.
• The redirection includes the ConsentId generated in the previous step.
• This allows the ASPSP to associate the established account access consent.
• The ASPSP authenticates the PSU.
• The ASPSP internally updates the status of the account access consent resource and indicates that the account access consent has been authorized.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

• After authorization, the PSU is redirected back to the AISP. In a separate flow, the ASPSP requests the PSU to grant approval from a different authentication device than the one used for interacting with the AISP.
• The separate flow is initiated by an AISP making a back-channel authorization request.
• The request includes a 'hint' identifying the PSU and is matched with the consent to be authorized. • The ASPSP authenticates the PSU and internally updates the status of the account access consent resource, indicating that the account access consent has been authorized.
• After authorization, the ASPSP can make a callback to provide an access token. The accepted principle is that consent is managed between the PSU and the AISP. Therefore, the details of the account access consent should not be altered at this step (with the ASPSP). The PSU can only fully approve or reject the account access consent details. During consent, the PSU selects the authorized accounts for AISP requests on the banking interface (GibHub, 2024).

B. Advantages and Functions of APIs

APIs facilitate the design and development of new applications while also enabling the integration and management of existing ones. This provides significant benefits to developers and large-scale organizations. Enhanced collaboration is just one of these advantages. On average, a bank uses nearly 1,200 cloud applications, many of which are independent of each other. APIs enable seamless communication between these platforms and applications, making integration possible. Through this integration, banks can automate workflows and enhance collaboration. Without APIs, many banks may experience connectivity gaps, leading to information silos that jeopardize productivity and performance.

Another benefit of APIs is accelerated innovation. Additionally, APIs offer flexibility, allowing banks to connect with new partners and introduce new services to existing markets. This flexibility ultimately provides banks with access to new markets that can generate significant returns and drive digital transformation. Additionally, many banks may prefer to generate revenue through data monetization via APIs. If an API grants access to valuable digital assets, banks can profit from selling access, a practice known as the API economy.

APIs are also crucial from a security standpoint. They separate the requesting application from the service responding to the request and provide security in layers during the communication process. Furthermore, APIs ensure end-user security and privacy. While providing additional protection within a network, APIs can also offer another layer of protection for individual users. When an application needs to access files via an API, operating systems use permissions for that access.

C. IP Address

An IP address, short for Internet Protocol Address, is a unique identifier assigned to devices connected to the internet. It serves as the address for devices or networks to communicate over the internet.

There are two main versions of IP addresses commonly used on the internet: IPv4 and IPv6. An IPv4 address is represented as a series of four decimal numbers separated by periods, such as 192.168.35.4. The first three numbers in an IPv4 address typically denote the network, while the last number represents the specific host within that network, such as a computer or server. On the other hand, an IPv6 address consists of eight groups of four hexadecimal digits separated by colons, like 2620:cc:8000:1c82:544c:cc2e:f2fa:5a9b.

Each IP address can transmit data to other IP addresses in discrete units called packets. These packets contain both the data being transmitted and a header containing packet metadata (Yasar, 2024).

IPv4

IPv4, short for Internet Protocol version 4, is a standard defining the format of IP addresses on the internet. An IPv4 address consists of four dotted decimal numbers, each representing an octet or byte, separated by dots. IP addresses can be represented in three different formats:

- Dotted Decimal: 172.16.30.55
- Binary: 10101100.00010000.00011110.00110111
- Hexadecimal: AC101E37

When examining the binary notation of an IPv4 address, it's important to note that IPv4 is comprised of 32 binary bits, divided into four octets (each consisting of 8 bits). Each octet can range from 0 to 255 or 00000000 to 11111111 in binary notation. With approximately 4.3 billion possible IP addresses (2^32 = 4294967296), IPv4 allows for around 4.3 billion network devices to connect simultaneously.
IPv4 is categorized into five classes;

Class A

- Class A ranges from 0 to 127.
- It is primarily used for default routing (0.0.0.0/0) and LAN card testing (127.0.0.0 to 127.255.255.255).

Class B

- Class B ranges from 128 to 191.
- The APIPA (Automatic Private IP Addressing) in DHCP uses this class range (169.254.0.1 to 169.254.255.254).

Class C

- Class C ranges from 192 to 223.
- There are no reserved IP addresses in this class.

Class D

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

- Class D ranges from 224 to 239.
- This class is reserved and not assigned to devices.
- Class D is used for multicasting purposes.

Class E

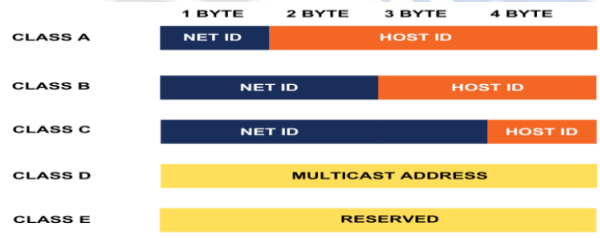
- Class E ranges from 240 to 255.
- This class is reserved for research and development purposes.

TABLE I. CLASSES OF IPV4

Class	Range	Subnet Mask	Default CIDR
Class A	0-127	255.0.0.0	/8
Class B	128-191	255.255.0.0	/16
Class C	192-223	255.255.255.0	/24
Class D	224-239	N/A	–
Class E	240-255	N/A	–

Source: **(**Khan, 2023) https://www.nwkings.com/what-is-an-ip-address-and-its-types

TABLE II. CLASSES REPRESENTİNG ID



Source: (Khan,2023) https://www.nwkings.com/what-is-an-ip-address-and-its-types

The first octet of Class A represents Network ID
The first 2 octets of Class B represent Network ID
The first 3 octet of Class C represents Network ID

IPv6
Despite IPv4 having approximately 4.3 billion addresses, which initially seemed like a vast number, the proliferation of network devices has already exceeded this limit. Consequently, IP addresses became scarce. IPv6 comes to the rescue as a solution to this scarcity. IPv6 utilizes a 128-bit address format represented by 8 hexadecimal numbers separated by colons (:).

For example: 2620:cc:8000:1c82:544c:cc2e:f2fa:5a9c.

IPv6 boasts a total of 2^128 addresses, which is considered sufficient at present.

a. Procedure of IP Addresses

IP addresses are a system that allows devices and websites to communicate with each other over the internet. When a device sends a request to access a website, it needs to know the location of the target website and how to reach it. This is where IP addresses come into play. The requesting device establishes a connection through a network router to reach the server hosting the target website. The server receives the request and sends back the requested website's information to the requesting device. Communication occurs because each device (requesting device, router, and server) has its unique IP address.

D. Open Banking and Near Field Communication Technology

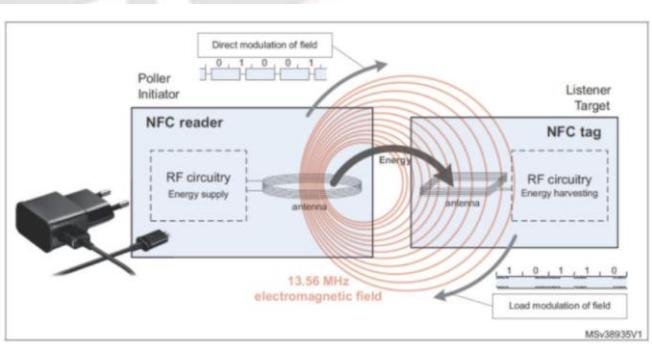
Near Field Communication (NFC) stands out as a technology that enables communication via radio signals, present in all smart devices capable of processing transactions. Widely available in smartphones, NFC technology facilitates numerous transactions to be conducted in a contactless manner. The most significant benefit of this development is the considerable increase in the importance of contactless transactions, especially following the worldwide Covid-19 pandemic.

a. Working Principle of NFC Technology

Near Field Communication (NFC) technology is based on simple principles that enable contactless communication. Essentially, NFC operates on radio signals. When a smartphone has NFC capability, and you wish to make a payment without using a credit card, communication occurs between your smartphone and the POS device. The smartphone gathers the necessary payment information into a signal, which is then transmitted to the POS device via radio signal. The POS device reads the information within the signal, facilitating the payment.

The most significant difference between NFC technology and other contactless communication technologies is its ability to operate without any power source. For instance, while the smartphone's charge is required to use Bluetooth, NFC technology can be used for documents such as identification cards, credit cards, and driver's licenses. By embedding NFC equipment into identity cards, identity information can be transferred and authenticated without physical contact. Similarly, through NFC technology integrated into credit cards, payments can be made without physically touching the POS device.

TABLE III. NFC OPERATİON PROCESS



Source: everythingRF (2024) https://www.everythingrf.com/community/what-is-nfc?gad_source=1&gclid

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

An active NFC device can operate in three modes: peer-to-peer, read/write mode, and card emulation. • Peer-to-peer mode (P2P): In this mode, two NFC-enabled active devices (such as smartphones) directly exchange files and information. While one device sends data, the other acts as the receiving device. Both devices generate radio waves alternately at a carrier frequency of 13.56 MHz.
• Read/write mode: In this mode, an NFC-enabled active device reads data from an NFC-enabled passive device (tag) or writes data to the tag by generating radio waves alternately at a carrier frequency of 13.56 MHz.
• Card emulation mode: In this mode, the NFC-enabled active device functions as a passive device to communicate with the receiving terminal. The active device does not generate any radio waves but responds to the receiving terminal for requested data transfer (everthingRF,2024).
The NFC technology, which is free and does not require any power source, is widely used in various fields today. Therefore, the number of smartphones, POS devices, and ATMs equipped with NFC feature is increasing day by day.

Areas where NFC feature is commonly used today include;
• Making payments,
• Receiving or sending various types of information,
• Receiving or sending phone number information,
• Receiving or sending photos, documents, and other data,
• Communicating with functional NFC tags found in various fields for different purposes,
• Connecting with Bluetooth devices.

b. Advantages and Disadvantages of NFC Technology

NFC technology offers unique features that significantly simplify daily life. Particularly, its ability to enhance operational efficiency for payment transactions is one of the most significant benefits. This provides consumers with ease of use and offers more security and convenience compared to traditional credit cards. NFC technology enables users to dynamically choose from multiple cards. However, the short working distance of NFC and its slower speed compared to other communication protocols may impose some limitations. This can restrict its usability, especially for applications on smartphones requiring sensitive data. Additionally, the chip-based nature of NFC technology may pose challenges for integration into certain applications compared to other technologies like QR codes.

c. NFC Application Development for Banking

The banking sector requires a secure payment environment to overcome unwanted risks resulting from the intense and challenging activities of the business world. Moreover, the introduction of electronic payments has further increased banks' responsibilities. Cyber threats are particularly undesirable for financial sectors. However, with NFC technology, financial sectors can avoid these attacks. One of the main reasons banks use NFC technology today is to ensure secure transactions. Technology giants worldwide, such as Apple Pay, Samsung Pay, and Google Pay, facilitate POS and finance departments through NFC technology.

d. Benefits of NFC Application Development

NFC mobile applications offer users a range of advantages, including;

1. Convenience and Speed:
    - Eliminates the need to carry a physical wallet or bank card, saving time and effort.
    - Seamless payment process by linking the card to a banking app, allowing users to simply unlock their phone, tap it to the terminal, and complete transactions without the need for signatures.
    - Payments can be made even without an internet connection, provided the NFC module is enabled.
2. Enhanced Security:
    - Data transmitted by the chip to the reader is encrypted using tokens, which change with each transaction, making it highly secure.
    - Additional security measures include setting a limit on payment amounts without requiring a PIN code. For larger transactions, users must enter their PIN to confirm the payment.
    - NFC digital wallets offer heightened security as credit card information stored on smartphones is protected by passwords or biometric data, reducing the risk of unauthorized access compared to traditional contactless cards.

Overall, NFC application development enhances both convenience and security for users, providing a more efficient and secure payment experience(Global Banking & Finance Review (2024).

E. The Relationship Between Open Banking and Firewalls

With the increasing use of internet banking and mobile applications today, various methods aimed at obtaining users' personal information have also increased. Methods such as email, SMS, and fake links are used to solicit users' card details, passwords, etc., with the goal of obtaining personal information. Additionally, through websites and malicious software, attackers may gain access to users' password information. To prevent such risks, banks advise their customers to carefully read and follow the security warnings and explanations in the internet banking login and security menu.

Firewall is also considered an important hardware that makes internet usage more secure. A firewall filters and blocks incoming and outgoing data on the network, thus preventing

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

potential threats. However, malicious requests from trusted sources can sometimes bypass the filter, so firewall systems are continuously being improved. By monitoring incoming and outgoing network traffic on your computer, a firewall prevents malicious software and viruses from entering the system without permission. Simply put, a firewall can be described as one of the most important security solutions in the digital world.

F. Firewall Bank Account

A firewall in banking refers to a regulatory barrier that prohibits the exchange of confidential information and the execution of financial transactions between commercial and investment banks. The restrictions imposed on collaborations between banks and brokerage firms by the Glass-Steagall Act of 1933 served as a type of firewall. One of the purposes of a firewall is to prevent banks from using funds deposited by regular customers to finance highly speculative activities that could endanger both the bank and its depositors.

In essence, a firewall bank account is a separate account used to add a security layer between an individual's primary bank account and external payment platforms or services. This helps protect the user's primary bank account from unauthorized access, fraud, and cyber attacks. Under the Glass-Steagall Act of 1933, financial institutions were prohibited from operating both as a bank and a broker, clearly delineating between banking and investment activities.

The Great Depression of the 1930s, during which approximately 8,000 US banks failed or suspended operations, shook public confidence in the banking system. To restore trust in the system, it was proposed that the connections between banking and investment activities be severed. These connections were believed to have played a significant role in the market crash of 1929 and the subsequent depression.

Supporters of the law argued that banks should protect the savings and checking accounts of their customers and refrain from using them for excessive speculative activities. Based on these observations, it was decided to install robust firewalls in buildings to prevent the spread of fire to all floors, as a metaphor for separating banking and investment activities. The aim was to prevent banks from extending credit to boost the prices of securities they owned and from using depositors' funds to support stock offerings.

The concept of "Firewall Bank Account" is crucial in emphasizing the fundamental role security measures play in safeguarding financial information and assets in the digital age. A "Firewall Bank Account" acts as a barrier between a user's primary bank account and online transactions, limiting the risk of potential cyber-attacks, fraud, or unauthorized access. In essence, a Firewall bank account is a unique financial management approach used to protect financial assets, especially against cyber-attacks, fraud, and unauthorized access. This concept is often derived from the technology term "firewall," which is designed to prevent unauthorized digital access or data breaches in computer networks. The primary purpose of a firewall bank account is to reduce risk and ensure financial security for businesses and individuals. With a firewall account, transfers and transactions are specifically made through a dedicated account, keeping the primary account secure. When funds need to be transferred or a transaction needs to be conducted, the user transfers the required amount to the firewall account from the primary account, and then the transaction is completed. This reduces the risk of financial losses resulting from cybercrimes or other fraudulent activities because most of the funds are kept in the primary account. Therefore, implementing a firewall bank account can provide peace of mind and enhanced security in today's digital age, where financial transactions are increasingly conducted online. A firewall bank account is a technology widely used by banks and other financial institutions to safeguard their customers' accounts.

Below are some examples from around the world of how security firewalls are used in the banking and finance sector:

• Online banking security: Banks use security firewalls to restrict unauthorized access and defend against cyber-attacks to protect online banking systems. The firewall monitors incoming and outgoing traffic to the bank's network, allowing only legitimate data to pass while blocking potential threats. This helps ensure the privacy, integrity, and availability of customers' account information. For example, banks like Bank of America, JP Morgan Chase, and Wells Fargo use security firewalls to protect their online banking systems.

• ATMs and Point of Sale (POS) terminals: In addition to securing online platforms, banks use security firewalls to secure the infrastructure for Automated Teller Machines (ATMs) and Point of Sale (POS) terminals. Firewalls prevent unauthorized access to backend systems that store customer account information and communication channels between ATMs, POS terminals, and bank servers. Most banks with ATM networks use security firewalls to ensure secure data transfer between the user and the bank's central processing system.

• Secure mobile banking: Mobile banking applications are widely used tools for customers to conduct banking transactions. To protect these applications, banks implement security firewalls that filter data traffic between mobile devices and backend servers. This enables financial institutions to block malicious traffic and prevent unauthorized access to customer data

V. CONCLUSION

The banking and finance sector is increasingly converging and creating intersections between different areas, ushering in a new era. Open banking, no longer just a strategy or necessity, is evolving into a key element shaping the future of the industry. The increase in data sharing and collaboration among financial institutions could lead to revolutionary changes in customer experience. Open banking applications are fundamentally transforming customer interaction with banking services, enhancing financial inclusion, and initiating significant transformation within the sector. These developments may further popularize open banking in the future. In our country, open banking is seen as a rising trend, and its future is expected to become more apparent with the implementation of regulations in this field. Additionally, technological advancements in open banking applications may lead to increased use of innovative tools such as artificial intelligence, big data analytics, and blockchain. This could result in more personalized services, more effective risk management, and the emergence of more competitive products. Therefore, with the impact of open banking, the financial system may progress towards a more dynamic, transparent, and innovative era. The use of artificial intelligence technology is widespread in various areas of the banking and finance sector. For example, artificial intelligence through text chats, voice systems, or chatbots can

provide bank customers with low-cost, human-like customer services or expert advice. Chatbots can also assist FinTech companies in saving time and costs. Artificial intelligence tools that track user behavior can help detect fraudulent attempts. Machine learning can be used to predict stock market dynamics and identify future risks. The recent fruition of banks' FinTech investments and positive feedback indicates that the financial sector may be a few steps ahead of other sectors in the future. Research in the literature shows significant progress in the correct use of data, efficient process management, increasing interest in FinTech partnerships, and accurate analysis of customer needs. While interest in API banking is increasing among banks in our country, demand for financial institutions' digital transformation and transition to the open banking model is gaining momentum. These developments enhance the importance of digitization and technology-focused innovation in the financial sector, enabling banks to rapidly adapt to this transformation. Particularly, increasing collaborations with FinTech companies to provide customer-centric services and gain competitive advantage enhance dynamism and diversity in the sector. Turkey's advancements in data management and analysis enable financial institutions to make more informed decisions and better understand customer needs. This can result in improved service quality and increased customer satisfaction. The growing interest in API banking is important for strengthening financial institutions' digital infrastructure and offering customers a wider range of services. With the increasing diversity of API markets in banks, developers and FinTech companies are expected to offer more value-added applications and services in the future. Among the recent preferences of banks, NFC technology improves the operation of banking institutions while providing consumers with convenience and security. NFC is expected to become the key to the competitive edge of financial institutions in the future. These developments are expected to provide significant competitive advantages to banks compared to other sectors in the financial sector. However, regulations and security measures should not be overlooked in this process. Data sharing brought by open banking should be supported by robust technical and legal infrastructure. This way, it may be possible to increase the trust of service providers and banks in customer data sharing, and open banking can further advance the financial services sector. While open banking brings revolutionary changes in the delivery of financial services, security is also of paramount importance in this new approach. Therefore, various security tools and measures are being used to ensure the security of open banking. However, concerns and threats regarding the security of financial data need to be continually assessed and addressed. This way, the potential of open banking can be fully realized, and financial services can be delivered more securely..

REFERENCES

[1] Akan E. N. (2023) "Bankacılık ve Finans Sektöründe Yapay Zeka Kullanımı" https://zeo.org/tr/kaynaklar/blog/bankacilik-ve-finans-sektorunde-yapay-zeka-kullanimi

[2] Appinventiv (2024) "AI in Banking – How Artificial Intelligence is Used in Banks" https://appinventiv.com/blog/ai-in-banking/

[3] Ashta A. and Herrmann H. (2021) "Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance" https://onlinelibrary.wiley.com/doi/abs/10.1002/JSC.2404

[4] Bilgel D. and Aksoy B. (2019) "Finansal Teknoloji Şirketleri ve Geleceğin Bankacılığı: Açık Bankacılık" https://dergipark.org.tr/tr/download/article-file/911681

[5] Daniel L. (2021) "Firewall: What It is, How It Works, Example" https://www.investopedia.com/terms/f/firewall.asp

[6] Devx (2023) "Firewall Bank Account" https://www.devx.com/terms/firewall-bank-account/

[7] elvtr (2023) "You Can't Afford To Wait On AI: The Impact Of Artificial Intelligence In Banking" https://elvtr.com/blog/the-impact-of-artificial-intelligence-in-banking

[8] everythingRF (2024) "What is NFC?" https://www.everythingrf.com/community/what-is-nfc?gad_source=1&gclid

[9] Finteo (2021) "Açık Bankacılık Rehberi Açık Bankacılık Nasıl Doğdu?" https://finteo.com.tr/acik-bankacilik-rehberi-acik-bankacilik-nasil-dogdu

[10] GitHub Pages Account and Transaction API Profile - v3.1.7 https://openbankinguk.github.io/read-write-api-site3/v3.1.7/profiles/account-and-transaction-api-profile.html Erişim: Ocak 2024

[11] Global Banking & Finance Review (2024) "How NFC Technology Is Changing Banking and Financial Software" https://www.globalbankingandfinance.com/how-nfc-technology-is-changing-banking-and-financial-software/

[12] GoCardless (2023) What are open banking providers (AISP & PISP) https://gocardless.com/guides/posts/what-is-tpp-in-open-banking/

[13] Gümüş E., Medetoğlu B. And Tutar S. (2020) "Finans ve Bankacılık Sisteminde Yapay Zekâ Kullanımı: Kullanıcılar Üzerine Bir Uygulama" https://dergipark.org.tr/en/download/article-file/1081451

[14] IBM (2024) "What is an application programming interface (API)?" https://www.ibm.com/topics/api

[15] İsimkayit (2024) "Firewall (Güvenlik Duvarı) Nedir?" https://www.isimkayit.com/index.php/knowledgebase/277/Firewall-Guvenlik-Duvar-Nedir.html

[16] itexus (2021) "NFC Banking App Development: Implementation Use Cases and Benefits" https://itexus.com/nfc-banking-app-development-implementation-use-cases-and-benefits/

[17] Jakšič M. and Marinč M. (2019) "Relationship banking and information technology: the role of artifcial intelligence and FinTech" https://link.springer.com/article/10.1057/s41283-018-0039-y

[18] Kantaş H. (2023) "Açık Bankacılık ve Riskleri: Verilerimiz Gerçekten Güvende mi?" https://fintechtime.com/2023/07/acik-bankacilik-ve-riskleri-verilerimiz-gercekten-guvende-mi/

[19] Kaya O. (2019) "Artificial intelligence in banking" https://www.dbresearch.com/PROD/RPS_ENPROD/PROD0000000000495172/Artificial_intelligence_in_banking%3A_A_lever_for_pr.pdf?undefined&realload=YDALdb21RU6C1u5q4qfOTIUPW5xruUzvbSls6~b8nbueAlmp0ql3nWNXsWfEedm9

[20] Khaled M., Mahbubul A. J., and Kazi S. (2023) "Fıntechecosystemacrossdevelopıngcountrıes: Cross-Countryexploratorycomparıson" https://journal.ibadu.edu/index.php/journal/article/view/11/43_2_5

[21] Kılınç Law and Consulting (2023) "Open Banking in Turkey and The World" https://kilinclaw.com.tr/en/open-banking-in-turkey-and-the-world/

[22] Kochhar K., Purohit H. and Chutani R. (2019) "The Rise of Artificial Intelligence in Banking Sector" http://spel3.upm.edu.my/max/dokumen/ICERP_ICERP_2019_-_PROCEEDINGS_(REVISED)_compressed.pdf#page=142

[23] Khan I. (2023) "What is an IP Address? – Explained" https://www.nwkings.com/what-is-an-ip-address-and-its-types

[24] Kaspersky (2024) "What is an IP Address – Definition and Explanation" https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address

[25] Kumar S. (2018) "Web application Firewall for Core Banking Application" https://medium.com/@santgutz2000/web-application-firewall-for-core-banking-application-faddb11ed32b

[26] MASAK (2020) "Ödeme Kuruluşları-Elektronik Para Kuruluşları Sektör Araştırma Raporu" https://ms.hmb.gov.tr/uploads/2020/12/Odeme-ve-Elektronik-Para-Kuruluslari-yayinlanan-VErsiyon.pdf

[27] Omarini A. E. (2018) "Banks and fintechs: how to develop a digital open banking approach for the bank's future" https://iris.unibocconi.it/handle/11565/4013970

[28] Özkan F. and Aydın Ö. (2021) "Security and Privacy Based NFC Wallet Design" https://dergipark.org.tr/en/download/article-file/1974297

[29] Özyeşil M. (2022) "Open Bankıng Concept And Open Bankıng Practıces İn Turkey" https://openaccess.istun.edu.tr/xmlui/bitstream/handle/20.500.13055/181/CURRENT-FINANCIAL-STUDIES.pdf?sequence=1&isAllowed=y#page=24

[30] Presidency of the Republic of Türkiye Finance Office (2022) WELCOME TO TURKISH FINTECH ECOSYSTEM https://www.cbfo.gov.tr/sites/default/files/docs/2023-03/the-state-of-turkish-fintech-ecosystem-v0.4-compressed.pdf

[31] PWC (2020) Açık Bankacılık: Dünya ve Türkiye www.pwc.com.tr

[32] Rahman M., Ming T. H., Baigh T. A. and Sarker M. (2020) "Adoption of artificial intelligence in banking services: an empirical analysis" https://www.emerald.com/insight/content/doi/10.1108/IJOEM-06-2020-0724/full/html

[33] Remolına N. (2019) "Open banking: Regulatory challenges for a new form of financial intermediation in a data-driven World" https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=1006&context=caidg

[34] Ryzhkova M., Soboleva E., Sazonova A. and Chikov M. (2020) "Consumers' Perception of Artificial Intelligence in Banking Sector" https://www.shs-conferences.org/articles/shsconf/abs/2020/08/shsconf_pfsd2020_01019/shsconf_pfsd2020_01019.html

[35] T.C Cumhurbaşkanlığı Mevzuat Bilgi Sistemi Resmî Gazete Tarihi: 15.03.2020 Resmî Gazete Sayısı: 31069 https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=34360&MevzuatTur=7&MevzuatTertip=5 Erişim: Aralık, 2023

[36] TCMB (2022) "Open Banking Press Release" https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Announcements/Press+Releases/2022/ANO2022-48

[37] timus (2024) "NFC Nedir? Nasıl Çalışır? Kullanım Alanları Nelerdir?" https://berqnet.com/blog/nfc

[38] Türkiye İş Bankası, Blog (2024) "Açık Bankacılık (Open Banking) Nedir? Açık Bankacılığın Avantajları Nelerdir?" https://www.isbank.com.tr/blog/acik-bankacilik-open-banking

[39] Umamaheswari S., Valarmathi A. and Raja lakshmi) M. (2023) "Role Of Artificial Intelligence inThe Banking Sector" http://sifisheriessciences.com/journal/index.php/journal/article/view/1722

[40] Yasar K. (….) "IP address (Internet Protocol address)" https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address Erişim: 12.01.2024.