Review

Security Challenges in Open Banking: A Systematic Review and Conceptualisation of a Tri-Dimensional Security Framework

Cristiano Wilson * and Carlos Tam

Posted Date: 11 February 2026

doi: 10.20944/preprints202602.0867.v1

Keywords: behavioural security; SecTech; RegTech; FinTech; psychological intention; tri-dimensional

Review

Security Challenges in Open Banking: A Systematic Review and Conceptualisation of a Tri-Dimensional Security Framework

Cristiano Wilson * and Carlos Tam

Universidade NOVA de Lisboa, Portugal

* Correspondence: 20220005@novaims.unl.pt

Abstract

Open banking (OB) is rapidly transforming financial ecosystems by enabling controlled dfata sharing among multiple actors. While this transformation promises innovation and competition, it also introduces complex security challenges that extend beyond purely technical considerations. Despite growing attention in both academic and professional domains, existing reviews offer limited integration of security concerns with patterns of global adoption and cross-regional variation. This systematic review addresses this gap by analysing empirical research published between 1999 and 2025, with particular attention to how security technologies, regulatory policies, and user behaviour jointly contribute to the resilience of OB environments. Building on this synthesis, the study develops a tri-dimensional security framework that integrates technological, regulatory, and behavioural dimensions, grounded in established theoretical perspectives. The framework elucidates recurring trends as well as persistent and emerging virtual security challenges within OB ecosystems. The paper concludes by outlining directions for future research and by offering practical implications for scholars, industry practitioners, and policymakers.

Keywords: behavioural security; SecTech; RegTech; FinTech; psychological intention; tri-dimensional

1. Introduction

Open banking has emerged as a transformative development in the financial services sector, redefining how financial data are accessed, exchanged, and leveraged by market participants. By relying on standardised application programming interfaces (APIs), OB enables authorised third-party providers (TPPs) to connect with consumer account data under controlled conditions (Omarini, 2018; Banerjee, 2024). This model brings innovation, enhanced customer experience, and intensified competition, while also promoting transparency and interoperability across financial systems. As a result, OB has accelerated the shift towards a more data-intensive and inclusive financial ecosystem, and at the same time, the growing interconnection among financial actors introduces heightened concerns related to security and privacy (Laplante and Kshetri, 2021; Braithwaite, 2024; Ngan, 2025). The circulation of sensitive financial information across multiple entities expands the potential attack surface, increasing exposure to threats such as fraud, phishing, and identity-related abuses. These risks directly challenge trust, which remains a foundational element of digital financial services.

Although OB has attracted substantial attention from both academic researchers and industry practitioners, existing studies often examine security-related issues in isolation. Prior research tends to focus separately on technical safeguards, regulatory and governance arrangements, or user behaviour factors, with limited integration across these perspectives (Casaló, Flavián and Guinalíu, 2007; Ege Oruç and Tatar, 2017). This fragmented approach constrains understanding of how security emerges within OB ecosystems, where technological infrastructure, institutional frameworks, and human behaviour interact continuously (Wang et al., 2024). As a consequence, there remains a lack

 doi:10.20944/preprints202602.0867.v1

of comprehensive reviews that explain how these dimensions jointly shape security effectiveness, adoption outcomes, and the development of security-oriented financial technologies within OB environments.

This study addresses this limitation by providing a systematic synthesis of empirical research published between 1999, when OB concepts first appeared in academic discourse, and 2025, a period reflecting its wider global diffusion. By covering this extended timeframe, the review captures both the conceptual foundations and the evolving practical implementation of OB across regions. Particular attention is given to the interplay between security focused technological solutions, regulatory and policy contexts, and behavioural dynamics that influence financial ecosystem resilience. In this respect, the review highlights the importance of user intentions and perceptions in shaping secure digital practices (Podsakoff et al. 2003; Hyon, Kleinbaum and Parkinson, 2020), while also considering how cultural and regional conditions affect cognitive patterns and security-related behaviour.

Building on this synthesis, the study develops a tri-dimensional security framework that conceptualises technological mechanisms, regulatory structures, and human behaviour as interdependent components of OB security. By explicitly incorporating behavioural dynamics alongside technical and institutional considerations, the framework reflects the practical realities of security management and user decision making in OB adoption across different regional contexts (Babina et al. 2025). This integrative perspective offers a more context sensitive and human-centred foundation for designing and governing effective security solutions within OB ecosystems.

The review reveals recurring patterns as well as persistent gaps within the existing literature, demonstrating how security challenges and responses vary across technological, regulatory, and behavioural domains. Based on these insights, the paper proposes directions for future research and provides implications aimed at supporting informed decision making by scholars, industry practitioners, and policymakers engaged in OB initiatives.

The remainder of the paper is structured as follows. **Section 2** describes the methodology employed for data selection and analysis. **Section 3** introduces the conceptual foundations of OB and the theoretical perspectives informing the review. **Section 4** synthesises prior empirical research, including studies related to APIs, FinTech, SecTech, RegTech, and market dynamics. **Section 5** discusses the comparative findings, outlines limitations of existing studies, and identifies opportunities for future research, before concluding the paper.

2. Methodology

This study adopts a systematic literature review approach to investigate how behavioural factors intersect with technological and regulatory dimensions in shaping security within OB environments. The review is guided by a behavioural-first perspective, which positions user intentions, trust, cognitive effort, and security-related practices as central mechanisms influencing the resilience of financial ecosystems (Oliveira et al. 2011; Daneshgadeh and Yıldırım, 2014). Rather than treating behaviour as a secondary outcome of technical or regulatory design, this approach allows for a more nuanced examination of how misalignments between human behaviour, security technologies, and governance structures generate persistent vulnerabilities and regulatory tensions in OB systems.

2.1. Inclusion and Exclusion Criteria

The initial search process yielded 569 records comprising scientific articles, empirical studies, and scholarly handbooks. Duplicate entries were identified and removed using reference management software. The remaining records were then subjected to a two-stage screening process. First, titles and abstracts were independently reviewed to eliminate clearly irrelevant studies. Second, full-text screening was conducted using predefined inclusion and exclusion criteria, supported by an adapted methodological quality checklist. Exclusion criteria were applied if the studies did not address OB or related topics, lacked empirical or theoretical contributions, had insufficient methodological reporting, used data outside the inclusion window, or were duplicate or earlier

 doi:10.20944/preprints202602.0867.v1

versions of the same work. Following this screening and quality appraisal process, 93 studies satisfied all criteria and were retained for the final synthesis **(Table 1)**.

Data sources and search strategies

The review draws on a comprehensive search of established academic databases and scholarly portals, including ScienceDirect, Web of Science, Scopus, Taylor & Francis, SAGE Journals, IEEE Xplore, Emerald Insight, SpringerLink, PubMed, and Google Scholar. The search strategy combined keywords and descriptors associated with OB and behavioural-security, encompassing themes such as APIs, data protection and privacy, financial regulation, cybersecurity, behavioural aspects of computing, regulatory technologies, financial technologies, security-oriented technologies, compliance mechanisms, data governance, financial inclusion, banking innovation, digital transformation, and consumer protection. The search focused on peer reviewed journal articles and academic books published in leading outlets, ensuring coverage of studies that explicitly address security challenges within OB contexts.

Regulatory policies sources

To complement the academic literature, regulatory and policy materials were systematically examined using targeted searches of authoritative institutional sources. At the supranational level, official documentation was consulted through the EU law portal, alongside guidance and regulatory instruments issued by the European Banking Authority (EBA, 2011), the UK Financial Conduct Authority (FCA, 2024), and the Data Protection Board (EDPB, 2020). These sources provided insight into the governance and compliance requirements shaping OB security across European jurisdictions.

In addition, national and regional regulatory frameworks were reviewed to capture cross market variation in OB implementation and oversight. These included materials published by the National Bank of Angola (BNA, 2023), the Central Bank of Kenya (CBK, 2024), the Central Bank of Nigeria (CBN, 2021, 2023) and the Reserve Bank of India (RBI, 2025). The regulatory analysis was further extended to data protection regimes beyond Europe, drawing on legislative sources such as the Brazilian data protection law (GOV.BR, 2018) and the United Arab Emirates data protection law (GOV.AE, 2021) Together, these policy sources supported a comparative assessment of how regulatory approaches influence security practices and expectations within OB ecosystems.

Table 1. Inclusion and exclusion criteria.

Inclusion criteria	Exclusion criteria
The study should address open banking, security behaviour, regulatory policies, compliance, financial regulation, cybersecurity, FinTech, RegTech or SecTech.	Studies that did not address open banking, security behaviour, regulatory policies, compliance, financial regulation, cybersecurity, FinTech, RegTech, or SecTech were excluded.
It should include a theoretical research model.	Editorials, posters, presentations, position papers, and publications in lower-tier journals were excluded.
Articles should be written in a language in which the reviewers are proficient.	Articles written in languages beyond the reviewers' proficiency were also excluded.
	Studies without full-text availability were excluded.

3. Open Banking Concept

Open banking represents a significant financial technology development that alters competitive dynamics within the banking sector by enabling controlled data sharing between incumbent institutions and new market entrants. By allowing customers to authorise third-party providers to

 doi:10.20944/preprints202602.0867.v1

access account information or initiate transactions on their behalf, OB challenges the traditional dominance of banks over financial data while expanding opportunities for innovation and service diversification (Arner et al. 2017; Jafri et al. 2024). This model relies on customer consent as a central governance mechanism and positions data portability as a driver of competition and consumer empowerment.

At the technological level, OB is operationalised through APIs that function as secure channels for data exchange between financial institutions and authorised TPPs. These interfaces support interoperability and enable the development of new financial products and services across institutional boundaries (Frei, 2023; Tariq, Maryam and Shaheen, 2024). while existing research on OB spans regulatory design, adoption dynamics, business models, and technological architecture, the present review concentrates specifically on the security challenges that arise from increased interconnectivity and data sharing within OB ecosystems.

3.1. APIs and Their Role in Open Banking

APIs constitute the foundational technological infrastructure of OB. They provide standardised mechanisms through which financial institutions and authorised TPPs exchange data in a controlled and auditable manner. Regulatory authorities play a central role in defining OB standards, ensuring that APIs operate consistently across jurisdictions while meeting baseline requirements for security, interoperability, and reliability (Nikkhah, Grover and Sabherwal, 2024; Modesti et al. 2025). Through these interfaces, customers are able to grant informed and granular consent, allowing external applications to connect with their bank accounts for specific purposes.

API enabled services support a wide range of use cases, including expenditure analysis, product recommendations, and the aggregation of financial information from multiple accounts into unified platforms. This represents a marked departure from traditional banking models, in which customer data are typically confined within institutional silos and accessed primarily through proprietary channels (Zhou, Lu and Wang, 2010; Chiew, Yong and Tan, 2018; Torshin, 2025). OB, by contrast, redistributes control over financial data, enabling customers to selectively share information with trusted third parties under predefined conditions.

Prior to the widespread adoption of API based access mechanisms, TPPs frequently relied on screen scraping techniques to obtain account information. This practice required customers to disclose their login credentials, creating vulnerabilities related to credential compromise, limited transparency, and weak control over data usage (Frei, 2023; Banerjee, 2024; Polo, Taburet and Vo, 2025). The transition towards API based architectures reflects an effort to address these shortcomings by introducing stronger security guarantees and more precise access control. Within this framework, API flows coordinate interactions among ecosystem participants by standardising processes such as user authentication, consent management, and authorisation (Boumediene Ramdani, 2020; Waliullah et al. 2025). These mechanisms ensure that access to sensitive financial data and payment functionalities is restricted to verified entities operating within defined regulatory boundaries.

In addition to facilitating secure data exchange, APIs support encryption, standardised communication protocols, and monitoring capabilities that enhance auditability and accountability (Beautement, Sasse and Wonham, 2008; Tam, Conceição and Oliveira, 2022; Torshin, 2025). Logging, real-time supervision, and fraud detection mechanisms embedded within API infrastructures contribute to the operational resilience of OB systems and strengthen compliance with regulatory expectations. Collectively, these features play a central role in mitigating malicious activity while reinforcing trust among users, providers, and supervisory authorities **(Figure 1)**.

External APIs serve as interfaces between financial institutions and TPPs, including fintech firms, payment service providers, and other regulated entities. Their primary function is to enable secure and standardised access to customer data and financial services, thereby supporting the development of applications such as budgeting tools, comparison services, and payment initiation solutions (Fett, Hosseyni and Kuesters, 2019; Hanif and Lallie, 2021). In the European context, external APIs are closely linked to regulatory mandates introduced under the revised Payment

 doi:10.20944/preprints202602.0867.v1

Services Directive (PSD2), which requires banks to facilitate access to account information and payment initiation services for authorised providers (Eu Commission, 2007; Official Journal of the European Union, 2015). From a conceptual standpoint, these interfaces extend the operational boundaries of banks, encouraging a shift from vertically integrated architectures towards ecosystem-based models in which collaboration with external actors complements competitive strategies (Eu Commission, 2007; Gimigliano et al. 2021; Adiningtyas and Auliani, 2024).

Internal APIs, by contrast, operate within financial institutions and enable communication between front end applications, middleware layers, and core banking systems. These interfaces provide structured access to functionalities such as balance enquiries, transaction histories, and payment processing, supporting efficient integration across internal systems (Merhi, Hone and Tarhini, 2019; Liu et al. 2024). By decoupling user-facing platforms from legacy infrastructure, internal APIs facilitate faster development cycles and greater organisational agility in delivering digital banking services, including mobile and online channels (Tam and Oliveira, 2017; Gill et al. 2019). Conceptually, internal APIs reflect the modularisation of banking information systems, allowing services to be recombined and reused while preserving the core banking system as the authoritative source of financial data and transactional integrity.

Figure 1. Open banking API architecture framework. Adapted from (Aws, 2024).

The core banking system (CBS) constitutes the technological backbone of financial institutions, supporting a wide range of critical functions such as deposit management, lending activities, payments, treasury operations, corporate services, and OB related modules. It enables real time transaction processing across branches and digital channels, including account administration, deposits and withdrawals, and credit operations (Puschmann, 2017; Cardoso and Martinez, 2019). Acting as the central repository for financial records, customer accounts, balances, and contractual information, the core banking system integrates with multiple specialised applications to support broader organisational processes.

Despite its central role, the inherent complexity, legacy dependencies, and performance sensitivity of core banking systems make direct external exposure neither practical nor secure (Niranjan, Raja and Rajini, 2018; Liao et al. 2022). Instead, these systems operate as the authoritative source of financial data, while intermediary layers abstract their functionality. APIs and service orchestration components mediate access to core banking capabilities, transforming internal processes into secure, standardised, and consumption ready services for both internal applications and authorised stakeholders.

 doi:10.20944/preprints202602.0867.v1

Within this architecture, the API gateway serves as the principal control point for all API based interactions. It routes incoming requests to appropriate backend services while enforcing security policies related to authentication and authorisation (Takieddine and Sun, 2015; Aws, 2024). In addition to access control, the gateway supports operational oversight through traffic management, rate limiting, and performance monitoring. By functioning as the institution's digital entry point, the API gateway reconciles the need for openness and scalability with consistent governance and control across customer facing applications, fintech partners, and internal development teams (Ling et al. 2016; Banerjee, 2024).

3.2. Open Banking Core Security

Security within OB ecosystems is underpinned by a set of interrelated principles designed to protect sensitive financial data and preserve transaction integrity across multiple participating entities. Rather than relying solely on technical safeguards, OB security encompasses strategic, technological, and regulatory measures that collectively support consumer protection, system reliability, and institutional trust (Andrade and Yoo, 2019; Modesti et al. 2025). This integrated approach reflects the distributed nature of OB, where responsibility for security is shared across banks, TPPs, and regulatory authorities.

Key elements of this security architecture include the protection of APIs, the deployment of robust identity and access management (IAM) mechanisms, and the implementation of transparent and revocable consent processes. Combined, these components ensure that access to financial data and payment functionalities is limited to authenticated and authorised actors operating within clearly defined permissions (Claire Greene et al., 2014; The wolrd bank, 2021). In addition, the secure management of cross-border data flows introduces further requirements related to data localisation, regulatory alignment, and supervisory oversight. When effectively combined, these measures establish a resilient security foundation that enables innovation while maintaining compliance and safeguarding consumer interests (**Figure 2**).

Figure 2. OB Core Security. Adapted from (Aws, 2024).

Strong customer authentication (SCA) constitutes a central control mechanism within OB security architectures. Its primary function is to establish reliable user identity verification by requiring a combination of at least two independent factors drawn from knowledge, possession, or inherence categories (Aboobucker and Bao, 2018; Desiraju, Mishra and Sengupta, 2024). By increasing the assurance level of authentication processes, strong customer authentication reduces the likelihood of unauthorised access to accounts and payment functionalities. Within OB environments, this mechanism plays a critical role in safeguarding interactions that involve multiple service providers and distributed access points. Consent management (CM) is closely intertwined with strong customer authentication, as it governs the conditions under which authenticated users authorise data sharing and transaction initiation. Effective consent management ensures that permissions are explicit, informed, and revocable, thereby preserving user agency over financial data

 doi:10.20944/preprints202602.0867.v1

and services (Desiraju, Mishra and Sengupta, 2024; Gounari et al., 2024). From a security perspective, consent mechanisms must be transparent in scope, time bound, auditable, and straightforward to withdraw, particularly in ecosystems where data flows extend across institutional and national boundaries.

Data protection and privacy controls further reinforce system security by limiting exposure and misuse of sensitive information (Official Journal of the European Union, 2016; ENISA, 2024). Encryption techniques applied during both data transmission and storage protect confidentiality and integrity, while complementary approaches such as anonymisation or pseudonymisation reduce the risk of re identification when data are processed or shared for secondary purposes (Moody and Siponen, 2013; Andrade and Yoo, 2019). These practices must be aligned with applicable regulatory frameworks, including the General Data Protection Regulation, which establishes requirements for lawful processing, data minimisation, and user rights.

At the operational level, OB security relies on the coordinated use of APIs and IAM mechanisms to ensure that only regulated and verified participants can interact with protected resources (Hanafizadeh, Keating and Khedmatgozar, 2014; Vanini et al. 2023). Widely adopted industry standards, such as OAuth 2.0 and OpenID Connect, enable delegated and scope limited access without requiring the disclosure of user credentials, thereby reducing attack surfaces associated with credential reuse and compromise (Souza and Redmiles, 2009; Li et al. 2023). Regulatory oversight reinforces these technical controls by mandating the registration and certification of TPPs, validating credentials, and requiring comprehensive audit trails covering API interactions, consent events, and transaction records.

Despite these layered controls, APIs remain a prominent source of security risk within OB ecosystems. Configuration weaknesses, inadequate monitoring, or inconsistent enforcement of access policies can give rise to vulnerabilities such as broken object level authorisation, excessive data exposure, token leakage, and session hijacking (Amin Lecturer, 2007; Hilal, Gadsden and Yawney, 2022). Maintaining consistent, time limited, and auditable consent across multiple providers and regulatory jurisdictions continues to pose practical challenges (Martins, Oliveira and Popovič, 2014; Xu et al. 2020). Consequently, effective OB security depends on a layered and integrated approach that combines technical safeguards, regulatory obligations, and user rights to enhance resilience, trust, and compliance across the financial sector.

3.3. Geographic Adoption and Regulatory Frameworks

Open banking adoption and regulation exhibit substantial geographical variation, reflecting differences in legal traditions, institutional capacity, and policy priorities (Babina et al., 2025). In the European Union and the United Kingdom, OB is governed by comprehensive regulatory regimes that combine data protection requirements under the GDPR with secure access mandates introduced through the revised PSD2. Collectively, these frameworks place strong emphasis on consumer consent, data protection, and competition, positioning OB as both a market enabling and consumer safeguarding mechanism financial sector (Gounari et al. 2024; PwC Netherlands, 2025). This regulatory maturity has contributed to relatively high levels of standardisation and supervisory oversight across European OB ecosystems.

Outside Europe, regulatory approaches are more heterogeneous and often adapted to local economic and institutional contexts. Australia's Consumer Data Right (Competition and Commission, 2025), represents a consumer centric model that grants individuals explicit control over how their data are accessed and shared, thereby prioritising transparency and accountability. In Canada, regulatory initiatives remain under development and seek to balance innovation objectives with privacy protections, although current proposals are generally less prescriptive than European counterparts. Across several African jurisdictions, including Angola and Kenya (Patrick Njoroge, 2022; BNA, 2023), regulatory frameworks are emerging gradually and reflect domestic legal structures, market readiness, and broader financial development strategies.

 doi:10.20944/preprints202602.0867.v1

A number of countries have also introduced national data protection and OB related regulations that operate alongside or independently of European style regimes. Brazil enforces OB through the General Data Protection Law, while the United Arab Emirates applies a dedicated data protection framework that governs the processing and sharing of personal financial information (GOV.BR, 2018; Serrado et al., 2020; GOV.AE, 2021). In India, OB initiatives are overseen by the Reserve Bank of India, which plays a central role in supervising data sharing arrangements and ensuring systemic stability (RBI, 2025). Despite jurisdictional differences, these regulatory frameworks consistently require explicit customer consent as a precondition for data sharing and transaction initiation, underscoring consent as a universal governance principle in OB (Babina et al. 2025). In most cases, central banks or financial supervisory authorities are responsible for enforcement and alignment with national legislation.

Table 2 presents descriptive statistics on OB regulatory policies across all 193 countries. Each column shows how many countries satisfy the respective criteria. The table is adapted from Babina et al. (2025).

Table 2. Summary statistics of regulatory policies across all 193 countries.

Variable	Worldwide	Africa & Middle East	Europa & Central Asia	LA & the Caribbean	North America	South-East Asia & Pacific
Number of Countries	193	65	50	25	3	50
Regulatory Initiatives	168	65	50	25	3	25
Promoting competition	65	9	39	3	1	13
Fostering innovation	65	9	39	3	1	13
Financial inclusion	66	10	39	3	1	13
Under discussion	80	16	40	8	2	14
Partial implementation	80	16	40	8	2	14
Fully implemented	80	16	40	8	2	14
Mandatory data sharing	57	6	37	2	1	11
Reciprocal data access	56	6	36	2	1	11
Regulatory tech standards	62	8	39	2	1	12
Extended scope	56	5	36	3	1	11
Data access only	58	6	38	2	1	11
Payment function	58	6	38	2	1	11
Integrated data & payments	58	6	38	2	1	11

The distribution of initiatives reveals that competition and innovation are the dominant global policy drivers. This suggests that OB regulation is frequently deployed not only as a technical framework but also as a strategic instrument for reshaping financial markets (Babina and Howell, 2024). In Europe and Central Asia, for example, 50 countries prioritise competition and innovation, reflecting long standing efforts to promote integrated markets and accelerate digital transformation. By contrast, Africa and the Middle East display lower levels of regulatory activity, indicating that

 doi:10.20944/preprints202602.0867.v1

adoption decisions are closely linked to economic development levels and institutional readiness (He, Huang and Zhou, 2023; Akyildirim et al., 2025).

Although 80 countries have fully implemented OB related policies, signalling a shift from planning to operational deployment, the uptake of more advanced features remains uneven. Reciprocal data access is implemented in only 57 countries, while integrated data and payment models are present in 58. These patterns highlight ongoing concerns related to data governance, infrastructure investment, and consumer protection (Hair et al., 2017; Scheepers et al., 2026). From an institutional theory perspective, regulatory diffusion tends to be uneven, with early adopting regions such as Europe establishing benchmarks that are later emulated by other jurisdictions. Regions with constrained resources or fragmented markets, including parts of Latin America and Africa, often prioritise foundational objectives such as financial inclusion before advancing towards more complex regulatory and technical arrangements (**Table 2**).

Table 3 provides descriptive statistics on open banking regulatory policies across all 193 countries. Each column reports the percentage of countries listed in Table 2 that satisfy the respective criteria. The table is adapted from Babina et al. (2025).

Table 3. Summary statistics of regulatory policies (%), all 193 countries.

Variable	Worldwide	Africa & Middle East	Europa & Central Asia	LA & the Caribbean	North America	South-East Asia & Pacific
Number of Countries	193	65	50	25	3	50
Regulatory Initiatives	48%	25%	80%	32%	67%	56%
Promoting competition	82%	67%	87%	100%	0%	77%
Fostering innovation	97%	100%	97%	100%	100%	92%
Financial inclusion	29%	40%	10%	100%	100%	54%
Under discussion	38%	75%	12%	75%	100%	36%
Partial implementation	18%	6%	12%	25%	0%	43%
Fully implemented	44%	13%	75%	0%	0%	21%
Mandatory data sharing	88%	67%	97%	100%	100%	64%
Reciprocal data access	18%	33%	0%	100%	100%	45%
Regulatory tech standards	39%	63%	15%	100%	100%	83%
Extended scope	34%	80%	3%	100%	100%	91%
Data access only	5%	0%	0%	50%	100%	9%
Payment function	0%	0%	0%	0%	0%	0%
Integrated data & payments	95%	100%	100%	50%	0%	91%

While innovation is a near universal driver of OB adoption globally, competitive pressure varies significantly, remaining relatively weak in Africa and the Middle East. In Latin America and the Caribbean, financial inclusion emerges as the primary motivation, whereas it plays a less prominent role in Europe and Central Asia. Technological implementation also differs markedly across regions (Strahan and Cetorelli, 2004; Anderson et al., 2010; Joseph F. Hair Jr. et al., 2021). Southeast Asia and the Pacific exhibit high levels of data and payment integration, while North America remains comparatively fragmented. Regulatory technology standards are fully implemented in Latin America and North America but are far less prevalent in Central Asia (**Table 3**).

These disparities indicate that the formal adoption of regulatory frameworks alone is insufficient to ensure effective OB implementation. Technological infrastructure, supervisory capability, and institutional capacity are critical determinants of practical outcomes. Prior research demonstrates that

 doi:10.20944/preprints202602.0867.v1

initial trust, shaped by institutional guarantees and provider reputation, plays a decisive role in the adoption of OB services under conditions of uncertainty (Chen et al., 2020; Chan et al., 2022). Earlier studies further suggest that private banks, industry groups, and other stakeholders with vested interests can influence both the pace and direction of regulatory development (Kroszner and Strahan, 1999; Tan and Teo, 2000). Taken together, these findings imply that inclusive stakeholder engagement may facilitate the design and implementation of more effective and context appropriate regulatory frameworks for OB.

4. Empirical Literature of OB Framework

This section synthesises empirical research on OB across technological, regulatory, and market dimensions, with particular attention to application programming interfaces, fintech innovation, and governance structures. The review consolidates evidence on how the OB framework has been operationalised in practice, evaluates the robustness and scope of existing studies, and identifies conceptual and empirical gaps that motivate the present research. Section 4.1 reviews studies that focus on API architectures and fintech technologies (**Table 4**), while Section 4.2 examines regulatory and market-oriented research (**Table 5**). Section 4.3 integrates these streams through a proposed tri dimensional analytical framework.

4.1. Studies on API and Fintech Technologies

A substantial body of research examines the technological foundations of OB, particularly the role of APIs in enabling secure data sharing and interoperability across financial institutions and third-party providers. Although APIs were not originally designed for highly regulated financial environments, advances in authentication protocols, encryption mechanisms, and standardised interfaces have enabled their effective deployment within OB ecosystems. Empirical studies in this domain predominantly focus on security robustness, system design, and user adoption dynamics.

Fett et al. (2019) provide a formal security analysis of the OpenID Financial Grade API, demonstrating how enhanced authentication and authorisation mechanisms address vulnerabilities associated with traditional API implementations. Complementing this technical focus, Tam et al. (2020) investigate factors influencing users' continuance intention to use mobile banking applications, highlighting the importance of perceived system quality, reliability, and virtual service design in sustaining long term engagement. These findings suggest that technical security alone is insufficient and must be accompanied by positive user experience to support adoption.

Table 4. Overview of open banking API and fintech technology studies.

Author(s)	Title / Journal	Key domain	Research Contributions
(Fett et al. 2019)	An extensive formal security analysis of the openid financial grade api. /IEEE symposium on security and privacy	Security and API protocols	Performs formal security analysis of api, identifies vulnerabilities in authentication flows, and proposes strengthened security mechanisms for open banking apis.
(Modesti et al. 2025)	Security analysis of the open banking account and transaction api protocol. /Cyber security and applications	Security and API standards	Analyses transaction and account api protocols; identifies potential security threats and recommends technical improvements for secure data sharing.

 doi:10.20944/preprints202602.0867.v1

(Gosman, Hedman and Sylvest, 2018)	OB: emergent roles, risks & opportunities. /Ecis 2018 proceedings	Ecosystem and strategic implications	Explores emergent roles in open banking ecosystem; discusses risks (data privacy, security) and opportunities (innovation, competition) for banks and fintechs.
(Pinochet et al. 2023)	Predicting the intention to use the investment aggregate functionality in the context of open banking using ann. /Procedia computer science	Consumer behaviour and technology	Uses artificial neural networks to predict consumer intention to adopt investment aggregation features; highlights factors driving adoption in open banking apps.
(Chan et al. 2022)	Towards an understanding of consumers' fintech adoption: the case of open banking. /International journal of bank marketing	Consumer adoption and trust	Examines factors influencing consumer adoption of open banking apps; highlights the role of trust, perceived benefits, and institutional guarantees.
(Liu et al. 2024)	The open banking era: an optimal model for the emergency fund. /Expert systems with applications	Financial modeling / open banking applications	Proposes an optimisation model for emergency fund management in the open banking era; demonstrates how OB apis can improve fund allocation and household financial resilience.
(Puschmann, 2017)	Fintech. /Business & information systems engineering	Fintech and open banking foundations	Provides one of the earliest comprehensive analyses of fintech, highlighting the foundations, evolution and the emergence of open banking ecosystems.
(Liao et al. 2022)	Blockchain-based identity management and access control framework for open banking ecosystem. /Future generation computer systems	Security and identity management	Proposes a blockchain-enabled framework for identity management and access control in open banking ecosystems; enhances privacy, authentication, and security.

Early conceptual contributions by Puschmann, (2017) offer a foundational understanding of fintech evolution, tracing the emergence of digital finance and the development of OB technology ecosystems. Building on this foundation, subsequent empirical research has increasingly examined how fintech innovations reshape banking processes and customer interactions. Oliveira et al. (2016), for example, analyse customers' psychological intentions to recommend mobile payment technologies within social networks, illustrating how social influence and user engagement accelerate fintech diffusion and contribute to the expansion of OB ecosystems.

More recent studies adopt a security engineering perspective. Modesti et al. (2025) conduct formal analyses of core API protocols, identifying residual vulnerabilities and proposing targeted

 doi:10.20944/preprints202602.0867.v1

improvements. Their work illustrates the transformation of APIs from generic data exchange tools into specialised financial infrastructures aligned with standards such as OAuth2 and Financial Grade API. Collectively, the studies summarised in Table 4 indicate that research on the technological dimension of OB has progressively evolved from exploratory assessments towards more rigorous security evaluation and behavioural integration.

4.2. Studies on Regulatory Policy and Market Analysis

Empirical research consistently demonstrates that regulatory frameworks and data access standards are central to shaping market behaviour, competitive dynamics, and innovation within OB ecosystems. Rather than functioning solely as compliance mechanisms, OB regulations actively restructure financial markets by redefining data ownership, access rights, and the relationships between incumbent banks and fintech firms.

Large-scale cross-country evidence provided by Babina et al. (2025) shows that customer data access regulations significantly increase fintech market entry, intensify competition, and expand consumer choice across 168 countries. However, the magnitude of these effects varies substantially by region, reflecting differences in institutional capacity, legal maturity, and financial market development. These findings suggest that the economic impact of OB depends not only on the presence of regulation but also on its effective enforcement and alignment with local market conditions.

At a more granular level, Dinçkol et al. (2023) examine the United Kingdom's OB regime and demonstrate how regulatory standardisation reshapes industry architecture. Their analysis shows that mandated technical and governance standards facilitate collaboration between banks and fintech firms, while simultaneously altering competitive boundaries and increasing coordination complexity. This highlights the dual role of regulation as both an enabler of innovation and a source of structural adjustment costs.

Comparative regulatory studies further underscore the diversity of OB models. Colangelo and Khandelwal, (2025) identify multiple regulatory rationales and implementation approaches, including mandatory, voluntary, and hybrid models, each associated with distinct policy trade-offs. In related analysis Colangelo, (2024) draws lessons from the European Union's experience for the United States, emphasising the benefits of regulatory driven data sharing alongside the challenges posed by fragmented supervisory structures and differing legal traditions.

Table 5. Overview of OB regulatory policy and market studies.

Author(s)	Title / Journal	Key domain	Research Contributions
(Babina et al. 2025)	Customer data access and fintech entry: early evidence from open banking. /Journal of financial economics	Regulation and market entry	Provides global evidence from 168 countries on how customer data access regulations affect fintech entry; shows that open banking policies significantly increase competition, promote innovation, and support consumer choice, but with regional variations.
(Colangelo and Khandelwal, 2025)	The many shades of open banking: a comparative analysis of rationales and models. /Internet policy review	Comparative regulation and models	Compares open banking rationales across countries; identifies different implementation models (mandatory, voluntary, hybrid) and their policy implications.
(He, Huang and shou, 2023)	Open banking: credit market competition when borrowers own	Market competition and data ownership	Investigates the impact of customer data ownership on credit markets; finds that open banking enhances

 doi:10.20944/preprints202602.0867.v1

	the data. /Journal of financial economics		competition and credit allocation efficiency.
(Dinçkol, Ozcan and Zachariadis, 2023)	Regulatory standards and consequences for industry architecture: the case of UK open banking. /Research policy	Regulation and industry structure	Analyses how UK open banking standards reshape banking industry architecture; shows implications for bank-fintech collaboration and market dynamics.
(de Araluze and Cassinello Plaza, 2022)	Open banking: a bibliometric analysis-driven definition. /Plos one	Literature mapping and conceptualisation	Provides a bibliometric analysis of open banking literature; proposes a structured definition and identifies emerging research trends and gaps.
(Colangelo, 2024)	Open banking goes to Washington: lessons from the EU on regulatory-driven data sharing regimes. /Computer law & security review	Regulation and comparative policy	Explores lessons from EU open banking regulation for us policy; highlights regulatory-driven data sharing benefits and challenges in cross-jurisdiction adoption.
(Fang and Zhu, 2023)	The impact of open banking on traditional lending in the brics. /Finance research letters	Open banking and credit markets	Analyses how open banking influences lending in brics economies; finds that data sharing enhances credit availability and reduces information asymmetry for borrowers.
(Kroszner and Strahan, 1999)	What drives deregulation? economics and politics of the relaxation of bank branching restrictions. /Quarterly journal of economics	Political economy of financial regulation	Uses hazard models to analyse state-level bank deregulation in the USA; finds that private interest group dynamics (large vs. small banks, competing industries) explain deregulation timing better than public interest or political-institutional models.

A growing body of literature also examines the implications of OB for credit markets. Liu et al., (2024), show that granting borrowers ownership and control over their financial data enhances competition among lenders, reduces information asymmetry, and improves credit allocation efficiency. Similar results are reported by He, Huang and Zhou, (2023), in the context of BRICS economies, where OB frameworks are found to increase credit availability, particularly for underserved borrowers. Beyond immediate market outcomes, several studies situate OB regulation within broader institutional and political economy perspectives. Kroszner and Strahan, (1999) provide early evidence that regulatory change in financial markets is strongly influenced by private interest group dynamics rather than purely public interest considerations. These insights remain highly relevant for understanding contemporary OB reforms, where incumbent institutions, fintech entrants, and regulators often have competing incentives.

Finally, meta level analyses contribute to conceptual consolidation in this rapidly evolving field. De Araluze and Cassinello Plaza, (2022) bibliometric methods to map OB research, identifying dominant themes, emerging areas of inquiry, and persistent conceptual gaps. Complementing this perspective, Alhelaly et al. (2023) examine the intersection of data protection, regulatory technology, and digital identity, highlighting how user awareness and expectations mediate the effectiveness of institutional and regulatory frameworks.

 doi:10.20944/preprints202602.0867.v1

4.3. A Tri-Dimensional Framework for Open Banking

Beyond the technological and regulatory dimensions, this study proposes a tri dimensional analytical framework that positions behavioural cognition as a third and equally essential pillar of OB security and adoption (**Figure 3**). This ecosystem-based approach integrates behavioural insights into technological and regulatory design, recognising that SecTech, RegTech, and behavioural science applied to technology are deeply interconnected and mutually reinforcing.

The integration of technological innovation, regulatory oversight, and human behaviour has the potential to fundamentally reshape the design, adoption, and resilience of OB security systems (*Proceedings of the 2008 New Security Paradigms Workshop*, 2013). Rather than treating users as passive recipients of security controls, this approach acknowledges individuals as active participants whose perceptions, decisions, and behaviours directly influence system effectiveness (Ng, Kankanhalli and Xu, 2009; Safa et al., 2015). By aligning technical mechanisms and regulatory requirements with actual user behaviour, security solutions can become more robust, usable, and sustainable.

Incorporating behavioural insights into technological and regulatory frameworks enables more accurate anticipation of user actions and security risks. It reduces human error through user-centred design, strengthens trust through transparency and perceived control, and supports adoption by aligning security measures with users' cognitive capabilities and expectations. This tri-dimensional perspective therefore moves beyond purely technical or compliance driven models towards a human-centred security paradigm, in which protection, usability, and trust are treated as interdependent objectives (Han and Kim, 2018; Kitkowska et al., 2023). As a result, it enables adaptive, ethically aligned, and resilient security architectures capable of supporting the long-term evolution of digital finance and OB ecosystems.

Recent literature increasingly reflects this integrated view. Gozman, Hedman, and Sylvest (2018) examine the strategic and behavioural implications of OB by analysing how shifting roles, risks, and value creation opportunities emerge within digital financial ecosystems. Their findings highlight the importance of organisational strategy and behavioural adaptation in navigating OB environments. Pinochet et al. (2023) adopt a user-centred perspective, identifying behavioural determinants such as trust, perceived benefits, and institutional guarantees as key drivers of consumers' psychological intention to engage with OB applications. Similarly, Chan et al. (2022) develop a trust-based model of OB adoption, providing empirical evidence that users' perceptions of security, reliability, and value significantly shape behavioural intention under conditions of uncertainty.

Collectively, these studies demonstrate that OB research extends beyond technical infrastructures and regulatory mandates to encompass strategic decision making and user behaviour. This body of evidence reinforces the need for a tri dimensional framework that systematically examines the interaction between SecTech, RegTech, and security behaviour. Such a framework provides a more comprehensive lens for understanding OB adoption and risk and offers practical guidance for designing ecosystems that are secure, compliant, and aligned with human behaviour.

Figure 3. Technological, regulatory & behaviour integration Framework.

 doi:10.20944/preprints202602.0867.v1

Recognising that user centricity is fundamental to OB, this study advances a tri dimensional security framework that integrates technical mechanisms, regulatory structures, and behavioural dynamics. By embedding behavioural cognition alongside technological and policy dimensions, the model reflects real world security practices, behavioural intentions, and adoption challenges across diverse regulatory and cultural contexts (Alsharida et al., 2023). This integrated approach provides a more realistic and user focused foundation for analysing security in OB ecosystems and supports the development of resilient, trusted, and inclusive digital financial services.

5. Discussion

5.1. Comparative Implications

The reviewed empirical literature reveals a clear distinction between studies that focus on the technological and security foundations of OB and those that examine regulatory, policy, and market dimensions (Kroszner and Strahan, 1999; Modesti et al., 2025). However, the persistent separation between technological and regulatory perspectives results in an incomplete understanding of OB security. Integrating behavioural considerations as a third analytical dimension enables a more comprehensive interpretation of how technological controls, regulatory objectives, and user security behaviour interact to shape effective security practices (Buckley, Caulfield and Becker, 2024). This integrated approach clarifies the dynamics underpinning organisational security decisions, regulatory enforcement, and market responses.

A systematic comparison demonstrates that technological and regulatory research streams are largely complementary. Technological studies provide insights into the secure and efficient operational implementation of OB, particularly in relation to APIs, authentication, and data protection mechanisms. In contrast, regulatory and market analyses focus on the institutional drivers of OB adoption, policy rationales, and broader economic implications (Casolaro et al. 2024; Jafri et al. 2024). Yet, when examined in isolation, these perspectives fail to capture how regulatory intent influences technical design choices, or how technological constraints shape regulatory effectiveness.

This separation underscores the need for integrative research that explicitly connects technological innovation with regulatory objectives and behavioural realities. Aligning security implementation practices with policy goals and user behaviour is critical for achieving regulatory compliance, trust, and sustained adoption (Esmaeilzadeh, 2020). While existing scholarship has advanced understanding of OB architecture, governance models, and market effects, further research is required to link regulatory ambition, technological execution, and user security behaviour within a unified analytical framework. Such integration is essential for translating policy frameworks into effective, real-world security outcomes.

5.2. Limitations and Future Research

Although research on OB has grown substantially, most studies remain confined to specific disciplinary perspectives. Technological research primarily concentrates on APIs, authentication protocols, and security mechanisms, while policy-oriented studies focus on regulatory frameworks, data sharing mandates, and market competition (Banerjee, 2024; Torshin, 2025). The limited integration of behavioural, technological, and regulatory perspectives restricts understanding of how user-centred security practices coevolve within the OB ecosystem.

Geographically, the literature is heavily concentrated in advanced economies with mature digital infrastructures, particularly the United Kingdom, the European Union, and Australia. Developing regions in Africa, Latin America, and parts of Asia remain underrepresented, constraining comparative analysis of regulatory effectiveness, technological readiness, and consumer trust across diverse institutional contexts. This imbalance limits the generalisability of existing findings and overlooks regions where OB may offer significant benefits for financial inclusion.

Methodological limitations are also evident. Many studies rely on cross sectional surveys, secondary datasets, or single country case studies, which restrict causal inference and longitudinal

 doi:10.20944/preprints202602.0867.v1

understanding. There remains a lack of comparative and multi-level research designs that link micro level user behaviour and security practices to macro level regulatory outcomes and market structures. In particular, user security behaviour remains underexplored, despite its central role in shaping adoption intentions, trust formation, and system resilience in Open systems.

Future research should adopt interdisciplinary approaches that integrate regulatory analysis, technological design, and behavioural science. The use of cross-regional datasets combining regulatory indicators, technology adoption metrics, and user behavioural measures would enable deeper examination of interactions between policy, infrastructure, and consumer practices. Longitudinal and comparative studies are particularly needed to assess how trust, security behaviour, and regulatory effectiveness evolve over time. Strengthening empirical attention to user security behaviour is essential for promoting secure, confident, and sustainable engagement with OB services.

6. Conclusions

This paper provides a comprehensive review of the literature on security challenges in OB, offering a comparative analysis of studies addressing technological and security foundations alongside those examining regulatory, policy, and market dimensions (Blihar et al., 2020). The review identifies a critical gap in existing research, namely the limited consideration of behavioural factors, and responds by proposing the operationalisation of a tri dimensional OB security framework.

The findings indicate that technological studies predominantly focus on data protection, authentication mechanisms, and secure API design, while regulatory and market-oriented research emphasises governance structures, data ownership, and the promotion of competition and innovation. When considered independently, these perspectives provide only a partial understanding of OB security. Incorporating behavioural considerations is essential, as user perceptions, trust, and security practices directly influence adoption, compliance, and system resilience.

By integrating technological, regulatory, and behavioural dimensions, this study advances a more holistic understanding of OB security. The proposed tri dimensional framework facilitates alignment between technical standards, regulatory coordination, market readiness, and user behaviour. Achieving a secure, trusted, and effective OB ecosystem therefore requires the combined and coordinated consideration of technology, regulation, and security behaviour. This integrated perspective provides valuable guidance for researchers, practitioners, and policymakers seeking to design resilient and user-centred OB systems.

Supplementary Materials: The following supporting information can be downloaded at the website of this paper posted on Preprints.org.

References

Aboobucker, I., & Bao, Y. (2018). What obstructs customer acceptance of Internet banking? Security and privacy, risk, trust, and website usability and the role of moderators. Journal of High Technology Management Research, 29(1), 109–123. https://doi.org/10.1016/j.hitech.2018.04.010

Adiningtyas, H., & Auliani, A. S. (2024). Sentiment analysis for mobile banking service quality measurement. Procedia Computer Science, 40-50. https://doi.org/10.1016/j.procs.2024.02.150

Akyildirim, E., Corbet, S., Sensoy, A., & Yarovaya, L. (2025). Global perspectives on open banking: Regulatory impacts and market response. Journal of International Financial Markets, Institutions and Money, 101, 102159. https://doi.org/10.1016/j.intfin.2025.102159

Alhelaly, Y., Dhillon, G., & Oliveira, T. (2023). When expectation fails and motivation prevails: The mediating role of awareness in bridging the expectancy-capability gap in mobile identity protection. Computers & Security, 134, Article 103470. https://doi.org/10.1016/j.cose.2023.103470

 doi:10.20944/preprints202602.0867.v1

Alhelaly, Y., Dhillon, G., & Oliveira, T. (2025). The impact of privacy intrusiveness on individuals' responses and engagement toward personalisation in online interactive advertising. Journal of Interactive Advertising, 25(1), 38–60. https://www.tandfonline.com/doi/epdf/10.1080/15252019.2024.2440318?needAccess=true

Alsharida, R. A., Alotaibi, A., Alharbi, M., & Alshehri, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. Technology in Society, 73, Article 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. Journal of Information Security and Applications, 48, Article 102376. https://doi.org/10.1016/j.jisa.2019.06.008

Anderson, R. E., Babin, B. J., Black, W. C., & Hair, J. F. (2010). Multivariate data analysis (7th ed.). Prentice Hall.

Amin, H. (2007). Internet banking adoption among young intellectuals. Journal of Internet Banking and Commerce. http://www.arraydev.com/commerce/jibc/

Araluze, G. K. B. de, & Cassinello Plaza, N. (2022). Open banking: A bibliometric analysis-driven definition. PLOS ONE, 17(10), Article e0275496. https://doi.org/10.1371/journal.pone.0275496

Arner, D. W., Barberis, J., Buckley, R. P., & Zetzsche, D. A. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. Northwestern Journal of International Law & Business. http://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2

Armitage, C. J., & Conner, M. (2010). Efficacy of the theory of planned behaviour: A meta-analytic review. British Journal of Social Psychology, 40(4), 471–499. https://doi.org/10.1348/014466601164939

Association for Computing Machinery (ACM). (2013). Proceedings of the 2008 New Security Paradigms Workshop. ACM Digital Library.

Australian Competition and Consumer Commission (ACCC). (2025). Targeting scams II: Report of the National Anti-Scam Centre on scams data and activity 2024. https://www.accc.gov.au

AWS. (2024). Financial services industry lens: AWS Well-Architected Framework. https://docs.aws.amazon.com/wellarchitected/latest/financial-services-industry-lens/welcome.html

Blihar, D., Delgado, J. L., Bury, D., & González, J. (2020). A systematic review of the neuroanatomy of dissociative identity disorder. European Journal of Trauma & Dissociation, 4(3), 100148. https://doi.org/10.1016/j.ejtd.2020.100148

Babina, T., & Howell, S. T. (2024). Entrepreneurial spillovers from corporate R&D. Journal of Labor Economics, 42(2), 469–509. https://doi.org/10.1086/723501

Babina, T., Boot, A. W. A., & Penas, M. F. (2025). Customer data access and fintech entry: Early evidence from open banking. Journal of Financial Economics, 169, Article 103950. https://doi.org/10.1016/j.jfineco.2024.103950

Banerjee, P. (2024). System integration, from middleware to APIs. International Journal of Computer Trends and Technology, 72(3), 37–45. https://doi.org/10.14445/22312803/ijctt-v72i3p106

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. Journal of the ACM, 55(3). https://doi.org/10.1145/1595676.1595684

BNA. (2023). Fintech and innovation. The National Bank of Angola. https://www.bna.ao/#/pt/sistema-de-pagamento/prestacao-tecnologia-financeira/detalhe/4

Braithwaite, J. (2024). "Authorized push payment" bank fraud: What does an effective regulatory response look like? Journal of Financial Regulation, 10(2), 174–193. https://doi.org/10.1093/jfr/fjae006

Buckley, G., Caulfield, T., & Becker, I. (2024). How might the GDPR evolve? A question of politics, pace and punishment. Computer Law & Security Review, 54, 106033. https://doi.org/10.1016/j.clsr.2024.106033

Cardoso, S., & Martinez, L. F. (2019). Online payments strategy: How third-party Internet seals of approval and payment provider reputation influence Millennials' online transactions. Electronic Commerce Research, 19(1), 189–209. https://doi.org/10.1007/s10660-018-9295-x

Casolaro, A. M. B., Rauber, G. N., & de Lima, U. S. M. (2024). Open banking: A systematic literature review. Journal of Banking Regulation. https://doi.org/10.1057/s41261-024-00262-x

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. Online Information Review, 31(5), 583–603. https://doi.org/10.1108/14684520710832315

 doi:10.20944/preprints202602.0867.v1

CBK. (2024). Banking sector innovation survey 2024. Central Bank of Kenya. https://www.centralbank.go.ke/2025/05/09/11296/

CBN. (2021). Regulatory framework for open banking in Nigeria. Central Bank of Nigeria. https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf

CBN. (2023). Operational guidelines for open banking in Nigeria. Central Bank of Nigeria. https://www.cbn.gov.ng/Out/2023/CCD/Operational%20Guidelines%20for%20Open%20Banking%20in%20Nigeria.pdf

Chan, R., Lee, V., & Wong, P. (2022). Towards an understanding of consumers' FinTech adoption: The case of open banking. International Journal of Bank Marketing, 40(4), 886–917. https://doi.org/10.1108/IJBM-08-2021-0397

Chen, P. H. A., Jolly, E., Cheong, J. H., Chang, L. J., & Wager, T. D. (2020). Intersubject representational similarity analysis reveals individual variations in affective experience when watching erotic movies. NeuroImage, 216, 116851. https://doi.org/10.1016/j.neuroimage.2020.116851

Colangelo, G. (2024). Open banking goes to Washington: Lessons from the EU on regulatory-driven data sharing regimes. Computer Law & Security Review, 54, Article 106018. https://doi.org/10.1016/j.clsr.2024.106018

Colangelo, G., & Khandelwal, P. (2025). The many shades of open banking: A comparative analysis of rationales and models. Internet Policy Review, 14(1), 1821. https://doi.org/10.14763/2025.1.1821

Correia, R., & Tam, C. (2025). Understanding the motivations for continuance usage of mobile apps. Journal of Computer Information Systems, 65(4), 474–488. https://doi.org/10.1080/08874417.2024.2302001

Daneshgadeh, S., & Yıldırım, S. Ö. (2014). Empirical investigation of Internet banking usage: The case of Turkey. Procedia Technology, 16, 322–331. https://doi.org/10.1016/j.protcy.2014.10.098

Desiraju, K., Mishra, A. N., & Sengupta, P. (2024). Customer perceptions on open banking apps: Insights using structural topic modelling. Journal of Retailing and Consumer Services, 81, Article 104029. https://doi.org/10.1016/j.jretconser.2024.104029

Dinçkol, D., Ozcan, P., & Zachariadis, M. (2023). Regulatory standards and consequences for industry architecture: The case of UK open banking. Research Policy, 52(6), 104760. https://doi.org/10.1016/j.respol.2023.104760

EDPB. (2020). Payment Services Directive and the GDPR. European Data Protection Board. https://www.fca.org.uk/firms/future-open-banking-joint-regulatory-oversight-committee

Esmaeilzadeh, P. (2020). The effect of the privacy policy of health information exchange on patients' information disclosure intention. Computers & Security, 95, 101819. https://doi.org/10.1016/j.cose.2020.101819

European Banking Authority (EBA). (2011). https://www.eba.europa.eu/

European Commission. (2007). Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance). Commission Européenne. https://ec.europa.eu/commission/presscorner/detail/fr/memo_15_5793

European Data Protection Board (EDPB). (2020). The future of open banking and the Joint Regulatory Oversight Committee. https://www.fca.org.uk/firms/future-open-banking-joint-regulatory-oversight-committee

Ege Oruç, Ö., & Tatar, Ç. (2017). An investigation of factors that affect internet banking usage based on structural equation modeling. Computers in Human Behavior, 66, 232–235. https://doi.org/10.1016/j.chb.2016.09.059

European Union Agency for Cybersecurity (ENISA). (2024). Guidelines on security measures under the General Data Protection Regulation (GDPR). https://www.enisa.europa.eu/topics/digital-identity-and-data-protection/cryptography

Fang, J., & Zhu, J. (2023). The impact of open banking on traditional lending in the BRICS. Finance Research Letters, 58, 104300. https://doi.org/10.1016/j.frl.2023.104300

FCA. (2024). The future of open banking and the Joint Regulatory Oversight Committee. Financial Conduct Authority UK. https://www.fca.org.uk/firms/future-open-banking-joint-regulatory-oversight-committee

Fett, D., Hosseyni, P., & Kuesters, R. (2019). An extensive formal security analysis of the OpenID Financial-grade API. IEEE. https://doi.org/10.48550/arXiv.1901.11520

 doi:10.20944/preprints202602.0867.v1

Frei, C. (2023). Open banking: Opportunities and risks. Electronic Journal, 167–189. https://doi.org/10.1007/978-3-031-23069-1_7

Gill, S. S., Singh, P., & Gupta, A. (2019). Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: Evolution, vision, trends and open challenges. Internet of Things. https://doi.org/10.1016/j.iot.2019.100118

Gimigliano, G., & Božina Beroš, M. (2021). The payment services directive II. Edward Elgar Publishing Ltd. https://www.elgaronline.com/edcollbook/edcoll/9781839105678/9781839105678.xml?rskey=DCUHCf&result=1

Gounari, M., Stavropoulos, T., & Katsikas, S. (2024). Harmonizing open banking in the European Union: An analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. International Cybersecurity Law Review, 5(1), 79–120. https://doi.org/10.1365/s43439-023-00108-8

GOV.AE. (2021). Federal Decree-Law No. (33) of 2021 regarding the regulation of employment relationship and its amendments. Ministry of Human Resources & Emiratisation.

GOV.BR. (2018). Brazilian Data Protection Law (LGPD). https://falabr.cgu.gov.br/

Gozman, D., Hedman, J., & Sylvest, K. (2018). Open banking: Emergent roles, risks, and opportunities. Investopedia.

Greene, C., Hancock, D., & Wilcox, J. (2014). Costs and benefits of building faster payment systems: The U.K. experience and implications for the United States. Federal Reserve Bank of Boston.

Hanafizadeh, P., Keating, B. W., & Khedmatgozar, H. R. (2014). A systematic review of Internet banking adoption. Telematics and Informatics, 31(3), 492–510. https://doi.org/10.1016/j.tele.2013.04.003

Hanif, Y., & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+): A mixed-method study using modified UTAUT and MTAM—with perceived cybersecurity, risk, and trust. Technology in Society, 67, 101693. https://doi.org/10.1016/j.techsoc.2021.101693

Han, J., & Kim, H. (2018). Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective. Information Technology & People, 32(2). https://doi.org/10.1108/ITP-09-2017-0298

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM) (2nd ed.). Springer.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2021). Classroom companion: Business partial least squares structural equation modeling (PLS-SEM) using R. Springer. http://www.springer.com

He, Z., Huang, J., & Zhou, J. (2023). Open banking: Credit market competition when borrowers own the data. Journal of Financial Economics, 147(2), 449–474. https://doi.org/10.1016/j.jfineco.2022.12.003

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. Expert Systems with Applications. https://doi.org/10.1016/j.eswa.2021.116429

Hyon, R., Kleinbaum, A. M., & Parkinson, C. (2020). Social network proximity predicts similar trajectories of psychological states: Evidence from multi voxel spatiotemporal dynamics. NeuroImage, 216, Article 116492.

https://doi.org/10.1016/j.neuroimage.2019.116492

Jafri, J. A., Rehman, M., & Shah, S. (2024). A systematic literature review of the role of trust and security on fintech adoption in banking. Heliyon. https://doi.org/10.1016/j.heliyon.2023.e22980

Kroszner, R. S., & Strahan, P. E. (1999). What drives deregulation? Economics and politics of the relaxation of bank branching restrictions. Oxford Academic.

Laplante, P. A., & Kshetri, N. (2021). Open banking: Definition and description. Computer, 54(10), 122–128. https://doi.org/10.1109/MC.2021.3055909

Li, J., Chen, T., & Zhao, L. (2023). Security and privacy problems in voice assistant applications: A survey. Computers & Security, 134, 103448. https://doi.org/10.1016/j.cose.2023.103448

Liao, C. H., Wu, C., & Lin, Y. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. Future Generation Computer Systems, 135, 450–466. https://doi.org/10.1016/j.future.2022.05.015

 doi:10.20944/preprints202602.0867.v1

Ling, G. M., Tan, H., & Lim, S. (2016). Understanding customer satisfaction of internet banking: A case study in Malacca. Procedia Economics and Finance, 37, 80–85. https://doi.org/10.1016/s2212-5671(16)30096-x

Liu, J., Oliveira, T., & Wang, H. (2024). The open banking era: An optimal model for the emergency fund. Expert Systems with Applications, 244, 122915. https://doi.org/10.1016/j.eswa.2023.122915

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. International Journal of Information Management, 34(1), 1–13. https://doi.org/10.1016/j.ijinfomgt.2013.06.002

Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. Technology in Society, 59, 101151. https://doi.org/10.1016/j.techsoc.2019.101151

Modesti, P., Rossi, F., & Bianchi, L. (2025). Security analysis of the open banking account and transaction API protocol. Cyber Security and Applications, 3, 100097. https://doi.org/10.1016/j.csa.2025.100097

Moody, G. D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. Information and Management, 50(6), 322–335. https://doi.org/10.1016/j.im.2013.04.005

Ng, B. Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Ngan, J. (2025). 'The view from below': Resistance and change in authorised push payment fraud. Journal of Economic Criminology, 9, 100166. https://doi.org/10.1016/j.jeconc.2025.100166

Nikkhah, H. R., Grover, V., & Sabherwal, R. (2024). Post hoc security and privacy concerns in mobile apps: The moderating roles of mobile apps' features and providers. Information and Computer Security, 32(1), 1–37. https://doi.org/10.1108/ICS-02-2023-0015

Niranjan, S. K., Raja, J., & Rajini, A. R. (2018). Proceedings of the 2018 International Conference on Communication, Computing & Internet of Things: IC3IoT 2018, 15–17 February 2018, Dept. of Electronics and Communication Engineering, Sri Sairam Engineering College, Chennai, India. IEEE.

Official Journal of the European Union. (2015). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366

Official Journal of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. Computers in Human Behavior, 61, 404–414. https://doi.org/10.1016/j.chb.2016.03.030

Oliveira, T., Rosario Oliveira Martins, M., & Fraga Martins, M. (2011). Literature review of information technology adoption models at firm level. The Electronic Journal Information Systems Evaluation, 14, 110.

Omarini, A. E. (2018). Banks and fintechs: How to develop a digital open banking approach for the bank's future. International Business Research, 11(9), 23. https://doi.org/10.5539/ibr.v11n9p23

OWASP. (2023). API security top 10. https://owasp.org/API-Security/

Patrick Njoroge. (2022). The Central Bank of Kenya Act. Central Bank of Kenya. https://new.kenyalaw.org/akn/ke/act/ln/2022/46/eng%402022-04-22?utm_source=chatgpt.com

Pinochet, L. H. C., Silva, R., & Gomes, T. (2023). Predicting the intention to use the investment aggregate functionality in the context of open banking using the artificial neural network approach. Procedia Computer Science, 733–740. https://doi.org/10.1016/j.procs.2023.08.045

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Puschmann, T. (2017). Fintech. Business and Information Systems Engineering, 59(1), 69–76. https://doi.org/10.1007/s12599-017-0464-6

PwC Netherlands. (2025). PSD2 in Europe: The start to a new future of banking? https://www.pwc.nl/en/industries/financiele-sector/risk-and-regulation/psd2-in-europe.html

RBI. (2025). Rethinking regulations in an interconnected financial system. Reserve Bank of India. https://rbi.org.in/scripts/BS_ViewBulletin.aspx?Id=23579

Safa, N. S., Von Solms, R., & Furnell, S. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Serrado, J., Hernantes, J., & Gallardo, G. (2020). Information security frameworks for assisting GDPR compliance in the banking industry. Digital Policy, Regulation and Governance, 22(3), 227–244. https://doi.org/10.1108/DPRG-02-2020-0019

Souza, C., & Redmiles, D. (2009). On the roles of APIs in the coordination of collaborative software development. Computer Supported Cooperative Work, 18, 445–475. https://doi.org/10.1007/s10606-009-9101-3

Strahan, P. E., & Cetorelli, N. (2004). Finance as a barrier to entry: Bank competition and industry structure in local U.S. markets. National Bureau of Economic Research.

Takieddine, S., & Sun, J. (2015). Internet banking diffusion: A country-level analysis. Electronic Commerce Research and Applications, 14(5), 361–371. https://doi.org/10.1016/j.elerap.2015.06.001

Tam, C., & Oliveira, T. (2017). Literature review of mobile banking and individual performance. International Journal of Bank Marketing, 1042–1065. https://doi.org/10.1108/IJBM-09-2015-0143

Tam, C., Santos, D., & Oliveira, T. (2020). Exploring the influential factors of continuance intention to use mobile apps: Extending the expectation confirmation model. Information Systems Frontiers, 22(1), 243–257. https://doi.org/10.1007/s10796-018-9864-5

Tan, M., & Teo, T. (2000). Factors influencing the adoption of internet banking. Journal of the Association for Information Systems, 1(1), 1–44. https://doi.org/10.17705/1jais.00005

Tariq, M., Maryam, S. Z., & Shaheen, W. A. (2024). Cognitive factors and actual usage of fintech innovation: Exploring the UTAUT framework for digital banking. Heliyon, 10(15), e35582. https://doi.org/10.1016/j.heliyon.2024.e35582

Torshin, I. (2025). Open banking and API-driven financial innovation: Opportunities and risks. https://www.researchgate.net/publication/390486463

Vanini, P., Rossi, M., & Bianchi, L. (2023). Online payment fraud: From anomaly detection to risk management. Financial Innovation, 9(1), 470. https://doi.org/10.1186/s40854-023-00470-w

Waliullah, M., Rahman, M. M., Hossain, M. A., & Islam, M. S. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. American Journal of Advanced Technology and Engineering Solutions, 1(1), 226–257. https://doi.org/10.63125/fh49gz18

Wang, S., Zhang, Y., Liu, H., & Chen, X. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Computers & Security, 147, Article 104051.
https://doi.org/10.1016/j.cose.2024.104051

Xu, Z., Chen, Y., & Li, H. (2020). PPM: A provenance-provided data sharing model for open banking via blockchain. ACM International Conference Proceeding Series. https://doi.org/10.1145/3373017.3373022

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. Computers in Human Behavior, 26(4), 760–767. https://doi.org/10.1016/j.chb.2010.01.013