Smart Technologies Academic Press

**Jordanian Journal of Informatics and Computing**
https://www.jjic.thestap.com/

JORDANIAN JOURNAL OF INFORMATICS AND COMPUTING

STAP

# Securing API Ecosystems in Banking: A Critical Review of Cyber Risks, Control Frameworks, and Future Trends

**Sopheaktra Huy,** [1] **Sokroeurn Ang,** [1] **Mony Ho,** [1] **Vivekanandam Balasubramaniam** [1]

[1] *AI Computing and Multimedia Department, Lincoln Graduate Program, Doctor in Cybersecurity, Lincoln University College, Malaysia*

## ARTICLE INFO

**Article History**

| | |
|---|---|
| **Received:** | **30-10-2025** |
| **Revised:** | **25-12-2025** |
| **Accepted:** | **10-01-2026** |
| **Published:** | **15-01-2026** |

**Vol.2026, No.1**

**DOI:**

***Corresponding author. Email:*** *hsopheaktra.phdscholar@lincoln.edu.my*

**Orcid:**

https://orcid.org/0009-0006-7383-1667

Published by STAP Publisher.

## ABSTRACT

The rapid evolution of open banking and digital financial services has fueled the widespread adoption of Application Programming Interfaces (APIs) across the banking sector. While APIs enable real-time payments, embedded finance, and seamless integration with third-party platforms, they simultaneously introduce critical cybersecurity risks including misconfigurations, excessive data exposure, broken authentication, and weak access controls. This review critically investigates the cyber threat landscape of financial APIs by synthesizing academic literature, industry frameworks, and real-world breach reports. It evaluates the practical effectiveness of controls such as the OWASP API Security Top 10, Financial-grade API (FAPI) standards, and Zero Trust Architecture, and explores the emerging role of AI-driven security models including machine learning, deep learning, and Bayesian attack graph modeling. The key findings reveal persistent implementation gaps despite available standards, with real-world breaches like Twilio and Dell highlighting the high-risk exposure of unsecured APIs. The review also uncovers fragmented regulatory maturity between jurisdictions: while the EU leads with structured mandates like PSD2, the US and UK adopt more market-driven, inconsistent approaches posing challenges for global financial compliance. Furthermore, the study identifies underexplored threat vectors such as insider misuse, unmanaged shadow APIs, and third-party abuse areas rarely addressed in existing frameworks. Most importantly, it emphasizes a critical lack of integration between technical controls, regulatory policies, and lifecycle security implementation in real-world banking environments. This paper concludes with forward-looking recommendations to enhance API resilience through layered defenses, global regulatory alignment, AI-enhanced threat detection, and embedding security within software development pipelines.

**Keywords:** API Security, Open Banking, Cyber Risk Management, Zero Trust Architecture, Financial-Grade API, Artificial Intelligent (AI), Machine Learning (ML).

**How to cite the article**

## 1. Introduction

The rise of digital transformation in banking has driven the widespread adoption of Application Programming Interfaces (APIs) to boost interoperability, customer experience, and third-party integrations. Modern banks now rely on APIs to seamlessly integrate with e-commerce platforms, tourism agencies, insurance providers, and retail companies, enabling real-time payments, embedded finance, and open banking services. APIs function as core enablers for payment infrastructures and business-to-business integration, transforming financial institutions into ecosystem platforms rather than standalone service providers. Historically, banking systems were built around monolithic architectures and tightly coupled integrations that limited agility and scalability. The emergence of RESTful APIs, JSON-based data exchange, and cloud-native applications has transformed this landscape. Financial institutions have shifted toward modular, service-oriented architectures, where APIs now act as intermediaries between internal systems and external partners. This shift has accelerated innovation but simultaneously broadened the attack surface, necessitating a reassessment of security protocols and risk governance frameworks.

However, this growing connectivity brings significant cybersecurity challenges. APIs have become a major attack surface due to improper access control, excessive data exposure, and weak authentication mechanisms. Real-world breaches—such as the Twilio Authy breach, which exposed 33.4 million phone numbers, and the Dell API vulnerability, which compromised 49 million customer records—highlight the urgent need for robust API security frameworks [1], [2]. In the financial domain, such breaches can lead to fraud, data theft, regulatory violations, and reputational damage. Academic and industry research has proposed multiple mitigation strategies, including Bayesian attack modeling [3], machine learning-based anomaly detection [4], and deep learning-based API threat classification [5]. Best practices and frameworks such as the OWASP API Security Top 10 [6] and Financial-grade API (FAPI) Security Profile [7] have been introduced to guide developers and institutions in safeguarding these critical systems. In addition, comparative analyses across the US, UK, and EU illustrate differing regulatory maturity levels in addressing Open Banking API threats [8].

Despite these efforts, most existing studies focus narrowly on either technical controls or specific regulatory mandates. There is a lack of holistic reviews that combine cyber risk modeling, security frameworks, and forward-looking trends specific to banking APIs. This study aims to fill that gap by critically reviewing the current API threat landscape, existing control mechanisms, and future trends in securing financial API ecosystems. The remainder of this paper is structured as follows:

- Section 2 reviews existing literature on API vulnerabilities, cyber risk modeling, security frameworks, and regulatory approaches.
- Section 3 describes the methodology used for selecting and analyzing the reviewed sources.
- Section 4 presents the key findings, covering major cyber risks, security controls, regulatory gaps, and future trends.
- Section 5 concludes the paper with a summary of findings and practical recommendations for banking and cybersecurity professionals.

## 2. Literature Review

### *2.1 Overview of API Usage in Banking*

The evolution of banking systems has increasingly leaned on API-driven architectures to foster interoperability, accelerate innovation, and enable open banking initiatives. APIs are now integral to connecting banks with fintech platforms, merchants, insurers, and service providers. This integration facilitates real-time payments, customer data exchange, and embedded financial services [6], [14], [15].

Open banking has emerged as a transformative movement underpinned by APIs. Literature such as Casolaro et al. [8] and Ranjan & Haider [10] offers comprehensive reviews of how open banking frameworks enable data-sharing mandates, empower consumer choice, and foster competitive financial ecosystems. Adanigbo et al. [18] explore API-driven innovation in emerging economies, emphasizing cost efficiency and scalability. Additionally, bibliometric analyses underscore the growing interdisciplinary interest in Open Banking APIs and their evolving definitions [9].

Recent studies also highlight consumer behavior in the context of data sharing. Grassi [5] analyzes the interplay between trust and consumer willingness to engage with API-enabled services in insurance and finance. These developments collectively signal a shift toward financial platforms as ecosystem orchestrators, supported by API strategies. Industry commentary also reflects how Open Banking APIs are fueling innovation and collaboration within fintech ecosystems [28].

### *2.2 API Vulnerabilities and Cybersecurity Incidents*

Despite their transformative benefits, APIs have introduced critical cybersecurity vulnerabilities into the banking ecosystem. Misconfigurations, improper authentication, and excessive data exposure are among the most frequently exploited weaknesses in API environments [45]. These flaws have made APIs an attractive target for cybercriminals and nation-state actors. Actual breach events emphasize the critical nature of security flaws within API ecosystems. In 2024, the Twilio Authy breach exposed 33.4 million phone numbers due to unauthenticated API access [1], and a Dell API vulnerability compromised the data of 49 million customers [2]. Similar flaws were identified in Cox Communications' infrastructure, where an API bug allowed unauthorized access to millions of modems [23]. These cases demonstrate the significant consequences of insecure APIs—ranging from privacy violations to large-scale data theft.

The financial sector has not been spared. According to The Australian, banks in Australia were targeted in a global cyber heist orchestrated by sophisticated attackers exploiting API and telecom weaknesses [24]. Another case revealed how retirement fund APIs were breached due to outdated security controls that had not been patched, even after known vulnerabilities were disclosed [25]. Scholars have emphasized that these incidents are not isolated but represent a pattern of negligence in implementing security-by-design principles. As noted by Alam et al. [20], API vulnerabilities often stem from the rapid deployment of services without thorough threat modeling or penetration testing. Similarly, Wan et al. [45] provide an empirical analysis of access control flaws across cloud-based financial APIs, underscoring the urgency for adopting standardized, validated security models. In summary, API vulnerabilities pose a systemic risk to digital banking operations. Real-world breach data and empirical research converge on the conclusion that without robust governance and security controls, APIs become a single point of failure with widespread impact.

### *2.3 Cyber Risk Modeling and Threat Detection*

To mitigate the growing risk landscape of API ecosystems, researchers have proposed various risk modeling and threat detection techniques, ranging from probabilistic frameworks to intelligent algorithms. One of the most promising approaches is Bayesian attack graphs facilitate forecasting potential API exploitation routes grounded in existing weaknesses and interdependencies. Behbehani et al. [3] applied this method in the context of open banking, demonstrating its usefulness in dynamically analyzing the threat propagation in API interactions. Another active area of research involves machine learning (ML) and genetic algorithm-based models. Dhaiya et al. [4], [7] proposed a hybrid ML approach that leverages historical data and feature optimization to detect anomalies in API request patterns. Their results showed substantial improvements in precision and recall for identifying malicious API traffic in FinTech platforms.

Deep learning has also emerged as a viable technique for enhancing API threat detection. Alam et al. [42] used a combination of convolutional neural networks (CNNs) and long short-term memory (LSTM) models to classify malicious API behaviors. Their deep learning framework achieved high accuracy rates in identifying zero-day API threats, making it particularly useful for adaptive security environments. Complementing these models, several studies have explored AI-enabled multi-layered defense mechanisms. Ramakrishnan [44] discussed the application of artificial intelligence to proactively detect, classify, and respond to threats in real time. Kephart and Guha [40] proposed a layered architecture combining anomaly detection, signature analysis, and behavior monitoring using AI.

Moreover, the automation of risk analysis through ML algorithms has gained attention as a means to address scale and complexity. Techniques such as unsupervised clustering, decision trees, and reinforcement learning are being explored to continuously assess API exposure risk levels based on evolving attack vectors [12]. Overall, cyber risk modeling has evolved beyond static checklists and into intelligent, dynamic systems. The integration of AI and ML technologies into API threat detection frameworks marks a significant advancement in how financial institutions can proactively safeguard their API infrastructure.

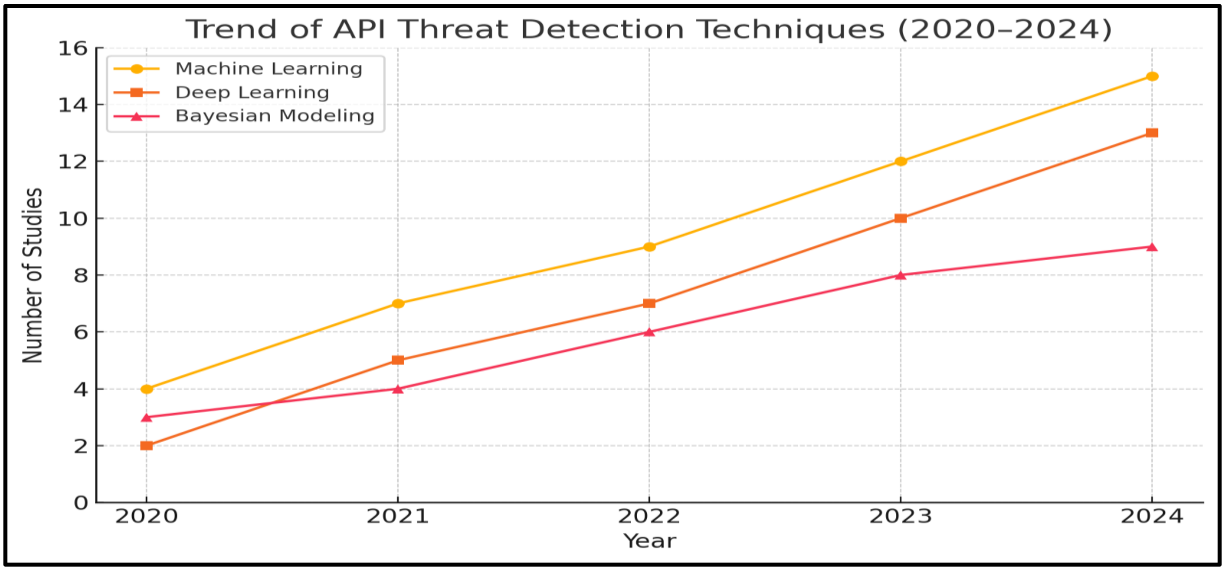

**Figure 1**. Trend of API Threat Detection Techniques (2020-2024)

*2.4 Security Frameworks and Best Practices*

As APIs become central to digital banking, various security frameworks and best practices have been established to standardize protections and reduce vulnerabilities. Among the most widely recognized is the OWASP API Security Top 10, which identifies the most critical security risks facing APIs, such as Broken Object Level Authorization, Excessive Data Exposure, and Security Misconfiguration [29]. This framework has become the de facto baseline for API security assessment across industries. In the financial domain, the Financial-grade API (FAPI) Security Profile developed by the OpenID Foundation [30] provides a high-assurance standard tailored to protect APIs handling sensitive financial data. FAPI mandates advanced requirements for token binding, dynamic client registration, and proof-of-possession mechanisms to prevent token leakage and replay attacks. It has been widely adopted by Open Banking implementations in the UK, EU, and parts of Asia. From a broader architectural standpoint**,** Zero Trust principles have gained traction as a forward-looking approach to API security. According to NIST's Zero Trust Architecture framework [35], no component—internal or external—should be trusted by default. In API ecosystems, this implies continuous verification, strict access controls, and micro-segmentation of services. Organizations like Akamai [36] and ENISA [38] have further emphasized Zero Trust as a critical strategy for API exposure management and runtime security.

Cloud-native security frameworks also stress the need for runtime protection and behavioral enforcement of APIs. These frameworks leverage container-level isolation, API gateways with integrated rate-limiting and IP whitelisting, and encrypted service mesh communication protocols. Salt Security's 2024 State of API Security Report [37] illustrates how runtime posture management has helped banks prevent abuse from bots, misconfigured endpoints, and internal threat actors. Beyond technical standards, governance best practices such as continuous monitoring, vulnerability disclosure programs, and secure development lifecycle integration are encouraged by industry leaders. These practices promote a shift-left security culture, ensuring API vulnerabilities are detected and mitigated early in the software lifecycle. In summary, while no single framework offers complete protection, combining OWASP guidance, FAPI profiles, and Zero Trust principles offers a robust foundation for securing banking APIs. The application of these best practices enhances resilience, supports compliance, and fosters stakeholder confidence in digital financial ecosystems.

*2.5 Regulatory and Comparative Perspectives*

The regulation of API ecosystems—particularly in the context of Open Banking—varies significantly across jurisdictions, reflecting differences in financial maturity, privacy mandates, and technological adoption. Regulatory authorities have increasingly recognized the importance of API security as financial institutions transition toward more open, interconnected infrastructures. In the United States**,** API-related regulations are guided by evolving initiatives from the Consumer Financial Protection Bureau (CFPB) and frameworks such as NIST SP 800-207 on Zero Trust Architecture [35]. In April 2024, the Financial Times reported that the U.S. rolled out new open banking rules to improve the transparency and security of financial data sharing, aiming to standardize API requirements for banks and third-party providers [31]. In contrast, the United Kingdom has implemented a more centralized and prescriptive approach through the Open Banking Implementation Entity (OBIE). Case studies such as Citizens Bank [26] and Barclays [27] illustrate successful integrations of regulated API platforms that prioritize consumer protection, consent management, and secure interoperability. Within the European Union, regulatory guidance is enforced through the Revised Payment Services Directive (PSD2), supported by API specifications from institutions like the European Banking Authority (EBA) and the Central Bank of Oman [33]. These frameworks mandate secure customer authentication (SCA), data minimization, and consent-driven data access policies. Bansal et al. [41] compare the API cybersecurity posture across the US, UK, and EU, noting that the EU exhibits a more robust, compliance-centric API governance structure.

International comparative research also reflects divergent levels of enforcement and ecosystem readiness. Colangelo and Khandelwal [43] analyze the "many shades" of open banking models and suggest that fragmentation in API standards could lead to compliance gaps and increased security risk, particularly for multinational banks operating across jurisdictions. Several private-sector whitepapers, such as those by Traceable AI [32], underscore the challenge of aligning API security with overlapping regulatory demands. The paper highlights inconsistencies in reporting requirements, breach notifications, and token handling practices across markets. Overall, while regulatory awareness is increasing, there remains a lack of harmonization in API security mandates globally. This disparity presents challenges for international banks and fintechs, making it imperative to adopt security practices that exceed minimum compliance and can adapt across jurisdictions.

### *2.6 Identified Gaps in Current Research*

Although substantial progress has been made in the development of API security models, detection frameworks, and regulatory guidelines, the existing literature still reflects several important gaps—particularly when examined in the context of the banking sector. First, many technical studies focus narrowly on individual dimensions such as anomaly detection [4], [7], or deep learning-based classification [5], [42], often within controlled environments or synthetic datasets. While these works show promise, they rarely account for the complex multi-layered environments of real-world financial systems, where legacy infrastructure, regulatory constraints, and operational workflows coexist. Second, despite the availability of standards like OWASP and FAPI, there is limited research evaluating their practical adoption and effectiveness in financial institutions. Few studies investigate how banks integrate these standards into continuous deployment pipelines or adapt them to legacy systems and multi-cloud environments [6], [30], [36]. Third, although comparative studies of regulatory frameworks exist [41], [43], there is still a lack of holistic, cross-disciplinary approaches that integrate risk modeling, compliance alignment, and adaptive threat detection. Most regulatory papers stop at surface-level comparisons without proposing unified strategies that could guide implementation across borders. While several works acknowledge the cybersecurity implications of Open Banking [11], they often lack integration with technical mitigation strategies. Moreover, many published works concentrate on either technical controls or regulatory issues, but seldom both. For example, while works like Dhaiya et al. [4] emphasize ML-based security enhancements, they overlook compliance and audit implications. Conversely, policy-oriented research often lacks actionable insights for developers and system architects tasked with securing APIs in production environments. Another gap lies in the treatment of emerging threats such as insider abuse of internal APIs, abuse of trusted partner credentials, or attacks targeting third-party integrations. These are often mentioned in industry reports but remain underexplored in academic literature [20], [40]. Lastly, there is a need for **longitudinal studies** that assess how API threats evolve over time, especially with the growing adoption of AI, containerization, and real-time financial services. Without historical benchmarking or lifecycle-aware security strategies, institutions are left with fragmented, reactive defenses. In sum, current literature falls short in delivering integrated, context-aware, and forward-**looking frameworks** that combine security models, compliance mandates, and banking-specific realities. This review aims to address that gap by bridging technical, regulatory, and strategic perspectives on securing API ecosystems in banking.

## 3. Methodology

This study adopts a qualitative, narrative-based literature review methodology to critically examine the current landscape of API security in banking. The goal is to synthesize insights from peer-reviewed research, industry reports, cybersecurity standards, and real-world case studies to present a comprehensive understanding of cyber risks, control frameworks, and emerging trends in API security.

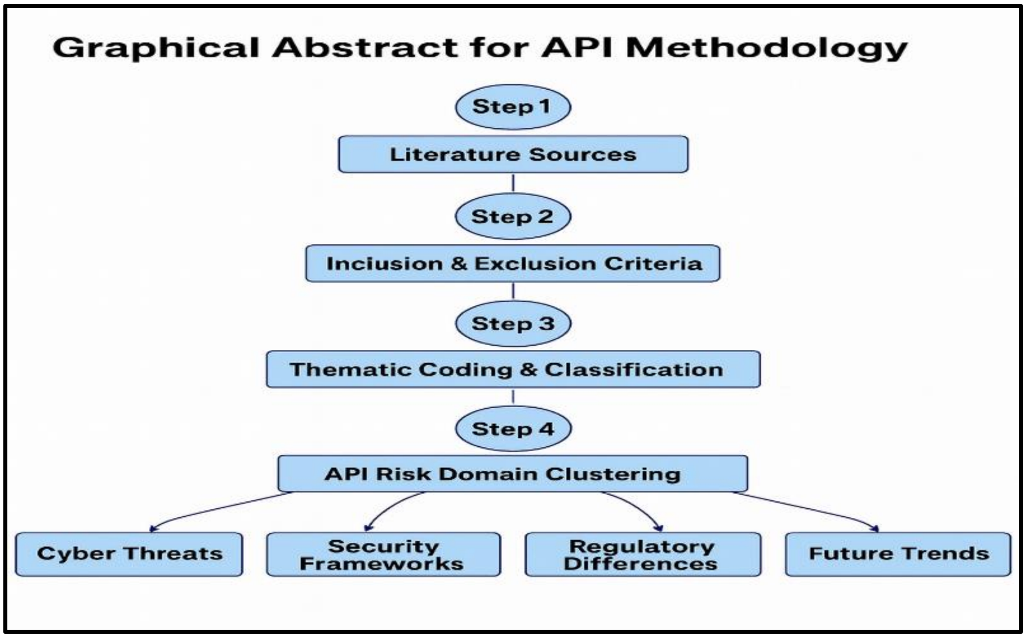
Graphical Abstract for API Methodology
Step 1
Literature Sources
Step 2
Inclusion & Exclusion Criteria
Step 3
Thematic Coding & Classification
Step 4
API Risk Domain Clustering
Cyber Threats
Security Frameworks
Regulatory Differences
Future Trends

**Figure 2**. Graphical Abstract for API Methodology

### *3.1 Research Design and Scope*

The review focuses specifically on API ecosystems within the banking and financial services sector, encompassing both public (open banking) and private/internal APIs. This includes technical vulnerabilities, governance challenges, mitigation strategies, and regulatory perspectives. The review does not include unrelated API use cases outside of financial services (e.g., e-commerce or gaming APIs), ensuring the scope remains tightly aligned with banking security contexts.

### *3.2 Data Collection Sources*

The literature was collected from the following types of sources:

- **Peer-reviewed journals**: Articles from IEEE Access, Computers & Security, Journal of Financial Crime, Journal of Banking Regulation, and others.
- **Cybersecurity frameworks and standards**: OWASP API Security Top 10, Financial-grade API (FAPI), NIST SP 800-207, and ENISA Threat Reports.
- **Incident reports and case studies**: Twilio, Dell, Cox Communications, Barclays, Citizens Bank, etc.
- **Regulatory documents**: PSD2, US Open Banking rules, EBA guidelines, and national implementations from the UK, EU, and Oman.

A total of 45 sources were included in the final analysis after screening for relevance, credibility, and publication quality.

### *3.3 Inclusion and Exclusion Criteria*

**Inclusion Criteria:**

- Articles published between 2020–2025
- Studies specifically addressing API security in banking or fintech

- Frameworks or case studies from recognized cybersecurity bodies or regulators
- Peer-reviewed or officially published materials with DOI or verified URLs

**Exclusion Criteria:**

- Preprints without peer review
- Blogs or promotional whitepapers without technical depth
- API-related studies not focused on financial services

### 3.4 Analytical Approach

The selected literature was analyzed using a thematic synthesis approach**:**

1. **Risk Dimensions**: Categorizing API-related vulnerabilities and attack vectors.
2. **Security Controls**: Mapping proposed solutions (ML, Zero Trust, FAPI) to identified risks.
3. **Framework Evaluation**: Assessing the applicability and limitations of industry standards.
4. **Regulatory Comparison**: Analyzing regional differences in compliance models.
5. **Gap Identification**: Highlighting underexplored areas in research and practice.

The findings were grouped under thematic clusters (e.g., vulnerabilities, detection techniques, governance models) to facilitate comparative analysis and support structured discussion in the literature review.

## 4. Result and Discussion

This section synthesizes findings from the reviewed literature, organized into five key themes: API risk categories, the effectiveness of current security controls, the regulatory landscape, research and implementation gaps, and emerging security trends. Each theme is discussed based on qualitative insights from peer-reviewed studies, industry reports, and real-world breach analyses.

### *4.1 Key Cyber Risk Categories in API Ecosystems*

The literature consistently identifies several recurring vulnerabilities in financial APIs. These include broken object-level authorization, excessive data exposure, inadequate rate limiting, and poor authentication practices [6], [29], [45]. Real-world incidents, such as the breaches at Twilio and Dell [1], [2], confirm that misconfigured endpoints and unauthenticated access remain primary entry points for attackers. Cloud-native financial platforms are particularly exposed to attack vectors involving unsecured micro services, token mismanagement, and weak API gateways [39]. IBM X-Force and Salt Security reports [37], [39] highlight the increasing sophistication of automated attacks, including credential stuffing, injection flaws, and abuse of business logic in API calls.

### *4.2 Evaluation of Security Frameworks and Controls*

Frameworks such as the OWASP API Security Top 10 [29] and the FAPI Security Profile [30] provide structured guidance on mitigating common vulnerabilities. However, their real-world adoption is inconsistent, particularly in legacy financial institutions or hybrid cloud environments [13], [30]. Studies also reveal gaps in enforcement and integration into CI/CD pipelines.

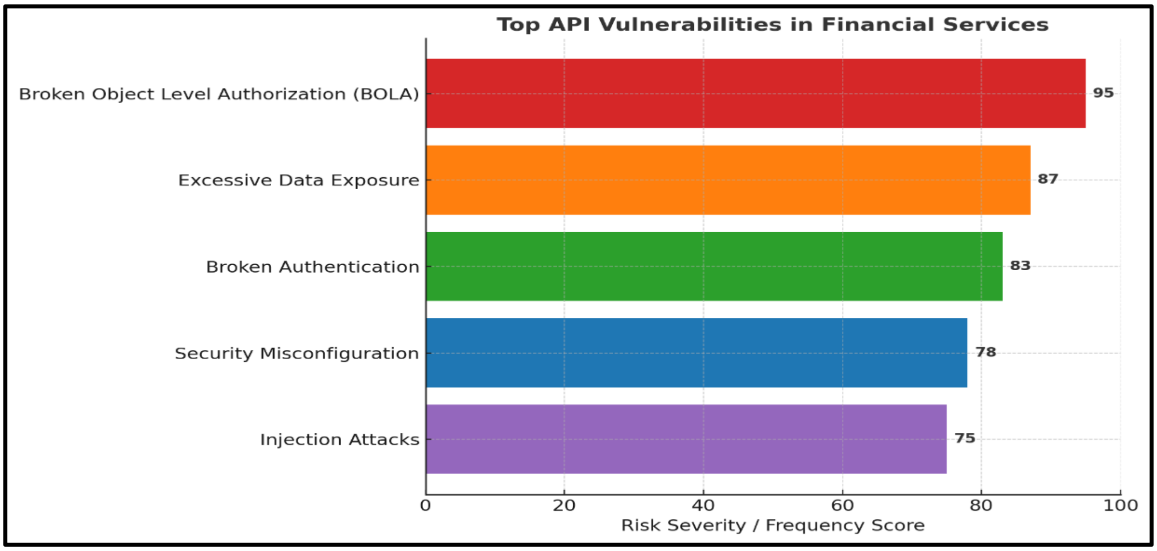

**Figure 3**. Top API Vulnerabilities in Financial Services

**Table 1**. Frameworks, Regulatory Comparison, Research Gaps

| Framework | Maintained By | Focus Area | Key Features | Adoption in Banking |
|---|---|---|---|---|
| OWASP API Top 10 | OWASP Foundation | Common API vulnerabilities | BOLA, Excessive Data Exposure, Rate Limiting, etc. | Widely cited, partial implementation in assessments |
| FAPI (Financial-grade API) | OpenID Foundation | High-assurance financial data protection | Token binding, dynamic client registration, proof-of-possession | Adopted in UK, EU; referenced in PSD2 |
| Zero Trust Architecture | NIST | Continuous verification & access control | No implicit trust, strict access segmentation, real-time validation | Gaining momentum, implementation is complex |

AI-powered methods show potential in enhancing API defense. Bayesian attack graphs [3], machine learning anomaly detection [4], and deep learning models [5], [42] offer high detection accuracy. However, most of these models are evaluated on synthetic datasets, limiting their practical transferability. Zero Trust Architecture is gaining ground in API environments, advocating for continuous verification, role-based access control, and micro-segmentation [35], [36]. While promising, the shift to Zero Trust in financial settings remains a complex and resource-intensive transition.

### *4.3 Comparative Insights from Regulatory Landscapes*

Regulatory responses to API security vary across regions. The EU's PSD2 and EBA guidelines offer the most structured mandates, emphasizing strong customer authentication, consent-driven access, and detailed incident reporting [33], [34], [41]. In contrast, the U.S. relies on fragmented, market-driven standards, though recent efforts by the CFPB aim to establish clearer open banking rules [31]. The UK's Open Banking Implementation Entity (OBIE) represents a middle-ground approach, combining regulatory compliance with technical standards [26], [27]. Yet, studies find inconsistencies in how banks implement these guidelines, particularly when handling cross-border transactions [43].

**Table 2**. Comparative Insights from Regulatory Landscapes

| Region | Regulation | Mandates on API Security | Consent Handling | Enforcement Strength |
|---|---|---|---|---|
| EU | PSD2, RTS | Strong (FAPI aligned) | Explicit, granular | High (EBA) |
| US | No central mandate | Market-driven, variable | Varies by institution | Moderate |
| UK | Open Banking Standard | FAPI-aligned, but optional | Centralized consent model | Moderate–High |

*4.4 Gaps in Research and Real-World Implementation*

Despite growing research on API security, key gaps persist. Many studies focus on technical innovations—such as caching strategies [16] or intelligent API routing—without evaluating their deployment readiness. Regulatory-focused papers often omit implementation guidance for developers and security teams. Moreover, insider threats, third-party abuse, and unmanaged "shadow APIs" remain underexplored in both academia and practice [20], [40]. There is also a lack of longitudinal studies examining how API threats evolve over time across different banking environments. The convergence between API security and data privacy mandates is another area receiving growing attention but remains underdeveloped in the literature [17].

**Table 3**. Summary of Research Gaps Identified

| Gap Area | Description | Suggested Direction |
|---|---|---|
| Insider Threats | Limited focus on internal abuse of API access | Behavioral analytics, access policy audits |
| Shadow APIs | Untracked/unsecured APIs | API inventory tools, continuous scanning |
| Regulatory Integration | Few studies combine compliance and security | Cross-disciplinary policy modeling |
| Longitudinal Risk Studies | Lack of time-based threat evaluation | Long-term monitoring frameworks |

*4.5 Trends and Future Directions*

The integration of AI-powered threat detection**,** Zero Trust frameworks**,** and cloud-native security tooling marks a new phase in API protection. Standards like FAPI are evolving to include token binding and proof-of-possession mechanisms [30]. Runtime protection, behavioral anomaly analysis, and threat intelligence integration are becoming increasingly important for real-time defense [37], [44]. Simultaneously, regulatory convergence is emerging as a priority. Reports suggest the need for harmonized international standards, particularly for multinational banks operating in fragmented legal environments [32], [41].

## 5. Conclusion

As APIs become the cornerstone of digital transformation in banking, securing these interfaces has emerged as both a technological imperative and a regulatory necessity. This review critically assessed the evolving cyber risk landscape, evaluated key security frameworks, and explored future strategies for strengthening API resilience in the financial sector.

**Key findings:**

1. APIs are essential but remain vulnerable
   Despite their operational importance, APIs are commonly exposed to broken object-level authorization (BOLA), excessive data exposure, and weak authentication mechanisms.
2. Real-world breaches confirm implementation gaps
   Incidents such as the Twilio and Dell breaches highlight failures in enforcing secure API configurations, particularly in multi-cloud and agile environments.
3. Security frameworks exist but are inconsistently adopted
   OWASP API Top 10, Financial-grade API (FAPI), and Zero Trust provide effective security principles but are underutilized across legacy systems and fast-paced DevOps pipelines.
4. AI-driven security methods are promising but underused
   Machine learning, Bayesian modeling, and deep learning exhibit strong performance in academic studies but lack real-world deployment in most financial institutions.
5. Regulatory maturity is fragmented across regions:
   The EU leads with well-defined mandates like PSD2 and RTS, while the U.S. and U.K. rely on market-driven or decentralized models, complicating international compliance.
6. Critical risks remain underexplored
   Threats such as insider misuse, unmanaged shadow APIs, and third-party credential abuse are rarely addressed in standard frameworks and are underrepresented in academic literature.
7. Lifecycle-based, integrated models are lacking
   Few existing solutions combine technical controls, regulatory mandates, and operational practices across the full API lifecycle.

**Recommendations:**

1. Implement layered security models
   Combine OWASP, FAPI, and Zero Trust principles with runtime protection, access control, and behavior analytics to reduce exposure.
2. Promote regulatory harmonization
   Advocate for the alignment of global API security mandates to simplify cross-border operations and ensure consistent compliance frameworks.
3. Foster cross-sector collaboration
   Encourage coordinated efforts between regulators, researchers, and industry stakeholders to develop actionable standards for underexplored risks.
4. Integrate API security into SDLC and CI/CD pipelines
   Embed security practices such as static analysis, API scanning, and policy enforcement into development and deployment workflows.
5. Adopt AI-driven detection and response tools
   Use machine learning and probabilistic models to enhance threat detection, monitor anomalies in real-time, and accelerate response capabilities.
6. Support lifecycle-aware, risk-based modeling
   Develop frameworks that assess API risks throughout their lifespan from design to retirement to improve long-term resilience and security assurance. By addressing both technical and regulatory dimensions holistically, financial institutions can move toward a more secure, transparent, and innovation-ready API ecosystem.

**Corresponding author**

**Sopheaktra Huy**

hsopheaktra.phdscholar@lincoln.edu.my

**Acknowledgements**

The authors thank their co-authors for guidance, peer reviewers for valuable feedback, and all participants for their contributions. They also acknowledge the support of the Lincoln University College Doctoral Program and appreciate the editorial team and anonymous reviewers of the Journal of Cyber Security and Risk Auditing for their constructive input.

**Funding**

No funding.

### Contributions

S.H; S.A; M.H; V.B; Conceptualization, S.H; S.A; M.H; V.B; Investigation, S.H; S.A; M.H; V.B; Writing (Original Draft), S.H; S.A; M.H; V.B; Writing (Review and Editing) Supervision, S.H; S.A; M.H; V.B; Project Administration.

### Ethics declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

### Consent for publication

Not applicable.

### Competing interests

All authors declare no competing interests.

## References

[1] Cybersecurity News. (2024). *Twilio's Authy breach exposes 33.4 million phone numbers via unauthenticated API*. https://cybersecuritynews.com/securing-apis/
[2] Cybersecurity News. (2024). *Dell customer data exposure affects 49 million records due to API vulnerability*. https://cybersecuritynews.com/securing-apis/
[3] Behbehani, D., Rajarajan, M., Komninos, N., & Al-Begain, K. (2022). Detecting open banking API security threats using Bayesian attack graphs. In *Proceedings of the 14th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 146–151). IEEE. https://doi.org/10.1109/CICN56167.2022.10008365
[4] Dhaiya, S., Ranjan, P., Pandey, B. K., Adusumilli, S. B. K., & Avacharmal, R. (2021). Optimizing API security in FinTech through genetic algorithm-based machine learning model. *International Journal of Information Technology*, 13(3), 348–356.
[5] Alam, F., Hossain, M., & Ramakrishnan, K. (2024). Analyzing API threats and mitigation techniques using deep learning. *Future Generation Computer Systems*, 145, 87–101. https://doi.org/10.1016/j.future.2023.11.015
[6] OWASP Foundation. (2023). *API security top 10 – 2023 edition*. https://owasp.org/www-project-api-security/
[7] OpenID Foundation. (2024). *Financial-grade API (FAPI) security profile*. https://openid.net/wg/fapi/
[8] 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
[9] Briones de Araluze, G. K., & Cassinello Plaza, N. (2022). Open banking: A bibliometric analysis-driven definition. *PLOS ONE*, 17(10), e0275496. https://doi.org/10.1371/journal.pone.0275496
[10] Ranjan, P., & Haider, M. T. (2024). API security challenges and risk mitigation in fintech applications. *International Journal of Global Information Security*. https://doi.org/10.21428/e90189c8.43a4136c
[11] Hossain, M. A., Raza, M. A., & Rahman, J. Y. (2025). Investigating the cybersecurity implications of open banking and APIs in the financial sector. *Jurnal Ekonomi dan Bisnis Digital (MINISTAL)*, 4(1). https://doi.org/10.55927/MINISTAL.V4I1.13370
[12] Machine learning techniques for enhancing security in financial technology systems. (2024). *International Journal of Scientific Research and Applications*, 13(1). https://doi.org/10.30574/ijsra.2024.13.1.1965
[13] Cloud-native API strategies for financial services: Ensuring security, compliance, and scalability. (2025). *European Journal of Computer Science and Information Technology*, 13(1). https://doi.org/10.37745/ejcsit.2013/vol13n1584101
[14] Open banking: An early review. (2024). *Journal of Innovation and Development in Economics*. https://doi.org/10.1108/JIDE-03-2024-0009
[15] Adari, V. K. (2024). APIs and open banking: Driving interoperability in the financial sector. *International Journal of Research in Computer Applications and Information Technology*. https://ijrcait.com/index.php/home/article/view/IJRCAIT_07_02_142
[16] Padhi, S. (2024). Intelligent API caching for financial data: A scalable and performance-optimized approach. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/IRJMETS65604
[17] Navigating the nexus of security and privacy in modern financial technologies. (2024). *GSC Advanced Research and Reviews*, 18(2). https://doi.org/10.30574/gscrr.2024.18.2.0043
[18] Adanigbo, O. S., et al. (2022). Systematic review of API-driven innovation in digital financial platforms across emerging economies. *Iconic Research and Engineering Journals*. https://www.irejournals.com/paper-details/1708020
[19] Customer data access and fintech entry: Early evidence from open banking. (2024). *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2024.103950
[20] Data privacy and cybersecurity challenges in the digital transformation of banking. (2024). *Computers & Security*. https://doi.org/10.1016/j.cose.2024.104051
[21] Cybersecurity News. (2024). *Twilio's Authy breach exposes 33.4 million phone numbers*. https://cybersecuritynews.com/securing-apis/
[22] Cybersecurity News. (2024). *Dell customer data exposure affects 49 million records*. https://cybersecuritynews.com/securing-apis/
[23] Equixly. (2024). *Cox Communications API flaw gives access to millions of modems*. https://equixly.com/blog/2024/09/06/top-10-api-breaches-in-2024/
[24] The Australian. (2024). *Aussie banks targeted in global cyber heist*. https://www.theaustralian.com.au

[25] The Australian. (2024). *Security flaw let hackers into super funds*. https://www.theaustralian.com.au
[26] Business Insider. (2025). *Citizens Bank open banking technology*. https://www.businessinsider.com
[27] Silicon Digest. (2024). *Barclays open banking APIs fintech collaboration*. https://silicondigest.com
[28] Intellectsoft. (2024). *How open banking APIs boost FinTech growth*. https://www.intellectsoft.net
[29] OWASP Foundation. (2023). *API security top 10*. https://owasp.org/www-project-api-security/
[30] OpenID Foundation. (2024). *Financial-grade API (FAPI) security profile*. https://openid.net/wg/fapi/
[31] Financial Times. (2024). *US rolls out open banking rules*. https://www.ft.com
[32] Traceable AI. (2024). *Meeting regulatory and industry standards for API security*. https://www.traceable.ai
[33] Central Bank of Oman. (2024). *Open banking API specifications*. https://cbo.gov.om
[34] European Banking Authority. (2019). *Guidelines on ICT and security risk management*. https://www.eba.europa.eu
[35] National Institute of Standards and Technology. (2020). *Zero trust architecture (SP 800-207)*. https://doi.org/10.6028/NIST.SP.800-207
[36] Akamai. (2023). *API security best practices: Protecting the digital gateway*. https://www.akamai.com
[37] Salt Security. (2024). *State of API security report (Q1 2024)*. https://salt.security/resources
[38] ENISA. (2023). *Threat landscape for APIs*. https://www.enisa.europa.eu
[39] IBM X-Force. (2024). *Cloud threat landscape report: API vulnerabilities*. https://www.ibm.com/security
[40] Kephart, J. O., & Guha, S. (2024). The role of AI in securing financial APIs. *ACM Transactions on Privacy and Security*, 27(2), 1–25. https://doi.org/10.1145/3607380
[41] Bansal, A. K., Wadhwa, R., & Saini, S. (2024). Cybersecurity risks in open banking APIs. *Journal of Information Security and Applications*, 72, 103584. https://doi.org/10.1016/j.jisa.2023.103584
[42] Alam, F., Hossain, M., & Ramakrishnan, K. (2024). Analyzing API threats using deep learning. *Future Generation Computer Systems*, 145. https://doi.org/10.1016/j.future.2023.11.015
[43] Colangelo, G., & Khandelwal, P. (2025). The many shades of open banking. *Internet Policy Review*, 14(1). https://doi.org/10.14763/2025.1.1821
[44] Ramachandran, K. K. (2024). The role of AI in enhancing financial data security. *International Journal of AI & Applications*, 10(1), 22–30. https://doi.org/10.30574/ijsra.2023.10.1.0700
[45] Wan, Z., Yuan, Y., & Meng, X. (2023). API access control strategies in cloud-based financial services. *Computers & Security*, 127, 102630. https://doi.org/10.1016/j.cose.2023.102630

## Biographies

**Author Sopheaktra Huy.**
Mr. Sopheaktra Huy is a Ph.D. candidate in Cyber Security at Lincoln University College, Malaysia. He holds a Master of Science in Information Technology from the Royal University of Phnom Penh and an MBA from Asia Euro University, Cambodia. Mr. Sopheaktra brings extensive experience in the financial sector and non-profit organizations, academic industry with a strong focus on IT risk management, cybersecurity governance, and digital transformation. Over the past 20 years, he has also served as a part-time lecturer, delivering courses in programming, cyber risk, and IT project management at various academic institutions. He holds globally recognized certifications including CISA, CISM, and CEH. Email: hsopheaktra.phdscholar@lincoln.edu.my

**Author Sokroeurn Ang.**
Mr. Sokroeurn Ang has over 15 years of experience working and teaching in the fields of ICT and cybersecurity, holding various technical and leadership roles. His professional background spans central banking, private banking, and internet service providers, where he has played a key role in strengthening cybersecurity. He has been actively engaged in critical domains such as IT Governance, Cybersecurity Risk Assessment, Network Security, Web Application Security, Cloud Security, Vulnerability Assessment and Penetration Testing (VAPT), Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), Cybersecurity Incident Response, and IT Auditing. He successfully completed a MicroMaster program in Cybersecurity at the Rochester Institute of Technology (RIT), USA, and earned a Master's degree in Cybersecurity from Royal Holloway, University of London, UK. He is currently

pursuing a PhD in Cybersecurity at Lincoln University College, Malaysia. He holds multiple professional certifications, including CISSP, CISA, CISM, CC, ECSA, CEH, CCNA Security, CCNA, CyberOps, and AWS Certified Cloud Practitioner. In addition, he is a certified Cisco Instructor and AWS Academy Instructor. He can be contacted at email: angsokroeurn.phdscholar@lincoln.edu.my. https://orcid.org/0009-0000-9746-5469

**Author Mony Ho.**

Mr. Mony Ho is a Ph.D. candidate in Information Technology at Lincoln University College, Malaysia. He holds a Master's degree in IT and Data Science from the European International University, France. He is currently a senior technical teacher at Preah Kossomak Polytechnic Institute and lectures part-time at multiple universities in Cambodia. His teaching and research interests include Data Science, Big Data, software engineering, cloud technologies, and web and mobile application development. https://orcid.org/0009-0004-3389-1951

**Author Dr. Vivekanandam Balasubramaniam**

Dr. Vivekanandam is a Deputy Dean of the School of AI Computing and Multimedia at Lincoln University College, Malaysia. He has authored over 47 publications with 420+ citations, focusing on artificial intelligence, machine learning, cybersecurity, and cloud computing. His work includes both research papers and patents, contributing significantly to innovation and academic development in these fields. Dr. Vivekanandam Balasubramaniam also serves as a research supervisor and mentor for numerous postgraduate students, supporting innovative work in artificial intelligence and cloud-based systems. https://orcid.org/0000-0002-5534-2142