KAUTILYA
SCHOOL OF
PUBLIC POLICY

Issue
Brief
Series

Exploring the Rise of Open Banking and Associated Cybersecurity Threats

Issue Brief Number: IB-2025-06

Submitted by: Mr. Vivek Kalhan Reshi Raina (MPP Cohort: 2023-25)

Under the Guidance of: Dr. Srinivas Yanamendra (Visiting Instructor at Kautilya School of Public Policy)

Cite this Article as *Raina, V. K. R. (2025).* Exploring the Rise of Open Banking and Associated Cybersecurity Threats *[online]. Available at:https://kspp.edu.in//issue-brief/*exploring-the-rise of-open-banking-and-associated-cybersecurity-threats

Exploring the Rise of Open Banking and Associated Cybersecurity Threats

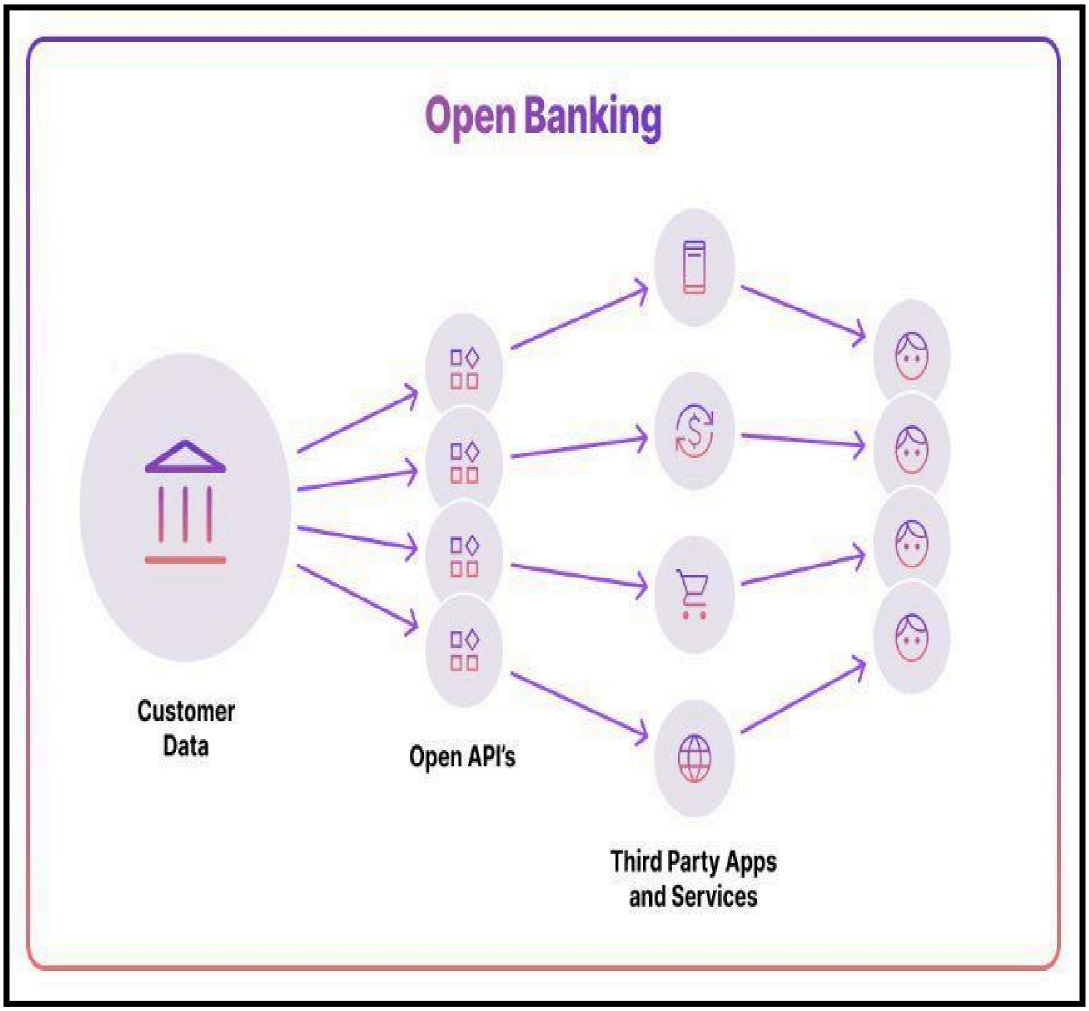
Abstract

Banking as a service has changed beyond its more traditional brick-and-mortar business approach to a more virtual sphere, due to the integration of technology for the provision of financial services through digital channels (Rao, 2024). The rise of Open Banking – a method where banks share their financial data with third-party software developers through Application Programming Interfaces (APIs - Amazon Web Services (AWS) define API as a tool that enables two software components to communicate with each other using a set of definitions and protocols) – has promised to be a better and more efficient model than the traditional one. But just as evolution has become customary in the world of technology and business, risks and concerns with respect to these areas have also evolved. In this paper, I explore Open Banking as a tool for financial inclusion and the cyber security risks that have emerged from the rise of this industry.

Introduction

Open Banking is a term from the world of financial services that incorporates the use of open (available to the public) Application Programming Interfaces (APIs) to provide secure access to financial services (Vagadia & Kanniappan, 2023). APIs make it easier for third party developers to interact and exchange data, and also create financial products and services with the help of financial data from banks. These third-party developers can then create a slew of financial service products like personal finance management tools and payment platforms.

Providing these third-party developers with user's financial data does not mean that users lose the right over their own data. Open banking regulations focus on providing their users with greater control, choice and convenience with regards to their financial data. Banks and third-party providers can only be granted access to certain specified data that the customers have provided their outright consent for (Drozdovica, 2024). This specific implementation can change from region-to-region or country-to-country, but on the whole, open banking procedures require banks to share certain financial data with authorized third-party providers under secure conditions.



Source: https://noda.live/articles/open-banking-security

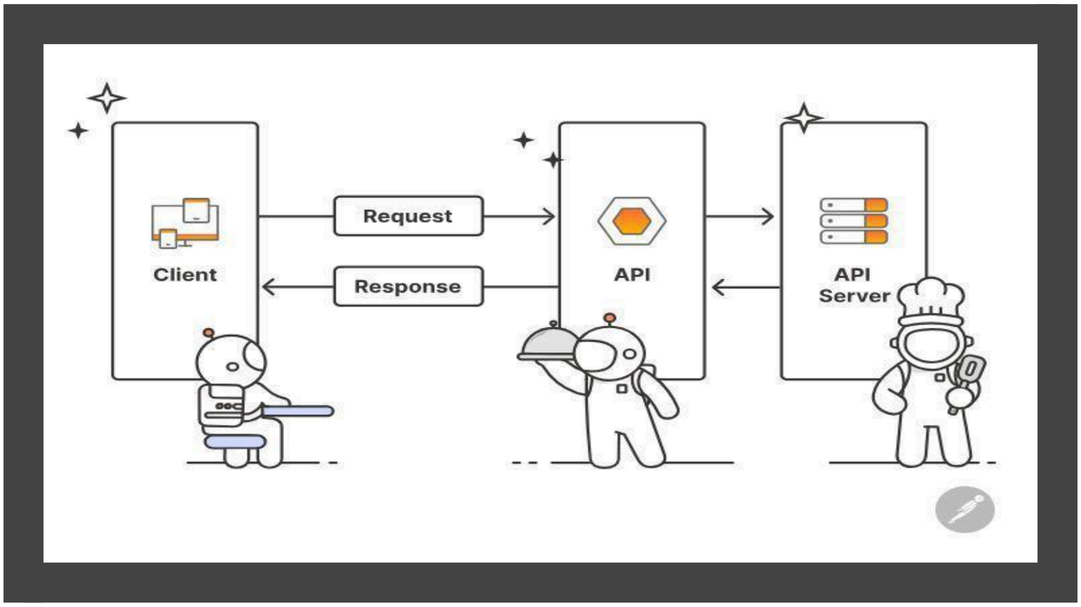
Open banking initiatives started in the 1980s as part of experiments conducted in Germany with the German Federal Post Office (Wrixon, 2024). The eventual introduction of standards like the Home Banking Computer Interface (HBCI) in 1998 and subsequent regulations like PSD1 and PSD2 by the European Union played a crucial part in contemporary open banking and improving banking security (Wrixon, 2024). These initiatives have seen an exponential rise on a global level in the last few years, driven by evolution of technology and due support provided by regulatory authorities and policies. Outside of the European Union, countries like Hong Kong and Australia have also opted for such regulatory approaches (Strachan, 2023). In turn, this has contributed in transforming the landscape of financial services and increased financial inclusion. In 2010, India too took first steps towards its own initiative called the India Stack, which represented a monumental change in the digital infrastructure of the country (IndiaStack, 2017). India Stack comprises APIs that are designed to enable “governments, businesses, startups and developers to utilize a unique digital Infrastructure to solve India’s hard problems towards presence-less, paperless, and cashless service delivery” (IndiaStack, 2017).

What is an Application Programming Interface (API) and how does it work?

It is important to understand the technology associated with Open banking. API as mentioned previously stands for Application Programming Interface. With regards to APIs, Application means a software with a distinct function. Interface can be a sort of a contract between two applications and it is this contract that lists how the two applications communicate with each other, using requests and responses.

API architecture can be explained in the context of a client and server. The application that sends the request is the client side and the side that generates the response is the server side.

APIs work by sharing data between applications, systems, and devices and this happens through a request and response cycle wherein the request is sent to the API, which retrieves the data and returns it to the user (Postman, Inc., 2023). Here's a diagram of how that process works:



Source: https://www.postman.com/what-is-an-api/

Benefits of API-driven financial inclusion

Access to financial services

API’s help fintech companies to make innovative, cost-effective financial services products that can be tailored to the needs of underserved groups of the population. For example, micro-lending platforms make use of alternative credit scoring APIs for analysing non-traditional data like usage of telecom data, utility payments and social behavior, to provide loans to rural SMEs and gig workers with no formal credit history (Perfios, 2025). In this day and age, where mobile phones have become commonplace, banking apps that are powered by APIs as such, have the capability of reaching areas where traditional banking institutions cannot. APIs lower the entry barrier and enable the development of micro-finance solutions and micro-insurance products that have the potential and capability to look after the needs of low-income individuals.

Renewed competition and increased innovation in financial products

Open banking APIs by nature create a level playing field that allows for smaller fintech firms to push and compete with well-established and celebrated financial institutions in the market (Ayade, 2024). The increased competition due to the open nature of the technology takes innovation to higher levels, leading to the development of better, diverse and specialized financial products. Because of the diverse financial marketplaces that can be created with the help of APIs, users can compare financial products and services easily and choose accordingly, building a dynamic and consumer-friendly ecosystem (Ayade, 2024).

User-friendly financial management tools

APIs have the provision for aggregating financial data from many sources, thus providing the users with a better and more holistic view of their financial situation. This complete view of data from multiple sources helps in the development of personal financial management tools that can provide deep financial insights and personalized advice to the users (Ayade, 2024). In addition to this, Machine learning algorithms can be used to analyze aggregated data gathered from APIs to offer financial planning to users, aiding them in making more informed decisions with regards to their savings and investments (Takyar, 2023).

Reducing costs and improved data sharing

With regards to financial firms, API-driven open banking has enabled more efficient sharing and integration of data. And, automated applications that make use of API-generated data have drastically reduced operational costs and driven down expected fees to be levied on customers for financial services.

Cyber security risks in Open Banking

Following are the cyber security risks and challenges associated with Open Banking:

Data Breaches and Unauthorized access

Open Banking APIs are connected with a wide array of applications and financial services, thereby creating an expanded surface for cyber-attacks. The huge volume of sensitive information that gets transmitted through APIs can have associated vulnerabilities with it, like unauthorized access and data breaches (Perfios, 2025). For example, in 2023, phishing attacks that targeted UPI users surged by as much as 35% (Perfios, 2025). Cyber attackers have the capability to exploit minute vulnerabilities to break in and access sensitive financial information of a customer such as their private data, credit or debit card details and bank account numbers.

API Endpoint Security

The safety of API endpoints is very crucial to the protection of the overall infrastructure of open banking. Malevolent actors oftentimes target susceptible API endpoints to launch their attacks like code injection attacks. Injection attacks are a category of cyber attack where attackers add malicious code into an application, thereby tricking it to implement certain unintended actions (Rajarathna et al., 2024). This brings another important risk into question, that of code injection. As is already known, bank APIs must have a strong security architecture in place without any gaps in-between, as these gaps act as vulnerable points that can be exploited by attackers through the injection of small bits of codes. It works in the following manner: Attackers try to send a script to a financial service provider's application server through an API request (Rajarathna et al., 2024). This has the potential to spill over into an Account Takeover incident and put the internal contents of the application at risk, by virtue of deleting data or planting false information inside the application.

Encryption and Data Integrity

The privacy and integrity of data that is transmitted via banking application APIs are at risk of attacks, if the encryption put in place by the application owners is not robust enough to protect data in transit.

Multiple Communication channels

API transactions are aided by multiple communication channels between systems and users that ensure smoother and quicker transactions. But at the same time, these channels can become susceptible to security issues like data manipulation, eavesdropping and man-in-the-middle (MITM) attacks (Verma, 2024).

Man-in-the-middle attacks

These attacks take place when malicious actors intercept communications between two systems that they believe are in direct communication with each other (Sharadin, 2023).

Third-party risks, cyber fraud and data privacy

Providing access to third parties forms the basis for open banking (Mastercard, 2024). But it adds an element of risk in the system. Any cybersecurity problem or vulnerability in these third-party systems has the potential to leak sensitive customer data and related financial information too (Bianco, 2024).

With a spike in the sharing of data regarding open banking and the use of APIs, there will be a greater risk of fraudulent activities in the financial and cybersecurity sector. As per Juniper's study, Open Banking usage has been predicted to grow by 470% globally from 102 billion API calls in 2023, to a whopping 580 billion API calls by 2027 (Juniper Research, 2023). As such, cybercriminals may impersonate customers or banks to deceive unsuspecting customers into divulging sensitive details about their financial or banking data.

Data protection regulations have been passed in a number of jurisdictions throughout the world like the European Union and India, but the volume of data that is being shared across various financial platforms over the internet is a cause of concern with respect to data privacy as data protection laws and regulations vary from country to country, region to region.

Current Regulatory and Policy Landscape with regards to Open Banking: Around the world and India

The regulatory landscape regarding Open banking and API-backed financial sector products/ applications is complex and changing, with different countries adopting different sets of regulations. The current landscape reflects the balance that regulators need to have between fostering innovation, protecting rights of the consumers, mitigating cybersecurity risks and also safeguarding financial stability. Following is an overview of existing open banking regulations:

Since its 2018 implementation in Europe, the revised Payment Services Directive (PSD2) has been a cornerstone of open banking regulation. According to PSD2, banks can provide access to third-party entities with regards to certain financial data of the customers through APIs, with prior consent of the customers (IntelliswiftMarketing, 2023). The aim of this regulation is to promote competition, innovation and transparency in the market of payment services.

At the time still part of the PSD2 framework, the United Kingdom in due course of time, created its own set of open banking standards through the Competition and Markets Authority (CMA) (Competition and Markets Authority, 2023). The regulations as per CMA are more prescriptive in that they lay out API standards and establish the Open Banking Implementation Entity (OBIE) to oversee implementation (Competition and Markets Authority, 2023).

When it comes to the United States, there is no comprehensive federal open banking regulation present there at the moment. The market is primarily steered by industry players and guidelines issued from bodies such as the Financial Data Exchange (FDX) (Akamai, 2024). Recognized standards like the Financial Data Exchange (FDX) by the Financial Services Information Sharing and Analysis Center (FS-ISAC) emphasize the importance of structured frameworks in improving data exchange (Akamai, 2024).

India has taken giant leaps towards open banking frameworks with initiatives such as Unified Payments Interface (UPI) which was launched in 2016. In addition to UPI, the Account Aggregator (AA) Framework brought out by Reserve Bank of India (RBI) in 2016 and operationalized in 2021 regulates open banking in India (Garg, 2022). But it does not have specific open banking regulations like the ones in the European Union or the United Kingdom (Strachan, 2023).

Nonetheless, the National Cyber Security Policy (NCSP), 2013, marked a significant change in India's approach to cybersecurity (Department of Electronics and Information Technology (DeitY), 2013). Before that, much of the cyber crimes and security related to cyberspace were looked at through the prism of the IT Act of 2000. When considering the effectiveness of NCSP 2013, in handling problems related to open banking and API security, the policy needs to be evaluated in the rapidly changing fintech landscape. Here is an analysis of the same:

Strengths of the policy:

a) Emphasis on information sharing

NCSP 2013, promotes the exchange of threat, vulnerability and best practice information. This blending is sensible given the collaborative nature of open banking ecosystems, where multiple stakeholders have to work together to be secure.

b) Focus on creating a skilled workforce

The policy acknowledges that the development of human resources in cybersecurity is necessary. It is crucial for the open banking sector, as it requires a skillset to prepare for more complicated API integrations.

c) Promotion of Public-Private Partnerships (PPPs)

With regards to the open banking context where the collaboration between financial institutions, fintech companies and regulators is a must, PPPs in cybersecurity is what the policy advocates for.

d) Encouragement of indigenous cybersecurity solutions

The policy encourages local mobilization with respect to cyber security. Such an aspect can be deployed in support of the development of indigenous solutions to meet the needs of open banking in India.

Existing gaps and challenges present in the current regulatory framework/(s)

A lot of the regulations in vogue have tried to address the issues related to data sharing and consumer protection. But there are significant gaps with regards to cyber security regulations in the context of open banking. A few of them are mentioned below:

Inconsistent Security Standards: API implementation in Open banking lacks uniformity and internationally accepted security standards. As mentioned previously, in the European Union it is the PSD2 framework, in the United States industry-led organisations such as the Financial Data Exchange (FDX) have established voluntary data-sharing standards and the Competition and Markets Authority defines open banking standards in the United Kingdom.

Third-Party Provider Oversight: The vetting and ongoing monitoring of third-party providers who access financial data via APIs is not an area that many regulations address well. This is because jurisdictions generally have protocols and standards for data transmission, storage and other information security requirements for banks, but these are not necessarily applicable to non-bank third parties that are part of open banking business models (Bank for International Settlements, 2019).

Cross-Border Data Flows: Open banking has slowly reached a global level of acceptance. But the corresponding regulations that control what does and doesn’t happen with the data flow across jurisdictions with different privacy and security laws have been unable to keep up. Bank for International Settlements mentions that more than 70 jurisdictions at present regulate open banking through ‘various approaches’, denoting that these open finance ecosystems mostly operate with dissimilar domestic standards and protocols, preventing smooth cross-border data flow (Hall, 2024).

Emerging Technologies: Present regulations with regards to Open banking do not fully take the cybersecurity implications of the emerging technologies such as Al into play (Wang et al., 2024).

With respect to National Cybersecurity Policy, 2013, these are the limitations in the context of open banking in the fintech industry and API security:

Lack of specific focus on financial sector cybersecurity: Although this policy outlines a general framework, it doesn't detail out sector specific challenges. Due to sensitivity of the nature of financial data, the open banking and API security in finance needs more specialized treatment.

Absence of API-specific security guidelines: The policy predates the widespread use of APIs in financial services. It doesn't specify how to secure API communications, which is key to open banking.

Limited coverage of emerging technologies: The policy doesn't really address the dos and don'ts of emerging technologies with respect to fintech such as AI, machine learning, or blockchain which might again be due to the timeline of the policy (it came out in 2013).

Insufficient focus on data privacy: The policy talks about data protection. But does not include more comprehensive guidance for data privacy, which is key to open banking. This drawback is however corrected to some extent with the Digital Personal Data Protection Act of 2023, which adds layers of data protection and regulatory requirements (Sadoian, 2025).

Other challenges in creating uniform global standards for API security in open banking

In addition to the aforementioned gaps, there are certain challenges in creating even standards on a global scale with regards to API security in the Open banking sector. Some of them are mentioned below:

Varying National Priorities: Financial inclusion, data protection, and innovation take different priorities in different countries, ultimately manifesting with different regulatory approaches (Colangelo & Khandelwal, 2025).

Technological Disparities: There are varying levels of technological infrastructure, across countries, making it impossible to implement uniform standards around the world (Consultative Group on Innovation and the Digital Economy, 2022).

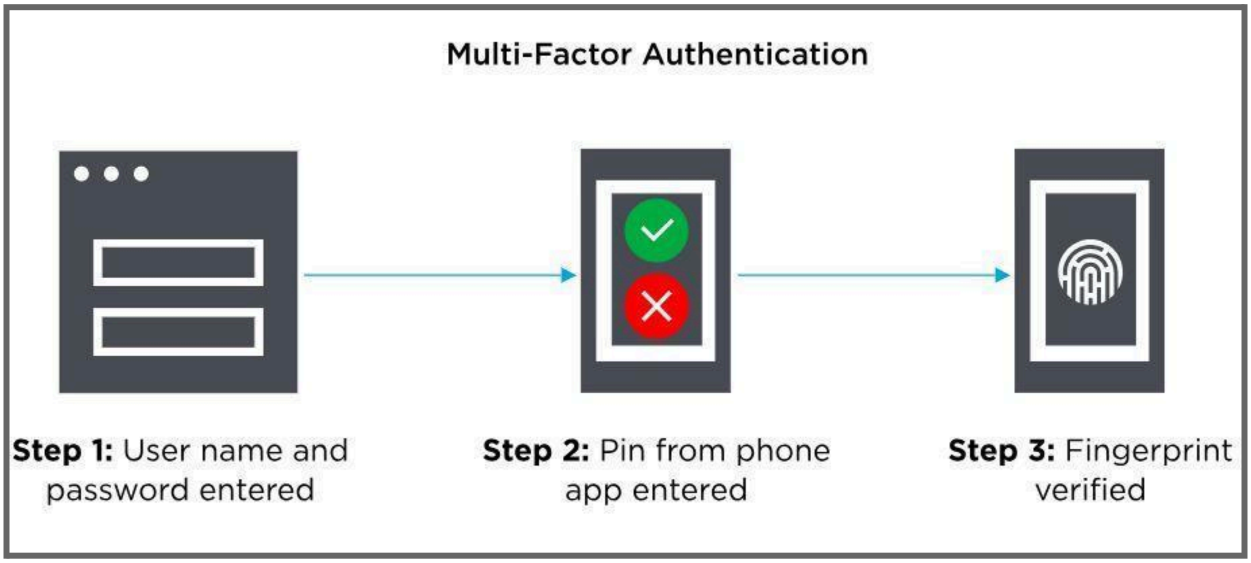
Rapid Technological Evolution: The speed of change in technology in the fintech sector makes it difficult for regulators to establish lasting standards that can’t be rendered obsolete in the blinding flash of a heartbeat (Dylan, 2023).

Balancing Innovation and Security: Thus far, the debate has continued on the best path for creating standards that not only guarantee that technology is robust but also don't stifle innovation crucial to financial inclusion (Dylan, 2023).

Way forward – Mitigation techniques of cyber security risks and policy recommendations

Some technical solutions that can help when it comes to mitigating cyber security risks are as follows:

Strong Authentication Mechanisms: To secure API access, multi factor authentication (MFA) is a must. This usually requires the users to provide multiple forms of identifications to access an application, and involves something that the user already knows like password, a code sent to a phone, a fingerprint scan and/or answering a secret question (OneLogin, n.d.).


Multi-Factor Authentication
Step 1: User name and password entered
Step 2: Pin from phone app entered
Step 3: Fingerprint verified

Source: https://www.onelogin.com/learn/what-is-mfa

Mobile banking apps have started adding an extra layer of security in the form of biometric authentication, like fingerprints or facial recognition. There is another authentication method called Adaptive authentication, which Citrix defines as a process of authentication wherein security requirements depend on risk factors such as location, device status, and end user behavior.

Encryption of Data in Transit and at Rest: Encryption of data in transit between clients and API endpoints via protocols like TLS 1.3 needs to be implemented along with end-to-end encryption (Cloudflare, n.d.). Data encryption when the data is not flowing between two endpoints and rests in databases and storage systems, should be done using strong encryption algorithms (e.g. AES-256). Proper key management practices including regular key rotation and secure storage of encryption keys should also be employed.

API Security Best Practices: Employing Rate limiting with regards to API to stop API abuse and potential DDoS attack is an industry best practice (Pragmatic Coders, 2024). Another good practice to secure APIs and develop protection against injection attacks is to use input validation and sanitization techniques. Implementation of secure authorization techniques using OAuth 2.0 and OpenID Connect are few other methods that can be utilized as best practices to enable API security at par with global standards (Pragmatic Coders, 2024).

Continuous Monitoring and Real-time Threat Detection: Security Information and Event Management (SIEM) systems can be used and deployed wherever needed in order to continuously monitor API infrastructure and analyze any security threats or other events (Kidd, 2025). Technologies such as Artificial Intelligence (AI) and Machine Learning (ML) should be utilized for anomaly detection to spot any abnormal (or unusual) patterns that may point to a breach (SIEM: A Complete Guide, 2024). To this end, real time alerting systems that notify security teams of security threats need to be implemented in order to proactively approach the problems in the realm of cyberspace.

Securing third-party service providers: Implementing a vetting process for all the third-party providers that access APIs is very crucial, as many threats emanate from these platforms (Raj, 2025). This can be achieved by using a sand-boxing approach and the environment provides room for experimentation while guiding regulation toward embracing emerging technologies (World Bank Group, 2020). Tests can be conducted with these third-party providers before production environment access is granted to them.

So far as policy recommendations are concerned, the aim has to be a balancing act between trying not to stifle a burgeoning and innovative open banking industry, but ensuring financial inclusion while providing adequate safeguards against cyber security risks. Few of them are as follows:

To meet the cybersecurity risks of Open Banking and Financial Inclusion through APIs, policymakers must put their efforts on creating a holistic cybersecurity framework that will set minimum cybersecurity standards for all participants while being capable to respond to the trends. The content of these frameworks should be kept updated and should be complemented by clear guidelines regarding best practices for API security, data protection, and incident response. Sharing intelligence reports on plausible security threats is crucial in encouraging collaboration between financial institutions, fintech companies and fintech regulators. Information sharing platforms and cross sector partnerships can be fostered to build this collaboration. To ensure the integrity of an open banking ecosystem, rigorous vetting processes must be applied for the third-party providers, including standards for accreditation as well as regular re-accreditation. Continued API security comes down to regular independent security audits, penetration testing, and vulnerability assessments for your API driven financial services. Academic effort to build a cybersecurity workforce and promote cybersecurity education among consumers of open banking services and employees in the financial sector is also very helpful to promote cybersecurity education.

The unique aspects of data sharing in open banking, including the need for strict consent and simple data handling guidelines, call for an enhancement of the existing data protection regulations to protect the user’s interests. Having an incident response team, escalation/responsibility and liability frameworks which are comprehensive can help with proper accountability in case of a security breach, or when fraud occurs from multiple parties. International cooperation in supporting global forums and creating bilateral agreements should be facilitated to develop harmonized standards for cross-border open banking initiatives. To strike a balance between cyber security and innovation in the Open banking sector, the policymakers should implement sandbox testing of new financial technology-based solutions before implementing regulations and reward organizations for exceeding minimum standards of security. Lastly, regular policy reviews and provisions for quick adjustments will help in keeping the regulatory landscape effective as technologies and cyber security threats evolve.

These policy recommendations can help in creating a robust, secure and innovative open banking ecosystem that promotes financial inclusion while also aiding with cyber security mitigation efforts.

References

Akamai. (2024). *API Security in Financial Services Mitigating risks and ensuring trust*. https://www.akamai.com/site/en/documents/white-paper/2024/api-security-in-financial-services-mitigating-risks-and-ensuring-trust.pdf

Ayade, P. (2024, September 16). How are open banking APIs levelling the playing field for traditional banks? GlobalFinTechSeries. https://globalfintechseries.com/featured/how-are-open-banking-apis-levelling-the-playing-field-for-traditional-banks/

Bank for International Settlements. (2019). *Basel Committee on Banking Supervision: Report on open banking and application programming interfaces.* Retrieved February 19, 2025, from https://www.bis.org/bcbs/publ/d486.pdf

Bianco, S. (2024, October 10). *Mitigating threats: Risk management and fraud prevention in open banking*. Powens. https://www.powens.com/blog/mitigating-threats-risk-management-and-fraud-prevention-in-open-banking/

Cloudflare. (n.d.). *Why use TLS 1.3?* Retrieved October 19, 2024, from https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/

Colangelo, G., & Khandelwal, P. (2025, January 23). The many shades of open banking: A comparative analysis of rationales and models. Internet Policy Review. https://policyreview.info/articles/analysis/open-banking-rationales-and-models

Competition and Markets Authority. (2023, January 12). Millions of customers benefit as Open Banking reaches milestone. Retrieved February 19, 2025, from https://www.gov.uk/government/news/millions-of-customers-benefit-as-open-banking-reaches-milestone

Consultative Group on Innovation and the Digital Economy. (2022). API standards for data-sharing (account aggregator). In *BIS Representative Office for the Americas.* Retrieved February 19, 2025, from https://www.bis.org/publ/othp56.pdf

Department of Electronics and Information Technology (DeitY). (2013). *National Cyber Security Policy - 2013*. https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013_0.pdf

IntelliswiftMarketing. (2023, October 13). *Banking & Finance: The impact of open banking and APIs on financial services innovation*. Nasscom | the Official Community of Indian IT Industry. https://community.nasscom.in/communities/bfsi/banking-finance-impact-open-banking-and-apis-financial-services-innovation

Drozdovica, J. (2024, December 11). *Open Banking Security: Navigating the New Age of Finance.* Retrieved February 18, 2025, from https://noda.live/articles/open-banking-security

Hall, I. (2024, October 17). *BIS launches project to connect open finance infrastructures across borders*. Global Government Fintech. https://www.globalgovernmentfintech.com/bis-project-aperta-cross-border-data-portability/#:~:text=The%20BIS%20states%20that%20about,scalability%20while%20increasing%20overall%20complexity

IndiaStack. (2017, June 6). WHAT IS INDIA STACK? Retrieved February 18, 2025, from https://web.archive.org/web/20170606184958/https://indiastack.org/about/

Kidd, C. (2025, January 3). *SIEM: Security Information & Event Management Explained.* Retrieved February 19, 2025, from https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html#:~:text=Short%20for%20%E2%80%9CSecurity%20Information%20and,can%20also%20increase%20organizational%20resilience.

Mastercard. (2024, November 2). What is open banking? Mastercard Newsroom. https://www.mastercard.com/news/perspectives/2024/open-banking-101/

Postman, Inc. (2023, December 14). What is an API? Retrieved February 18, 2025, from https://www.postman.com/what-is-an-api/

Perfios. (2025, February 13). How fintech APIs are shaping the future of financial services? Perfios. https://perfios.ai/blogs/how-fintech-apis-are-shaping-the-future-of-financial-services/#:~:text=APIs%20cut%20operational%20costs%20by,saving%2030%25%20in%20administrative%20costs.

Raj. (2025, January 3). *Why Protecting Third-Party APIs is Essential for Enterprise Security. AppSentinels.* https://appsentinels.ai/blog/why-protecting-third-party-apis-is-essential-for-enterprise-security/

Rajarathna, V., Yarger, B., & Salazar, G. (2024, December 21). Protect APIs Against Injection Attacks with Content Inspection. Kong Inc. https://konghq.com/blog/product-releases/content-inspection-injection-attack-protection

Rao, K. S. (2024, August 15). Digital transformation in the financial sector. *Times of India Blog*. https://timesofindia.indiatimes.com/blogs/kembai-speaks/digital-transformation-in-the-financial-sector/

Sadoian, L. (2025, January 8). India’s Blueprint for Cyber Safety: The National Security Policy 2013. Retrieved February 19, 2025, from https://www.upguard.com/blog/national-security-policy-2013#:~:text=The%20National%20Security%20Policy%202013%20includes%20initiatives%20to%20educate%20the,in%20maintaining%20national%20cyber%20hygiene.

Sharadin, G. (2023, December 21). *What is MITM (Man in the Middle) Attack | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/#:~:text=A%20man%20in%20the%20middle,distinct%20phases:%20interception%20and%20decryption.

Security Information and Event Management (SIEM): A complete guide. (2024, December 17). Tata Communications. https://www.tatacommunications.com/knowledge-base/siem-complete-guide/

Spiridon, Ș. (2024, June 20). API Security in Financial Services - Safeguarding Data for Open Banking Products. *Imagination*. https://www.itmagination.com/blog/api-security-in-financial-services-safeguarding-data-for-open-banking-products

Strachan, D. (2023, January 3). Open Banking around the world. Retrieved February 18, 2025, from https://www.deloitte.com/global/en/Industries/financial-services/perspectives/open-banking-around-the-world.html

Takyar, A. (2023, May 13). AI in financial planning: Personalizing financial advice for the digital age. LeewayHertz - AI Development Company.

https://www.leewayhertz.com/ai-in-financial-planning/#The-role-of-AI-in-financial-planning

Vagadia, S., & Kanniappan, S. (2023). *Open Banking Security-Risks and Solutions*. https://resources.trendmicro.com/rs/945-CXD-062/images/Updated_WhitePaper_OpenBanking.pdf

Verma, S. (2024, July 3). *Tackling banking API security challenges to create secure financial landscape*. Handcrafted by Robosoft Technologies Pvt. Ltd. All Rights Reserved Since 1996. All Trademarks Are Registered Marks or Trademarks of Their Respective Companies. https://www.robosoftin.com/blog/tackling-banking-api-security-challenges

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, *147*, 104051. https://doi.org/10.1016/j.cose.2024.104051

What is Adaptive Authentication? | OneLogin. (n.d.). OneLogin. https://www.onelogin.com/learn/what-why-adaptive-authentication

What is an API? - Application Programming Interface Explained - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/what-is/api/#:~:text=API%20stands%20for%20Application%20Programming,other%20using%20requests%20and%20responses.

What is MFA? - Multi-Factor Authentication and 2FA Explained - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/what-is/mfa/#:~:text=is%20AWS%20identity?-,What%20is%20MFA%20(multi%2Dfactor%20authentication)?,system%20password%20has%20been%20compromised.

What is Multi-Factor Authentication (MFA)? | OneLogin. (n.d.). OneLogin. https://www.onelogin.com/learn/what-is-mfa

What is Open Banking? Benefits, Challenges, & Regulations. (n.d.). https://www.getfocal.ai/knowledgebase/what-is-open-banking#:~:text=By%20breaking%20down%20traditional%20barriers,and%20drives%20overall%20industry%20innovation.

Wrixon, C. (2024, August 5). *The history of open Banking: industry, APIs and payments*. Ozone. https://ozoneapi.com/blog/the-history-of-open-banking-industry-apis-and-payments/#:~:text=Key%20Takeaways%20*%20Open%20banking%20began%20with,support%2C%20significantly%20transforming%20the%20financial%20services%20landscape.