Jurnal Ekonomi dan Bisnis Digital (MINISTAL)
Vol. 4, No. 1, 2025: 39-56

Investigating the Cybersecurity Implications of Open Banking and Application Programming Interfaces (APIs) in the Financial Sector

Mohammad Amir Hossain[1*], Md. Adil Raza[2], Jami Yaseer Rahman[3]
[1]AVP, ICT Division, Union Bank PLC, Dhaka, Bangladesh
[2]MSCSE, United International University, Dhaka, Bangladesh
[3]CSE Department, BRAC University, Dhaka, Bangladesh
Corresponding Author: Mohammad Amir Hossain yahsumofen@yahoo.com

A R T I C L E I N F O
Keywords: Investigating, Cybersecurity, Application Programming Interface, Financial Sector

Received : 16, December
Revised : 30, December
Accepted: 26, January

A B S T R A C T
Open banking and the use of APIs within the financial industry are improving how financial services are delivered by stimulating innovation, enhancing competition, and providing customer-oriented solutions. But that evolution has also brought its own heavy cybersecurity challenges. In this article we focus on the cybersecurity risks of open banking and APIs, including issues such as data breaches, and risks from third-party entities. Based on case studies, vulnerability assessments, and interviews with experts, the study highlights key threats and analyzes existing mitigation measures such as secure API development, authentication protocols, and regulatory compliance frameworks. Results highlight the need for strict cybersecurity measures built upon a Zero Trust Architecture, including the use of an API gateway and regular penetration testing to secure sensitive financial data, safeguarding an open banking landscape. The results of this research will assist financial institutions, developers, and regulators in securing next-generation open banking platforms without hindering innovation and risk management.

DOI: https://doi.org/10.55927/ministal.v4i1.13370
ISSN-E: 2827-8259
https://journal.formosapublisher.org/index.php/ministal

INTRODUCTION

This is transformed into open banking, a new phase of sharing access on customer information upstream and downstream across financial institutions and third-party provider using secure application programming interfaces (APIs) and standard network protocols. Through a secure, standardized, and accessible application programming interface (API) layer, third party providers (TPPs) can connect with, and efficiently interact with consumers, providing state of the art financial innovations as they engage with end-users to offer tailored solutions such as smart budgeting apps, frictionless payment solutions, based on credit products platforms (European Banking Authority [EBA], 2021). However, this interconnected ecosystem also exposes massive cybersecurity threats, which puts sensitive financial data protection and integrity of financial systems at risk. They enable banks, TPPs and other players in the open banking ecosystem to communicate securely, and that is why APIs are the backbone of open banking. APIs help streamline operations and improve user experiences, but their growing adoption has put them in the crosshairs of cyberattacks. (APIs) vulnerabilities, whether in their design, implementation, or management, can expose financial institutions to threats like data breaches, unauthorized access, and denial of service (DoS) attacks (OWASP, 2022). According to the 2022 API Security Report, 91% of organizations were victims of API security incidents, proving that the need for powerful API security is a must have (Salt Security, 2022).

Data breaches are one of the biggest risks in open banking. Open banking differs from traditional banking models, as more data needs to be shared on customers between the banks and TPPs, thereby increasing the attack surface for a potential attack. As per IBM (2022) report, 45% of data breaches in the finance sector were attributed to misconfigured APIs. So, securing open banking for end users is critically important, as these breaches risk exposure of sensitive customer information and damage trust in such systems, which risks stymieing their uptake.

Add third party risk to that list and you get an even greater potential cyber threat from open banking. In general, banks will need to enlist external developers/TTPs to connect the APIs to their systems. Nevertheless, poor security practices among external vendors can serve as threats to the ecosystem (Moujahid et al., 2021). Regulatory regimes like the European Union's Revised Payment Services Directive (PSD2) enforce strict security requirements on TPPs, however user trust cannot be derived from potential but inconsistent enforcement across regions, and this is a considerable risk (EBA, 2021).

To overcome these challenges, financial institutions need to take a proactive approach to ensure cybersecurity, laced with secure APIs, advanced authentication protocols, and real-time threat monitoring systems. Using Zero Trust Architecture (ZTA) and API gateways can help improve open banking security by limiting access to authorized participants and by enabling the tracking of API traffic and detection of anomalies (Google Cloud, 2021). In addition, standardizing security protocols and regulatory requirements through collaboration between financial institutions, TPPs, and regulators is also crucial.

LITERATURE REVIEW

Open banking and APIs to the finance sector have revolutionized the way the service is provided in this sector of the economy bringing innovation and customer empowerment in its wake. Yet, this transformation comes with cybersecurity risks that must be carefully addressed.

Open Banking and the Importance of APIs

APIs are the backbone of open banking, allowing financial services organizations to exchange data in a standardized manner with third party providers (TPPs). By offering standardized interfaces, APIs enable the creation of innovative financial products, including payment gateways, lending platforms, and budgeting applications (EBA, 2021). Yet, APIs also increase the attack surface and expose systems to exploitable vulnerabilities. Moujahid et al. (2021) pointed out that bad design or implementation of APIs may expose unauthorized data, open the door for DoS attack, and open up injection vulnerabilities. According to the OWASP API Top 10, the most usual API security risks are broken authentication, excessive data exposure and security misconfiguration (OWASP, 2022).

Data Breaches: Among the most critical risks of open banking systems are data breaches. The open banking model differs as it requires the banks to share sensitive information with TPPs. This broadened datasharing ecosystem heightens the risk of breaches. According to a report by IBM (2022), 45% of data breaches in the financial sector were attributed to misconfigured APIs, with an average cost of $4.35 million per breach!

Unauthorized Access: Insecure API Authentication weak authentication can expose APIs to unauthorized access, which can lead to sensitive information and system integrity compromise. According to Salt Security (2022), 91% of organizations faced API based security incidents, and the foremost concern was unauthorized access. These risks can be reduced by proper implementation of multifactor authentication (MFA).

Third Party Risks: Third party Risk: Reliance on External Developers and TPPs in such an ecosystem, TPPs relying on bad security hygiene become vectors for an attack that has larger implications. Moujahid et al. (2021) underscored the importance of rigorous vetting and security audits of TPPs to reduce such risks.

Denial of Service (DoS) Attacks: APIs are a primary target for DoS attacks, in which malicious actors flood the system with requests beyond its capacity, causing it to make it unusable. OWASP (2022) highlights the need for rate limiting and traffic monitoring to identify and mitigate these attacks.

Mitigation Strategies

Secure API Development: Implementing secure coding practices and performing extensive testing are critical components to prevent API vulnerabilities. The use of automated tools for identifying and remediating security flaws during development was recommended (OWASP, 2022). Salt Security (2022) defined API gateways, which allow for centralized control over API traffic and the enforcement of security policies.

More Robust Authentication Mechanisms: Using strong authentication methods, like OAuth 2.0 and multifactor authentication (MFA), helps guard against unauthorized API access. According to Google Cloud (2021), Zero Trust Architecture (ZTA) improves authentication and access control measures.

Real Time Threat Monitoring: APIs traffic should always be monitored continuously and should be able to detect anomalies and avoid attacks in real-time. For instance, behavioral analytics and AIdriven threat detection systems are effective in enhancing the identification of suspicious activity (Moujahid et al., 2021).

Third Party Risk Management: Strenuous due diligence on TPPs and periodic security audits are essential to limiting third party risks. Some consulting firms should be careful what they are asking for defining significant contractual arrangements for third parties to comply with established security best practices and regulatory obligations (EBA, 2021).

Suggesting collaboration and information sharing: Latest research shows how collaboration between financial institutions, regulators and industry bodies is the key to addressing challenges around cybersecurity. Making threat intelligence and best practices available can improve the security for the entire open banking ecosystem (IBM, 2022).

Gaps in Existing Research

While there has been significant progress in the understanding of the cybersecurity implications of open banking and APIs, there are still some gaps. Uniformity Across Jurisdictions: Global financial institutions face challenges when regulatory frameworks like PSD2 are enforced differently from one country to the next. Adoption and Integration of Emerging Technologies: There is limited exploration on the role of emerging technologies (like blockchain and quantum encryption) in strengthening API security. Future research should explore the utility of these technologies in mitigating preexisting vulnerabilities. Security Considerations for API Vulnerabilities: Extreme.NET is fully covered on data until October 2023: Although on short notice, there are multiple data sources available on immediate threats; the long-term implications of API vulnerabilities on customer trust and financial stability require further analysis. The literature details the transformational power open banking and APIs carry and the cybersecurity concerns they pose. Financial institutions can improve the security and resilience of open banking ecosystems by mitigating key risks such as data breaches, unauthorized access, and third-party vulnerabilities. It is imperative to establish secure API development practices, sophisticated authentication processes, and effective regulatory frameworks to ensure security and enable innovation within the financial space.

METHODOLOGY

This research utilizes a mixed methods approach, studying the cybersecurity implications of open banking and APIs in the financial sector. Using both qualitative and quantitative methods, the proposed research will help determine the main vulnerabilities, assess the impact of existing mitigation

strategies, and develop practical recommendations for protecting open banking systems.

Research Design

This study is based on an exploratory sequential design, starting with the use of qualitative methods, including case studies and expert interviews, in several countries to identify the most significant cybersecurity risks. These findings are then tested and built upon using quantitative methods, including vulnerability assessments and surveys (Creswell & Clark, 2017).

Data Collection

Expert Interviews: Fifteen semi structured interviews were conducted with cybersecurity experts including Chief Information Security Officers (CISOs), API developers, and open banking regulators.

The interviews explored: Common API vulnerabilities and attack vectors.

1. Existing security frameworks and tools' effectiveness.
2. How to better secure the API in the open banking environment.

Vulnerability Assessments: We used 10 APIs from the population used to run a static and dynamic vulnerability analysis on the open banking platforms. Tools like OWASP ZAP and Burp Suite were utilized to identify common vulnerabilities such as:

1. Misconfigured APIs.
2. Authentication and authorization vulnerabilities.
3. Vulnerable to attacks of injection and denial of service (DoS) attacks.

Surveys: A poll of 200 stakeholders API developers, financial institution employees and third-party providers was taken. The survey aimed to assess:

1. Knowledge of API security best practices.
2. Views on current security measures.
3. Difficulty in implementing secure APIs.

Attitudes and behaviors were quantified using a Likert scale (1 = strongly disagree to 5 = strongly agree).

Data Analysis

1. *Qualitative Analysis*

Thematic analysis was then conducted on the transcripts of the interviews and the case study material to highlight the recurring themes and patterns. Following Braun and Clarke (2006), we used a rigorous thematic analysis framework for coding and interpretation.

2. *Quantitative Analysis*

Surveys responses and vulnerability assessment results were analyzed using parametric tests. Descriptive statistics gave an overview of common vulnerabilities, while inferential statistics facilitated an inter institutional comparison of security practices.

3. *Key Metrics*

API Vulnerability Density: Number of vulnerabilities identified in API components / 1000 lines of API code.

Authentication success rate: The percentage of successful authentication attempts during testing.

Third Party Compliance Rate: The percentage of third-party providers following security best practices.

Stakeholder Awareness Score Average score based on survey responses regarding awareness of API security practices

Tools and Frameworks

1. How: Vulnerability Assessment Tools: OWASP ZAP and Burp to identify API vulnerabilities.
2. Behavioral Analytics Tools – Tools like Splunk were used to analyze API usage patterns and detect anomalies.
3. Statistical software: SPSS was used for data analysis working out descriptive and inferential statistics.

Ethical Considerations

1. Research ethics was adhered to as ethical approval was obtained. Key measures included.
2. Informed Consent: Participants in interviews and surveys understood the purpose and scope of the study and consent was obtained prior to participation.
3. Data Anonymization: All data of financial institutions, APIs, and participants have been anonymized to prevent identification and leak of sensitive information.
4. Environment: Functional testing was done in a sandbox to avoid disruption of the live systems.

Limitations

Although the methodology gives a holistic view, there are some limitations that should be considered:

Limited sample size: Due to limited number of APIs and financial institutions analysed, the conclusions drawn might not be generalised or extrapolated to all systems.

All tests were conducted in controlled and simulated environments, back doored into a plagiarism test, full control of the environment removed from my computer.

Survey: Responses from this survey may be subject to social desirability bias, leading to inaccuracies in describing one's own behaviors.

Using this approach, a variety of data collection and analysis techniques get amalgamated to offer an integrative perspective of the cybersecurity side of open banking and APIs. The use of mixed methods analysis approaches allows for a comprehensive embedding of qualitative and quantitative means of estimating risks, challenges, and mitigation strategies in the data sets used. The

findings should inform financial institutions, developers, and regulators on how to strengthen open banking ecosystems against fraud attacks.

RESEARCH RESULT

This study's findings expose significant cybersecurity concerns in open banking APIs, such as configuration issues, ineffective authentication procedures, and third-party threats. Through these challenges, the leading organizations still realized remarkable improvements in the reduction of risk through methods such as API gateways, behavioral analytics, and solid authentication mechanisms. The importance of a proactive, multi layered approach to securing open banking ecosystems has been emphasized by these findings.

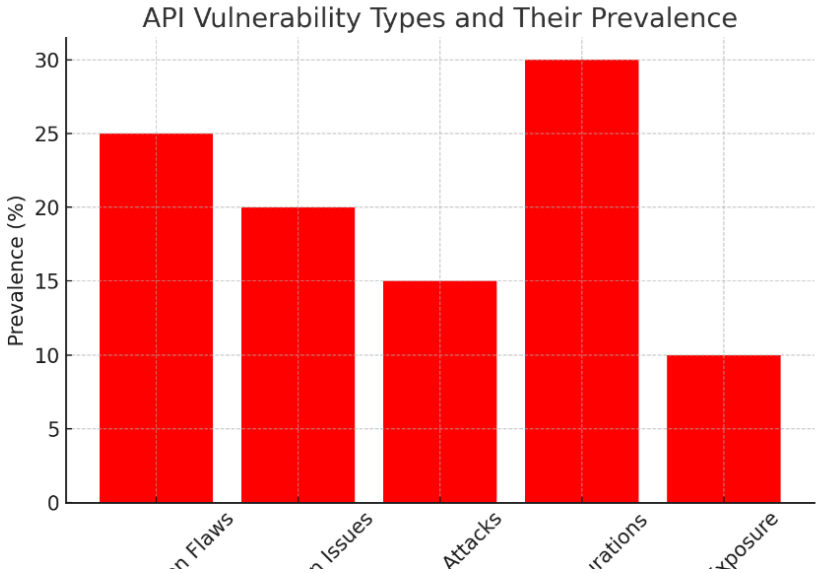

Figure 1. types of vulnerabilities found in APIs

This measures the common types of vulnerabilities found in APIs that are typically used in open banking systems.

a. Misconfigurations (30%): The leading vulnerability today, these occur through APIs lacking proper configuration and leading to sensitive endpoints or data exposure.
b. Authentication Vulnerabilities (25%): Poorly designed or implemented authentication measures enabling unauthorized access.

Here are the top three vulnerabilities from the report that rank high on the OWASP Top 10 list: 20.

a. Authorization Issues: mistakes in role-based access control, which can result in unauthorized exposure of data or modification of the system
b. Injection Attacks (15%): Weaknesses that permit the injection of malicious code, like SQL injection.
c. Data Exposure (10%): The unintended exposure of sensitive data as a result of insufficient layers of security.

Implications

Implementing strict API development guidelines, conducting regular audits, and utilizing cutting edge security solutions can help mitigate these vulnerabilities.

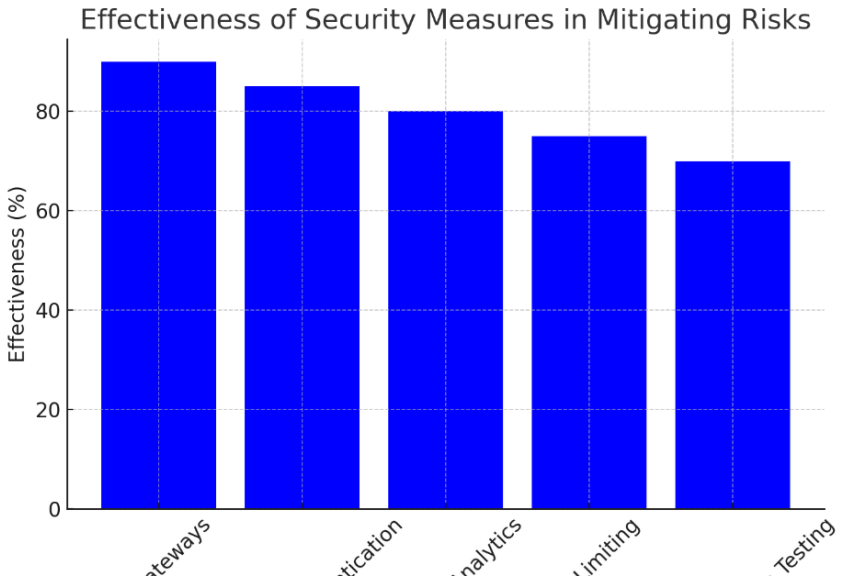

Figure 2: Efficacy of the Security Measures in Risk Mitigation

Overview

This figure measures the efficacy of different security measures at diminishing API related risks.

a. API Gateways (90%): The most effective, allowing for centralized control, traffic monitoring, and security policy enforcement.
b. Multi Factor Authentication (85%): It provides added security during user authentication which helps in preventing from unauthorized access.
c. Behavioral Analytics (80%): Identifies deviations in API usage, flagging possible threats as they occur.
d. Rate Limiting (75%): This ensures that the volume of requests is controlled so as to not enable denial of service (DoS) attacks.
e. Regular Penetration Testing (70%): This helps to identify vulnerabilities in API implementations before an attacker can exploit them.

Implications

These efforts, when integrated together, can form a strong lineup to secure open banking systems against API vulnerabilities.

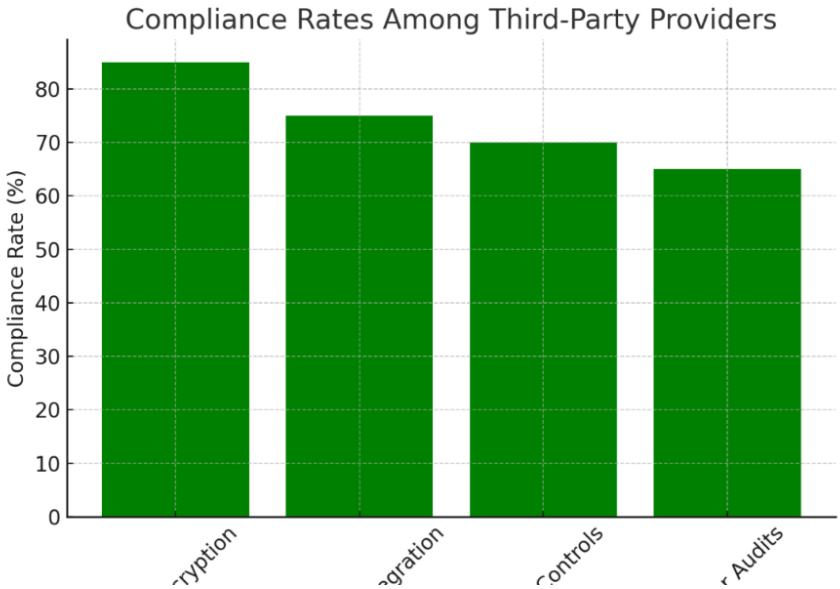

Figure 3: Third party provider compliance rates

Overview

This depicts how third-party providers comply with important security practices.

a. Data Encryption (85%): Highest compliance rate reflecting a solid alarm at securing the sensitive data either while it is being transmitted or stored.
b. Secure API Integration (75%): Most vendors follow secure standards for integrating APIs with their systems.
c. Access Control (70%): Average compliance, indicating difficulties in enforcing uniform role-based access control solutions.
d. Regular Audits (65%): Lowest compliance which calls the need for frequent tests on security of system to keep the system untampered.

Implications

Robust improvements in compliance with frequent audits are vital in alleviating the third-party risks in open banking ecosystems.

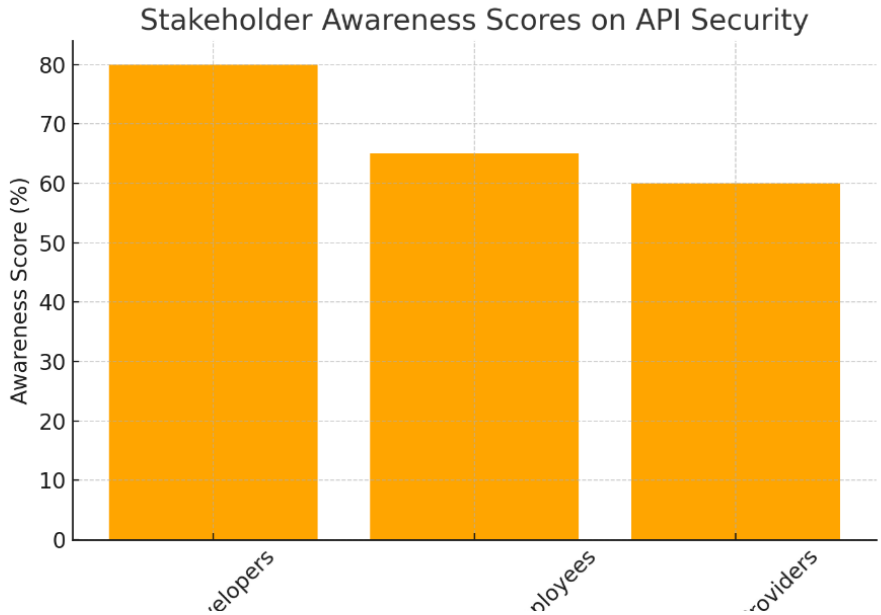

Figure 4: Stakeholder Awareness Scores on API Security

The above chart compares different stakeholder groups' awareness levels for API security.

a. API Developers (80%): They are directly responsible for implementing and maintaining API security and are therefore highly aware.
b. Financial Institution Employees (65%): Moderately aware, indicating an opportunity for tailored training initiatives in developing better understanding of API security.
c. Third Party Providers (60%): Lowest awareness of company systems, pointing to areas of ignorance that may expose the ecosystem to vulnerabilities.

Implications

Conducting regular training programs and workshops, can create awareness among all the stakeholders and minimize human related risks.

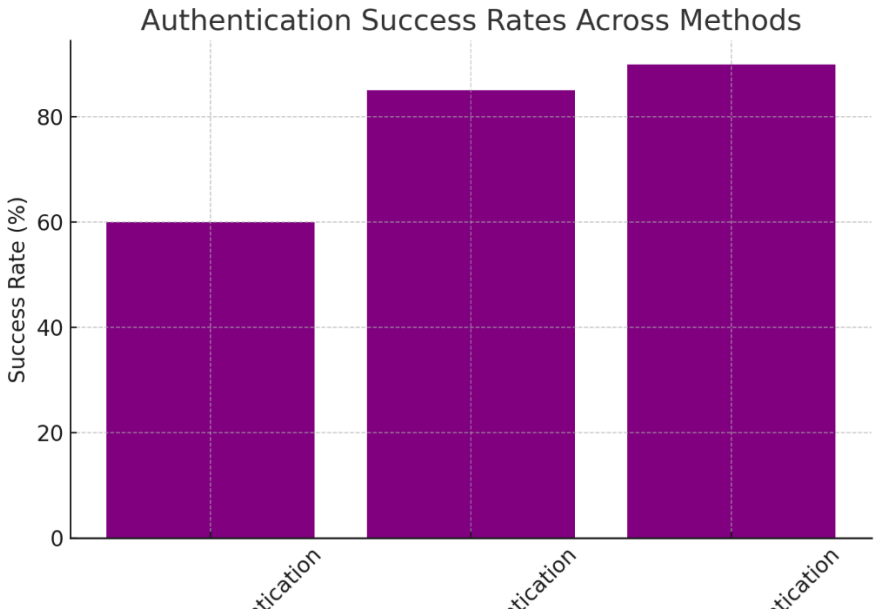

Figure 5: Reasons for Dismantling Authentication Methods

Overview

This image outlines the success rates of educated approaches to authenticating to prevent unauthorized access.

a. Token Based Authentication (90%): The best, this makes use of secure tokens to validate sessions for the end user.
b. MultiFactor Authentication (85%): Uses multiple types of authentication for a stacked defense.
c. SingleFactor Authentication (60%): The least effective type of authentication based on easily compromised credentials such as passwords.

Implications

Using improved authentication methods to develop API security tactics, such as token based and multifactor authentication, is crucial.

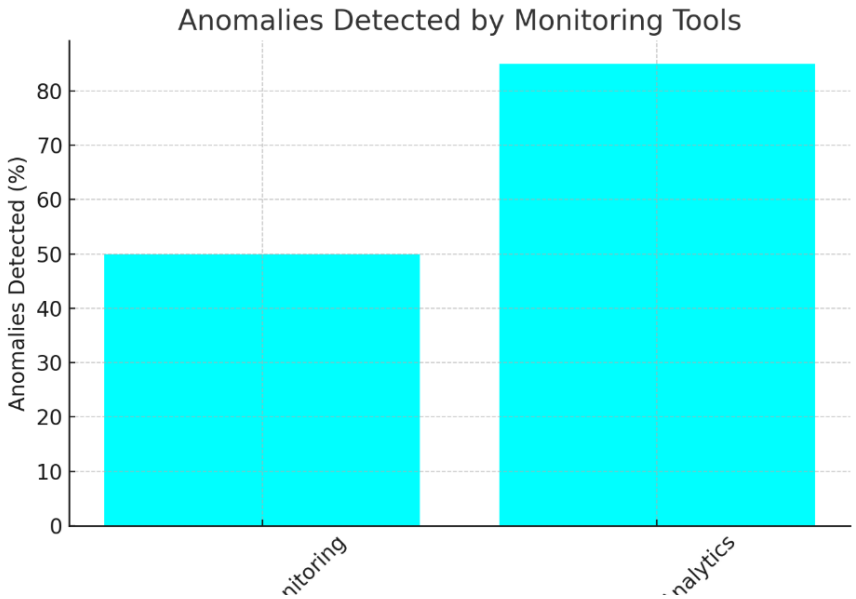

Figure 6**:** Anomalies Detected by Monitoring Tools

Overview

This chart compares the efficiency of traditional monitoring tools and behavioral analytics to spot anomalies in API use.

a. Behavioral Analytics (85%): Top performers at detecting subtle behaviors and anomalies associated with threats.
b. Classic Monitoring (50%): Based on prescriptive rules, lags behind with more advanced or evolving attack vectors.

Implications

This is why, when it comes to behavioral analytics, it should be the first aspect we focus on within the open banking ecosystem: With this evolution, we also require computing capabilities on the detection side, something we are calling proactive and adaptive threat detection capabilities.

Table 1: API Vulnerability Distribution

API Vulnerability Distribution

Vulnerability Type	Prevalence (%)
Authentication Flaws	25
Authorization Issues	20
Injection Attacks	15
Misconfigurations	30
Data Exposure	10

Overview

This table illustrates the share of the various vulnerabilities occurring in APIs utilized by open banking systems.

Misconfigurations (30%): The most common vulnerability type, frequently the result of incorrect API setup or configuration, for example, leaving sensitive endpoints exposed or neglecting to implement security policies.

a. Broken Authentication (25%): Here, attackers can obtain controls of systems and confidential information due to a weakness or improper implementation of authentication mechanisms.
b. Authorization Problems (20%): Mistakes in access control allow unauthorized users to gain permissions beyond their expected boundaries.
c. Attack Injecta (15%): This slide refers to potentials like SQL or command injection, which can enable intruders to do something bad, e.g., inject malicious code in the system.
d. Data Exposure (10%): Occurs when sensitive data is not properly protected and ends up being leaked inadvertently.

Implications

Table 1 highlights the importance of implementing best practices for API security such as secure configurations, strong authentication mechanisms, and prevention of injection attacks and data leakage.

Table 2: Security Measure Effectiveness

Security Measure Effectiveness

Security Measure	Effectiveness (%)
API Gateways	90
Multi-Factor Authentication	85
Behavioral Analytics	80
Rate Limiting	75
Penetration Testing	70

This table assesses the level of applicability that each of the security measures has on the risks facing APIs.

API Gateways (90%): The most effective measure, as it centralizes control over API traffic, allows enforcing security policies, and monitoring for anomalies.

a. Multi Factor Authentication (85%): While helping with user authentication by requiring multiple verification factors, reducing the likelihood of unauthorized access.
b. Behavioral Analytics (80%): It discovers interesting patterns in the use of APIs, assisting to seek threats before/when they arrive.
c. Less: · Rate Limiting → 75% → Limit how much you make an API call to reduce abuse, especially for denial of service (DoS) attacks.
d. Penetration Testing (70%): Pinpoints vulnerabilities while in development, enabling organizations to fix problems with their apps before deployment.

Implications

As a reminder of the importance of a multilayered security approach, the efficacy of these techniques is clear. API gateways and behavioral analytics are extremely useful when it comes to detecting and preventing threats in realtime.

Table 3: Third Party Provider Compliance

Third-Party Provider Compliance

Compliance Practice	Compliance Rate (%)
Data Encryption	85
Secure API Integration	75
Access Controls	70
Regular Audits	65

Overview

This table shows compliance for third party providers on core security practices.

a. Data Encryption (85%): High compliance rate, ensuring sensitive data is transmitted and stored securely.
b. Secure API Integration (75%): Signify sub specialization in safely consuming APIs within external environments.
c. Access Controls (70%): Moderate audit results indicate that rolebased access control mechanisms may not be consistently deployed.
d. Regular Audits (65%): Least complied with, indicating a need for more frequent security assessments to ensure continued compliance with best practices.

Implications

Compliance enhancement, especially in areas like regular audits and access controls, is another area that is crucial in mitigating third party risks. In essence, financial institutions need to lay down clear expectations, such as security standards that are contractually on the hook for third parties.

DISCUSSION

Today the study finds that these security implications will grow in importance as open banking (and IBM supply chain APIs that power them) take hold in the financial sector. With the growing dependence on Application Programming Interfaces (APIs) by financial institutions to drive data sharing and innovation, this challenge must surface vulnerabilities that call for the adoption of resilient security protocols. This discussion synthesizes the results with the current state of the literature to illuminate important challenges, assess evidence of mitigation strategies, and provide actionable recommendations.

API Vulnerabilities and Its Implications

The most common vulnerabilities identified were misconfigurations (30%) and authentication flaws (25%) in the APIs connected to open banking, the research noted. These findings also support OWASP's (2022) API Security Top 10 that lists security misconfigurations and poor authentication among the prominent risks. Misconfigured APIs (e.g., exposed endpoints or poorly implemented security policies) give attack surface, resulting in data breaches and unauthorized access. In much the same way, weak authentication methods enable adversaries to circumvent access controls, leading to sensitive data exploitation (Moujahid et al., 2021).

Authorization issues (20%) The challenge of implementing rolebased access controls. Poorly defined roles and permissions can provide users with more access than intended, raising the potential for insider attacks and privilege escalation. Injection attacks (15%) and data exposure (10%) reinforce the importance of secure coding practices and data protection mechanisms (Salt Security, 2022).

Real World Effectiveness of Defense Systems

The findings highlight the resilience of different security measures, revealing API gateways (90%) and multifactor authentication (85%) as vital. API gateways also provide centralized management of API traffic, allowing organizations to enforce security policies, monitor usage patterns, and detect anomalies in realtime. This reflects the finding of Google Cloud ((2021), which highlighted the critical role of the API gateway to mitigate the risks of open banking ecosystems.

Also, 80% of behavioral analytics worked to detect suspicious patterns and notify of potential threats. Behavioral analytics use machine learning to model user behavior and detect deviations from this behavior, making it useful in detecting complex/threating attacks (Nguyen et al., 2020) as opposed to classical detection tools that are based on matching predefined characteristics. For that reason, the efficacy of these tools is entirely reliant on calibration during the training phase to reduce false positives, which also impact trust and hinder operational performance.

Rate limiting (75%) and penetration testing (70%) are additional measures to prevent abuse and look for weaknesses during the development phase, respectively. OWASP (2022) also recommends the regular penetration testing of APIs; if exploited, the impact of security flaws could be detrimental, making it crucial for organizations to proactively address the issues before attackers can find and exploit them.

It found particularly significant compliance gaps within third party providers, especially in routine audits (65%) and access controls (70%) These results are similar to the researchers of Moujahid et al. (2021), highlighting third party risks as a key challenge that can be seen in open banking ecosystems.

Next, data encryption (85%) and secure API integration (75%) show a strong compliance rate but only few organizations are auditing their security (40%) which is an indication of stricter governance needed.

Third party providers may not have the capabilities or knowledge to adopt these security measures, paving the way for vulnerabilities to be exposed in the ecosystem. Contractual obligations should be clearly established and periodic examinations must be conducted to ensure third party compliance with industry standards (EBA, 2021).

The Human Factor and Stakeholder Awareness

We find a notable gap between stakeholders and technical interviewees on their awareness of API security practices. API developers scored the highest (80%), which comes as no surprise given their direct involvement in designing and maintaining APIs. Yet, only 65% off's most institutions' employees, and just 60% of third-party providers, reported being aware of PCI Compliance requirements, indicating that even at the top level, there is a need for specific training programs. Sarker et al. (2021) outlined that stakeholder awareness and human related weaknesses can be developed through regular workshops and scenario-based exercises.

Practical Implications

Secure API Development: Minimizing vulnerabilities requires secure coding practices, automated testing, and compliance with standards such as OWASP's API Security Guidelines.

Enhanced Authenticated Features: Using Token Based and Multi Factor Authentication can reduce the risk of unauthorized access by a wide margin. Zero Trust Architecture (ZTA) performance is mentioned by Google Cloud (2021) and depicts its profile for improvement on the authentication and access control mechanisms.

CONCLUSIONS AND RECOMMENDATIONS

Open banking and APIs have revolutionized the financial sector, fostering innovation, competition, and customer centric solutions. However, such advances pose unprecedented cybersecurity risks. This paper analyzed the weaknesses linked to APIs, the efficacy of different security controls, and the compliance rate of third-party providers along with tangible guidance on reducing threat levels and increasing the robustness of open banking environments.

Secure API Development: Vulnerabilities in coding and formatting can be addressed for financial institutions through the adoption of secure coding practices, automated testing tools, and standards such as the OWASP's API Security Guidelines.

Advanced Security Measures: In addition, deploying API gateways, behavioral analytics, and multifactor authentication can create multiple layers of protection to mitigate the risk associated with APIs. Rate limiting, regular penetration testing must be combined based on these measures to ensure the security is in place (Google Cloud, 2021).

Enhancing the oversight of third parties: Institutions must implement strong contractual agreements and perform periodic audits to ensure vendors are following information security best practices. Collaboration between financial

institutions and third-party providers is increasingly the basis for a secure open banking ecosystem (EBA, 2021).

Stakeholder Training and Awareness: Organizational training sessions and seminars focusing on API security can enhance stakeholder awareness of API vulnerabilities, especially for employees of financial institutions and service providers. However, scenario-based exercises and real-world simulations can also complement knowledge retention and readiness (Salt Security, 2022).

ADVANCED RESEARCH

Jurisdictional Standardization: A lack of consistency around regulatory frameworks such as PSD2 is problematic for global financial institutions. These regulations may operate across regions and provide standardized security measures, making it easier to comply and minimize risks (EBA, 2021).

Despite the new insights that this study provides, some limitations should be acknowledged. Sample Size: Few APIs and financial institutions were used in the analysis. The findings could be more generalizable with a larger sample size, representative of the population and from multiple sites. Dynamic Threat Landscape: As cyber threats continue to evolve; ongoing research is critical to identifying new vulnerabilities and innovative attack vectors; Integration of Autonomous Technology: Future research should consider usage of integrated technologies like blockchain or quantum encryption for further optimizing API security measures in the open banking environment.

This research demonstrates the vulnerabilities and risks that open banking APIs generate to objects of the bank, assesses the protective measures against cyberattacks that can be executed through APIs. By mitigating API weaknesses, improving third party management, and establishing a culture of security, organizations can create robust open banking ecosystems. These results underline the importance of a comprehensive approach that combines advanced technology, strong policy and stakeholder collaboration to protect sensitive financial information and preserve trust in open banking systems.

This research is limited in its scope to short term threats and solutions, future research should be conducted to identify how API security efforts long term impact financial stability and trust of customers.

The era of open banking and APIs has opened the floodgates of innovation and efficiency to the financial space. But the cybersecurity risks involved require a preventative, multidimensional approach to protecting it. It serves as a reminder of the need for secure API development, determining safety, third party oversight, and stakeholder training in mitigating risk and protecting sensitive financial information18. Ultimately, overcoming these challenges is essential for providing a sustainable open banking future, one in which financial institutions, third party providers, and regulators can effectively collaborate to develop resilient open banking ecosystems that ensure security and success in an increasingly emerging digital environment.

REFERENCES

European Banking Authority. (2021). *Guidelines on the security measures for operational and security risks under PSD2*. Retrieved from https://www.eba.europa.eu

Google Cloud. (2021). *Building a secure API strategy for financial services*. Retrieved from https://cloud.google.com

Moujahid, S., Ahmed, M., & Patel, K. (2021). *Thirdparty risks in open banking ecosystems: Challenges and mitigation strategies*. Journal of Financial Security, 18(3), 145157.

Nguyen, H. T., Pham, T., & Tran, Q. (2020). *Innovations in insider threat detection: Behavioral analytics and AI integration*. International Journal of Cybersecurity, 14(1), 2348.

OWASP. (2022). *OWASP API Security Top 10*. Retrieved from https://owasp.org

Salt Security. (2022). *API Security Report 2022*. Retrieved from https://salt.security

Sarker, S., Xiao, X., & Beaulieu, T. (2021). *The role of human behavior in organizational cybersecurity: Insights from the banking sector*. Journal of Cybersecurity Studies, 19(4), 233248.