NuSummit Cybersecurity

WHITEPAPER

Securing the Digital Banking & Financial Services Ecosystem with API Security & Governance

API SECURITY

Table of Contents

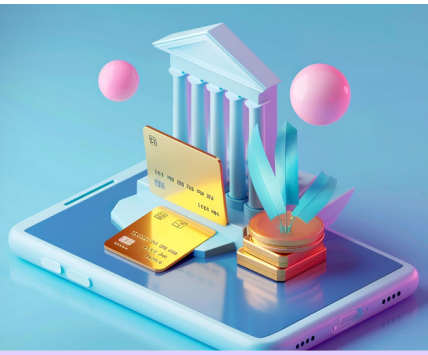
Need for Digital Transformation in Financial Institutions

Digital transformation is reshaping global financial institutions and fundamentally changing how the end customers perceive banking. Existing customers, who are already accustomed to smooth digital experiences in oin other industry domains such as retail and entertainment, now expect the same from financial institutions. With the rapid adoption of digital technologies, particularly in payments and personal finance, traditional banks will become irrelevant if they do not modernize.

One prime reason for this ongoing transformation is the emergence of digital payment platform providers. These FinTech companies have raised the bar by offering user-friendly, digital-first platforms unburdened by legacy systems and manual operating models. These agile competitors address changing customer expectations and innovate rapidly. Traditional banks must react by streamlining processes and offering frictionless digital experiences to remain competitive.

Apart from customer expectations, digital transformation lowers transaction costs, makes operations more efficient, and enables faster returns on investment on effective implementation. It also enhances compliance capabilities— modern platforms are better equipped to adapt to dynamic regulatory requirements and support ongoing audit and litigation readiness.

Trends in Digital Banking & Financial Services



Hyper-Personalization Through AI

Banks now leverage artificial intelligence to transform raw data into meaningful customer insights. By analyzing transaction patterns, digital interactions, and financial behaviors, institutions deliver truly personalized services. Modern banking AI doesn't just react to customer needs—it anticipates them. Banks now identify financial opportunities or challenges before they arise, positioning themselves as proactive financial partners. This shift from reactive to proactive service has deepened customer relationships and increased institutional loyalty.

API Banking

API banking enables banks and other financial organizations to expose their products and services through third party applications. This would help banks to provide services quickly to customers along with the flexibility for product customization. Open APIs play a significant role in providing banking services with high availability through third party service integration.

Embedded Finance Integration

Financial services now integrate seamlessly into non-banking platforms and everyday activities. Whether shopping online, managing business operations, or planning travel, customers access banking services without leaving their primary activity platform. This integration creates new revenue streams for banks through partnerships with digital platforms and service providers. Banks provide the financial infrastructure while partners deliver the customer interface, creating mutually beneficial relationships.

IOT Enabled Payment Devices

In this era, Internet of Things is attractive for banking and financial organizations to provide advanced payment experience with a variety of payment methods, the use of payment applications, tracking devices. NFC chips and sensors etc. Banks have already started accepting payment.

Benefits of Digital Banking Initiatives

Ease of Banking

Internet connection has enabled banking benefits to one and all. Using Smartphone apps, customers from both urban and rural and locations can check their account balance. transfer funds, check transaction history, raise support issues, etc. Thus, improving customer experience. satisfaction and service.

More than Websites

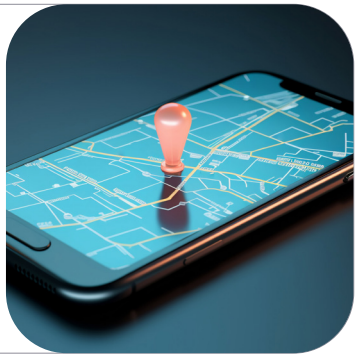
Banks have moved a step further by introducing added features to the websites, apart from the basic banking services. such as financial planning tools. loan calculators, etc.

Direct Connect with Customers

Reduction in intermediation costs since banks can directly deal with customers, reducing third party service providers. This would help the banks to strengthen the direct relationship with customers and to improve the time to market.

Mobility of Services

Ease of Virtual banking for customers, as they have access to Banking services at the tip of their fingers by use of mobile apps/ websites thus enabling easier banking operations and services.



Cost Effective Solution

With mobility and convenience. costs for banks and customers have reduced. in addition to the less human errors due to automations via online banking.

Digital Strategies

Banks have put in efforts and wisely invested in adopting **Digital Strategies** to compete with the non-banking sectors.

Example: 'Augmented reality' technology. initiative by Common Wealth Bank of Australia, through a mobile app to help inhabitants buy home/property.

Advanced Data Analytics

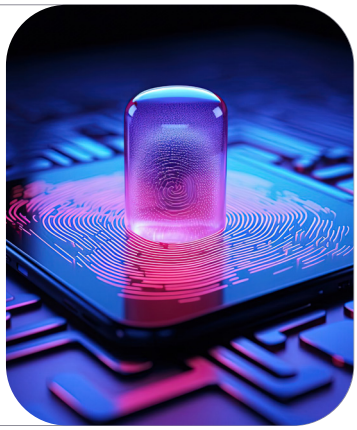
Banks are helping customers to make informed decisions in their digital journey using Advanced data analytics and big data. specifically in Marketing and Channels.

Example: Bank of England uses advanced analytics units to develop and apply advanced analytical techniques.

Digital Authentication and Security

Improving the user experience overall while enhancing the security against hackers and other threats.

Example: Apple is offering TouchID. a finger print recognition feature; Many banks are working on initiatives to use technologies to replace dependency on passwords.



Key Security Issues

Imagine this: A major bank suffers a massive data breach. Customer credit card information, social security numbers, and transaction data – all exposed. The culprit? It is not a sophisticated phishing attack but a vulnerability in a seemingly innocuous application programming interface (API).

This scenario is not far-fetched. In today's hyper-connected world, APIs are the invisible threads that weave together our digital experiences. APIs facilitate seamless data exchange from the apps on your phone to the systems that power global commerce. However, this interconnectedness also creates a significant security risk.

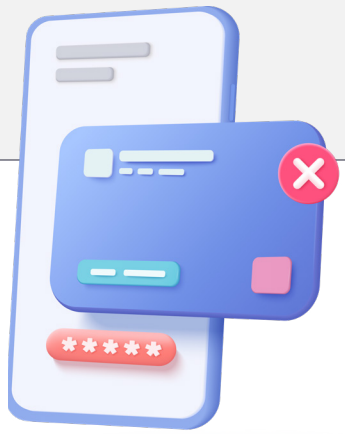
According to the 2024 Gartner API Strategy Survey, 82% of respondents stated that their organizations leveraged APIs internally, while another 71% reported using APIs provided by third-party vendors such as SaaS providers.[i] The API-first paradigm will evolve as technology service providers (TSPs) globally lead Gen AI adoption across application interfaces. Gartner predicts that by 2026, more than 30% of the demand surge in APIs will be driven by AI and tools using large language models (LLMs).[ii]

[i] Source: https://www.gartner.com/en/documents/5551595

[ii] Source: https://www.gartner.com/en/newsroom/press-releases/2024-03-20-gartner-predicts-more-than-30-percent-of-the-increase-in-demand-for-apis-will-come-from-ai-and-tools-using-llms-by-2026

Proof of Problems

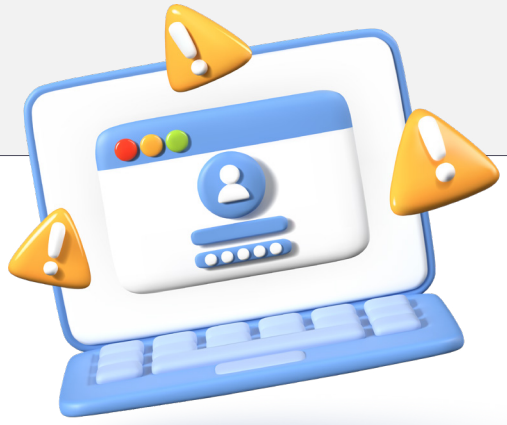
Banking frauds rise, the amount involved jumps eightfold: RBI report 2024



The Reserve Bank of India reported the number of frauds during April-September 2024 stood at 18,461 involving Rs 21,367 crore compared to 14,480 cases involving Rs 2,623 crore in the comparative period of 2023. Based on the date of occurrence of frauds, in 2023-24, the share of internet and card frauds in the total stood at 44.7% in terms of amount and 85.3% in terms of number of cases.

Source: https://www.business-standard.com/industry/banking/banking-frauds-rise-in-h1fy25-amount-involved-jumps-8-time-rbi-report-124122600769_1.html

Growing attacks in the Global Banking ecosystem



In 2023, a breach at NCB Management Services affected Bank of America's 495,000 customers. This security incident exposed Social Security Numbers and credit card information.

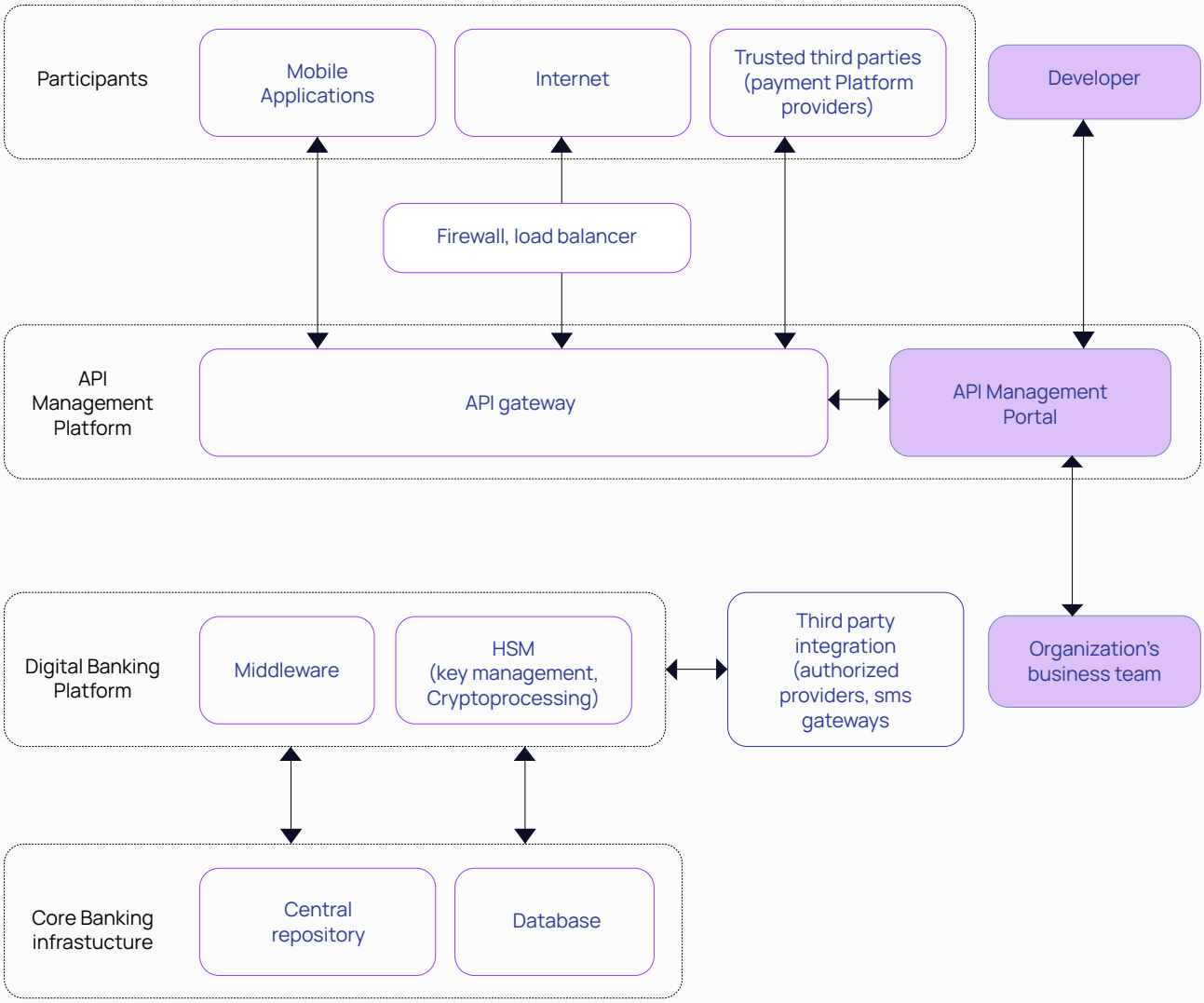
Source: https://www.metomic.io/

The Australian Securities and Investments Commission (ASIC) initiated legal action against HSBC for failing to protect its customers from scams and fraud. Between October 2023 and March 2024, customers lost nearly $16 million due to the bank's insufficient controls on its mobile and online banking platforms.

Source: .https://www.theaustralian.com.au/

Finastra, a prominent financial technology company serving numerous global banks, experienced a cyberattack in 2024. Hackers infiltrated its systems and extracted approximately 400 GB of data. The breach involved unauthorized access to a secure file-transfer platform, potentially compromising sensitive information from major financial institutions. Source: https://www.wsj.com/

API Banking Architecture



The above shows the flow of data from originating channels (Mobile apps, TTPs) toward the core banking infrastructure. This end user could be a bank customer or a trusted third party utilizing the services provided by the bank via APIs.

Whenever a consumer entity initiates a request for a service via multiple channels. it first lands on the API management platform.

This platform consists of an API gateway and a developer portal used by developers for deploying APIs which are consumed by end users. API platform takes care of multiplesecurity as well as management tasks. Hence. the business team from the bank also have some inputs for proper API management from business point of view. These tasks include protection against threats, rate limiting, access control, and encryption. API versioning, logging, Commissioning/De-commissioning of service URLs, Monetisation of APIs,etc. In the case of third-party integrations, the API gateway is responsible for providing a uniform platform for communication to take place.

The platform, after verifying the request and identifying the API in consideration, forwards the request to the next hop in the cycle. This could be an SOA, middleware, or directly to an application server. If any third-party authenticator is being used, it can be integrated at this level. As most of banking transactions consist of multiple validations and sub-steps, the device then communicates with multiple core banking systems, and a consolidated action is taken.

The response to a request flows back via the same hops in reverse order. Based on the originating request, the gateway decides the valid channel for the response.

Top 6 Security Concerns

Business Logic Attacks (BLA)

Business logic attack exploits the flaws mostly present due to functional level complications and restraints, managing the exchange of information between a user interface and the application's supporting database. Programming flaws may also contribute but due to logical anomalies rather than syntactical errors.

APIs enable business related operations available as procedure calls. making it easier to attack the business logic of a company using an API attack. These attacks include legitimate input values, thus making it difficult to detect the attack. These abuse the functionality of the application.

Examples are:

- Modification of authentication flags and privilege escalations.
- Business constraint exploitation/ modification or business logic by-pass to generate fraudulent transactions.
- Parameter modification.
- Cookie tampering and business process/logic bypass.
- Exploiting client side business routines embedded in JavaScript.
- Flash, or Silverlight.
- Identity or profile extraction.
- LDAP parameter identification and critical infrastructure access.

Integration with Third Parties

Third Party APIs would require an environment that might not always be compatible. Additional work would be required to fix these compatibility issues. Additionally, there is less control over the API lifecycle. as these are usually defined by the provider's needs. Working on those aspects might outweigh the benefit of going for third party integration. Also, since the client would be integrating its products with third parties, the security of client's products and services completely rely upon the safeguards and security measures followed by the third party API. There could be inherent incompatibility issues, fixing which on integration would require cost-benefit analysis. Also, integrating third party with client complex legacy system infrastructure needs to be well thought upon, based on feasibility and business functionality.

Compliance & Regulatory Issues

APIs are expected to help banks meet new regulatory requirements around the world. The PSD2 Directive introduced compliance requirements for banks and other financial institutions, including the enforcement of new security requirements and interoperability standards aimed at reducing barriers to entry for nonbank card and internet payment providers. APIs are essential for regulation and compliance. and for leveraging big data. Few regions have open regulatory standards, while others mandate regulatory behaviour. Compliance risk has become one of the most significant ongoing concerns in the BFSI domain. Customers and partners prefer to look for moral bankers, failure to abide by the same leads to loss of business, reputational risks. and financial impacts.

Data Sharing Issues

Data exchange should ensure proper authentication and authorization. Unauthorized access and failure to follow required levels of consent may lead to data leakage, and breach of confidential data. For data sharing, access to data must be ensured on access to least privilege. Other unnecessary privileges and data irrelevant for the specific functionality should be later destroyed; else the system functionality would be affected. which would disrupt business processes leading to operational loss.

Interfacing with Legacy Core Banking Systems

Considering technical compliance overhead to provide requested responses after customer inputs details, banks need to create TTP-facing. open access front ends, with technical challenges in the back-office integration of legacy core banking systems. If the integration however. fails, it would be of no/little value to banks and banks would fail to leverage hold on the customer data details. Also, if the data held in the database, goes underutilized, ineffective usage of technology. may lead to limited access to refined customer data.

Issues in Managing Digital Identities

The pace at which the digital environment is growing, managing digital identities has become a major problem. As multiple agencies are being integrated for providing a service. data sharing and data privacy issues are looming large. Due to high face value, financial data has always been a high-profile target for hackers. As the number of integrations increase.

Top Four Mitigation Strategies

Things which we can't miss during API economy governance

API Governance should include the following four checks:

Validate User and App Identity

API key validation is required to be controlled at the management tier. Ensure Authentication and authorization is separately handled. Applying flexible run-time policies and managing these policies from a centralized management console increases the flexibility and control of API provider over these parameters.

Integrate a Full API Lifecycle Management Tool (Efficient Implementation of API Gateway)

The API development processes must be approached in a holistic manner with a security mindset. This can be ensured if you consider the below security features.

- Implement strong authentication and authorization for access to connected devices across gateway and ensuring strong customer authentication.
- Consider monitoring, logging, and analysing data traffic to track API consumption, and usage as per availability and performance. It could also help in monitoring security incidents/breaches. and errors. Attacks could be prevented by use of features such as whitelisting. managing firewall, considering rate limitation per defined time frame per given app.
- Creation of buffer zones by segregating API servers to mitigate reverse engineering attacks against API's.
- Ensuring strong access control, CIA, threat detection against threats such as data encryption. message validation, traffic management, etc. is essential.
- Efficient implementation of API Gateway, using of API keys for rate limitation, QoS, embed multi modal authentication and authorization mechanisms.

Implement Organization Wide Security Policies

Comprehensively define policy-procedure-standard across API lifecycle. i.e. its separate documented policies and their implementation on planning, design, testing, and development stages is required. Instead of individually creating and governing API solution, corporate API security policies and best practices must be enforced at the management level.

Encrypt Message Channel

- Provide authentication by digital signatures and use of encryption for data privacy.
- Keys – add to another level security. Keys could be passwords, algorithm generated numbers/code, digital fingerprints, etc. Encryption can be used during communication to avoid attacks if keys are intercepted in transit.
- Encryption - XML encryption to protect data privacy. encrypting message containing sensitive data using strong cipher encryption. encrypting and decrypting content and representing using XML.
- Enabling SSL/TLS encryption - it would help specify type of certificate exchanged between nodes, key messaged authentication. secure key hashing for message authentication code.

Conclusion

With the onset of APIs, we are at the cusp of API economy where banks need to embrace openness of APIs and consider the security procedures around it, given the data being explicitly shared and the risks involved. Regardless, the API threats are manageable with a commitment to strong cyber security compliance standpoint. Banks need to strategize their API approach in line with the business decision-making model. Banks need to pace up the approach of securing API conforming to Global risk governance and regulations and utilise the strategic opportunities brought about by API sharing and the revenue that can be raised by them. Banks need to adapt on all the three fronts of cyber security – People, Process and Technology, including their API eco system with a continual improvement approach to align themselves with their strategic and business objectives.

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com** or write to us at **cybersales@nusummit.com**

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai Mumbai I New Delhi I Bangalore

Follow us at: