Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14328
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Capability-Based API Gateway Technology Selection Analysis for Banking Cybersecurity Solution Using AHP Method

Riama Santy Sitorus[1)*], B. Junedi Hutagaol[2)], Dita Madonna Simanjuntak[3)]
[1)] Information Technology,, Computer Science, ASA University Indonesia,Jakarta, Indonesia
[2)] Information System, Computer Science, ASA University Indonesia,Jakarta, Indonesia
[3)]Information System, Computer Science, IPWIJA University,Jakarta, Indonesia
[1)]riama@asaindo.ac.id, [2)]junedi@asaindo.ac.id, [3)]ditasimanjuntak@gmail.com

Submitted :Dec 15, 2024 | **Accepted** : Jan 11, 2025 | **Published** : Jan 18, 2025

Abstract: The growing reliance on APIs in the banking sector, driven by digital transformation, necessitates robust API Gateways that balance performance with strong security measures to address risks like API abuse, man-in-the-middle attacks, and data scraping, while ensuring compliance with regulations such as PCI-DSS, GDPR, and OJK standards. This study bridges the gap in technical guidance by developing a comprehensive evaluation framework using the Analytic Hierarchy Process (AHP) to determine the most suitable API Gateway for banking. The findings identify Apigee as the optimal choice, scoring 1.4277 for its superior authentication, traffic encryption, threat detection, deployment flexibility, cloud integration, and API management. IBM API Connect, scoring 0.6186, is a strong alternative with excellent security and management features but limited scalability and deployment flexibility. Kong and Axway API Gateway follow with scores of 0.4215 and 0.4627, excelling in deployment and integration but lacking critical security features for banking. This research emphasizes the strategic importance of selecting the right API Gateway to bolster cybersecurity and API management in banking, recommending Apigee as the primary solution and IBM API Connect for complex IT infrastructures. It also contributes to the literature by providing a structured, quantitative approach to API Gateway selection and suggests future research exploring AI integration, advanced analytics, and cost-benefit analyses for informed decision-making in the financial sector.

Keywords: *AHP; API; API Gateway; Banking; Cybersecurity*

INTRODUCTION

The increasing dependence of the financial industry, both fintech and banking, on Application Programming Interfaces (APIs) and the digital ecosystem of the banking industry is currently undergoing a massive digital transformation (Hanafizadeh & Amin, 2023). Banks no longer operate only as traditional service providers, but also as digital platforms that enable integration with various external services, such as fintech, e-commerce, and other financial technology providers (Dinçkol et al., 2023). This increasing dependence on APIs requires an API Gateway architecture that not only supports scalability and performance, but also offers strong security protection (Cota et al., 2023).

Research conducted by (Hutagaol et al., 2024) on mobile banking users in Indonesia, stated that 51% of respondents had experienced attempted cybercrime and 21% of them were victims. It was also found that the level of respondent awareness varied between 3.49 to 4.05 on a Likert scale (1-5), significantly influenced by age, occupation, experience as a victim, and interactions between variables. API Gateway is an essential component in modern software architecture, especially microservices-based systems (Cota et al., 2023). The ability to choose the right API Gateway can reduce security risks and make operational processes more (Subramanian & Jeyaraj, 2018).

API Gateway acts as a single entry point for all API requests, providing a unified interface to access various services and data (Dinova & Utomo, 2024). By separating client applications from backend microservices, API Gateway simplifies API management and improves overall system performance and security (Matias et al., 2024).

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14328
e-ISSN : 2541-2019
p-ISSN : 2541-044X

According to recent reports from several cybersecurity agencies, attacks on APIs in the financial sector continue to increase, including attacks such as API abuse, man-in-the-middle attacks, and data scraping (Access et al., 2023). APIs that are not properly protected can be a loophole for attackers to access sensitive data, steal customer identities, or even disrupt banking services (Ranjan et al., 2022). This shows that cybersecurity on APIs cannot be taken lightly and needs to be a primary consideration in choosing API Gateway technology. By choosing the right technology and having strong security integration, this risk can be minimized. The banking industry in various countries, including Indonesia, is regulated by strict regulations regarding data security and privacy, such as the Financial Services Authority (OJK) regulations, the Payment Card Industry Data Security Standard (PCI-DSS), and GDPR (Zulfa Qur'anisa et al., 2024). Strong cybersecurity is directly proportional to the level of customer trust (Cloramidine & Badaruddin, 2023). In the digital era, customers tend to be more careful in choosing banking services that can maintain the privacy and security of their data (Utomo & Rahman, 2024).

This study introduces a novelty with a comprehensive approach to API Gateway selection in the banking sector that has not been widely discussed in literature or industry practice. Most current studies tend to focus on the technical aspects of API Gateways, such as API performance and management (Bondel et al., 2021), but this study does not integrate cybersecurity criteria to assess API Gateway capabilities holistically. There are few technical guidelines or frameworks that focus on selecting the best API Gateway for the banking sector, particularly those addressing cybersecurity needs. This creates a gap for banks in choosing the right technology to secure their APIs. This research aims to help the banking industry select the optimal API Gateway for safe, reliable, and regulatory-compliant digital transformation. This approach provides practical recommendations for banks in selecting technologies that meet security and regulatory needs. Thus, this study provides not only technical but also strategic value, which can help banks protect their digital infrastructure from complex cyber threats.

Analytic Hierarchy Process (AHP) is one of the most effective decision-making methods for evaluating the capabilities of technology (Belinda et al., 2021). The technology includes technical capabilities and risks, especially in the context of API Gateway security. AHP offers a systematic approach by breaking down complex problems into several hierarchical levels, such as goals, criteria, sub-criteria, and alternatives (Mahmoud et al., 2024). This hierarchical structure facilitates the identification and evaluation of various API Gateway capabilities (e.g., scalability, performance throughput, and security features) and relates them to security risks.

METHOD

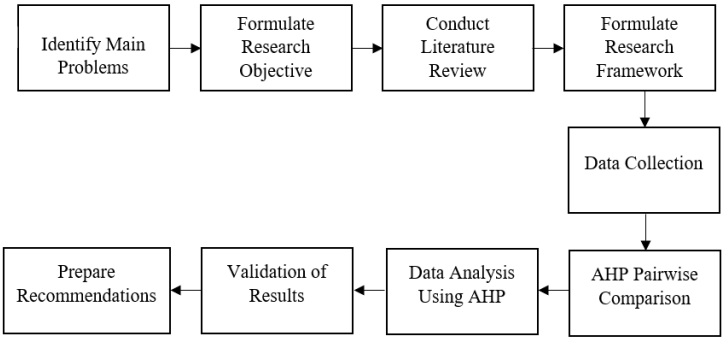

Fig. 1 Research Method

This research begins by identifying the main problems that will be discussed in this study, namely the difficulty in choosing an API Gateway that suits the needs of the banking industry. From the identification of existing problems, the main objective of the research is determined in the form of formulating recommendations for selecting an API Gateway based on cybersecurity capabilities and solutions. The next process carried out is to conduct a literature review to collect the latest information on API Gateway technology and cybersecurity aspects that are relevant to the banking industry, analyze previous studies related to API Gateway performance, capabilities, and security, and identify research gaps that have not been discussed by previous studies. The formulation of research framework and hypothesis is carried out to compile a research framework that includes criteria and sub-criteria for selecting API Gateway, identifying variables to be analyzed, such as capabilities (scalability, performance, and protocol support) and security aspects (authentication, encryption, attack mitigation), and formulating hypotheses or research questions to be tested. This process begins with collecting data related to the API Gateway to be evaluated, then identifying the capabilities and security features of each API Gateway through technical documentation, vendor reports, and internal test results. Furthermore, conducting pairwise comparisons using the AHP technique to determine the priority weights of the criteria and sub-criteria.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14328
e-ISSN : 2541-2019
p-ISSN : 2541-044X

The data analysis process involves applying the Analytical Hierarchy Process (AHP) to calculate priority weights for each predetermined criterion and sub-criterion, computing global scores, and comparing alternative API Gateways based on the generated weights (Mork, 2024). The analysis aims to identify the most appropriate API Gateway by evaluating performance, security, and compliance aspects. Validation of the results is conducted through expert discussions with professionals in banking IT and cybersecurity. Finally, recommendations for selecting the optimal API Gateway are prepared, including practical guidance and implementation strategies tailored to the banking environment.

In this research, the Analytic Hierarchy Process (AHP) was employed to assess and prioritize the components selected for evaluation. As noted in the research by (Kreuzberger et al., 2023), a solution architect plays a crucial role in defining and reviewing appropriate technologies and systems that address and fulfill the business requirements of a company. Their expertise helps ensure that the technological infrastructure aligns with organizational goals and can efficiently support operational needs (Kreuzberger et al., 2023). A Solution Architect with expertise in banking systems was interviewed to provide pairwise AHP evaluations for these components, leveraging their specialized knowledge in designing, securing, and integrating complex banking systems. Their expertise ensured that the AHP assessments reflected practical insights relevant to the banking industry, particularly in the areas of cybersecurity and API management. Additionally, the Solution Architect was asked to test the selected API gateway tools, with the testing results used to validate the AHP findings. This combined approach of expert evaluations and practical testing provided a robust framework for analyzing and selecting the most suitable API gateway tools based on both theoretical and empirical evidence.

RESULT

As a key component of API Management, API Gateway combines strong security mechanisms to keep APIs secure while providing optimal performance. API management and API gateway complement each other in modern architecture. API management focuses on managing the entire API lifecycle, including development, documentation, security, analytics, and monetization, While the API gateway acts as a technical intermediary that handles API traffic with functions such as authentication, rate limiting, load balancing, and requesting routing to microservices in the back end. The integration of the two ensures efficient API management and optimal service performance. The focus of this study is on the API gateway as the main solution in facing cybersecurity challenges in application architecture. The API gateway functions as the first layer of protection that manages authentication, authorization, and data encryption to prevent unauthorized access and cyberattack threats.

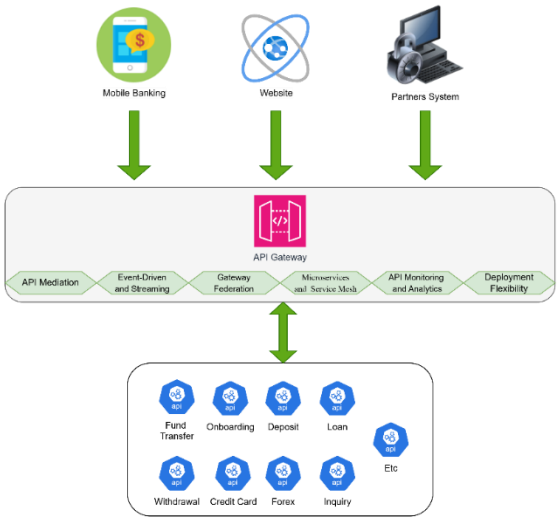

Fig. 2 System Architecture to Implement API Gateway in Banking System Solution

Enterprise Architecture (EA) framework becomes essential as a blueprint for the organization's digital ecosystem. The application architecture for mobile banking systems, banking websites, and third-party partners that communicate with the bank's internal APIs can be built by utilizing API Gateway as a central component. API Gateway functions as the main bridge connecting the front-end (such as mobile banking applications and banking websites) with the back end consisting of the bank's internal APIs and third-party services. As the main entry point, API Gateway manages all API requests coming from various sources and distributes them to the appropriate services in the backend. API Gateway will receive requests from the front-end and forward them to various internal

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14328
e-ISSN : 2541-2019
p-ISSN : 2541-044X

bank services that handle business logic, such as core banking systems, account management, transaction processing, and customer data management. All of this communication occurs through isolated internal APIs within the bank's network, and API Gateway is tasked with managing this communication path to keep it secure and efficient. API Gateway also facilitates communication between banks and third-party partners (such as fintech, payment service providers, or other third-party applications) through external APIs. For example, banks can work with payment service providers to make payment transactions directly from mobile banking applications or banking websites. API Gateway will handle routing to third-party services, perform authentication, and ensure the security of communications between the bank and the third party. API Gateway provides monitoring and analytics that allow banks to track API performance, identify potential issues, and analyze API usage patterns. With real-time metrics and log management, API Gateway provides greater visibility into the entire application architecture, which is essential for maintaining stability, security, and regulatory compliance as illustrated below.

As a trusted partner for global companies and institutions, Gartner offers relevant guidance to understand technology trends and choose the best solutions to support business growth. According to (Gartner, 2024) the main capabilities that API management must have are as described in the following table. API Gateway is a component of API Management; it means not all the API management capabilities are the core capabilities of API Gateway. In the context of the core functionality of API Gateway, some capabilities from the list presented can be classified as core functionality, while others are more related to overall API management. Capabilities such as API Security, API Mediation, Event-Driven and Streaming, Gateway Federation, Microservices and Service Mesh, API Monitoring and Analytics, and Deployment Flexibility are core to API Gateway because they support traffic management, security, inter-system communication, and deployment flexibility.

In contrast, capabilities such as API Consumption, API Design, API Monetization, API Testing, Developer Portal, and Versioning and API Governance are not considered core API Gateway functionality. These capabilities are more relevant to the overall management and lifecycle of APIs, which is the domain of API Management solutions as such, while API Gateway can support some of these functions to a limited extent, full management of these capabilities is outside the primary scope of API Gateway.

Breaking down API Gateway capabilities into smaller features is essential in using the Analytic Hierarchy Process (AHP) method to determine the right solution. By breaking down large capabilities like API Security or API Mediation into more granular elements, the evaluation becomes more specific and objective, allowing for a more accurate comparison between different API Gateway solutions. It also helps in setting clear priorities based on the organization's needs, whether it is more focused on security, performance, or scalability. In doing so, AHP can provide more measured and evidence-based decisions, clarifying which features best meet the organization's business and technical goals.

Table 1. Critical Capabilities for API Management

API Management Capabilities	Description	Features
API Security	Involves mechanisms to protect APIs from security threats, including authentication, authorization, data encryption, protection against attacks such as DDoS, rate limiting, and input validation. API Security ensures that only authorized users or applications can access the service.	Authentication and Authorization, Traffic Encryption, Rate Limiting and Throttling, IP Whitelisting or Blacklisting, Threat Detection and Mitigation.
API Consumption	Refers to the use of APIs by developers or third-party applications. This component supports API access management, including documentation, tokenization, and the use of analytics to understand consumption patterns.	The domain of API Management solutions is not limited to API Gateway.
API Design	Focuses on designing APIs that are intuitive, reusable, and standard-compliant. This includes defining endpoints, data formats (such as JSON or XML), HTTP methods (GET, POST, etc.), and the use of tools like Open API for documentation.	The domain of API Management solutions is not limited to API Gateway.
API Mediation	Acts as an intermediary between clients and back-end services, managing tasks such as data transformation, response aggregation from multiple APIs, and protocol translation to ensure compatibility and efficiency.	Protocol Translation, Data Transformation, Request and Response Aggregation, Dynamic Routing.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14328
e-ISSN : 2541-2019
p-ISSN : 2541-044X

API Monetization	A strategy for monetizing APIs by implementing models such as pay-per-use, subscriptions, or premium access restrictions. This supports control and usage tracking for billing purposes.	The domain of API Management solutions is not limited to API Gateway.
API Monitoring and Analytics	Involves tracking API performance, such as response time, error rates, and traffic patterns. Analytics provide insights into API usage for service improvement, issue detection, and performance optimization.	Real-Time Metrics, Usage Analytics, Alerting and Notifications, Log Management.
API Testing	The process of testing APIs to ensure functionality, security, performance, and reliability. This includes integration testing, load testing, regression testing, and real-world usage simulations to minimize production errors.	The domain of API Management solutions is not limited to API Gateway.
Deployment Flexibility	API management capabilities to support various deployment models, such as on-premises, cloud, or hybrid. This allows organizations to choose solutions that suit their business needs and infrastructure.	On-Premises Deployment, Cloud Deployment, Hybrid Deployment, Containerization and Orchestration.
Developer Portal	A platform designed for developers, providing API documentation, testing tools, and the information needed to effectively leverage APIs. The portal may also offer community support and token access.	The domain of API Management solutions is not limited to API Gateway.
Event-Driven and Streaming	Support for event-driven APIs and real-time data streaming. This feature is essential for applications requiring instant responses to data changes, such as notifications or live analytics.	WebSocket Support, Server-Sent Events (SSE), Message Queues and Streams, Event Filtering and Transformation.
Gateway Federation	Enables centralized management of multiple API gateways in distributed environments. This supports large organizations with numerous API endpoints across different geographic locations or platforms.	Centralized Policy Management, Multi-Region Deployment, Inter-Gateway Communication, Failover and Redundancy.
Microservices and Service Mesh	Support for integrating APIs with microservices architectures, including the use of service meshes for managing inter-service communication, such as security, monitoring, and orchestration.	Service Discovery, Circuit Breaking, Traffic Shaping, Observability.
Versioning and API Governance	The process of managing API versions to maintain compatibility with client applications while enabling innovation. API governance ensures APIs adhere to corporate policies, technical standards, and regulations.	The domain of API Management solutions is not limited to API Gateway.

In the analysis of selecting the optimal API Gateway platform as a cybersecurity solution, there are several capabilities that are very crucial to consider. Based on the existing literature review, three main capabilities, namely API Security, API Monitoring and Analytics, and API Mediation, are known to have a significant influence in determining the effectiveness of the API Gateway platform in maintaining the integrity and security of the system in the banking industry. API Security focuses on data protection and authentication, which are very important to prevent cyber threats such as hacking and API misuse. API Monitoring and Analytics allows real-time monitoring of performance and potential threats, providing early detection capabilities for problems that may arise. Meanwhile, API Mediation plays a role in managing the integration and processing of data between different services, which also contributes to the ease of scalability and management of various external and internal APIs safely. Therefore, a deep breakdown of these capabilities is important to ensure that the selected API Gateway platform not only meets the technical aspects but can also accommodate the high security standards required by the banking sector.

Based on the explanation above, the criteria that will be analysed are as follows:

Table 2 API Gateway Criteria with ID

Criteria	ID
Authentication and Authorization	1
Traffic Encryption	2

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14328
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Rate Limiting and Throttling	3
IP Whitelisting/Blacklisting	4
Threat Detection and Mitigation	5
Real-Time Metrics	6
Usage Analytics	7
Alerting and Notifications	8
Log Management	9
Protocol Translation	10
Data Transformation	11
Request and Response Aggregation	12
Dynamic Routing	13
Microservices and Service Mesh	14
Gateway Federation	15
Event-Driven and Streaming	16
Deployment Flexibility	17

In the AHP method, a comparative value of 1 to 9 is used to assess the relative importance of the criteria to each other: 1: Both criteria are of equal importance. 3: The first criterion is slightly more important. 5: The first criterion is clearly more important. 7: The first criterion is very much more important. 9: The first criterion is very dominant. Values of 2, 4, 6, 8 are used for smaller intermediate degrees. This scale helps in constructing a comparative matrix to calculate the priority weights of the criteria. Solution Architect with expertise in banking system solutions to provide pairwise AHP evaluations for the components I have selected in this research. The role of a Solution Architect is ideal for this task because they possess a deep understanding of designing, evaluating, and integrating complex systems, particularly in the banking domain where cybersecurity and API management are critical. Their expertise ensures that the assessments are informed by practical insights into system requirements, architectural constraints, and industry best practices. This alignment between their knowledge and the research objectives enhances the reliability and relevance of the pairwise comparisons, ultimately supporting more accurate and robust decision-making in the study. After the pairwise matrix is created, the next step is to normalize each column by dividing each value by its column total.

Table 3 . Normalize Matrix Result

ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	0,219	0,526	0,424	0,363	0,322	0,164	0,130	0,107	0,097	0,108	0,102	0,094	0,088	0,082	0,075	0,060	0,060
2	0,044	0,105	0,303	0,259	0,250	0,164	0,130	0,107	0,097	0,108	0,102	0,094	0,088	0,082	0,075	0,060	0,060
3	0,031	0,021	0,061	0,155	0,179	0,164	0,130	0,107	0,097	0,108	0,102	0,094	0,088	0,082	0,075	0,060	0,084
4	0,031	0,021	0,020	0,052	0,107	0,164	0,130	0,107	0,097	0,108	0,102	0,094	0,088	0,082	0,075	0,060	0,084
5	0,024	0,015	0,012	0,017	0,036	0,164	0,130	0,107	0,097	0,108	0,102	0,094	0,088	0,082	0,075	0,060	0,084
6	0,073	0,035	0,020	0,017	0,012	0,055	0,217	0,179	0,162	0,108	0,102	0,094	0,088	0,082	0,075	0,060	0,084
7	0,073	0,035	0,020	0,017	0,012	0,011	0,043	0,179	0,162	0,108	0,102	0,094	0,088	0,082	0,075	0,060	0,084
8	0,073	0,035	0,020	0,017	0,012	0,011	0,009	0,036	0,097	0,108	0,102	0,094	0,088	0,082	0,075	0,060	0,084
9	0,073	0,035	0,020	0,017	0,012	0,011	0,009	0,012	0,032	0,065	0,102	0,094	0,088	0,082	0,075	0,060	0,084
10	0,044	0,021	0,012	0,010	0,007	0,011	0,009	0,007	0,011	0,022	0,044	0,040	0,038	0,035	0,045	0,060	0,084
11	0,031	0,015	0,009	0,007	0,005	0,008	0,006	0,005	0,005	0,007	0,015	0,040	0,063	0,082	0,075	0,100	0,084
12	0,031	0,015	0,009	0,007	0,005	0,008	0,006	0,005	0,005	0,007	0,005	0,013	0,038	0,058	0,045	0,060	0,009
13	0,031	0,015	0,009	0,007	0,005	0,008	0,006	0,005	0,005	0,007	0,003	0,004	0,013	0,035	0,045	0,040	0,009
14	0,031	0,015	0,009	0,007	0,005	0,008	0,006	0,005	0,005	0,007	0,002	0,003	0,004	0,012	0,045	0,060	0,009
15	0,044	0,021	0,012	0,010	0,007	0,011	0,009	0,007	0,006	0,007	0,003	0,004	0,004	0,004	0,015	0,060	0,009
16	0,073	0,035	0,020	0,017	0,012	0,018	0,014	0,012	0,011	0,007	0,003	0,004	0,006	0,004	0,005	0,020	0,009
17	0,073	0,035	0,020	0,017	0,012	0,018	0,014	0,012	0,011	0,007	0,005	0,040	0,038	0,035	0,045	0,060	0,028

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 9, Number 1, January 2025
DOI : https://doi.org/10.33395/sinkron.v9i1.14328
e-ISSN : 2541-2019
p-ISSN : 2541-044X

After normalization, the weights of each criterion were determined as follows: Authentication and Authorization (0.178), Traffic Encryption (0.125), Rate Limiting and Throttling (0.097), Real-Time Metrics (0.084), IP Whitelisting/Blacklisting (0.076), Threat Detection and Mitigation (0.086), Usage Analytics (0.073), Alerting and Notifications (0.059), Log Management (0.051), Protocol Translation (0.029), Microservices and Service Mesh (0.033), Deployment Flexibility (0.019), Data Transformation (0.015), Request and Response Aggregation (0.014), Dynamic Routing (0.014), Gateway Federation (0.016), and Event-Driven and Streaming (0.028).

In line with the purpose of this study to evaluate the best API Gateway platforms to support cybersecurity, this study will analyze four leading platforms such as Apigee, Kong, IBM API Connect, and Axway API Gateway. The sample selection was based on the Gartner Magic Quadrant report, which identifies leaders in the API Management category in the October 2024 period. The emphasis on leaders in the Gartner Magic Quadrant reflects a strategic approach to selecting platforms that are globally recognized in terms of innovation, market execution, and technical capabilities. The focus of this study is to evaluate the security capabilities offered by each platform as a critical element in a cybersecurity solution.

The assessment in this study will be carried out by giving weight to each API Gateway platform capability by a Solution Architect who is experienced in the banking sector. Direct experience in designing and managing IT systems for financial institutions allows the Solution Architect to provide valid and relevant weights based on a deep understanding of critical cybersecurity needs in the banking industry. With a strong background in ensuring regulatory compliance and managing security risks in complex environments, the assessment given is believed to reflect the right priorities in choosing the best API Gateway solution and is reliable for the purpose of this study.

After performing pairwise comparisons for each existing criteria on the selected API gateway, a summary of the results of the AHP matrix analysis for each of criteria can be seen in the table below:

Table 4 . AHP Matrix Analysis for Each Criteria

Criteria's	Weight				The Most Optimal API Gateway Platform
	Apigee	Kong	IBM	Axway	
Authentication and Authorization	**0,5579**	0,2633	0,1219	0,0569	Apigee
Traffic Encryption	**0,4805**	0,1756	0,2734	0,0705	Apigee
Rate Limiting and Throttling	**0,5308**	0,2808	0,0828	0,1055	Apigee
IP Whitelisting/Blacklisting	**0,5430**	0,2445	0,1360	0,0765	Apigee
Threat Detection and Mitigation	**0,4780**	0,0727	0,2789	0,1704	Apigee
Real-Time Metrics	**0,5430**	0,2445	0,1360	0,0765	Apigee
Usage Analytics	**0,5117**	0,0780	0,2378	0,1725	Apigee
Alerting and Notifications	**0,5036**	0,0964	0,2536	0,1464	Apigee
Log Management	**0,5117**	0,0780	0,2378	0,1725	Apigee
Protocol Translation	**0,4482**	0,0775	0,1841	0,2903	Apigee
Data Transformation	**0,4738**	0,0567	0,1952	0,2742	Apigee
Request and Response Aggregation	**0,4482**	0,0775	0,2903	0,1841	Apigee
Dynamic Routing	**0,4524**	0,1587	0,2222	0,1667	Apigee
Microservices and Service Mesh	0,2903	0,1841	**0,4482**	0,0775	IBM
Gateway Federation	**0,5036**	0,0964	0,1464	0,2536	Apigee
Event-Driven and Streaming	**0,5382**	0,1572	0,2311	0,0735	Apigee
Deployment Flexibility	0,2071	**0,2894**	0,2713	0,2321	Kong

Based on the table above, the total value of each API Gateway platform in the selection of optimal API Gateway technology for the capability-based banking industry as a cyber security solution is as follows: Apigee achieved the highest score with 1.4262, followed by IBM API Connect with 0.6180. Axway API Gateway scored 0.4622, slightly outperforming Kong, which had a score of 0.4210.

DISCUSSIONS

The main focus of this research was to investigate how API Gateways can be an effective solution for addressing security challenges in application architecture, where the API Gateway functions as the first line of

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

defence, managing authentication, authorization, data encryption, and preventing unauthorized access and cyber threats (Kondam, 2024). The research findings, as presented in the previous chapter, confirm that the API Gateway indeed plays a central role in enhancing API security in banking systems. The evaluation using the Analytic Hierarchy Process (AHP) method revealed that platforms such as Apigee stand out in several key security features such as authentication and authorization, traffic encryption, and threat detection and mitigation. This aligns with the expectations outlined in the Introduction about the central role of API Gateways in supporting banking security (Matias et al., 2024).

In the introduction, it was mentioned that the API Gateway manages API traffic with features such as rate limiting, load balancing, and access filtering to protect against cyber threats. The research findings reinforce this statement by demonstrating that features like Rate Limiting and Throttling as well as Traffic Encryption are indeed dominant in the evaluation. Platforms such as Apigee excel in managing these features, which directly contribute to preventing attacks that could jeopardize customer data and financial transaction security. This comparison also shows that while platforms like IBM API Connect and Axway API Gateway also have strong capabilities in microservices and service mesh, they are not as optimized as Apigee in terms of API security and API mediation. This is consistent with the understanding in the introduction and research from (Hamed et al., 2023) that API security is a top priority in banking, requiring a more robust solution for data management and service interactions.

API Security was identified as one of the primary components in the research. API security was expected to involve several features such as authentication, authorization, data encryption, and protection against attacks such as DDoS and rate limiting (Mathijssen et al., 2020). The research findings using AHP confirm that Apigee outperforms other platforms in these security aspects, scoring the highest in Authentication and Authorization as well as Traffic Encryption. This reinforces that Apigee implements the necessary security technologies required by the banking sector. Additionally, the research emphasizes the importance of Monitoring and Analytics, which was identified as a key achievement in the Introduction. By utilizing Real-Time Metrics and Alerting and Notifications, Apigee not only provides protection for APIs but also offers real-time monitoring features that are useful for detecting threats and analysing API performance. This is crucial for the banking industry, which requires high visibility over transaction data and user interactions (Sorongan et al., 2023) (Navaretti et al., 2022).

The introduction explained that the API Gateway serves as the main bridge between frontend applications, such as mobile banking apps or websites, and backend services related to user data and core financial systems. The research findings support this view, demonstrating that the API Gateway is highly effective in managing communication between various banking services and third-party integrations, such as fintech providers. The Gateway Federation advantage possessed by Apigee demonstrates that this platform also supports large-scale and geographically distributed banking system architectures. This is highly relevant for banks that need to manage services across various locations and platforms, as highlighted in the Introduction regarding the importance of Enterprise Architecture (EA) in supporting the digital ecosystem of banks (Purawidjaja et al., 2024).

The research findings validate the capabilities described in the introduction, especially in terms of API Mediation and Microservices, which significantly influence the management and integration of APIs in banking systems (Kipyego, 2023). The selection of the best API Gateway platform, based on the AHP analysis, shows that although some platforms like Kong and IBM API Connect excel in Deployment Flexibility and support for Microservices, platforms like Apigee are superior in security and API management capabilities. Thus, this discussion underscores that while different platforms offer various advantages relevant to banking needs, the selection of the optimal API Gateway platform depends heavily on the primary banking priorities of cybersecurity and API performance, which were the central focus of this research.

CONCLUSION

In conclusion, the findings of this study underline the importance of selecting an API Gateway that not only supports the technical needs of a banking environment but also ensures strong security and regulatory compliance. Apigee, with its comprehensive suite of security features and high performance across multiple criteria, is the most optimal choice for securing APIs in the banking sector. However, depending on specific organizational needs, such as microservices integration or deployment flexibility, alternatives like IBM API Connect or Kong may also offer valuable solutions. Future research could explore the implementation of these platforms in real-world banking environments to further validate these findings and provide deeper insights into their practical

This study highlights the critical importance of selecting an API Gateway that ensures both strong security and regulatory compliance for banking environments. Apigee stands out as the optimal choice due to its robust security features and high performance across multiple criteria. However, depending on specific organizational needs, such as microservices integration or deployment flexibility, alternatives like IBM API Connect or Kong may also be suitable options.

For banking stakeholders, especially IT decision-makers, Apigee is recommended as the preferred platform for securing APIs. IBM API Connect may be a good alternative for organizations with complex IT infrastructures. This study contributes to the theoretical understanding of API Gateway selection for banking cybersecurity and

*name of corresponding author

provides a quantitative evaluation method through AHP. Future research should explore real-world implementations, investigate the impact of AI and advanced analytics on threat detection, and assess cost and ROI factors to guide future decisions in API Gateway adoption.

REFERENCES

Access, O., Rao, B., & Suvarna, S. G. (2023). Trust & Security Issues in Mobile Banking and Its Effect on Customers. *International Research Journal of Modernization in Engineering Technology and Science*, *05*. https://doi.org/10.56726/irjmets39238

Belinda, B. I., Emmanuel, A. A., Solomon, N., & Kayode, A. B. (2021). Evaluating Software Quality Attributes using Analytic Hierarchy Process (AHP). *International Journal of Advanced Computer Science and Applications*, *12*(3), 165–173. https://doi.org/10.14569/IJACSA.2021.0120321

Bondel, G., Landgraf, A., & Matthes, F. (2021). API Management Patterns for Public, Partner, and Group Web API Initiatives with a Focus on Collaboration. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3489449.3490012

Cloramidine, F., & Badaruddin, M. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). *Jurnal Sosial Dan Humaniora*, *8*(1), 57–73. https://doi.org/10.47313/pjsh.v8i1.1957

Cota, D., Martins, J., Mamede, H., & Branco, F. (2023). BHiveSense: An integrated information system architecture for sustainable remote monitoring and management of apiaries based on IoT and microservices. *Journal of Open Innovation: Technology, Market, and Complexity*, *9*(3). https://doi.org/10.1016/j.joitmc.2023.100110

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

Dinova, C. A., & Utomo, I. C. (2024). Pengembangan Arsitektur Microservice pada Learning Management System E-learning Menggunakan Metode Web Service. *Jurnal Ilmu Komputer Dan Informatika*, *3*(2), 125–141. https://doi.org/10.54082/jiki.102

Gartner. (2024). *Critical Capabilities for API Management*. https://www.gartner.com/document/5852879?ref=solrAll&refval=438481844&

Hamed, M., Hefny, M., Helmy, Y., & Abdelsalam, M. (2023). *Open Banking API Framework to Improve the Online Transaction between Local Banks in Egypt Using Blockchain Technology*. *14*(4). https://doi.org/10.12720/jait.14.4.729-740

Hanafizadeh, P., & Amin, M. G. (2023). The transformative potential of banking service domains with the emergence of FinTechs. In *Journal of Financial Services Marketing* (Vol. 28, Issue 3). Palgrave Macmillan UK. https://doi.org/10.1057/s41264-022-00161-0

Hutagaol, B. J., Sitorus, R. S., & Hutagaol, N. (2024). Identifikasi Tingkat Kesadaran Pengguna Mobile Banking terhadap Ancaman Cybercrime. *Jurnal Teknologi Sistem Informasi Dan Aplikasi*, *7*(3), 1043–1054. https://doi.org/10.32493/jtsi.v7i3.41639

Kipyego, F. (2023). *DETERMINANTS OF ADOPTION OF MICRO-SERVICES IN DIGITAL BANKING*. *June*.

Kondam, A. (2024). *International Journal of Advanced Research and Emerging Trends (JARET) International Journal of Advanced Research and Emerging Trends (JARET)*. *1*.

Kreuzberger, D., Kuhl, N., & Hirschl, S. (2023). Machine Learning Operations (MLOps): Overview, Definition, and Architecture. *IEEE Access*, *11*(April), 31866–31879. https://doi.org/10.1109/ACCESS.2023.3262138

Mahmoud, T., Balachandran, W., & Altayyar, S. (2024). Advancing Sustainable Healthcare Technology Management: Developing a Comprehensive Risk Assessment Framework with a Fuzzy Analytical Hierarchy Process, Integrating External and Internal Factors in the Gulf Region. *Sustainability (Switzerland)*, *16*(18). https://doi.org/10.3390/su16188197

Mathijssen, M., Overeem, M., & Jansen, S. (2020). *Identification of Practices and Capabilities in API Management: A Systematic Literature Review*. http://arxiv.org/abs/2006.10481

Matias, M., Ferreira, E., Mateus-Coelho, N., Ribeiro, O., & Ferreira, L. (2024). Evaluating Effectiveness and Security in Microservices Architecture. *Procedia Computer Science*, *237*, 626–636. https://doi.org/10.1016/j.procs.2024.05.148

Mork, T. (2024). *Tormod Mork Müller Master ' s thesis Enhancing Vendor Selection in Software Ecosystems : A Decision- Making Tool*. *June*.

Navaretti, G. B., Calzolari, G., Mansilla-fernández, J. M., & Pozzolo, A. F. (2022). *Open Banking ' s Promise of a Financial Revolution : Are We Falling Short ? 1 Open Banking ' s Promise of a Financial Revolution : Are*. 1–21.

Purawidjaja, R. A., Chudra, G., Indrajit, E., Dazki, E., & Yohannis, A. (2024). Leveraging Enterprise Architecture to Empower KOMINFO's Business Core Operations: A PMO Perspective. *Sinkron*, *8*(3), 1272–1285.

*name of corresponding author

https://doi.org/10.33395/sinkron.v8i3.13656

Ranjan, P., Khunger, A., Batchu, C., Venkata, V., & Dahiya, S. (2022). *Threat Modeling and Risk Assessment of APIs in Fintech Applications*. *2*(2), 44–61. https://doi.org/10.56472/25832646/JETA-V2I2P108

Sorongan, F. A., Legowo, M. B., & Subanidja, S. (2023). *Model of Banking and Fintech Collaboration in Indonesia : Present and Future Challenges*. *6*(08), 1–10.

Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers and Electrical Engineering*, *71*(July 2017), 28–42. https://doi.org/10.1016/j.compeleceng.2018.06.006

Utomo, B. C., & Rahman, A. A. (2024). Analisis Kesadaran Keamanan Data Pribadi pada Pengguna E-Wallet DANA. *Jurnal Riset Sains Dan Teknologi*, *8*(2), 155–166.

Zulfa Qur'anisa, Mira Herawati, Lisvi Lisvi, Melinda Helmalia Putri, & O. Feriyanto. (2024). Peran Fintech Dalam Meningkatkan Akses Keuangan Di Era Digital. *GEMILANG: Jurnal Manajemen Dan Akuntansi*, *4*(3), 99–114. https://doi.org/10.56910/gemilang.v4i3.1573

*name of corresponding author