International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November - December 2025||

DOI:10.15662/IJRPETM.2025.0806004

Banking Ecosystem Modernization with Privacy-Preserving AI-Cloud Networks, SAP, and API Integration

Richard Christopher Adams

Senior AI Consultant, Paris, France

ABSTRACT: The rapid evolution of digital banking demands secure, scalable, and intelligent infrastructures that can handle high-volume transactions while safeguarding sensitive financial data. This paper presents a Privacy-Preserving AI-Cloud Network Framework designed to modernize banking ecosystems through the integration of SAP-driven data management and API-based interoperability. The proposed architecture leverages Artificial Intelligence (AI) to enable real-time analytics, fraud detection, risk assessment, and predictive decision-making across distributed banking networks. Cloud infrastructure ensures scalability, high availability, and efficient resource utilization, while privacy-preserving mechanisms, such as encryption, access control, and anonymization, safeguard sensitive customer and transactional data. SAP integration provides enterprise-grade workflow automation, regulatory compliance, and operational transparency, whereas API-driven connectivity allows seamless interoperability between internal banking systems, fintech partners, and digital services. The framework fosters a secure, intelligent, and adaptive banking ecosystem that enhances operational efficiency, customer trust, and resilience against cyber threats, supporting the transformation toward next-generation digital banking platforms.

KEYWORDS: AI-Cloud Network, Privacy-Preserving Framework, Banking Ecosystem Modernization, SAP Integration, API-Driven Architecture, Cybersecurity, Predictive Analytics, Secure Digital Banking.

I. INTRODUCTION

Open Banking—popularized in the EU through the Payment Services Directive (PSD2)—mandates standardized third-party access to customer payment and account data. While enabling innovation (open APIs, fintech services, personalized financial products), this paradigm increases the attack surface for critical financial workflows: insecure OAuth implementations, token misuse, and improper session/consent handling can produce high-impact breaches. To mitigate such risks the industry has coalesced around stronger API security profiles (the OpenID Foundation's FAPI specifications) and hardened OAuth/OIDC practices for high-value financial flows. At the same time, financial institutions seek to harness AI for fraud detection, personalized underwriting, and customer experience. Centralized ML model training conflicts with privacy and regulatory constraints (e.g., GDPR), motivating privacy-aware strategies. Network Function Virtualization (NFV) offers programmable, deployable network services (WAF, DDoS mitigation, traffic steering) and supports placing inference near transaction origins to meet strict latency targets. Embedding AI into the API management plane provides automated anomaly detection, adaptive throttling, and policy recommendations, but also requires MLOps for reproducibility, drift monitoring, and secure model deployment. This paper describes an integrated, cloud-native architecture that combines FAPI-compliant API management, NFV for network control and edge inference, and privacy-preserving FL + DP for decision intelligence. The design emphasizes auditable consent flows, defense-in-depth, and operational observability, and it is validated through a mixed evaluation strategy covering security, privacy, performance, and developer experience. Key references guiding our design include PSD2, the FAPI specifications, NFV security guidance, and the academic literature on federated learning and differential privacy.

II. LITERATURE REVIEW

Regulatory & API security foundations. PSD2 established legal requirements for third-party access to payment accounts and set the stage for secure API ecosystems; implementers need to show consent, strong customer authentication (SCA), and auditability. The Financial-grade API (FAPI) specifications extend OAuth2/OIDC for high-value scenarios, prescribing sender-constrained tokens (MTLS/private_key_jwt), strict token handling, and conformance testing to reduce common OAuth mistakes. Practitioner reports and OWASP guidance highlight recurring

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November - December 2025||

DOI:10.15662/IJRPETM.2025.0806004

API vulnerabilities—broken authentication, insufficient authorization, and lack of rate limiting—that FAPI and hardened gateways aim to address.

API management + AI. Research and practitioner work demonstrate that ML methods (sequence modeling, behavioral profiling, anomaly detection) can materially improve detection of API misuse and reduce false positives compared to static rules, while explainability techniques help operators interpret model outputs during investigations. Integrating AI into API gateways enables adaptive policy enforcement (dynamic throttling, targeted blocking) but increases the model attack surface (poisoning, evasion) and operational demands for monitoring and retraining. Robust MLOps practices (CI/CD for models, monitoring for drift, explainability) are therefore critical for productionization.

NFV and programmable networking. NFV literature (and ENISA guidance) shows that virtualized network functions allow on-demand instantiation of security and performance functions and permit placing compute/inference closer to end users (edge/PoP) to meet latency SLAs. However, NFV's orchestration and management planes introduce new security considerations—isolation, RBAC, and hardened orchestration APIs are essential to avoid lateral movement and supply-chain risks. Applied to Open Banking, NFV can implement per-tenant policies, rapid DDoS mitigation, and edge inference for time-sensitive fraud scoring.

Privacy-preserving ML. Federated learning provides a practical way to train models across distributed data sources without moving raw records to a central store; seminal FL work showed communication-efficient aggregation for decentralized deep models. But model updates leak information unless combined with cryptographic secure aggregation and differential privacy (DP), which provides quantitative leakage guarantees at the cost of added noise and potential accuracy loss. Many surveys and applied studies recommend the triad of FL + secure aggregation + DP for regulated domains, while noting tradeoffs (utility vs. privacy, communication cost). MLOps must also manage versioning, provenance, and governance to avoid "hidden technical debt" in ML systems.

Synthesis. Each technology thread—FAPI/hardened API gateways, AI for API defenses, NFV-based network control, and privacy-preserving federated ML—has been studied independently. Fusing them into an operational, cloud-native ecosystem for Open Banking requires careful interface design (consent and token propagation across NFV and ML components), governance for model audits and privacy budgets, and developer tooling to reduce onboarding friction. This paper contributes a cohesive reference architecture and a reproducible evaluation plan that quantifies the tradeoffs between security, privacy, latency, and developer experience.

III. RESEARCH METHODOLOGY

1. **Requirements & compliance mapping:** collect legal/regulatory requirements from PSD2 and privacy obligations (GDPR), plus operator non-functional targets (latency p99 for fraud scoring). Translate these into technical controls: FAPI/OAuth profiles, consent ledger capabilities, token lifetimes, and acceptable DP epsilon ranges.
2. **Reference architecture design:** produce a cloud-native blueprint combining (a) a FAPI-capable API gateway + authorization server, (b) Kubernetes clusters hosting microservices and VNFs (containerized WAF, rate limiter, edge inference), (c) a service mesh for mTLS and telemetry, (d) an NFV orchestrator for VNF lifecycle and placement, and (e) an MLOps pipeline supporting FL, secure aggregation, and DP noise injection. Define clear data-flow diagrams and trust boundaries.
3. **Prototype implementation:** build a proof-of-concept using open source components where possible (Kubernetes, Istio/Linkerd service mesh, a FAPI-compliant gateway or gateway + FAPI extensions, an NFV orchestrator or lightweight placement controller, and a federated training coordinator with secure aggregation). Implement an auditable consent service and token propagation across components.
4. **Security testing:** conduct STRIDE threat modeling; run FAPI conformance suites and API fuzzing; perform adversarial tests (token replay, IDOR, auth bypass). Evaluate NFV control plane hardening (RBAC, API auth) and VNF isolation. Metrics: vulnerability counts, time-to-exploit, and gatekeeping success rate.
5. **Privacy experiments:** train comparable models under centralized, federated, and federated+DP setups. Compute DP epsilon for each configuration, measure model utility (accuracy/AUC), and run membership/attribute inference attacks to empirically evaluate leakage. Validate secure aggregation correctness under partially honest participants.
6. **Performance & NFV placement benchmarks:** measure API latency (p50/p95/p99) and throughput under different NFV placements (central cloud, regional PoP, edge). Measure inference latency for fraud/scoring when running centrally vs. at edge VNFs; capture orchestration overhead and cost. Produce latency–cost frontiers to inform placement heuristics.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November - December 2025||

DOI:10.15662/IJRPETM.2025.0806004

7. **AI-in-API evaluation:** deploy anomaly-detection models in the gateway pipeline; compare precision/recall against static rules; measure false positive rates and operator triage effort. Add explainability aids for incident response and instrumentation for model drift detection.
8. **Developer experience testing:** simulate third-party onboardings with FAPI enforcement; measure time-to-integrate with SDKs and sandbox pipelines; collect developer feedback to refine onboarding tools.
9. **Analysis & sensitivity studies:** synthesize results into tradeoff curves (accuracy vs. epsilon, latency vs. PoPs, security hardening vs. developer friction) and recommend default operational knobs and governance policies.

Advantages

- **Regulatory & audit readiness:** mapping PSD2/FAPI and GDPR requirements into technical controls produces auditable trails for compliance.
- **Stronger runtime protection:** AI-enhanced API management reduces attack surface and operator load through adaptive defenses.
- **Latency-sensitive delivery:** NFV-driven edge placement for inference reduces p99 latency for critical scoring/fraud tasks.
- **Privacy-first intelligence:** FL + DP + secure aggregation enable collaborative model improvements while minimizing raw data movement and providing quantifiable leakage bounds.

Disadvantages / Tradeoffs

- **Stack complexity & operations:** combining FAPI, NFV orchestration, MLOps, and DP increases operational burden and requires skilled teams.
- **Utility vs. privacy:** DP noise can reduce model accuracy; FL adds communication overhead—careful tuning and compression are required.
- **Developer friction:** rigorous FAPI enforcement can slow third-party onboarding unless clean SDKs and sandboxes exist.

IV. RESULTS AND DISCUSSION

This is a design + prototype evaluation; results are planned and expected rather than final. Security testing should show that FAPI-compliant gateways (with MTLS/private_key_jwt and strict token handling) plus AI filters lower the incidence of common API vulnerabilities (token misuse, unauthorized access) and reduce false positives versus static-rule systems. Privacy experiments are expected to show that federated+DP training can preserve useful model accuracy for many financial tasks at modest epsilon values, while extreme privacy budgets materially degrade utility; secure aggregation should block direct recovery of training records from updates. NFV placement experiments are expected to reduce p99 latency for scoring when inference executes at edge PoPs, while increasing orchestration cost and complexity; results will produce latency–cost frontiers for decision makers. AI-in-gateway models should reduce operator triage time but will require MLOps instrumentation to detect model drift and adversarial manipulation. The discussion will present recommended default configurations (e.g., FAPI + mTLS + PKCE for payment endpoints; federated+DP for cross-bank collaborative models with conservative epsilon ranges; NFV placement heuristics based on latency thresholds and cost caps).

V. CONCLUSION

We presented an integrated AI-powered cloud architecture for Open Banking that unites FAPI-based API hardening, NFV for programmable network and edge inference, and privacy-preserving decision intelligence (FL + DP + secure aggregation). The design balances regulatory compliance, low-latency operational needs, and privacy constraints. While complexity and operational overhead increase, disciplined MLOps, NFV governance, and developer tooling can make the approach practical for banks and platform providers seeking trusted AI-enabled services. The evaluation blueprint provides reproducible benchmarks and tradeoff analyses to inform real-world deployments.

VI. FUTURE WORK

1. **Verifiable remote inference & attestation:** integrate hardware-backed attestation (TPM/SGX/SEV) and verifiable computation to increase trust in outsourced inference.
2. **Context-aware privacy budgeting:** adapt DP epsilon based on transaction sensitivity, user consent, and model criticality.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November - December 2025||

DOI:10.15662/IJRPETM.2025.0806004

3. **Cross-jurisdiction consent orchestration:** design consent translation layers that reconcile differing legal obligations across markets.
4. **Cost-aware NFV placement optimization:** use learning-based placement to trade latency, privacy implications, and operational cost.
5. **Developer SDKs & sandboxes:** create tooling to reduce FAPI onboarding friction while preserving security guarantees.

REFERENCES

1. European Parliament & Council. (2015). Directive (EU) 2015/2366 (PSD2) of 25 November 2015 on payment services in the internal market. EUR-Lex.
2. Reddy, B. V. S., & Sugumar, R. (2025, April). Improving dice-coefficient during COVID 19 lesion extraction in lung CT slice with watershed segmentation compared to active contour. In AIP Conference Proceedings (Vol. 3270, No. 1, p. 020094). AIP Publishing LLC.
3. Madathala, H., Yeturi, G., Mane, V., & Muneshwar, P. D. (2025, February). Navigating SAP ERP Implementation: Identifying Success Drivers and Pitfalls. In 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) (pp. 75-83). IEEE.
4. OpenID Foundation — FAPI Working Group. (2019). Financial-grade API (FAPI) 1.0 — Part 2: Advanced. OpenID Foundation.
5. Komarina, G. B. (2024). Transforming Enterprise Decision-Making Through SAP S/4HANA Embedded Analytics Capabilities. Journal ID, 9471, 1297.
6. Amuda, K. K., Kumbum, P. K., Adari, V. K., Chunduru, V. K., & Gonepally, S. (2021). Performance evaluation of wireless sensor networks using the wireless power management method. Journal of Computer Science Applications and Information Technology, 6(1), 1–9. https://doi.org/10.15226/2474-9257/6/1/00151
7. ENISA. (2022). NFV security in 5G: Challenges and best practices. European Union Agency for Cybersecurity.
8. Balaji, P. C., & Sugumar, R. (2025, April). Accurate thresholding of grayscale images using Mayfly algorithm comparison with Cuckoo search algorithm. In AIP Conference Proceedings (Vol. 3270, No. 1, p. 020114). AIP Publishing LLC.
9. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of AISTATS / arXiv.
10. Sangannagari, S. R. (2022). THE FUTURE OF AUTOMOTIVE INNOVATION: EXPLORING THE IN-VEHICLE SOFTWARE ECOSYSTEM AND DIGITAL VEHICLE PLATFORMS. International Journal of Research and Applied Innovations, 5(4), 7355-7367.
11. Peddamukkula, P. K. (2024). The Impact of AI-Driven Automated Underwriting on the Life Insurance Industry. International Journal of Computer Technology and Electronics Communication, 7(5), 9437-9446.
12. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science.
13. Google Cloud. (2020). MLOps: Continuous delivery and automation pipelines in machine learning. Google Cloud Architecture Center.
14. OWASP. (2019). API Security Project / API Security Top 10. Open Web Application Security Project.
15. Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D., ... & Young, M. (2015). Hidden technical debt in machine learning systems. Proceedings of NIPS.
16. NCCS / Industry guidance. (2023). Network function virtualization guidance for cloud deployments. (Practitioner guidance on VNFs and virtual security appliances).
17. Karvannan, R. (2024). ConsultPro Cloud Modernizing HR Services with Salesforce. International Journal of Technology, Management and Humanities, 10(01), 24-32.
18. Arjunan, T., Arjunan, G., & Kumar, N. J. (2025, May). Optimizing Quantum Support Vector Machine (QSVM) Circuits Using Hybrid Quantum Natural Gradient Descent (QNGD) and Whale Optimization Algorithm (WOA). In 2025 6th International Conference for Emerging Technology (INCET) (pp. 1-7). IEEE
19. Kumbum, P. K., Adari, V. K., Chunduru, V. K., Gonepally, S., & Amuda, K. K. (2023). Navigating digital privacy and security effects on student financial behavior, academic performance, and well-being. Data Analytics and Artificial Intelligence, 3(2), 235–246.
20. Practitioner resource: FAPI 2.0 overview and implementation notes. (2022). FAPI 2.0 Security Profile overview. OpenID Foundation / vendor docs.
21. Joyce, S., Pasumarthi, A., & Anbalagan, B. SECURITY OF SAP SYSTEMS IN AZURE: ENHANCING SECURITY POSTURE OF SAP WORKLOADS ON AZURE–A COMPREHENSIVE REVIEW OF AZURE-NATIVE TOOLS AND PRACTICES.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November - December 2025||

DOI:10.15662/IJRPETM.2025.0806004

22. Research review: Federated Learning with Differential Privacy (systematic survey). (2022). Survey/Review papers on DP-FL.
23. Konda, S. K. (2023). Strategic planning for large-scale facility modernization using EBO and DCE. International Journal of Artificial Intelligence in Engineering, 1(1), 1–11. https://doi.org/10.34218/IJAIE_01_01_001
24. Practitioner whitepaper: API management and secure Open Banking implementation guidance (developer and operator notes). (2021–2022).