Deep Science Publishing
https://doi.org/10.70593/978-93-49910-62-1 _11

DeepScience
Open Access Books

Chapter 11: Building secure, scalable cloud-enabled architectures for future-ready banking solutions

11.1. Introduction

In the present times, banks are looking for Cloud-enabled solutions that are secure, scalable, and capable of meeting the complex operational requirements of a 21st-century business. The primordial focus of banks today is to protect the interests of their depositors by being transparent, securing sensitive data from being compromised, making their operations a zero-breach model, and by mustering huge resources in order to strengthen their Cyber Security posture. However, there is also a compulsion for banks to decide and invest in Modern Banking solutions that are Cloud-ready and capable of solving challenges faced by the banking industry due to massive growth and relentless competition in Financial Technology. This paper investigates the possibility of using Cloud as a viable solution for the banking industry. In particular, it covers a banking solution that is capable of offering secured Operations through Digital Enabled Channels and help the Banks offer Services at speed in cost-effective manner with Cloud based Modern Banking Solution. It also details the considerations that Banks must go through while choosing the Cloud as a Deployment option (Khan et al., 2022; Adewale, 2023; Akande et al., 2024).

The Banking ecosystem is now broken into a set of Service Providers with very tight partnerships. Core Banking service is at the centre which is built on Specialized Architecture on Integrated Platform. The tools used to integrate these Service Providers need to be flexible and support Micro Services Architecture since banks may have to pick from several Service Providers to fulfill their needs. The Niche Collaboration will bring in a great Customer Experience. But the challenge will be to make sure that the Data is secured and Communication is tightly controlled to lessen the Cyber Security Risk. Cloud has matured as Technology and is now used by all Major Technology Companies for Internal and External Solutions. Today accepting Cloud as one of the Deployment Option is Mandatory for Banks in order to remain relevant. In this paper we present a specialized Banking Architecture using Cloud as a Deployment Option. This architecture takes care of the Cyber Security Factors a Bank must consider while Building Cloud Enabled Solutions (Penaloza et al., n.d.; Subramanyam, 2021; Paleti, 2025).

Fig 11.1: Building Secure, Scalable Cloud-Enabled Architectures

11.1.1. Background and Significance

Financial technologies and digital banking have made rapid technological advancements in recent years. Simultaneously, consumer and business requirements in terms of usability, convenience, availability, and a complex range of options have grown significantly. With the adoption of instant payment services and banking procedures, the possibilities for innovative and beneficial first and third-party payment algorithms and services are endless. The pandemic accelerated this growth by moving even the most traditional of financial services wholly online. In the form of digital banks, companies from outside the financial sector introduced financial products with a new and streamlined user experience that challenged existing financial institutions and bank service offerings. Digital-only non banks went on to raise funds at valuations that were unprecedented at the time and invested heavily to transition traditional banking to digital-only products and processes. As new market entrants have continued to emerge, the long-standing competitive advantage held by established banks and financial institutions is now being challenged by financial platforms and innovative tech-first companies looking to address an underserved or an entirely new target audience.

The digitization of banks and the launching of digital wallets, APIs, and third-party service providers have not only revolutionized banking operations and customers' interface with banks but have also offered opportunities for third-party service providers to challenge long-standing banking service and product lines through add-on services. Using opportunities, fintechs have been able to free disparate data that traditional banks inadvertently had possession of and that were necessary enablers of technology-led financial inclusion. With customer data dynamically available from a multitude of sources, fintechs have innovated and challenged the status quo for issuing credit to consumers and businesses to fill in a previously underserved and high-interest space. More recently, advances in artificial intelligence, data aggregation, blockchain, and machine learning are being exploited by today's fintechs to address these gaps in financial inclusion and expand the umbrella of affordable financial services to the unbanked.

11.2. The Evolution of Banking Technology

The banking business has been in operation for almost four centuries. The genesis of banking lies in the basic functions such as custody, safekeeping, clearing, and the lending of surplus funds to the deficit sector. Travelling from England to all over the world during the 16th century with coins and huge gold reserves was quite a risk. Thus the erstwhile bankers safeguarded the valuables of trade guilds, aristocrats, noblemen, and even royals as custodians. The very need to protect wealth already in existence began during the inception of this unique business of being a custodian, the initial technological support derived from the ledger, where records were maintained. The advancement of banking began with the introduction of paper currency, and thereafter, deposit banks secured by reserves of currency. With the business of banking expanding, the growth of banks demanded more complicated technology for the continued safekeeping, transacting, and lending of surplus funds. With the advent of and rapid growth of needs for more such technology, banking began to compete against itself for providing more sophisticated technology and customer service. This led to a whole new dimension called retail banking. What started as a safe keeping of cash became custodian, clearing, dealing, remitting and general agent for goods, services and assets of all professions and income groups, it became a true financial supermarket.

The light of the current computerized age of information providers, during which a huge revolution in computing and telecommunication takes place at enormous speed over the past four decades, began a heavy fund and resource rationalization process. Banks began to realize that their actual business did not require a large amount of physical business and recovery costs. This enabled the banks to create financial products which are without geographical barriers and rampant financial services from different locations became available to customers across the world through wire and satellite networks, the networked virtual banking.

11.3. Understanding Cloud Computing in Banking

Cloud computing is the delivery of various services over the internet. It allows banks and financial institutions to store and manage core applications without maintaining the infrastructure. It includes data storage, servers, networking, databases, intelligence, software, analytics, and more. These services can be structured into three types - software as a service, platform as a service, and infrastructure as a service. Software as a service allows organizations to access statistical probability as an application. An example of SaaS is where you upload your data and you receive the result without any installation in your own machine. The bank has the option to either build its analytical infrastructure on its own or rent platform capacity from a cloud vendor. Organizations can rent infrastructure as servers, storage, and other services.

Fig 11.2: Cloud Computing in Banking

Banking is a highly competitive field, with small margins. Cloud computing is benefitting financial institutions in many ways. Unfortunately, it’s too good to be true. We hardly see banks moving to the cloud. The cloud couldn’t be envisioned as some random application that gives you some new feature. The cloud is a federal platform for all organizations. Banks and financial institutions have heavy regulations, complex infrastructure, very high security and privacy requirements, and a public environment where frauds are on the rise.

11.3.1. Definition and Types of Cloud Services

Cloud computing is an as-a-service computing model that enables ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing entrusts remote services with a user's data, software and computation. This entrustment means that security and privacy are the most important issues in cloud computing. These issues affect the customers' acceptance of cloud computing, as well as the reliability of cloud infrastructure.

Data security, for example, focuses on the prevention of unauthorized access and data breaches, while privacy refers to the individual privacy of users that utilize protected information. Cloud computing is the delivery of hosted services over the Internet. Companies provide these services to enable a customer's business to run at lower costs while also providing flexibility and scalability. Cloud services include infrastructure, storage, design, and applications. IT resources can be expanded as a customer's business grows. Moving to a cloud service can reduce upfront expenses by alleviating the need to maintain and upgrade hardware or software. There are three main types of cloud services that can be offered: Infrastructure as a Service, Software as a Service, and Platform as a Service. These three types cover a variety of cloud offerings. Many companies offer services that bridge multiple areas.

11.3.2. Benefits of Cloud Computing for Financial Institutions

The migration of Financial Services to the cloud has become an inevitable trend in their digital transformation journey. Such migrations allow for optimized operational overhead and improved financial performance for Financial Institutions in an increasingly competitive market. This has led to the adoption of cloud computing solutions by traditional banks and institutions. Banks are required to adapt their PaaS and IaaS models for the rapidly evolving customer preferences and partner collaboration models. The demand for FinTech services is on the rise and banks find their traditional exclusive roles of savers and lenders disrupted by innovative technologies of Cloud and Distributed Ledgers. Moving to a cloud would allow banks to make substantial operational efficiencies, allowing them to redirect resources to their primary business value creation activities. The increased market competition owing to regulatory changes is forcing banks and institutions to invest heavily in the digital revolution, moving their services to be remotely accessible to customers. In the absence of Cloud solutions, these disruptions would require non-trivial investments in hardware and software infrastructure by the traditional financial institutions. Cloud solutions can serve as a great remediative option given the restrictive budgetary measures. The changing technology demands for enhanced customer engagement and new customer base expansion require selected banks and financial service institutions to diversify their customer offerings. Such diversification may involve some unique technology investments to remain competitive and to hedge with Collaborating FinTech players. Non-trivial technology investments by the traditional and incumbent banks can benefit greatly by leveraging the economies of scale offered by the Cloud solution models. Cloud would allow for these institutions to offload their infrastructure investments for these specialized service offerings and collaborate with selected proactive partners. The banking solution vendors also able to migrate their solutions to conform to the Cloud ecosystem would derive a competitive advantage in the marketplace. A survey of Tier-1 banks show substantial investments over the next 3-5 years aiming to migrate mission-critical applications to the Cloud to enhance their business offerings and make them agile.

11.4. Security Challenges in Cloud Banking

The adaptive economic environment of the banking industry requires the highest level of security, data privacy, and compliance. The cloud-stack ecosystem continuously introduces newer challenges: stronger hacker attacks, efficient hosting model, shared infrastructure, data privacy, and virtualization vulnerabilities, etc. This is further complicated by the fact that every component of the cloud-stack model is liable to be developed and hosted by a different player in cloud computing and can employ different strategies. Security breaches can and do happen: a cloud-based user's sensitive data was accessed by hackers as a result of a lapse in user identity authentication. Public cloud infrastructures have also been breached. Stolen cloud credentials through denial-of-service attacks were used to detect loopholes in the service provider's security and gain access to sensitive patient data.

The potential for data breaches to lead to sensitive customer information being released is more pronounced in the cloud model than in traditional, on-premise solutions. Payment and personal identification information is just one example of types of data that consumer-facing businesses process and protect. Similarly, in the case of banks, the loss of customer information is a top question in any escalation call. This has led to strong government input on the privacy and compliance of areas related to banking, particularly the data explosion era that we live in where customer and transaction records can be stored in the millions or billions. High-profile data scandals have also led to regulations which impose strict penalties on any bank breaching business. The important consideration is that it is the responsibility of the bank to ensure the details are protected and have backup and recovery in place.

11.4.1. Data Privacy Concerns

Privacy issues are an important barrier to cloud banking and are further complicated because of stringent security standards. Banks commonly manage highly sensitive personal financial data and provide a key conduit for Western economies' movement of money. Service providers cannot be granted total unfettered access to private consumer data inside cloud computing environments, meaning that regulations must establish clear procedures for handling and monitoring such data. Governed data must be dealt with in ways that fall below the encryption level, and even then, particularly sensitive affected data may need to be handled with the utmost caution in terms of access limitation, transaction logging, and encryption.

Consumer privacy regulations also need to account for possible intrusion by nation-states into monitored clouds and uncontrolled foreign access to consumer data that is stored or transported. Rules also must sufficiently control what sensitive functions are processed in the cloud. Banks have been instructed to avoid cloud processing of Social Security numbers, credit/debit numbers, and any sensitive personal health data, and for good reason. Clouds, for all their advantages of consumer convenience and expense reduction, expose consumers to a greater risk of data theft. One bank that recently moved business analysis to the cloud saw four million sensitive records hacked. The cloud was used to monitor customer transactions in order to gauge banking product selling opportunities. So it makes sense that the feds keep a close eye on cloud-based banking, again for good reason.

11.4.2. Regulatory Compliance Issues

When it comes to banking-related data security regulation, businesses across the cloud ecosystem have some heavy lifting to do. In addition to abiding by industry standards, banks also have to comply with an amalgamation of banking regulations pertaining to the same set of compliance goals. Violation of this set of rules could spell disaster as would not be upfront enough in event of any such violations. It could cut into service, hurt customer loyalty and retention, and as a last resort, get the service provider and/or bank fined. All of this could mean that heavy-duty restrictions like on-premise-only data vaults are enforced for banks. In an effort to gain increases in demand-generating infrastructure efficiency and elasticity, neither the cloud banking service providers nor the banks may find parallel cloud vault systems particularly helpful.

One of the primary goals of compliance standards is data security. Considering that modern-day banking, whether traditional or neo, has evolved to happen in cyberspace, bank customers expect their physically-paper based data to also be electronically-paper based. This means that paper statements are a very low-revenue scenario. In cash-strapped countries, banks may even strike this off the list in favor of just bringing within regulatory requirements adjacency-granting digital signature solutions for individuals conducting large money transfers and trading in digital currencies. In addition, security lapses or perceived breaches in security could hurt customer loyalty and retention for banks just as much. Financial services security is the backbone of trust people put in banks and any violation-affecting event could persuade customers to afford ridiculous rates for trade-offs for transacting through alternative non-established options on the market while pretending otherwise.

11.5. Designing Scalable Architectures

An efficient architecture is able to accommodate usage needs and business goals with better performance and minimal costs. The cloud allows on-demand provisioning of resources, such as computing, storage, infrastructure, and networking, and companies in their architecture must look for a suitable level of resources for anticipated levels of use. Companies building future ready solutions in banking space need solutions that are secure, scalable, and cost effective, with rapid time to market. Cloud capabilities are basically led through scalability- vertical and horizontal. Use of shorter building blocks that are tested and managed allows future-ready solutions in the banking space to be updated incrementally and easily, and add new capabilities faster than traditional solutions. As applications move to the cloud, enterprises would be better served by creating cloud-specific native applications which use the full stack of available services. We believe that as cloud computing becomes more widely accepted across different industries and as the major cloud service providers continue to innovate, the scenario for building future-ready solutions will become much easier and as these solutions will meet the ever-growing needs in banking and financial services. Applications deployed on cloud environments can drive a desired growth in revenue without a corresponding increase in costs. Future-ready banking applications run on distributed architectures created with cloud computing capabilities in mind. Coupled with cloud services for data storage, real, or near real-time analytics, machine learning capabilities, IoT connectivity, security, and industry-specific core services, these microservice-based architectures provide a high degree of scalability while remaining cost-effective. Solutions can also use serverless for those cloud functions that would require short bursts of computation, managing functions with variable loads and where.

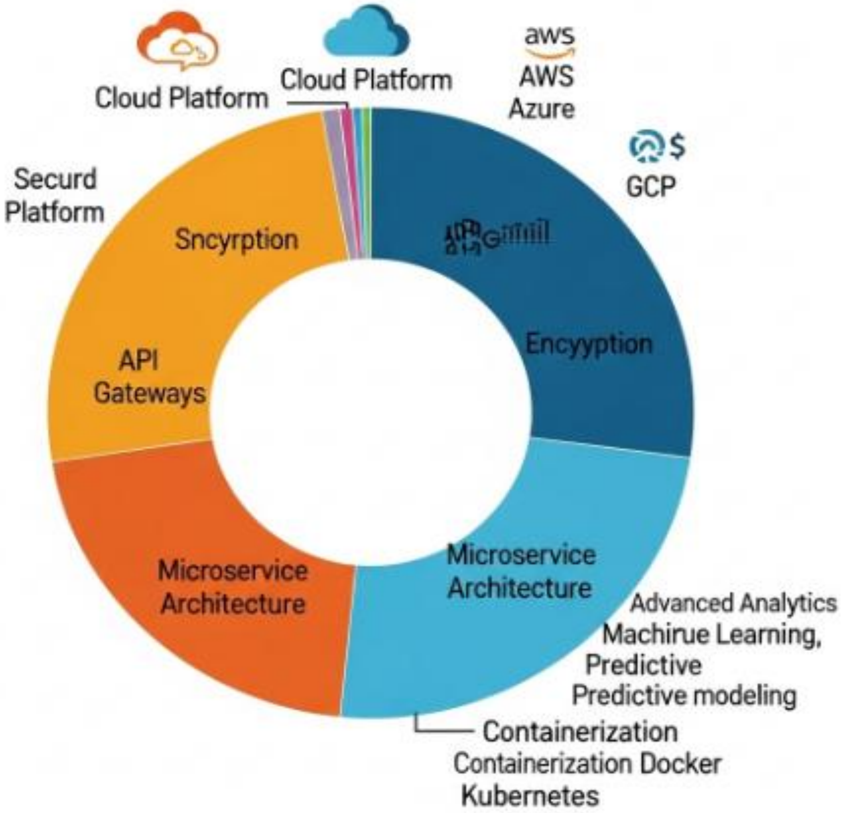

Fig : Building Secure, Scalable Cloud-Enabled Architectures for Future-Ready Banking Solutions

11.5.1. Microservices Architecture

Microservices are discrete, stateless APIs focused on well-defined business functionality. Microservices architectures consist of a collection of such microservices enabling a loose coupling of solution components and allowing for independent scalability, evolution, and deployment. While microservices per se are not a new concept, their adoption and usage within enterprise solutions are accelerating. Especially heavy-duty enterprise solutions positioning themselves toward the digital and cloud fronts are being planned and deployed as microservices-heavy architectures. With popularity come questions and concerns regarding how best to adopt or adapt those patterns. How many microservices make a microservices architecture? Microservices architectures inherently address many of the problems we have been struggling with as we evolved from monolithic to distributed architectures. Yet, many questions around how best to implement microservices as functional distinct and optimized APIs remain. Much of the time, the trick is to balance microservices with the need for transaction coordination across these APIs. Too many transaction-oriented APIs demand for a transaction coordination consensus pattern between them. The API orchestration pattern makes such orchestration easier.

The challenges in microservices design are basically management of the so-called canonical data model and how to handle transactions that need to span multiple APIs. APIs may include queues, event buses, and back-end services that to the client app behave like APIs but are considered as back-end services contained with a single microservice. Do we require a common message pattern for collaboration between the different teams responsible for the design of the different microservices responsible for their own domains in conjunction with the design of the within-domain back-end services?

11.5.2. Serverless Computing

When a product is conceived to be offered on the cloud, it is a best practice to consider the product's architecture as cloud-native from day zero. This is because the decisions taken in those early days will shape up the way the product will be managed as it is released and as it scales, and it will determine the operational costs for the lifetime of the product. Even if the latter may vary depending on critical decisions we take along the way, every business entity needs to minimize costs. Therefore, our teams should be careful when setting the infrastructure for our future banking solutions. Serverless computing offers a great deal of abstraction with regard to the operational tasks necessary to deploy and maintain a component of a particular service. Specialized parties allow organizations to concentrate their efforts on improving the business logic of their core processes, rather than losing precious time and effort on deployment tasks. However, like a double-edged sword, the advantages that serverless computing offers can quickly turn into a nightmare.

Using a serverless architecture in a small-scale implementation allows teams to focus their efforts on the business logic of the system. Serverless architectures are managed platforms on which we upload our latest code implement, where the Function as a Service provider abstracts the operational burden of deploying and running our microservices. These companies have worked hard in the last several years in order to shape the operating systems of the present and the future, and higher-level cloud services are becoming more intuitive, avoiding the tedious tasks that have taken the lion's share of time and resources from our teams through the years. Who would have thought that deploying our code would be as simple as pushing a button, without worrying about the bottom layers anymore?

11.6. Conclusion

While these banking systems and their workloads are not trivial, building them in the cloud is a scalable option to take. Cloud has a world-wide presence and built-in features for high-availability and delivery of the latest features. While some concerns exist about security, bank accounts are being opened, and products deployed, every day using cloud systems. As cloud gets traction in banking, being able to build products that span cloud, on-premise, and hybrid models will allow banks to leverage their existing systems while still taking advantage of modern capabilities in cloud for delivering new products. Cloud vendors as well as third parties are investing in banking-ready components so that common patterns of banking workloads can be built quickly while providing solutions that remain under the control of the banks. Workflows will be constructed in such a way as to enable verification of all of the components of those banking systems. Cloud systems, while global, can utilize embedded security features that help to limit data availability. Banks can use specific country resources to guarantee that no customer transactional data will leave that country. Security requirements can sometimes be met by this geo-fencing capability.

Cloud Native is much more than just deploying virtualization technology in the cloud. The previous sections of this chapter explain these capabilities and demonstrate their use for load-testing and disaster recovery. This knowledge, along with the evolving security and compliance considerations will dictate the transition to the bank of the future. The transition journey will require investments in skill development and the creation of appropriate processes. As financial services continue to permeate every aspect of our lives, the need for speed and failure recovery will dictate the adoption of the cloud native model.

11.6.1. Future Trends

There is a future need for low latency and data-intensive applications that can enhance sustainable digital banking needs. In this study, we focused on deployment of cloud platforms, microservices architecture and outcomes of open and closed banks, which can cater and support future banking services requirements. However, many new technologies and new approaches to the bank's cloud journey could also be considered to be included in future bank services research and study. Given the fast pace of the technological changes, many influencing factors for banks to start and utilize these technological changes needed to be highlighted. Technological development and changing market landscape concepts can provide bank changes especially in speed, scale and availability of services. This is considered mainly because of the introduction and the great benefit of the resident and innovative capabilities of cloud computing. Examples such as banking as a service, open banking relative technological developments such as new currencies, digital ledgers, the growing emphasis on sustainability as well as new business models were the discussion points.

Currently, the focus for banks, on their cloud journey, is also the development of low latency and data-intensive technology platforms, most of them being aligned with the need to enhance digital bank products and services. Given the money intensive nature of the banking services and products, it is imperative that previous assumptions of banking solutions enabling availability affinities were beaten. The velocity of change is almost planned with their technology supply chain partners as their gears enable them to fulfil promises and customers expectations of products and services delivery. How can banks be supported and implemented new cloud solutions that allow the focus to be a continuous investment, and not distraction from the core business and reliance on ever better technology partners.

References

Subramanyam, S. V. (2021). Cloud computing and business process re-engineering in financial systems: The future of digital transformation. International Journal of Information Technology and Management Information Systems (IJITMIS), 12(1), 126-143.

Adewale, T. (2023). Harnessing Cloud and AI for Seamless Digital Transformation: Key Technologies and Business Impact.

Penaloza, D. M., Ruiz, C. J., Soto, V., Mendoza, R. F., Saptu, J., & Auja, A. Adaptive Cloud Architectures for Scalable and Secure Payment Systems: A Strategic Lens on Modernization Trends.

Paleti, S. (2025). Smart Finance: Artificial Intelligence, Regulatory Compliance, and Data Engineering in the Transformation of Global Banking. Deep Science Publishing.

Khan, M. M., Haque, R., & Bajwa, A. (2022). A Systematic Literature Review on Energy-Efficient Transformer Design For Smart Grids. American Journal of Scholarly Research and Innovation, 1(01), 186-219.

Akande, J. O., Mugova, S., & Odularu, O. I. (2024). *Information Processing and Accounting Standards*.