**Cloud Security Challenges and Remedies in Banking and Finance.**

**Amer Mohammed** (1)

Researcher (1), University of the Cumberland’s, 6178 College Station Drive, Williamsburg, KY 40769. JP Morgan Chase US Corp (1)., USA

DOI:

**Abstract**

The banking and finance industry has significantly leveraged cloud computing to enhance operational efficiency, reduce costs, and drive innovation. Cloud resources' scalability and on-demand nature have been instrumental in these advancements. However, adopting cloud technology has also brought about security challenges, particularly in an industry that deals with highly sensitive financial and personal data. These challenges include data breaches, unauthorized access, insider threats, misconfigured cloud settings, insecure application programming interfaces, and a lack of control over data location and governance. Moreover, financial institutions must navigate complex regulatory frameworks such as GDPR, PCI-DSS, and local banking compliance regulations, which demand robust data protection and auditing mechanisms.

The intricacies of the cloud's shareability model often create uncertainty regarding which party the cloud provider is accountable to concerning specific security matters, leading to possible vulnerabilities. Moreover, limited visibility into the third-party infrastructure of shadow IT and rapid DevOps practices heighten the risk of data exposure and regulatory non-compliance.

To confront these issues, a thorough and strategic security framework is essential. It includes adopting robust identity and access management (IAM) systems featuring multi-factor authentication, comprehensive data encryption, and ongoing monitoring and threat detection utilizing cloud-native security solutions. This continuous monitoring and threat detection should provide reassurance about the ongoing protection of your data. Financial institutions should also focus on regular security audits, formulate incident response strategies, and ensure compliance with region-specific data residency and governance standards.

This document explores these challenges in detail and offers practical solutions that banks and financial entities can implement to protect vital assets in cloud environments. By adopting a multi-layered and proactive security strategy, the sector can minimize risks, maintain trust, and fully realize the potential of cloud computing securely, compliantly, and resiliently. This proactive approach empowers the industry to take control of its security and adapt to the evolving landscape of cloud computing.

Keywords: Cloud-Computing, Banking, financial system, security, data privacy.

**Introduction**

In the next few years, cloud computing will be one of the most rapidly advancing technologies in banking and financing. Most cloud service investments will focus on secure business applications for banks, moving away from on-premises solutions towards cloud-based services, especially for critical business operations such as customer relationship management and enterprise resource planning. Customer relationship management) Furthermore, ERP (Enterprise Resource Planning) and BPM (Business Process Management) are two frequently mentioned terms that people often confuse with each other (Capgemini, 2017).

The banking and finance sectors are proceeding cautiously with cloud computing, as no single cloud service delivery model will likely emerge as the dominant one. The appropriate cloud services delivery model will align best with their requirements. The cloud computing needs of a company can provide financial institutions with numerous benefits, including:

1. Cost savings and billing based on reducing environmental cost

Financial institutions can use distributed computing to convert a significant upfront capital expenditure into a more manageable ongoing operating expense. There's no need to waste money on purchasing new hardware and software. Furthermore, due to the dynamic nature of distributed computing, financial organizations can selectively choose the services they need and pay as they go.

2. Operational continuity without downtime

With cloud computing, the service provider is responsible for managing the technology. It provides banking institutions with enhanced data security, resilience against non-critical failures, and improved disaster recovery capabilities. Additionally, cloud computing provides greater redundancy and backup options at a lower price than traditional managed solutions.

3. Business flexibility for future upgrades

Thanks to the adaptability of cloud-based operating models, financial institutions can experience reduced product development timelines. This enables quicker and more efficient responses to banking customers' demands. As the cloud is available on demand, there is less need for significant infrastructure investment, leading to a swifter initial setup process. Cloud computing also facilitates the creation of new products without capital investment.

Moreover, cloud computing allows organizations to transfer non-essential services to the cloud, such as software updates, maintenance, and other computing tasks. Consequently, firms can concentrate on their core financial services rather than IT concerns.

4. Environmentally friendly technology

Organizations can leverage cloud computing to migrate their services to a virtual platform, thereby decreasing energy consumption and the carbon footprint associated with maintaining a physical infrastructure. It also results in more efficient utilization of computing power and reduced idle time. Cloud service models enable financial institutions to shift from a capital-heavy strategy to a more adaptable business framework that lowers operational expenses. Choosing the right cloud services model to fit business requirements is crucial for success. This section will explore various cloud computing services, operations, and deployment models (Capgemini, 2017).

**Literature Review**

As previously stated, cloud computing has gained traction across various sectors, including banking and finance. The advantages of utilizing cloud-based services are steadily growing, alongside the challenges and corresponding solutions that arise from their application in different industries.

When discussing cloud computing, a range of components falls under its umbrella in one way or another. For example, frequently mentioned aspects of cloud computing include hardware, software, networks, systems, big data, the Internet of Things, communication channels, security protocols, data security issues, access concerns, cyberattacks, and the virtualization of physical components.

Conversely, the banking and finance sector often highlights aspects such as customer personal information, transaction records, access to services like loans, collections, mortgages, credit histories, and trading of stocks, shares, and options. The overlap between these two domains primarily lies in big data, accessibility, storage, and security. While cloud computing offers a variety of services, the banking and finance industry leverages these services according to their specific needs and requirements.

A significant challenge associated with cloud computing is security. Although cloud usage presents numerous benefits for businesses, it can also introduce security vulnerabilities such as cyber threats, hacking incidents, and issues related to accessibility, the virtualization of resources, attacks on virtual machines in the cloud, as well as network and storage challenges, which may depend on the service package chosen (De Donnon et al., 2019).

It is also understood that the cloud provides services through various models, and each model may present specific issues if not properly implemented or adopted. As noted by Iqbal et al. (2016), prevalent security concerns associated with the three primary models—SaaS, PaaS, and IaaS—include data leakage, storage vulnerabilities, virtualization, connections to networks, and the sharing of infrastructure. Additional issues may encompass hardware or software update interruptions, modifications to specific systems, misuse of infrastructure, and accountability (Iqbal et al., 2016).

Several developments have been made in the realm of cloud computing, a technology that has proven its adaptability and potential across various sectors. However, the exploration of potential security issues has not been adequately addressed. Research conducted by De Donno et al. (2019), Iqbal et al. (2016), and Tahirkheli et al. (2021) indicates that there is still a gap in studies related to the applications of IoT and the adoption of big data in cloud computing. Nevertheless, the implementation of cloud computing across various sectors is quite remarkable.

A significant advantage of cloud computing is the decrease in management costs, the availability of extensive virtual storage, and the ability to associate from anywhere at any time as long as users are connected (Jamsa, 2013). While users can access data from any place, security concerns persist. This is particularly concerning for the banking and finance sector, which handles sensitive customer information and is adapting to open banking; hence, this matter can be quite alarming. Therefore, these industries are subjected to continuous oversight and regulations to ensure data and transaction safety (Mahalle et al., 2018).

In the banking and financial sector, customers frequently engage in monetary transactions. Some may be opening their first account, while others might be finalizing a stock market transaction, applying for a first-time loan, or paying off existing loans. The interactions involved, along with the extensive documentation generated during these processes, must be securely stored, typically in either an in-house or cloud-based data warehouse. It is crucial for businesses to safeguard their infrastructure to mitigate potential security threats associated with such data. Edu et al. (2021) pointed out that common failure points include inadequate backups, firewalls not functioning as required, and the absence of regular security audits. Furthermore, Edu et al. (2021) suggested that without appropriate oversight and management, subsequent security concerns could arise from inadequate control management and failure to securely identify users and third parties.

The existence of security issues and challenges indicates that there are feasible, proposed, and effective solutions available. The solutions a business chooses to adopt primarily depend on the specific issue, financial considerations, security protocols, and infrastructure. Some of the frequently suggested and implemented solutions include data encryption, both for information stored in the cloud and during transfer, utilizing blockchain technology and access keys, multi-factor authentication, secure gateways, and model-view-controller architecture, among others tailored to business needs.

For example, as noted by Omar and Abed (2020), fully homomorphic encryption can encrypt data and enable users to perform tasks without decrypting it. Conversely, simpler solutions like implementing multi-factor biometric fingerprint authentication and tokenizing a secure gateway can protect data against potential theft (Nagaraju & Parthiban, 2015). One of the most discussed solutions is the application of blockchain technology. It has been suggested for access control and data encryption due to its secure nature and operational methodology (Park & Park, 2017). Park and Park (2017) projected that blockchain technology for security would capture a market share of USD 20 billion by 2020, indicating a significant increase in its application for security purposes. In the research conducted by Riad et al. (2022), blockchain technology was suggested and tested, concluding that it could serve as an effective safeguard against attacks within the banking and finance sector.

**Analyzing Services, Deployment, and Operating Areas**

This part will examine these cloud models to identify the various security risks associated with each method in finance and banking. It will ultimately help financial institutions make informed choices that balance operational efficiency and authentication protocols with strong safeguards against potential cyber threats.

**Cloud Service Models**

Business Process as a Service (BPaaS): Billing, payroll, and human resources are examples of standard cloud-based business processes. All other service models can be integrated with process expertise in BPaaS.

Quality of Service (QoS): As financial institutions use cloud computing for operations, it is recommended that they implement strong quality measures and use the partnerships of cloud service providers to design the highest security standards. This creates a shared responsibility model, fortifies defenses against emerging threats, and custom creates a secure environment for sensitive financial data.[1]

SaaS (Software-as-a-Service): A service provider houses the business software and related data in the cloud, and users access the software and data via a web browser. Accounting and customer relationship management software are two examples of software that can be used.[1]

Platform-as-a-Service (PaaS): A cloud service provider provides a complete platform for the development, storage, and testing of applications, interfaces, and databases. Businesses can use this to streamline the environment development process, maintenance, and support of custom applications, lowering IT costs and reducing the need for hardware, software, and hosting environments.

Infrastructure-as-a-Service (IaaS): Instead of creating servers or clusters, data centers, or network equipment, this cloud model enables businesses to buy those resources as a fully outsourced service.

**Cloud Deployment Models**

Service providers typically implement cloud computing in three primary forms:

The cloud infrastructure is exclusively utilized by a single organization. The team can be set up internally or outsourced to a third party and hosted on-site or off-site. This type of cloud environment is considered the most secure option for cloud services.

The cloud infrastructure developed and held by a company offering users cloud services. These services are available to the public or a broad industry group.

The cloud infrastructure consists of two or more distinct clouds (private or public) that operate independently but work together to deliver services.

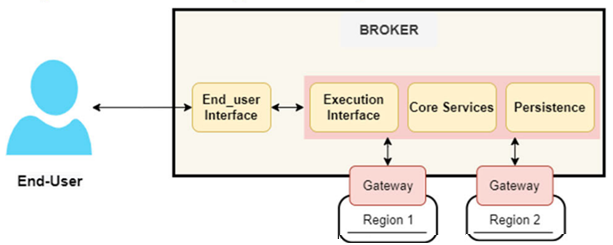


FIGURE 1. The Client ATM Transaction Hybrid Model

**Cloud Operating Models**

The third component of selecting the optimal cloud services delivery model involves determining the most suitable operational model for the desired mix of assets and resources. We have identified three operational models for cloud services:

a) Staff augmentation

Financial institutions can acquire cloud expertise by hiring individuals with the appropriate skills from service providers. An additional developer can be assigned at the company's offshore center for 24-hour development and troubleshooting. This operational model enables businesses to select the resource for each specific requirement.

b) Virtual captives

Virtual captives must maintain a dedicated number of resources or data centers to support the cloud system and on-demand support. This cloud operational architecture is a viable alternative to full outsourcing.

c) Outsourcing vendors

This model considers offshore centers where facilities and personnel from a third-party vendor manage cloud operations. It combines resources and investments to fulfill the cloud service needs of multiple banks

**Impact of Security Threats on Banking Operations**

In the contemporary banking landscape, security threats pose significant challenges that directly influence operational integrity and customer relations. This section explores the ramifications of these threats, examining a comprehensive summary of prevalent security issues and their detrimental effects on customer trust and institutional reputation. By elucidating these impacts, we aim to underscore the critical need for effective cloud security measures within the banking sector.

**Possible Summarization of Security Issues**

When a bank migrates to the cloud, it faces 2 primary challenges:

1.Ensure customer information security:

Confidential personal and financial information and essential applications must remain private and secure. Banks cannot risk a security breach.

2.Regulatory and compliance:

Numerous banking regulators require security measures that financial data belonging to banking customers be stored in the same country where the customers reside. Specific compliance regulations necessitate data segregation from other information on shared servers or databases. Therefore, banks need to be mindful of where their data is located in the cloud.

Financial institutions must select the right services, such as data encryption and secure access controls, deployment strategies, such as private or hybrid cloud, and operating models, such as shared responsibility, to tackle security and compliance issues. Initially, banks are expected to manage and operate the cloud as they begin adopting cloud computing. As the technology evolves and stricter regulations emerge, service providers begin to take on greater ownership and control of the cloud infrastructure.

**Damage to Customer Trust and Reputation**

The advantages of cloud computing are significant; however, the complexity of its model and underlying technology has led to management and security challenges. As the number of elements involved—such as networks, APIs, hardware, and architectures—grows within the cloud paradigm, the complexity of management issues increases.

**Enhancing Cloud Security for Financial Industries**

Cloud computing presents several advantages but brings complexities that create significant management and security challenges. As the cloud landscape grows and encompasses various components—including networks, APIs, hardware, and architectures—the difficulties of efficient management become more pronounced. Tackling these challenges is essential for harnessing the benefits of cloud technology while maintaining a secure and effective environment. The configuration, statistics, and query engines work together to ensure the collection, storage, and analysis of monitoring data, delivering a comprehensive range of monitoring capabilities.

**A.** **NUMERICAL DATA AND SEARCH ENGINES**

CONFIGURATION MODULE Engines: A crucial, adaptable, and trustworthy component, the configuration engine acts as a highly distributive system, enabling effective cloud infrastructure management and forming the basis for the monitoring strategy. This monitoring strategy determines the variables and events that need to be tracked, the tools to be employed, the individuals involved, and the actions to be taken.

STATISTICAL ENGINE: The statistical engine allows for evaluations of the cloud infrastructure's dynamics under normal conditions or when anomalies do not impact the findings.

QUERY ENGINE The query engine is a part that executes queries to reply to tenant requests by utilizing the configuration engine and the statistic engine. The benefit is that the query engine can be guided to the exact location of the data rather than needing to move the data to different nodes within the cloud infrastructure.

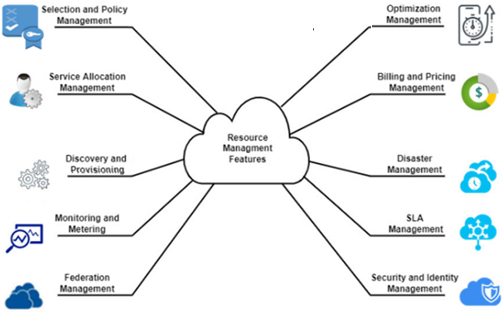
**B. THE CONFIGURATION ENGINE** The configuration engine functions as a reliable and highly available repository of configurations that also facilitates consensus, maintains configuration storage, sets up communication methods, and identifies failures for other components. The configuration engine serves as a dependable and accessible collection of configurations that provides agreement, preserves configuration data, creates communication frameworks, and monitors failures for the o other components.

Figure 2. Taxonomy and Characteristics of Cloud Resource Management

The publish/subscribe distributed architecture involves Node Monitor Agents and Node Supervisor Agents. NMAs are responsible for gathering and monitoring data, then transmitting it to interested parties. On the other hand, NSAs serve as the user access points to the cloud monitoring data. However, adjustments are needed in the placement of the NMAs and NSAs. The NSA component offers a versatile API that enables users to access local monitoring data stored in each cloud infrastructure node.

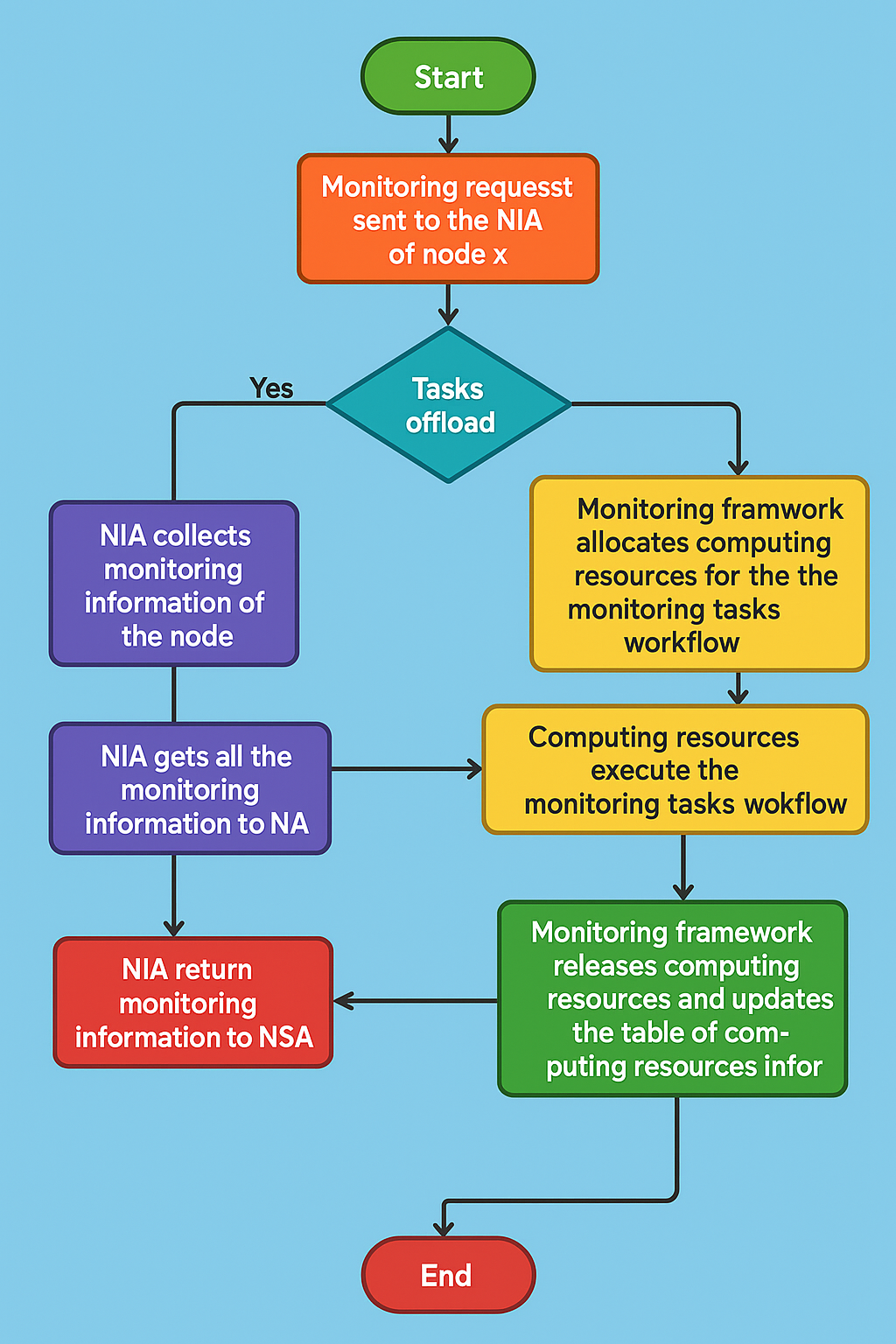


Figure 3. Flowchart for Overseeing Communication Among Agents

**Implementing Security in the Banking/Financial Sector**

Cloud computing offers a superior alternative to traditional data management methods, currently providing banks with an unmatched level of readiness, security, and flexibility (Sector & Walker, 2018). Its importance primarily lies in its ability to quickly adapt to standard environments better than any other technological service. It enables the operation of various software without needing to be installed on devices, allowing access to our media files via the internet. Managing the vast amounts of data that banking and financial institutions hold can be complex and risky without cloud support.

Cloud computing enhances business agility by improving organizations' overall capacity to respond quickly. It facilitates a more effective and speedy response to the demands of banking customers and shifting economic conditions. Additionally, cloud computing allows for streamlined product testing in real time, enabling companies to quickly adapt to market acceptance or rejection. It improves and creates methodologies for building new customer experiences, formulating market offerings, and optimizing operations.

Moreover, cloud computing empowers financial institutions to achieve significant efficiency gains and cost reductions, as the technology

**Advantages of Cloud Computing**

Cloud computing provides numerous advantages for your business. It allows you to establish a virtual office, enabling you to manage your business from anywhere, at any time. According to North (2021), the benefits of cloud computing include the following:

1. Cost Reduction

Cloud computing enables banks and financial institutions to cut costs. This means that no physical infrastructure is necessary. Transitioning to the cloud helps financial organizations avoid excessive capital expenditure and substantial upfront costs associated with building infrastructure. IT budgets cover hardware purchases, cooling, power, space, recruitment, and staff training.

2. Enhanced Customer Relations

Cloud technology significantly accelerates application development and deployment, allowing financial institutions to swiftly respond to customer needs. The time previously spent searching for sophisticated data insights can be reallocated to a traditional system, focusing on more beneficial and effective analysis and decision-making.

3. Robust Security

Virtual applications provide features such as data encryption, SSL management, and enhanced credentialing. In the financial sector, where security is a top priority, cloud services have become increasingly crucial. Cloud computing providers are tasked with managing the technology, and they adhere to stringent security standards that far exceed those of outdated systems vulnerable to data manipulation.

4. Improved Efficiency

Cloud technology can integrate various data and operational systems, enhancing efficiency. Partnering with a reliable cloud service provider allows banks and financial institutions to upgrade and respond to market demands as quickly as they need.

Cloud computing fosters better customer relationships through prompt and secure service. In light of the contemporary needs for advanced office technology, investment in cloud computing solutions is continuously progressing. Conversely, spending on traditional in-house IT is declining (Sector & Walker, 2018).

**Security Need of Banking and Financial Sector**

The banking and finance sector faces growing threats from cyberattacks, making it essential to implement strong security measures to protect sensitive customer data and financial transactions. This situation highlights the need for a well-rounded cloud security strategy that includes key components such as data encryption, access controls, and continuous monitoring. Furthermore, the need for regulatory compliance in this sector drives the adoption of sophisticated security measures, requiring institutions to align their operations with established regulations, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). As these elements come together, they underscore the urgent demand for a strong security framework in cloud environments tailored to banking and finance.

**Challenges during implementation**

The implementation of cloud computing in the banking and finance sector presents a myriad of challenges that must be addressed to ensure robust security and operational integrity. This section explores the critical obstacles encountered during deployment, including security vulnerabilities, data storage concerns, risks associated with application and data transmission, and complexities of distributed cloud architectures. Each subsection will delineate specific challenges and propose actionable solutions to enhance the resilience of cloud systems in financial institutions.

**Security Challenges and Possible Solutions**

In the context of cloud computing within the banking sector, security challenges are paramount, particularly concerning data confidentiality and compliance adherence. The safeguarding of sensitive financial information necessitates the implementation of advanced encryption methodologies alongside stringent access controls to mitigate unauthorized access risks. Additionally, the varying regulatory landscapes across different jurisdictions pose significant compliance challenges; therefore, establishing comprehensive governance frameworks and conducting regular audits become essential measures to ensure that institutions remain aligned with legal mandates. By addressing these critical security issues, banks can enhance their cloud infrastructures while maintaining trust and integrity in financial operations.

**Data Storage Security**

The adoption of cloud computing in the banking and finance sector brings with it a range of significant challenges that must be carefully managed to maintain strong security and operational efficiency. This section examines the key issues faced during deployment, such as security threats, data storage limitations, vulnerabilities in application and data transmission, and the intricacies of managing distributed cloud infrastructures. Each part will highlight these challenges in detail and offer practical solutions to strengthen the stability and reliability of cloud systems within financial institutions.

Algorithm 1 Severity Level Detection

Input: nTraffic, opK[]

Output: severity []

def ids\_frame(n\_traffic):

frames = []

while n\_traffic >= 1:

frame = ["identity\_of\_Frame", "frame\_element"]

frames.append(frame)

n\_traffic -= 1

return frames

def get\_severity(n\_traffic, op\_k):

current\_frame = ids\_frame(n\_traffic)

n\_alarm = {}

for e in current\_frame:

if has\_alarm(e):

v\_type = classify(e)

if v\_type in n\_alarm:

n\_alarm[v\_type] += 1

else:

n\_alarm[v\_type] = 1

severity = {}

for v\_type in n\_alarm:

severity[v\_type] = k(n\_alarm[v\_type], op\_k.get(v\_type, 0))

return severity

**Application and Data Transmission Security**

In the realm of banking and finance, the security of application and data transmission is paramount, as sensitive financial information is particularly vulnerable to interception by malicious entities. Ensuring the integrity and confidentiality of this data requires the implementation of robust encryption protocols and secure transmission channels that act as barriers against potential breaches. Additionally, comprehensive application security measures, including regular vulnerability assessments and advanced threat detection systems, are crucial for addressing risks associated with insecure application programming interfaces (APIs) and software vulnerabilities that threaten data integrity. These strategies form a critical foundation for safeguarding financial transactions in an increasingly digital landscape.

**Distributed Cloud Computing Challenges**

In the banking and finance sector, the move towards distributed cloud computing brings a complex set of challenges that need to be addressed thoughtfully. The dependence on multiple cloud service providers can create substantial difficulties in managing data governance and ensuring compliance with regulations, making it harder for banks to comply with various legal requirements across different regions. Furthermore, the division of data among different cloud locations raises serious issues related to data integrity and security; varying security measures across these locations may lead to vulnerabilities that can be exploited by cybercriminals. As these issues arise, it becomes crucial to examine the consequences for banking institutions that aim to uphold strong security standards while maneuvering through a complicated technological environment.

**Final Reflections on Cloud Security in Banking and Finance**

In summary, the investigation into cloud security issues within the banking and finance industry highlights the vital necessity of strong protective measures as financial institutions progressively transition to cloud-based solutions. The complex landscape of service models, deployment methods, and operational structures introduces distinctive vulnerabilities that can profoundly affect banking functions. As discussed in our review of existing literature, a variety of security threats—spanning from data breaches to compliance failures—represent significant risks to both institutions and their customers. To effectively address these challenges, it is crucial for financial organizations to embrace a multifaceted strategy for enhancing cloud security. This should involve the implementation of sophisticated encryption methods, strong identity management frameworks, and thorough risk assessment protocols. Moreover, cultivating a culture of cybersecurity awareness among staff is essential for reducing human error, which continues to be a prominent factor in numerous security incidents. Although there are challenges faced during implementation, such as adhering to regulatory standards and integrating with legacy systems, the advantages of cloud computing in boosting operational efficiency and customer interaction are undeniable. By proactively tackling security issues through innovative solutions and cooperative efforts with cloud service providers, banks can protect sensitive data while taking advantage of the benefits that cloud technologies provide. Ultimately, as we traverse this shifting digital landscape, it is crucial for key players in the banking and finance sectors to emphasize security practices that not only safeguard their assets but also foster trust with their clients. Adopting a progressive approach to cloud security will be essential for maintaining growth and resilience in an increasingly competitive landscape.

# References

Amazon, W. P. (2009). Introduction to Amazon Virtual Private Cloud. Amazon. Retrieved March 6, 2022, from aws.amazon.com/about-aws/whats-new/2009/08/26/introducing-amazon-virtual-private-cloud

Amidon, S. (2016). *Security*. Amazon. Retrieved March 6, 2022, from https://aws.amazon.com/security/

Bhandayker, Y. R. (2019). An overview: Security solutions for cloud environment. *International Journal for Scientific Research and Development*, 7, 1596-1598.

Business Wire. (2019). The Cloud Security in Banking Market, 2019 to 2024 - Leading Players is Google Cloud Platform*, Salesforce, Vormetric.* <https://www.businesswire.com/news/home/20190717005583/en/Cloud-Security-Banking-Market-2019-2024-->

Capgemini. (2017). Cloud computing in banking - . Retrieved March 6, 2022, from https://www.capgemini.com/wp-content/uploads/2017/07/Cloud\_Computing\_in\_Banking.pdf

De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., & Mazzara, M. (2019). Cyber-storms come from Clouds: Security of Cloud Computing in the IoT Era. *Future Internet, 11*(6), 127. doi:https://doi.org/10.3390/fi11060127

Edu, A. S., Agoyi, M., & Agozie, D. (2021). Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis. *PeerJ. Computer science, 7*, 658. doi:https://doi.org/10.7717/peerj-cs.658

Iqbal, S., Kiah, M. L., Anuar, N. B., Daghighi, B., Wahab, A. W., & Khan, S. (2016). Service delivery models of cloud computing: security issues and open challenges: Cloud computing security. *Security and communication networks, 9*(17), 4726-4750. doi:https://doi.org/10.1002/sec.1585

Jamsa, K. (2013). *Cloud Computing: SaaS, PaaS, IaaS, virtualization, business models, mobile, security and more.* Burlington, MA: Jones & Bartlett Learning.

Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure. *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))*, (pp. 407-413). doi:https://doi.org/10.1109/CSCWD.2018.8465318

Misra, S. C., & Doneria, K. (2018). Application of cloud computing in financial services: an agent-oriented modelling approach. *Journal of modelling in management, 13*(4), 994-1006. doi:https://doi.org/10.1108/JM2-12-2017-0131

Nagaraju, S., & Parthiban, L. (2015). Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. *Journal of cloud computing : advances, systems and applications, 4*(1), 1-23. doi:https://doi.org/10.1186/s13677-015-0046-4

Omar, Z. T., & Abed, F. S. (2020). A Proposed Fully Homomorphic for Securing Cloud Banking Data at Rest. *UHD Journal of Science and Technology, 4*(1), 87-95. doi:https://doi.org/10.21928/uhdjst.v4n1y2020.pp87-95

Park, J., & Park, J. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry (Basel), 9*(8), 164. doi:https://doi.org/10.3390/sym9080164

Riad, K., Elhoseny, M., & Jafari Navimipour, N. (2022). A Blockchain-Based Key-Revocation Access Control for Open Banking. *Wireless communications and mobile computing, 2022*. doi:https://doi.org/10.1155/2022/3200891

Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., . . . Kim, K.-I. (2021). A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Electronics (Basel), 10*(15), 1811. doi:https://doi.org/10.3390/electronics10151811

K. Subba Reddy, K. Rajendra Prasad, K. Nageswara Reddy, P. Anjaiah, "An Efficient Hybrid Fuzzy Image Encryption Models for the Secured Cloud Accessing in Portable Robotics Devices,", 2023. doi: 10.21203/rs.3.rs-2642523/v1

Q. Yuhuan, "Cloud Storage Technology," Big Data and Cloud Innovation, vol. 1, no. 1, 2017. doi: 10.18063/bdci.v1i1.508