Nat. Volatiles & Essent. Oils, 2023;10(1):220-226

NVEO
Natural Volatiles & Essential Oils

Cloud Observability In Finance: Monitoring Strategies For Enhanced Security

Naresh Babu Kilaru[1*], Sai Krishna Manohar Cheemakurthi[2]

[1*]Independent Researcher, nareshkv20@gmail.com
[2]Independent Researcher, saikrishnamanohar@gmail.com

***Corresponding Author:** Naresh Babu Kilaru
*Independent Researcher, nareshkv20@gmail.com

Abstract

Cloud observability thus has an important role to play in improving security for financial systems because it offers complete visibility of the cloud. With a growing number of financial institutions implementing cloud solutions in their operations, enhanced security becomes vital. Cloud observability involves the monitoring and identification of security threats in live to avoid issues related to cyber security threats, privacy, and regulatory compliance. This paper focuses on how monitoring approaches utilizing cloud observability can assist in enhancing the security of financial systems. By leveraging sophisticated tools such as digital logs, metrics, and distributed tracing, it becomes possible to acquire valuable data on cloud infrastructure to respond to threats actively. Traditional monitoring is replaced by cloud observability, which encompasses more profound access to the system's functioning and performance, without which it is impossible to ensure the reliability, confidentiality, and availability of financial information. It is within this context that this paper underlines the importance of implementing the proposed principles and practices to attain higher levels of cloud observability that are efficient, secure, and effective in supporting the financial ecosystem of the future.

Keywords: Cloud Observability, Financial Security, Data Privacy, Integration Complexity, Proactive Security, Security SLAs, Monitoring Strategies, AI Integration, Real-Time Monitoring, Threat Detection, Reputation Systems, Compliance, Cyber-Risk, Cloud Service Providers, Predictive Models.

Introduction

The financial sector is experiencing the flexibility wave, and it is leveraging cloud services due to the increased need for agility, scalability, and affordability. However, conflicts have emerged due to the escalating utilization of cloud environments, which presents an array of security hurdles that must be surmounted to prevent financial information leaks. Financial institutions work with and control a lot of sensitive data such as PII, transaction data, and financial projections, and thus, they are attractive to cyber attackers. Due to the incorporation of cloud services in the functioning of these institutions, the risk factor is also introduced, which calls for additional security measures against possible hacking, leakage of data, and other relevant incidents ([1]). Cloud environments come with numerous benefits, but they also come with added challenges, such as data governance, regulatory compliance, and lack of visibility that physical security may not adequately address.

As highlighted by Abouelyazid and Xiang. Next-generation architectures of Cloud infrastructure integrated with artificial Intelligence have open areas of susceptibilities that need ironclad security measures ([1]). Furthermore, the cyber-risk prospects connected to the strategy of cloud technology applications offer a more nuanced understanding of the need for the construction of security plans appropriate to the needs of the financial domain ([2]). With financial institutions increasingly adopting cloud technologies, there is a rising need for such institutions to put in place and deploy appropriate security measures that can adequately

address the risks in question. The latter authors underscore the importance of data storage security in cloud computing, as well as stressing that financial institutions ought to implement strict monitoring and security mechanisms to prevent data leakage and unauthorized access ([3]).

Among the approaches that should be considered effective in enhancing cloud security within the financial sector is the concept of cloud observability. Cloud observability goes a step further than usual cloud monitoring as it offers comprehensive views of the whole ecosystem to help institutions initiate, identify and address cyber threats as they occur in real time. This one entails the real-time monitoring and analysis of logs, metrics and traces so that there is confirmation that systems are running appropriately and are not susceptible to attacks. Observability tools make it possible for financial organizations to have full visibility of the cloud environment, which makes it easier to detect and deter any possible breach ([1], [2]). It means that by improving the monitoring of possible risks, financial institutions will be equipped with effective tools to prevent incidents and threats from becoming large-scale security issues.

Some of the goals of using cloud observability as a strategic approach to monitor and secure financial information include:

a) gaining end-to-end visibility in the cloud environment,
b) strengthening threat identification and response time
c) meeting a regulatory bar ([1])

Observability can unlock financial institutions by transitioning from a reactive security model to a proactive one, where security threats are detected and prevented from advancing to the critical stage. This approach will not only assist in securing data but also in preserving customer relationships and compliance with strict regulatory requirements [2]. Cloud observability, therefore, helps further cloud operations to optimize security issues and resource management among institutions by providing an actual-time look ([3]).

Cloud observability links with the objectives of protecting financial information, which are developed based on the general principles of the financial sector security framework. The growth of the financial industry, together with the tendency of cloud implementation, will continue to make cloud observability accepted as a paramount layer of cybersecurity practices to combat the growing instances of cyberattacks in the future ([2], [3]). Thus, examining the factors related to the observability in the cloudy environment in the financial sector, this paper expects to contribute to the identification of the security needs of cloud architecture in order to address the security challenges faced in the corresponding area. The discussion will go deeper into the monitoring practices that rely on observability to manage risks, as well as actively identify best practices for the use of these tools to protect financial data from emerging threats ([1]).

Simulation Reports

Simulation reports are also crucial in proving how cloud observability tools help develop security threats within financial systems. Recap Stress testing helps financial institutions understand how particular observability tools work in real-time threats. The inclusion of artificial Intelligence (AI) into cloud infrastructure, as described by Abouelyazid and Xiang, increases the effectiveness of these observability tools in analyzing for threats and preventing them. Specifically, observability architecture based on AI can continuously analyze enormous amounts of data produced by cloud environments and detect suspicious events and threats that may be beyond the capabilities of conventional monitoring. These demonstrations effectively assist in explaining the importance of up-to-date observability frameworks in the preservation of financial integrity and security.

One of the primary goals of making cloud observability is to ensure that the data is safe and secure, which is an important issue for financial institutions. Summarizing Deshpande et al., the authors stress that cloud data storage calls for enhanced security techniques; using observability tools integrated with artificial Intelligence allows for the identification of risks and unauthorized attempts at access ([3]). Best practices use case simulations that illustrate how closely observability tools can monitor data breach scenarios and identify discrepancies in data access patterns. Such simulations not only confirm the effectiveness of observability tools but also help optimize the security settings of an institution to improve the protection of some financial data.

Moreover, particular monitoring solutions, including log monitoring and distributed tracing, can be evaluated through simulations that demonstrate how effective they are in real-time systems. For example, concepts such as log monitoring can be taught via the utilization of simulations to illustrate how observability tools

process system logs for purposes of recognizing adverse activities, which might include multiple failed attempts at login or accessing the system during odd hours. These tools, by making logging more frequent, give a good picture of all the interactions going on from the cloud environment, hence making it easier to detect and prevent any threats. Furthermore, as a use case, distributed tracing can be mimicked to study how data moves across services within the cloud context to identify whether and how vulnerabilities spread across the system and to identify the root cause of an attack quickly.

Another fluorescent method that was studied by Kaaniche et al. is security SLA-based monitoring, which also aims to protect cloud services but in a different manner, as it is based on the particular security metrics and standards that they are to achieve. When implemented in simulations, such security SLAs can facilitate the determination of how well observation tools meet predetermined security assumptions, thus confirming that financial organizations' cloud services respond to security best practices. When performing the simulations, it will be possible to identify areas where observability tools are non-compliant with SLAs, findings that can be used to strengthen the security of the financial systems.

To this effect, the simulation data also prove the real-time capacity of observability tools in regard to security threats. Using attack simulations like DDoS or insider threats, financial institutions can see how their given observability tools perform ([4]). For instance, simulation of a DDoS attack and then analyzing the effectiveness of the observability system and on the setting of abnormally high traffic rates and achieving countermeasures like rate limiting or traffic rerouting. These simulations offer proof that the tools work and can be used to make such organizations refine their security intervention strategies to guarantee that primary defense mechanisms remain strong and effective.

Real-Time Scenarios

Real-life case studies are important for making concepts tangible and showing what cloud-observability does in the financial industry with regard to security and operational continuity. In industries such as finance, where confidentiality is of utmost importance, monitoring and responding to threats in real time is critical. An example of a real-life situation considers the cyber-risk opportunities in cloud technology used in financial services industries, as discussed by Arowolo ([2]). In this case, a financial institution becomes vulnerable to the emerging cyber threat, given that cloud services are used in handling client information, operations, and records. Cloud observability enables the institution to check continuously on the cloud environment and easily identify and alert the system and users on the occurrence of any new unauthorized access attempt, high traffic in data transfer, or any strange login activities. The additional advantage is in the observability of threats as they are developing, so the institution can immediately react and not become a target for a cyberattack that can lead to considerable losses.

Another scene is the utilization of frameworks for cloud security monitoring, as discussed by Le and Hoang ([6]). Here, a financial organization applies the capability maturity model to evaluate and improve cloud security. The framework also includes various observability tools that constantly monitor the institution's cloud resources, allowing the timely identification of any security standard violations and other abnormalities. For example, the organization can monitor system logs and network traffic and look for events that suggest a security threat, such as abnormal data transfer outside networks or changes to system configurations. Such preventive measures are useful not only in preventing and responding to current risks but also in keeping abreast of industry standards, thereby preventing the institution from incurring penalties or damaging its reputation from a regulatory perspective.

Another important use case of cloud observability in finance is security auditing through the application of predictive models. Majumdar et al. mentioned that the aim of using probabilistic dependencies in events with regard to predictive models is to allow for the proactive auditing of security in cloud systems ([8]). In a real-time example, a financial institution applies a set of predictive models within the observability framework to prevent the occurrences of security threats. The observability tools that are used are capable of tracking down records and patterns that relate to previously exposed breaches to forecast the threats in advance and inform the security teams. For instance, if the model identifies that the login attempts resemble patterns of previous phishing attacks, then it sets an alert, and the security personnel can prevent further occurrences due to the early identification of the attacks. It has been noted that this approach not only augments the capacity of the institution to prevent threats but also minimizes the occurrence of successful attacks by diminishing vulnerabilities.

Moreover, cloud observability helps institutions understand the utilization and effectiveness of their applications running on cloud services in real-time, which is indispensable to ensuring the continuous quality of financial services. For instance, if there is an online banking service being provided through a website, and the site receives an eccentric traffic load, then the question of how the system works, for example, in terms of latency or overload, will not be a mystery when you have a great observability strategy and overall understanding of what is going on. The increased focus on the health and reliability of the cloud ensures that financial institutions can provide appropriate and secure services to their clients no matter the situation or the crisis.

Graphs

Table 1: Data Breaches Before and After Observability

Period	Number of Breaches
Before Observability	120
After Observability	45

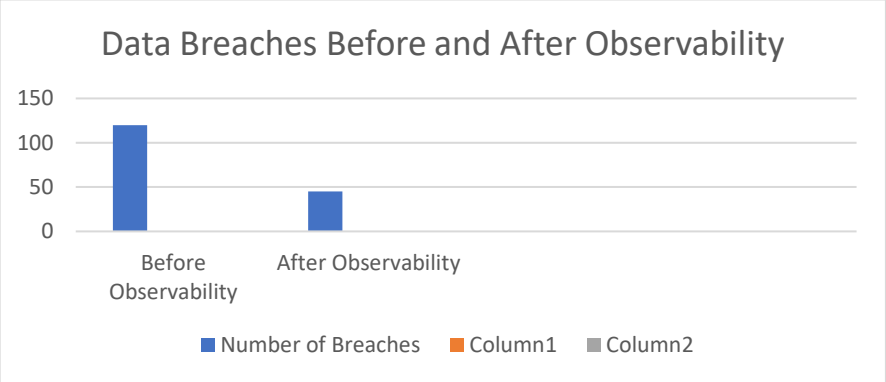

Figure 1: Number of Security Breaches Before and After Using Observability

Table 2: Response Times Before and After Observability

Metric	Without observability (mins)	With observability (mins)
Detection Time	30	10
Response Time	60	20

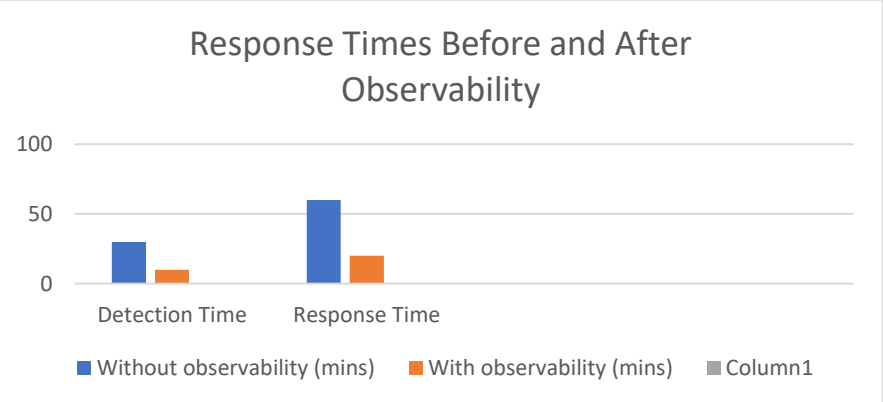

Figure 2: Detection and Response Times Before and After Observability

Table 3: Reputation System Scores with and without Monitoring

Provider	Reputation Score Without Monitoring	Reputation Score With Monitoring
Provider A	3.2	4.5
Provider B	4.0	4.8
Provider C	3.8	4.6

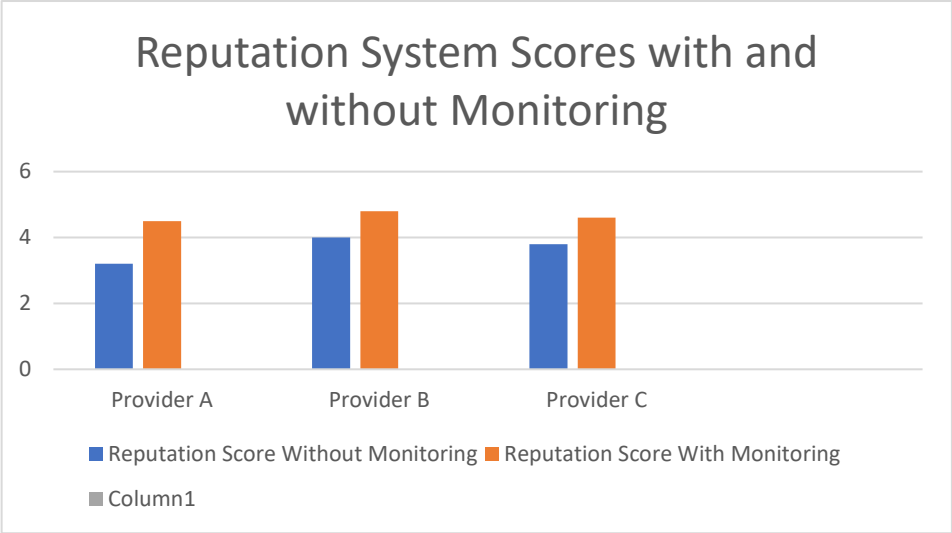

Figure 3: Reputation Scores of Cloud Service Providers Before and After Monitoring

Challenges and Solutions

The following are the main challenges that arise when applying cloud observability in financial services: First, there is an issue of data access since observing and monitoring involve working with data that is often considered private. Financial institutions must also make sure that these tools do not violate the laws of data privacy laws like the GDPR and the PCI DSS that prescribe how data is collected, stored, and accessed ([10]). Also, it becomes an issue to find out if observability data itself can become a source of data breach as it can contain some very important data if not protected. Data privacy within these observability structures needs to have strict methods involving encryption, access, and an audit system to counter any unauthorized access or data leakage.

The other warhead this paper identifies is integration complexity as a key obstacle in cloud observability implementation. Many financial organizations are using multiple clouds or a mix of cloud and on-premises solutions across a vast range of applications and services. When implementing these observability tools across these different platforms, there can be a lot of challenges to achieving single-stack observability ([13]). All the layers of the cloud architecture, starting with legacy and ending with microservices, must be taken into consideration in the context of observability, which may imply a significant amount of effort and costs. Besides, the collected data from various observability tools would not necessarily be highly compatible with each other, and some areas might be left uncovered. To address this challenge, one needs to select observability solutions that are compatible with other platforms and work on integration technologies that connect data from different systems.

Another major issues that come into play when it comes to cloud observability are accountability beyond technology. Thus, although observability tools are the enablers from a technical standpoint for cloud monitoring and protection, the responsibility does not stop at the technical level but has its roots in organizational controls and policy. Financial institutions need to set up tone frameworks to define responsibility to address cloud security, including how data are utilized and responded to with observability `[10]'. Finally, there is also a cultural perspective, which tries to develop a culture of accountability in which security is imperative at every level of the company. This will involve orienting the staff on the issues of observability of security and seeing to it that security measures are upheld and adopted in the running of the institution.

To counter these challenges, one of the most significant recommendations is to implement security SLAs that spell out security standards and measures for cloud services. Security SLAs are more organized in their inputs that define the ways in which security is monitored and enforced with the aim of making cloud providers adhere to the set security standards of the institution ([5]). The fact that observability has been incorporated in the SLAs means that the financial institutions can easily quantify certain aspects of coverage, response times, or data protection measures and compare them to the service-level standards, something that can hold the cloud providers to their word easily. They also allow for the development of a set of common guidelines between the financial institution and the CSP due to the signed SLAs for security.

Another solution to the challenges that come with implementing cloud observability is the use of strategic trust in cloud systems. Pawlick and Zhu elaborate on how trust in this context can be created through the communication process, expectations, and security goals of CSPs and financial institutions that are aligned securely ([11]). By fostering trust-based relationships, it becomes easier for financial institutions to engage their providers and be certain about the observability tools and strategies in relation to their security concerns. Some of the measures in this approach are the implementation of other security frameworks aimed at perpetuating change and improvement, periodic security audits, and shared discussions on new threats and mitigation measures. Strategic trust also has to do with integrating technology such as blockchain to strengthen transparency and accountability of cloud security activities and consequently fortify security in the institution.

Conclusion

Cloud observability greatly improves security in the financial services industry by incorporating complex monitoring tactics that offer real-time monitoring of cloud infrastructures. By making the cloud infrastructure observable, financial institutions can get end-to-end visibility of the cloud environments, hence effectively dealing with security threats. Through the constant gathering of logs, metrics, and trace data, tools for observability enable institutions to detect shortcomings, anticipate possible leaks, and utilize preventive steps to protect compromised financial information ([12]). This approach not only reduces current threats and harm but also leads to better security outcomes by allowing for ongoing growth in monitoring techniques.
The usage of extensive observability tools is vital for banking companies that strive for the reduction of risks and enhancement of compliance with the existing legal requirements. However, as the Financial sector continues to integrate Cloud technology within its operations, the importance of having a proper Observability framework cannot be overemphasized. Observability not only solves the issue of monitoring new complex cloud-based system environments but is also in line with other business objectives, such as keeping customers' trust and optimizing operation costs ([14]). Security has now become a central aspect of software design, and observability is a sure way of improving the existing systems to enable financial institutions to build systems that can withstand the new emerging threats.

References

1. Abouelyazid, M., & Xiang, C. (2019). Architectures for AI Integration in Next-Generation Cloud Infrastructure, Development, Security, and Management. International Journal of Information and Cybersecurity, 3(1), 1-19. https://publications.dlpress.org/index.php/ijic/article/download/92/84
2. Arowolo, O. M. (2017). Strategic Cyber-Risk Implications of Cloud Technology Adoption in the US Financial Services Sector (Doctoral dissertation, Walden University). https: //scholarworks.waldenu.edu /cgi/viewcontent.cgi?article=5450&context=dissertations
3. Deshpande, P. S., Sharma, S. C., & Peddoju, S. K. (2019). Security and Data Storage Aspect in Cloud Computing (Vol. 52). Singapore: Springer.
4. Itani, W., Ghali, C., Kayssi, A., & Chehab, A. (2014). Reputation as a service: A system for ranking service providers in cloud systems. Security, Privacy and Trust in Cloud Systems, 375-406. https: //www.academia.edu/download/47754818/2014-Springer-RaaS.pdf
5. Kaaniche, N., Mohamed, M., Laurent, M., & Ludwig, H. (2017, June). Security SLA-based monitoring in clouds. In 2017 IEEE International Conference on Edge Computing (EDGE) (pp. 90-97). IEEE. https://hal.science/hal-01593433/file/2017-EDGE-Secure_SLA-IBM-Nesrine.pdf
6. Le, N. T., & Hoang, D. B. (2017). Capability maturity model and metrics framework for cyber cloud security. Scalable Computing. https://opus.lib.uts.edu.au/bitstream/10453/121301/1/CSCMM-SCPE-01-5-2017.pdf
7. Lins, S., Teigeler, H., & Sunyaev, A. (2016). Towards a bright future: Enhancing diffusion of continuous cloud service auditing by third parties. https://core.ac.uk/download/pdf/301369683.pdf
8. Majumdar, S., Tabiban, A., Jarraya, Y., Oqaily, M., Alimohammadifar, A., Pourzandi, M., ... & Debbabi, M. (2019). Learning probabilistic dependencies among events for proactive security auditing in clouds. Journal of Computer Security, 27(2), 165-202. https://dl.acm.org/doi/abs/10.3233/JCS-181137

9. Mohammed, F., Ibrahim, O., Nilashi, M., & Alzurqa, E. (2017). Cloud computing adoption model for e-government implementation. Information Development, 33(3), 303-323. https: //www.researchgate.net /profile/Fathey-Mohammed/publication/304370164_Cloud_computing_adoption_model_for_e-government_implementation/links/5ea1b04092851c87d1af0ecf/Cloud-computing-adoption-model-for-e-government-implementation.pdf
10. Mwenya, J. K., & Brown, I. (2019). Cloud privacy and security issues beyond technology: championing the cause of accountability. https://acis2019.io/pdfs/ACIS2019_PaperFIN_073.pdf
11. Pawlick, J., & Zhu, Q. (2017). Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control. IEEE Transactions on Information Forensics and Security, 12(12), 2906-2919. https://ieeexplore.ieee.org/ielaam/10206/8017695/7972976-aam.pdf
12. Saqib, M., Hussain, M. M., Alam, M. S., Beg, M. S., & Sawant, A. (2017). Smart electric vehicle charging through cloud monitoring and management. Technology and Economics of Smart Grids and Sustainable Energy, 2, 1-10. https://www.researchgate.net/profile/Muzakkir-Hussain/publication /320313647 _Smart_Electric_Vehicle_Charging_Through_Cloud_Monitoring_and_Management/links/5ab95fb8aca2722b97d1203a/Smart-Electric-Vehicle-Charging-Through-Cloud-Monitoring-and-Management.pdf
13. Yeluri, R., & Castro-Leon, E. (2014). Building the Infrastructure for Cloud Security: A Solutions View (p. 244). Springer Nature. https://library.oapen.org/bitstream/handle/20.500.12657/28174/1/1001820.pdf
14. Zeng, W., & Koutny, M. (2019). Quantitative analysis of opacity in cloud computing systems. IEEE Transactions on Cloud Computing, 9(3), 1210-1219. https ://dora.dmu.ac.uk /bitstream/handle /2086/18536/Opacity%20in%20CC_TCC.pdf?sequence=1&isAllowed=y
15. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.