Phoenix: International Multidisciplinary Research Journal
Vol 1, No.4, Oct-Dec, 2022
ISSN: 2583-6897

SECURE MULTI-CLOUD ARCHITECTURE PATTERNS FOR HIGH-AVAILABILITY FINANCIAL APPLICATIONS

Nikita Chawla
Email: nikitachawla83@gmail.com
Independent Researcher, USA

Abstract - This study discusses secure multi-cloud architecture patterns, with the intention of providing high availability in financial applications. As financial institutions have been relying more on cloud services, it has become necessary to ensure that these services are resilient, secure, and compliant with regulations. The study assumes an explanatory qualitative and quantitative research design that causes secondary data which is corroborated by authentic literature and UK-based case-studies. It discusses noteworthy and multi-cloud trends, such as, cloud, native design, distributed storage, and cross-cloud orchestration, and replicates their success in overcoming the concentration risk and service outages. The results indicate that even though multi-cloud architectures can offer high levels of both availability and fault-tolerance, they also pose some issues to trust administration, data coherence, governance, and complexity. The research finds that the adoption of effective security measures, robust governance mechanisms and explicit data strategies can ensure a successful implementation of the solution to strike a balance between resilience and performance and compliance in financial settings.

Index Terms- Multi-Cloud Architecture, Financial Applications, orchestration, Recovery Time Objective (RTO), Recovery Point Objective (RPO), cloud resource orchestration, cloud brokerage, inter-clouds, cloud interoperability/portability

I. INTRODUCTION

A. Background of the Study

Multi-cloud refers to more than one public cloud being engaged in the assistance of one or more applications, rather than a single public cloud [1] ***[Refer to Figure 1]***. Single provider dependence can enhance outage and concentration risk because financial institutions are moving critical workloads to the cloud to enhance resilience, speed, and compliance. The patterns of multi-clouds like active deployments, distributed data services, and portable security controls enhance fault tolerance among regions and vendors and satisfy very high requirements in terms of latency, auditability, and data protection. Flexera announced that in 2020, there were 93% multi-cloud strategy enterprises [2]. In the case of banks, high availability architecture shields against payments, trading as well as customer confidence.

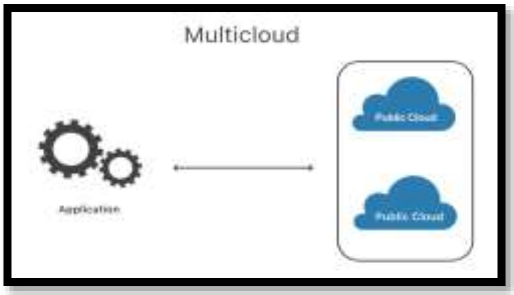

Figure 1: Multi-Cloud
(Source: [1])

B. Overview

This study discusses the secure multi-cloud architecture designs to resources of ensuring high availability in financial applications. It evaluates the concepts of cloud-native design, the approaches to deploying various cloud technologies and services and the strategies used to achieve both resilience and operational continuity. The study measures the advantages, issues, and performance impacts of adopting multi-cloud using secondary data, peer-reviewed literature and case studies of the adoption in the UK. The results emphasise the importance of multi-cloud architecture in enhancing the availability/reducing the concentration risk, with the conclusion that the success of multi-cloud architecture relies on the use of integrated protection and trust management as well as governance to provide reliability and compliance demands of the financial sector [3].

C. Aim and Objectives

The aim is to establish secure multi-cloud architecture patterns that provide high availability to financial applications. Objective 1: To find reference designs of active-standby and geo-distributed designs. Objective 2: To test security measures fulfilling the criteria of identity, encryption, network isolation, monitoring, and incident response. Objective 3: To evaluate major issues, such as data integrity, regulatory adoption, latency, cost, and vendor lock-in. Objective 4: To recommend feasible solutions and a guide to pattern choices to architects. The emphasis is put on production-grade resilience deployments

D. Problem Statement

Financial applications should be accessible when there are cyber-attacks and regional outages as well as operational failures, but most cloud migrations only centralise services to an individual cloud provider or region [3]. This poses a systemic risk, as a failure, misconfiguration, or supply chain will break payments, trading, and access by customers. Concurrently, multi-cloud brings forth intricate security and administrative issues on identity, key custody, data replication, and audit evidence [4]. Thus, there is a need to provide clear patterns of architecture that will provide availability without compromise to the security or compliance of institutions.

E. Scope and Significance

The scope encompasses architecture-level patterns of secure, highly available financial applications that will be implemented in two or more public clouds, which could be interoperable with private cloud or on-premises systems. It puts emphasis on the application layer, the data layer, the identity layer, and the network layer, such as the failover orchestration, encryption, logging, and compliance controls. Exclusively included are a comparison of vendor products and low-level scripting of a product. The importance of having a less concentrated risk, better operational resilience, and a reusable blueprint to facilitate audits, regulatory analyses and business continuity testing is significant.

II. LITERATURE REVIEW

A. Multi-Cloud Architecture Patterns

The patterns of multi-cloud architecture explored in the literature conceptualise the means to deal with heterogeneity, resilience, and control in independent cloud producers instead of just replicating deployments. Arguably, successful multi-cloud patterns are based on orchestration layers that can model, deploy as well and dynamically adjust applications across providers [5]. This opinion resumes architecture as an issue of control, that portability and policy implementation are more important than similarity in infrastructure. On the same note, it is found that there have existed repetitive patterns of architecture like roles of broker-based orchestration, policy-based placement and monitoring feedback loops used to coordinate cross-cloud patterns [6]. More importantly, such trends do not eliminate complexity but recycle it down the hierarchy between infrastructure and governance and automation networks. Moreover, cloud resource orchestration is covered by multi-cloud resource orchestration, cover-up cloud resource orchestration, and partially sharing themes covered by the cloud brokerage, inter-clouds and cloud interoperability/portability [6] ***[Refer to Figure 2]***. In the case of high-availability systems, especially in finance, this change is dramatic: hardware redundancy to obtain resilience has been replaced by software-defined coordination. Nonetheless, the literature advises that in the absence of strict abstraction demarcations, multi-cloud trends may turn imperfectly to close-coupling orchestration systems and cripple the reasonability of flexibility and resiliency.

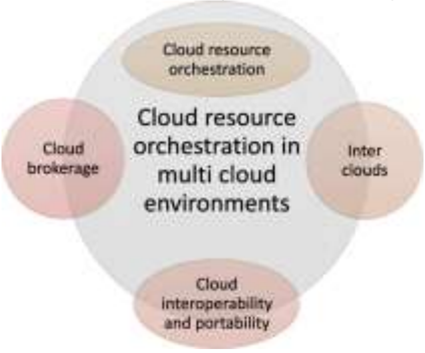
Cloud resource orchestration
Cloud brokerage
Cloud resource orchestration in multi cloud environments
Inter clouds
Cloud interoperability and portability

Figure 2: Cloud resource orchestration in a multi-cloud environment

(Source: [6])

B. Importance of Secure Multi-Cloud Architecture Patterns for High-Availability Financial Applications

The academic literature always reiterates that the adoption of multi clouds without integrated security patterns is likely to enhance, as opposed to mitigating operational risk. It is argued that distributed cloud is bringing challenges to governance and compliance due to the fragmentation of the security responsibilities by geographic units of the law as well as by the service providers [7]. In the case of finance applications, such fragmentation poses a direct threat to the availability since a security breach often results in the shutdown of the service or a regulatory investigation. Writers reinforce this claim by supporting the idea and multi-layered models of security where the identity, encryption, access control, and monitoring are deployed uniformly through cloud boundaries and beyond [8]. In a critical standpoint, however, secure multi-cloud patterns have significance not just in dispelling breaches but also in determining that mechanisms of failover and redundancy are not circumvented by security controls [9]. Financial systems need to be highly available; hence, high availability in financial systems needs to be security-preserving availability. The literature suggests that resilience, where the security is not guaranteed, is merely an illusion because non-compliance with the rules by the regulation or data breach may invalidate the advantages of using multiple clouds in the course of operations.

C. Key Challenges in Multi-Cloud Architecture Patterns

Among the challenges, the literature recognises the data consistency, control of regulation, latency, cost, and vendor lock-in as interconnected challenges and not separate ones. Authors illustrate that consistency models can be diverse in various distributed systems, and multi-cloud replication frequently makes trading-offs between correctness and availability [10]. This is a serious limitation in the case of financial transactions: because the foundations of financial transactions are architectural patterns that undermine consistency, doing so can improve uptime effectiveness but compromise transactional integrity. This is further enhanced by compliance with regulations. Writers demonstrate that multi-cloud environments make auditability and legal responsibility a challenging task to carry out, particularly when data crosses borders [7]. The concepts of latency and cost are inextricably linked as well; researchers state that cross-cloud communication raises the response time and operational costs, thus threatening to burden real-time financial costs [6]. Lastly, the concept of vendor lock-in is no longer removed but creates variations, where the reliance will be between cloud providers and orchestration systems. Multi-cloud challenges are therefore positioned in the literature in terms of a governance issue framed by architectural design.

D. Recommendations to Secure and Strengthen Multi-Cloud Architecture Patterns

Based on the literature, effective recommendations focus on architectural discipline, as opposed to ad-hoc mitigation. Orchestration logic is advocated as a way to implement security and availability controls, as the authors propose that deployment, scaling, and failover activities impose consistent policies [5] [6]. This lessens configuration drift, which produces enormous cloud outages. Other Authors suggest that financial systems must implement differentiated data strategies, where core transactions are highly consistent and replicated, and eventually, consistent layers are provided to read-intensive services [10]. Governance-wise, authors suggest that compliance should be designed as an architectural capability, which comprises standardised controls, logging, and collecting evidence across providers [7]. Also, defence-in-depth techniques are advocated by the authors, where cloud trust is limited [8]. Taken together, the literature implies that the concept of a successful multi-cloud strategy relies on matching the objectives of availability with security, compliance, and data accuracy instead of considering them as conflicting ones.

III. METHODOLOGY

A. Research Design

This study adopts an explanatory research design aiming to expound how the secure multi-cloud architecture patterns can lead to high availability of the financial applications. Explanatory research design concentrates on proving cause-and-effect relationships with the variables, to bring forth temporal causal connections and architectural decisions such as active, active deployment, distributed security controls and failover mechanisms, with the results of resilience in addition to security assurance and continuity [11]. Explanatory research is an appropriate choice since such research will allow performing analysis based on existing literature and real-world demonstrations aimed to explain whether multi-cloud architectures enhance the availability and resolve the issue of risks to financial institutions.

B. Data Collection

The study relies on secondary data collection techniques, which involve both qualitative and quantitative data. Authentic journal articles, regulatory papers and any other open-source industry reports are used to gather the qualitative data with the analysis of architectural patterns, security frameworks, and governance practices [12]. The quantitative data will involve the publicly accessible statistical data of cloud reliability, outage reports, and performance benchmarks that indicate the improvement in the availability and recovery. This combination of secondary methods will provide a broad and balanced viewpoint regarding the idea of cloud security adoption in financial settings.

C. Case Studies and Example

Case Study 1: HSBC UK

In order to improve operational resiliency and minimise concentration risk, HSBC uses a cloud-first plus multi-cloud policy [13]. By spreading workloads and jobs among several cloud providers, the bank enhances access to digital banking services and integrates security and compliance checks.

Case Study 2: Lloyds Banking Group

Lloyds Banking Group makes use of hybrid and multi-cloud architecture in an attempt to modernise old systems [14]. The high availability of customer-facing financial applications during peak times and outages is implemented through automated recovery and redundancy systems.

D. Evaluation Metrics

The research compares patterns of secure multi-cloud architectures based on important metrics: availability and uptime to determine the continuity of services, Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to confirm the effectiveness of failovers, latency to check their user-friendliness and security, and such metrics as audit logging and encryption coverage to analyse financial performance contrasting the benefits of resilience to the extra effort and money spent in financial multi-cloud implementation [15].

IV. RESULTS

A. Data Presentation

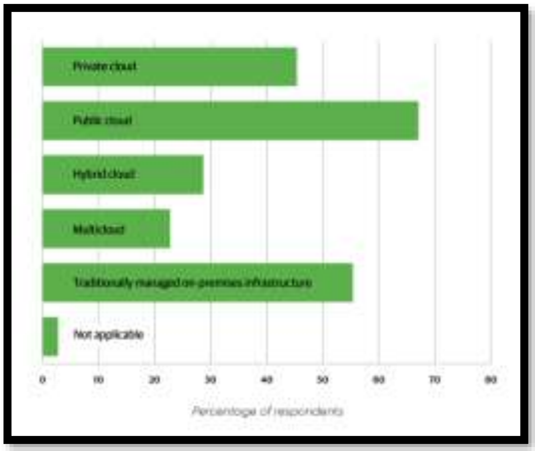

Figure 3: Cloud Technology Usage
(Source: [16])

Figure 3 shows how the use of cloud technology has continued to rise among organisations with more adoption of public, private, and hybrid cloud applications [16]. The statistics suggest that businesses are based more on the cloud infrastructure to facilitate scalability, flexibility and operational resiliency. The tendency is indicative of an increasing trust in cloud services that can be used to host enterprise workloads, and it forms the basis of considering multi-cloud solutions as a way of providing availability and the avoidance of overreliance on any particular providers.

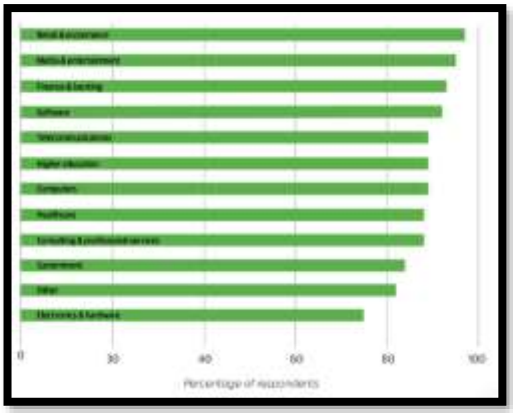

Figure 4: Cloud usage by industry

(Source: [16])

Figure 4 indicates industries where cloud is mostly used, with financial services, technology and retail sectors being the most found to use cloud [16]. Banking institutions are proving to be very dependent on cloud systems to facilitate e-banking, analytics, and real-time solutions. The figure indicates that the sector is relying on cloud infrastructure, which underlines the necessity of providing secure multi-cloud architecture as a solution to address availability and security risks, as well as regulatory risks related to concentrated cloud usage.

B. Findings

The findings suggest that the use of clouds is widespread and industry-dependent, especially in the financial services sector. The increased dependence on cloud technologies builds bigger scalability and innovativeness, but refines operation and concentration risk [16]. The conclusions indicate that the dependency on a single cloud can present financial applications to outages and regulatory problems. In turn, secure multi-cloud architecture patterns become a required approach in enhancing high availability, resilience, and continuity and ensuring security and regulatory compliance in financial settings.

C. Case study outcomes

Case Study	**Strategy**	**Relevance to the Research**	**Key Outcome**
HSBC UK	Adoption of cloud-first and multi-cloud strategy to distribute workloads across providers [13]	Demonstrates how secure multi-cloud architectures reduce concentration risk and support high availability in large-scale financial applications while meeting regulatory and security requirements	Improved system availability, reduced operational risk, and enhanced real-time decision-making across digital banking platforms
Lloyds Banking Group	Use of hybrid and multi-cloud architecture to modernise legacy systems and improve resilience [14]	Illustrates the practical application of multi-cloud patterns to achieve high availability and scalability in customer-facing financial platforms	Greater service reliability, faster recovery from disruptions, and improved customer experience during high transaction volumes

D. Comparative Analysis

Aspect of Literature Review	**Focus**	**Findings**	**Gap**

[17]	Cloud-native application design	The study explains how cloud-native architectures use microservices and containerisation to improve scalability and resilience. These principles support portability across cloud platforms, indirectly enabling multi-cloud availability.	Limited discussion on security controls and regulatory challenges relevant to financial multi-cloud environments.
[18]	High availability and integrity in multi-cloud storage	The authors propose a high-availability and integrity layer that distributes data across multiple clouds to reduce outage and tampering risks. The study strongly supports multi-cloud for resilience and fault tolerance.	Focuses mainly on storage integrity; broader application-level availability and compliance are underexplored.
[19]	Trust management in cross-cloud federation	This survey highlights trust evaluation mechanisms required when services operate across multiple cloud providers. It argues that trust frameworks are essential for secure cross-cloud interoperability.	Does not directly evaluate high-availability performance or financial transaction workloads.
[20]	Blockchain and cloud integration	The paper discusses integrating blockchain with cloud systems to enhance decentralisation, integrity, and trust. These characteristics can strengthen secure multi-cloud architectures for distributed environments.	Latency and cost impacts make the approach challenging for real-time financial applications.

[21]	Challenges of cloud adoption	The study identifies organisational, security, and compliance challenges in cloud adoption. Its findings highlight governance and risk concerns applicable to multi-cloud financial systems.	Focuses on healthcare systems; financial-sector-specific availability requirements are not analysed.
[22]	Cloud-native CRM on hybrid cloud	This work demonstrates how hybrid and cloud-native architectures enhance scalability and service continuity. It supports gradual migration toward multi-cloud strategies.	The analysis is solution-specific and lacks evaluation of cross-provider failover and security.
[23]	Overview of multi-cloud computing	The authors provide a comprehensive overview of multi-cloud models, architectures, and challenges, emphasising availability and vendor lock-in mitigation.	Security implementation details and regulatory compliance are discussed only at a high level.
[24]	Cloud security technologies	This survey reviews encryption, authentication, and intrusion detection techniques used in cloud security. These technologies form the foundation for securing multi-cloud architectures.	High-availability and cross-cloud operational resilience are not explicitly examined.

V. DISCUSSION

A. Interpretation of results

The findings suggest that modularity, portability, and fault tolerance are the key features of cloud-native and multi-cloud architecture that contribute largely to system availability. Containers and microservices offer applications to heal fast after a failure and be cross-platform, which enhances financial system resiliency [17], [22]. Redundancy and distributed storage mechanisms also enhance continuity and data integrity of services of multiple providers, especially in multi-cloud setups [18]. The above rise in cloud dependency in the financial services is also attesting that organisations with multi-cloud strategies are offering cloud dependency as a way of mitigating the danger of vendor concentration and uninterrupted services provision [23].

B. Practical Implications

The results indicated that to realise the full benefits of secure multi-cloud deployment in full, financial institutions needed to incorporate cloud-native principles in system design. When the applications are designed to be portable and scalable by the providers, then high availability can be better accomplished [17]. Cloud interoperability security needs secure evaluation frameworks and standardised access control to avoid security loopholes in inter-cloud activities [19]. Besides, multi-layered security controls like encryption, authentication, and intrusion detection must be installed throughout so that valuable financial information is safeguarded without interfering with the availability [24].

C. Challenges and Limitations

Although these advantages are proven, the adoption of secure multi-cloud structures presents serious challenges. Trusting heterogeneous cloud providers is not as simple and may restrict the smooth interoperability [19]. Data integrity and consistency in a distributed storage environment also add overhead to operation, especially to high-availability systems [18]. Efficient utilisation of multi-cloud strategies is further restricted by organisational and governance issues such as regulatory compliance and lack of skills [21]. One of the major drawbacks of this research is the use of secondary data, as it does not allow one to view proprietary structures and real-time functioning performance.

D. Recommendations

Cloud-native application design must be given priority by financial organisations to offer portability, scalability and resilience between more than one cloud provider [17]. Formal mechanisms of trust management must be part of the multi-cloud implementations to help secure the interactions between providers and minimise security vulnerabilities [19]. Distributed environments must be protected by using the same strategy applied to use security technologies, including encryption and intrusion detection, to ensure that the environments are available [24]. The new technologies, such as blockchain, have the potential to improve integrity and trust in multi-cloud systems, but the effects of using them must be carefully considered [20].

VI. CONCLUSION AND FUTURE WORK

This study summarises that safe multi-cloud architecture designs are crucial towards the attainment of high availability to financial applications in more and more cloud-reliant systems. Multi-cloud strategies help to decrease the concentration risk by sharing workloads and introducing controls on security and governance needs, and expanding regulatory and operational resilience measures. Nevertheless, they can be effective only with a well-thought-out architectural design and strict performance. The annual studies are encouraged to refer to the empirical performance assessments of multi-cost deployments in financial institutions, such as real-time performance assessment of latency and cost. Emerging technologies could be further explored through literature to understand the way of improving adaptive resiliency of multi-cloud financial systems using AI-driven orchestration.

VII. REFERENCE LIST

[1] cloudflare.com 2022. *Multicloud explained | What is multicloud?* Cloudflare.com. Available at: https://www.cloudflare.com/en-in/learning/cloud/what-is-multicloud/ [Accessed on: 15th April 2022].

[2] Itasca 2020. *Flexera Releases 2020 State of the Cloud Report*. www.flexera.com. Available at: https://www.flexera.com/about-us/press-center/flexera-releases-2020-state-of-the-cloud-report. [Accessed on: 15th April 2022]

[3] Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. 2020. *Operational and cyber risks in the financial sector*. Available at: https://www.bis.org/publ/work840.pdf. [Accessed on: 18th April 2022]

[4] Essien, I.A., Cadet, E., Ajayi, J.O., Erigha, E.D. and Obuse, E. 2019. Integrated Governance, Risk, and Compliance Framework for Multi-Cloud Security and Global Regulatory Alignment. *Iconic Research And Engineering Journals*, 3(3), pp.215–224. Available at: https://www.irejournals.com/paper-details/1710218 [Accessed on: 19th April 2022].

[5] Kritikos, K., Zeginis, C., Iranzo, J., Gonzalez, R.S., Seybold, D., Griesinger, F. and Domaschka, J., 2019. Multi-cloud provisioning of business processes. *Journal of Cloud Computing*, *8*(1), p.18.

[6] Tomarchio, O., Calcaterra, D. and Modica, G.D., 2020. Cloud resource orchestration in the multi-cloud landscape: a systematic review of existing frameworks. *Journal of Cloud Computing*, *9*(1), p.49.

[7] Brandis, K., Dzombeta, S., Colomo-Palacios, R. and Stantchev, V., 2019. Governance, risk, and compliance in cloud scenarios. *Applied Sciences*, *9*(2), p.320.

[8] Al-Aqrabi, H. and Hill, R., 2018, June. Dynamic multiparty authentication of data analytics services within cloud environments. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 742-749). IEEE.

[9] Moyou Metcheka, L. and Ndoundam, R., 2020. Distributed data hiding in multi-cloud storage environment. *Journal of Cloud Computing*, *9*(1), p.68.

[10] Mahfoud, Z. and Nouali-Taboudjemat, N., 2019. Consistency in Cloud-based database systems. *Informatica*, *43*(3).

[11] Pawar, N., 2020. Type of research and type research design. *Social Research Methodology*, *8*(1), pp.46-57.

[12] Egerton, T., Diamond, L.E., Buchbinder, R., Bennell, K.L. and Slade, S.C., 2017. A systematic review and evidence synthesis of qualitative studies to identify primary care clinicians' barriers and enablers to the management of osteoarthritis. *Osteoarthritis and cartilage*, *25*(5), pp.625-638.

[13] DIGFIN 2019. *HSBC goes cloud-first*. Digital Finance. Available at: https://www.digfingroup.com/hsbc-cloud/. [Accessed on: 19th April 2022]

[14] Speed, R. 2020. *You can't hold black horse down: Brit bank Lloyds goes full multi-cloud, signs up with Google as well as Microsoft*. Theregister.com. Available at: https://www.theregister.com/2020/03/10/lloyds_multicloud_google_microsoft/ [Accessed on: 20th April 2022].

[15] Andrade, E. and Nogueira, B., 2020. Dependability evaluation of a disaster recovery solution for IoT infrastructures. *The Journal of Supercomputing*, *76*(3), pp.1828-1849.

[16] Loukides, M. 2021. *The Cloud in 2021: Adoption Continues*. O'Reilly Media. Available at: https://www.oreilly.com/radar/the-cloud-in-2021-adoption-continues/. [Accessed on: 24th April 2022]

[17] Gannon, D., Barga, R. and Sundaresan, N., 2017. Cloud-native applications. *IEEE Cloud Computing*, *4*(5), pp.16-21.

[18] Naidu, P.R., Guruprasad, N. and Gowda, V.D., 2021, May. A high-availability and integrity layer for cloud storage, cloud computing security: from single to multi-clouds. In *Journal of Physics: Conference Series* (Vol. 1921, No. 1, p. 012072). IOP Publishing.

[19] Ahmed, U., Raza, I. and Hussain, S.A., 2019. Trust evaluation in cross-cloud federation: Survey and requirement analysis. ACM Computing Surveys (CSUR), 52(1), pp.1-37.

[20] Nguyen, D.C., Pathirana, P.N., Ding, M. and Seneviratne, A., 2020. Integration of blockchain and cloud of things: Architecture, applications and challenges. IEEE Communications surveys & tutorials, 22(4), pp.2521-2549.

[21] Al-Marsy, A., Chaudhary, P. and Rodger, J.A., 2021. A model for examining challenges and opportunities in use of cloud computing for health information systems. Applied System Innovation, 4(1), p.15.

[22] Saxena, I., 2019. Cloud-Native Crm Architecting Salesforce Solutions on A Hybrid Red Hat Infrastructure. environment, 7, p.4.

[23] Hong, J., Dreibholz, T., Schenkel, J.A. and Hu, J.A., 2019, March. An overview of multi-cloud computing. In Workshops of the international conference on advanced information networking and applications (pp. 1055-1068). Cham: Springer International Publishing.

[24] Vindhuja, E. and Umadevi, N., 2020. A Brief Survey on Various Technologies Involved in Cloud Computing Security. Asian Journal of Applied Science and Technology, 4(3), pp.119-128.

[25] Konda, R. End-to-End Observability in API-Driven Architecture using MuleSoft and Prometheus.

[26] Goli, S. R. (2021). SRE in Fintech: Ensuring High Availability and Compliance In Cloud-Based Financial Services. Available at SSRN 5741643.

[27] Chintale, P., Korada, L., Ranjan, P., Malviya, R. K., & Perumal, A. P. (2021). The Impact of Covid-19 on Cloud Service Demand and Pricing in the Fintech Industry. Journal of Harbin Engineering University, 42(7).

[28] Goli, A. K. R. (2021). CLOUD-FIRST STRATEGIES: A COMPARATIVE STUDY OF BUSINESS OUTCOMES IN MULTI-CLOUD VS. HYBRID ENVIRONMENTS. Journal of Critical reviews, 8(1).