World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Cloud-driven modernization of financial systems

Ruthvik Uppaluri *

FP&A Data & Systems, USA.

World Journal of Advanced Research and Reviews, 2025, 26(01), 147-157

Publication history: Received on 14 February 2025; revised on 31 March 2025; accepted on 02 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1030

Abstract

The modernization of financial systems through the adoption of cloud computing has emerged as a transformative force in the financial sector. This paper explores how cloud technologies have reshaped financial institutions' IT infrastructure, focusing on system modernization, disaster recovery, and resilience. With legacy financial systems being constrained by scalability, flexibility, and security issues, the cloud provides a scalable, cost-effective, and dynamic solution for meeting the evolving demands of the financial industry. The research examines the role of cloud computing in facilitating operational efficiency, improving disaster recovery strategies, and enhancing business continuity through real-time data replication, failover capabilities, and high availability. The study also delves into the regulatory challenges and compliance considerations associated with cloud adoption in financial services. Through a comprehensive review of industry reports, case studies, and expert interviews, this paper provides insights into the adoption trends of cloud technologies in the financial sector, along with the potential for future advancements. Ultimately, the research highlights the key benefits and challenges of cloud-driven financial system modernization, offering strategic recommendations for financial institutions looking to leverage cloud solutions for enhanced resilience and innovation.

Keywords: Cloud Computing; Financial System Modernization; Disaster Recovery; Business Resilience; Cloud Adoption; Financial Institutions; Compliance; Regulatory Challenges; Operational Efficiency; High Availability; Data Replication; Cloud Technologies; Financial Services Transformation

1. Introduction

1.1. Overview of Financial Systems Modernization

This paper aims at analyzing the changes that have occurred in the financial industry due to technological innovations and the growth of the financial services industry in particular. The overall modernization of financial systems has the aim of increasing the functionality, security and effectiveness with the minimum cost and within the parameters set out by the regulations. Taken for granted and relying heavily on mainframe systems, financial institutions are gradually migrating to more flexibility and scalability oriented cloud systems.

This modernization includes integrating of several technologies, use of operating systems to enable robotized, in addition to improving on the security aspect of transactions (Zimmerman D. 2014). Cloud computing is credited with having had a central role in such a change because it offers versatile architecture that organizations in the financial sector can easily adapt to depending on the customers' demands. Advanced financial systems in the modern institution improve in managing data, customer satisfaction, and most importantly recognition of market or regulatory shifts.

* Corresponding author: Ruthvik Uppaluri

1.2. Cloud Computing in the Financial Sector: A Paradigm Shift

Cloud computing has produced drastic changes in the feasibility of firms, especially in the financial industry. Instead of handling in house IT resources institutions are employing the services of CSP for hosting and other important applications, data storage and analytical tools (Nigam, V. K., & Bhatia S. 2016). Cloud services provide institutions with on-demand computing resources which not only save resources but also cut on infrastructure overheads, expand adaptability, and efficiency.

With cloud computing, the financial sector now benefits from real-time data processing has become possible and customers benefit from improved experiences and the sector has enhanced its regulatory compliance (Trivedi H. ,2013). Thus, as cloud platforms develop, they are beginning to play a far more significant role in offering new financial products and services.

Another advantage of cloud is the capacity to deliver disaster recovery and business continuity for various financial institutions. Redundancy, automatic backup, and data distribution of cloud platforms allow institutions' data to bounce back from service disruptions and cyber-attacks more gainfully and expeditiously.

1.3. Objectives and Scope of the Research

The purpose of this study is to consider cloud computing as an enabler for enhancing financial systems in the context of disaster recovery (Trivedi, 2013). This paper will discuss the pros and cons of cloud adoption within the financial industry, consider the regulatory issues and investigate the technology enablers of cloud solutions.

Financial services: This research is also a limited review of cloud adoption across the various financial subsectors including banks and insurance companies and fintech firms. It will also evaluate how cloud technologies augment efficiency in service delivery, the business continuity management as well as the procedural compliance management in order to meet ever changing regulatory requirements (Kazmi, Abid, & Iqbal, 2016). Consequently, this paper seeks to undertakes an analysis of different case studies in furthering an understanding of the practicality, relevance, and risks involved in the application of the cloud technology supported financial modernization agenda.

2. Cloud Computing and Its Impact on Financial Systems

2.1. Cloud Computing: Definition, Characteristics, and Models

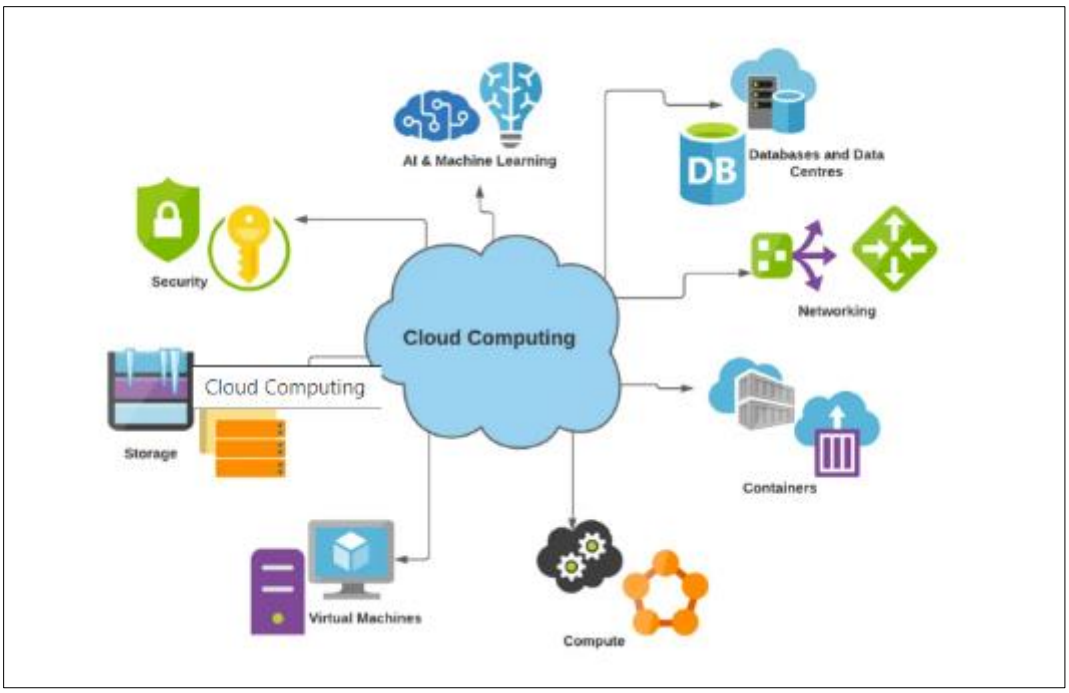

Figure 1 Cloud Computing(ostechnix,2015)

Cloud computing means that rather than having computing resources including servers, storage and software within their own facilities, organizations can obtain these through the internet (Raj, 2012). According to the National Institute of Standards and Technology (NIST), is an abstract model which allows for dynamic provisioning of computing resources for shared IT services with little to no intervention.

Cloud computing is typically categorized into three service models: Division of Cloud Computing – IaaS, PaaS, and SaaS (Turkama, 2015). IaaS pays for the infrastructure used for computing resources while PaaS offers platforms for the computing applications and SaaS provides the users with complete solutions in their applications.

To financial institutions, these models greatly eliminate the need for a huge capital outlay in physical facilities. IaaS, PaaS, and SaaS help the financial services by providing resources, options, and the ability to rapidly create more services.

2.2. The Role of Cloud in Financial System Modernization

Today cloud computing is the major force behind the financial systems' modernization. This enables the financial institutions to shift from preconditioned traditional systems to modern cloud solutions that are efficient, flexible affordable for use (Hayder & Safiniaynaini, 2015). The fact that it is possible to scale resources depending on the need also makes it easier for the banks and other financial services to adapt to ecological conditions prevailing in the market.

Cloud solutions help financial companies pursue digitalization strategies and the deployment of new products and services, enhance internal processes, and better serve customers (Nodehi, 2015). The agility of processing data in real-time ad heightened customer understanding resulting from cloud functionality are crucial necessities of the modern financial institutions. Furthermore, cloud services are in place enabling the open banking policy, which involves sharing of data among banks and the third parties in order to promote innovation.

2.3. Advantages of Cloud Computing for Financial Institutions

The following is an outline of the advantages associated with cloud computing to financial institutions. There is a decrease of operational cost among the benefits accrued by companies having social media presence (Peter, 2015). Instead of investing heavy amounts for setting up the local units, the financial institutions can manage their expenses through cloud services which constitute an expenditure that directly depends on the services that an organization actually uses.

Also, the cloud solutions present high flexibility, allowing for the variation of resource quantities in response to varying needs. It is particularly effective during the periods of push, for instance, during high volatility or many customers (Palmintier, Broderick, Mather, Coddington, et al., 2016). Disaster recovery also benefits from cloud computing because cloud offers the best backup and redundancy tools that keep businesses operational in case disaster strikes the system.

In addition to that, the cloud may foster flexibility in the provision of financial services. They can easily create new applications or modify current systems to suit altering customer needs. Cloud platforms also enhance teamwork, meaning different departments and teams in the financial institutions get access to, as well as work with, the same data seamlessly.

3. Technological Foundations of Cloud-Based Financial Systems

3.1. Cloud Service Models: IaaS, PaaS, and SaaS in Financial Systems

Cloud computing shifts the model for construction, installation and extension of new financial systems at their core. Three primary service models are as follows – IaaS for basic infrastructure needs, PaaS for supporting programmable applications and SaaS for software requirements of clients in the financial sector. IaaS including AWS EC2 and Azure Virtual Machines affords a more flexible, elastic infrastructure to financial institutions but they do not have to manage hardware expenses (DePalo, 2011). PaaS provides developers with environment in which they develop the applications without concerning the infrastructure and this is useful when establishing the financial application with high scalability like risk assessments or trading interfaces. It is important for PaaS solutions to cater to high-velocity deployment and incorporation of financial technologies and products such as Google App Engine. Finally, SaaS delivers fully functional applications, where banking applications commonly for CRM in salesforce or accounting, such as quickbook online, exclude them from the responsibility of software maintenance.

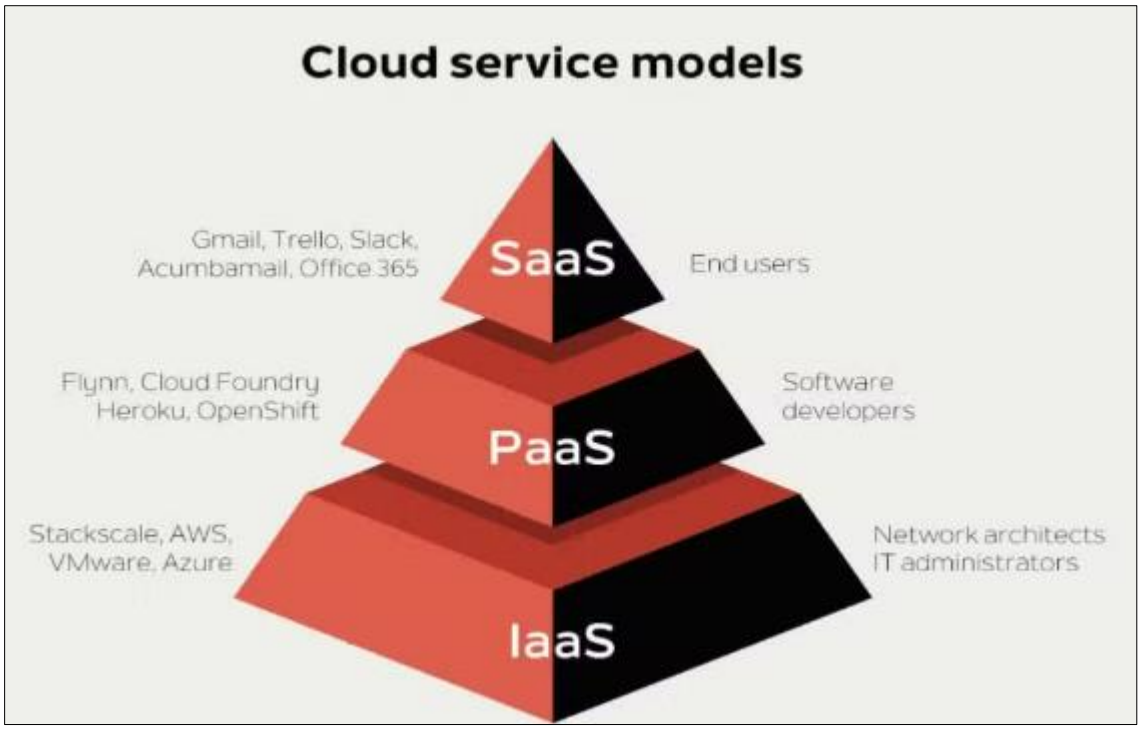

Figure 2 Cloud Service Models(stackscale,2016)

These models provide an option of the degree of control and management financial institutions require enabling them to address their exact technology needs.

3.2. Key Technologies Enabling Cloud-Based Financial Solutions

Flexible and scalable cloud-based solutions utilize several important technologies to improve business capabilities (Parsons, Hummon, Cochran, Stoltenberg, et al., 2014). Microservices, which is an approach of building applications as a large number of small independently deployable services, is critical for allowing for quick updates and differential scaling of components, such as payment or fraud detection.

Also, the use of containers, facilitated by Docker and Kubernetes it helps in the creation of homogeneity in the system hence making it easier for the financial applications to run at scale (Wang, 2016). For real-time transaction processing, approaching such as AWS Lambda or Azure Function that offer serverless computing services enable institutions to process events in a dynamic manner without considering the underlying environment. These make it easier to be more responsive and perform faster with regard to updates and scaling.

4. Disaster Recovery in Cloud Financial Systems

4.1. Defining Disaster Recovery in the Context of Cloud Financial Systems

Disaster recovery (DR) refers to the measures taken to recover financial services and data after a catastrophic event including system crash, corrupted data, hacker attacks, or natural disasters (Endicott-Popovsky, Popovsky, Osterli, et al., 2015). Large investment banks, megafunds and other financial institutions acting on behalf of numerous clients transferring sensitive data and undergoing round-the-clock operations are to develop strict disaster recovery procedures in order to sustain service availability and minimize losses.

With the help of cloud computing, the disaster recovery in the financial sector has flexibly evolved to more affordable and requirements-based DR solutions (Palmintier, Broderick, Mather, Coddington, et al., 2016). The old style backup was expensive in terms of backup data centers and backup hardware and had very little geographical diversity. On the other hand, cloud providers have multi-region solutions that actually sync into different areas so that it is possible to bounce back even if one location has been affected.

4.2. Key Considerations for Financial Systems Disaster Recovery Planning

Before one can understand the importance of disaster recovery planning concerning financial systems, one has to look at these critical success factors. RTO and RPO should first be established. RTO is the time beyond which recovery must be effected and RPO is the amount of data which can be lost due to the disaster (Scholl & AlAwadhi, 2016). Most organizations seek high-value RTO and low RPO, and this may be in the region of minutes, if not seconds, in order to reduce the impact of IT disasters on business transactions and other vital financial services.

Data redundancy and geographic distribution follow as the remaining basic requirements for defending financial systems from localized failures. Cloud providers themselves provide disaster recovery as a service that wings data to other AZs and regions, so that even if one area fails, the data is still present and accessible (Hummon, Cochran, Weekley, Lopez, Zhang, et al., 2014). Furthermore, failure of a primary system requires financial institutions to account for failover systems meant for standby use to replace the primary system.

Last but not the least, testing and certification is required from time to time for Disaster Recovery plan so that system is clear with the procedures which has to be followed in case of actual calamities. Financial institutions should engage their disaster recovery plans in realistic exercises and drills as well as stress tests to evaluate their plans for failing points and compliance with regulatory demands on system availability time.

4.3. Cloud-Based Disaster Recovery Strategies

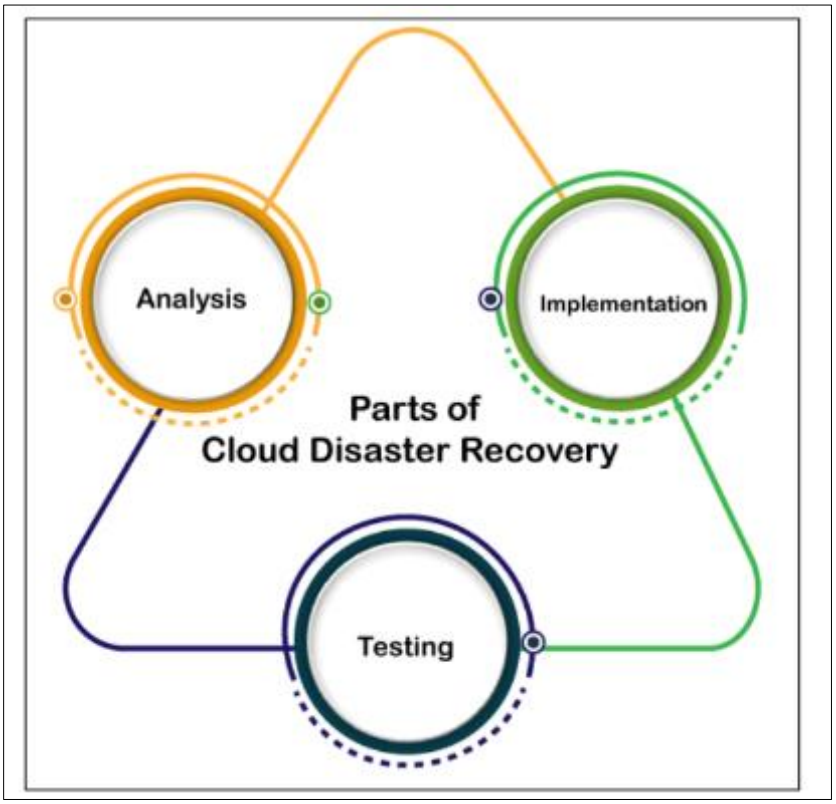

Figure 3 Cloud Disaster Recovery(javatpoint,2016)

Disaster recovery on the cloud is a highly effective solution in comparison with the on-premise disaster recovery technique. The most used model is C2C, cloud-to-cloud recovery in which data is copied and can be recovered among cloud services is used by most financial institutions. As such, institutions can avoid a significant level of capital expenditure regarding maintaining several on-premise, copiable data centers by using the cloud's elasticity on storage and compute (de Sousa, 2015). Disaster can easily reach the data on cloud, and a lot can be recovered and systems can be provisioned to keep the business going.

BaaS, or backup-as-a service model is regarded as one of the most common approaches in the implementation of cloud-based DR. In this model, organizations replicate their important data (for example transaction logs, customer data, and financial reports) online (Williams, 2015). Most cloud prosumers provide automatic backup options with a replication

element integrated into the systems to guarantee the redundancy of data. Also, disaster recovery-as-a-service (DRaaS) enlists protection of complete IT settings to the cloud. In case of failure, all the environment including the applications can be easily recovered which reduces on the downtime.

Multi-cloud disaster recovery is another popular strategy in which the financial institutions avoid getting locked into a single cloud provider by using many of them in case of disaster (Zimmerman, 2014). This is particularly effective in this model because critical financial data and systems are duplicated across at least two cloud providers (for instance, AWS and Azure). This particular copes with the second principle of resilience because it indirectly prevents the failure of some cloud providers to drag critical services.

4.4. Benefits and Limitations of Cloud for Disaster Recovery in Finance

Disaster recovery and business continuity have been well supported by cloud computing in the financial sector. Definitely one of the benefits that can be highly rated is the one that touches on economic benefits; financial institutions do not need to invest in expensive disaster recovery structural facets (Nigam & Bhatia, 2016). Cloud services often come with self-service for backup, copying data for various regions, and rapid service restoration in cases of an outage. This makes it enables the business reduce on the incidences of downtime and thus maintain a continuous flow of business which is very essential for a business, especially in the financial type of business.

Finally, cloud-based disaster recovery solutions are also very elastic; their flexibility increases the ability of organizations to scale. The resources can be flexibly managed as per the requirements of the institutions and the business recovery to catastrophes and other mishaps can be done at a cheaper cost (Trivedi, 2013). Cloud platforms also offer far more versatility; any disaster situated in an area can be modeled to completion on another; in this way, no matter where the catastrophe takes place, recovery is prompt in a corresponding cloud region.

Nevertheless, there are certain disadvantages of disaster recovery residing on the cloud environment. Data security issues are still an issue, especially, because, rather recklessly; financial data is removed and stored off-site (Trivedi, 2013). A risk of cloud computing is thus that institutions must guarantee the cloud providers have strict regulatory policies and regulations on security. Also, reliability of cloud services greatly depends on the performance of the provider, and any problems with provider's services directly ... affect the recovery capabilities.

Table 1 Advantages and Limitations of Cloud-Based DR

Advantages of Cloud-Based DR	**Limitations of Cloud-Based DR**
Cost-effective, no need for secondary data centres	Data security and compliance concerns
Fast recovery times (minutes)	Potential for vendor lock-in
Geographic redundancy for high availability	Requires continuous monitoring and testing
Scalability to handle increasing demand	Complexity in managing multi-cloud environments

5. Resilience in Cloud Financial Systems

5.1. The Concept of Resilience in Financial Systems

IT business continuity and resilience: In financial systems, the resilience is a long term continuity of essential services together with the capability of an institution to rapidly restore services when a disruption, for instance hardware, cyber-attack or an unexpected event occurs (Kazmi, Abid, & Iqbal, 2016). That is why the financial sector is very vulnerable to any disruptions in services because even temporary service unavailability can result in massive financial loss, legal liabilities, and tainted reputation. Hence, it's not sufficient to 'describe' building institutional financial resilience as the inclusion of the ability to avoid disasters; rather, achieving quick recovery and prolonged stoppage of operation needs to be accomplished.

Telecommunication is a perfect storm for building resilience in the field of computing as we know it (Raj, 2012). Such characteristic implementations as distributed architecture, geographic redundancy, and elastic scaling enable the maintenance of operational integrity of financial systems during such strains as extreme situations. AWS and Google Cloud and Microsoft Azure have high fault tolerance limits, and ensure catastrophe resistance, both micro- and macro-failures levels.

5.2. Resiliency Frameworks for Cloud Financial Systems

By using knowledge of and approaches to business continuity risks and disruptions, a robust cloud-based financial system must be configured with preventative and recovery procedures. The proactive approach involves protection and has elements like information duplicate, load splitting and failover (Turkama, 2015). For instance, auto-scaling can enable systems to scale up in the provision of resources each time there is traffic during periods when financial applications are used most, for example, during trading periods. Likewise, distributed databases including Amazon RDS or Google Spanner are created with replication for various zones to contain data in the case of failure of a zone.

The reactive approach operates on the assumption that the goal is to minimize the duration of disruption. It also involves automated recovery solutions like DRaaS that enables institutions backup their entire infrastructure at the cloud and make a switch to the backup systems due to any natural disaster (Hayder & Safiniaynaini, 2015). The incorporation of built-in self-repair technologies that are capable of identifying and solving problems on their own is gaining high significance in the aspect of having fast and, to some extent, independent recovery.

5.3. High Availability and Load Balancing in Cloud-Based Financial Systems

Resilience strategies are organized into four elements, including high availability (HA) which means a system can be primarily intended to open and continuously run. In financial systems, HA makes sure that important services including the execution of any transactions, customer accounts administration and risk assessment are always available (Nodehi, 2015). High Availability is attained to cloud platforms by the Distribution of workloads across availability zones (AZs) and regions. For instance, AWS and Azure mirror data and applications in multiple AZs in a region; this means when one AZ goes down, another AZ can come in to take its place and nobody will know.

Load balancing is considered to be a fundamental aspect of HA. AWS's load balancers called Elastic Load Balancers or Azure Load Balancer helps in a manner that the traffic which is received does not overload one server or instance at a time. This minimizes the problem of congestion as well as the failure of segregating permissions so that financial transactions can be processed at any one time.

6. Challenges and Barriers in Cloud-Driven Financial System Modernization

6.1. Organizational and Cultural Resistance to Cloud Adoption

While cloud computing presents a myriad of opportunities to a firm, financial institutions participate in them, and they encounter a great deal of resistance when implementing the technologies. This resistance usually arises from culture where basic systems and conventional IT environments have been built over the years (Peter, 2015). The target groups of decision makers are company's employees and executives who are used to control and stability on the on-premise solutions, they may be skeptic about the threats of using cloud computing, such as security concerns, data sensitive information and system unreliable factor.

However, for the financial institutions which are carrying a big legacy system, it would be difficult to really see where the key or immense benefits of modernisation would lie. Transition to the cloud involves such changes as redesigning business flows and processes, staff training and overcoming resistance to change (Palmintier, Broderick, Mather, Coddington, et al., 2016). The final factor repeats the first one with the addition of risk perception related to deadlines and stability of specific fields is also an issue – some sectors are extremely sensitive to interruptions in their daily operations, and the idea of implementing cloud solutions puts them at risk of major disruptions.

6.2. Data Security and Privacy Concerns in the Cloud

Two of the biggest challenges regarding to cloud adoption for financial institutions are securing data and personal information. Financial systems deal with very sensitive customers 'information such as PII, financial transactions and other sensitive financial information (DePalo, 2011). Here it is clear that security of data is provided through direct collaboration with the cloud vendor and the financial institution and this may lead to issues regarding the security of the particular cloud vendor.

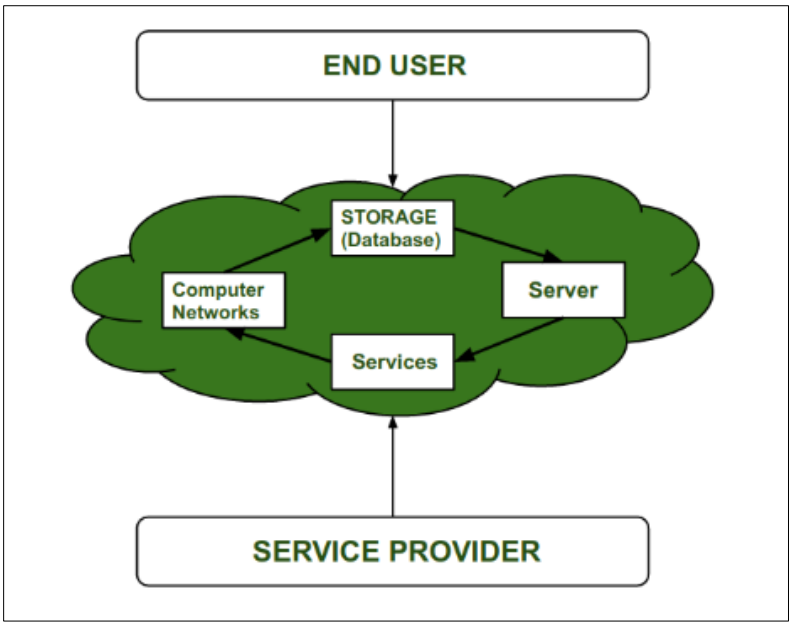

Figure 4 Security Issues(geeksforgeeks,2014)

This is specifically so because these risks affect the clients financial data, financial information that is transmitted over the internet, their financial information in the database, their online financial transactions, their financial data records and other similar incidents that can cause data loss, fraud and other related mishaps (Parsons, Hummon, Cochran, Stoltenberg, et al., 2014). An unauthorized access or leakage in a cloud-computing based financial framework can cost high legally, monetarily and in terms of reputation. Hearing such reassurances from many cloud providers, including end-to-end encryption, using multi-factor authentication, and adherence to industry standards (PCI-DSS, GDPR and others), organizations are still concerned about a loss of sovereignty over their information (National Institutes of Health, n.d.). This challenge mandates that institutions undertake vast scrutiny to the cloud providers, robust scrutinization, obligation of predefined service level agreements that articulate roles and responsibilities regarding security.

6.3. Compliance with Industry Regulations and Standards (e.g., GDPR, PCI-DSS)

The financial industry still remains one of the most heavily regulated markets all across the world, and migration of any services to the cloud levels requires compliance with a vast number of legal and statutory guidelines. GDPR regulation along with MiFID II (Markets in Financial Instruments Directive) and the Basel III regulate policies with specific rules of data retention, analysis and discretion (Wang, 2016). Implementing solutions in the cloud requires compliance with such regulations in order to avoid sanctions as well as to guarantee compliance with the legislation concerning client information.

Adherence to these standards may be tough especially for international and regional financial institutions that have to deal with different regulations in different areas of their operation. Current cloud providers have enactments, certifications, and tools that can be used to tackle these needs, but it is the financial institution which is charged with the responsibility of accomplishing them (Endicott-Popovsky, Popovsky, Osterli, et al., 2015). It further complicates the handling of scalar data within a multisite environment because cloud providers may store data in several global locations. Organizations must therefore verify that their cloud solutions meet relevant compliance requirements including places where data can be stored, how data is encrypted and manners of generating audit trails.

6.4. Integration of Legacy Financial Systems with Cloud Platforms

This is particularly the case with legacy financial systems which are based on technology that may be a decade or more old, are one of the biggest hurdles to cloud-driven modernization. More often than not, these applications are not intended to be compatible with the new cloud platforms, and even when the migration to the cloud is needed, it is normally very costly as it demands the refactoring of several core apps.

While some financial institutions continue to adopt the step-by-step evolution of costly traditional financial systems through the use of hybrid cloud, in which only the peripheral parts of financial services are outsourced to cloud services,

the core is maintained within the firm (Palmintier, Broderick, Mather, Coddington, et al., 2016). It is flexible and practical, but it complicates the administration of both local and cloud networks at the same time. Routinely however, organizations find that the complete transition of mainframe applications to the cloud is essential to fully realize the efficiencies brought by cloud-based transformation, including increased flexibility, affordability, and resilience.

7. Future Trends and Directions in Cloud-Driven Financial System Modernization

7.1. The Evolution of Cloud Technologies

Cloud solutions have been rapidly changing over the last 5 years, with the focus on the concept of edge computing and the integration of AI and machine learning. Current cloud service solutions from cloud providers also include AI analytical and predictive modeling for financially related organizations to use in making their decisions and automating their routine processes (Scholl & AlAwadhi, 2016). Another related development has also occurred: multi-cloud adoption, primarily to avoid dependency on one provider and gain greater agility through the use of services from multiple cloud providers.

7.2. AI, Machine Learning, and Cloud in Financial System Innovation

The financial services are now at a faster rate adopting AI and machine learning from the cloud platforms. Cloud computing for example enables financial institutions to develop and deploy fraud detection systems and risk management models for analysis of big data sets besides supporting development and delivery of customer tailored solutions (Hummon, Cochran, Weekley, Lopez, Zhang, et al., 2014). Such AI applications are empowering the trading systems, improving models of credit scoring and providing better instruments for predictive analysis.

7.3. The Future of Disaster Recovery and Resilience in Cloud Financial Systems

Thus, disaster recovery and business resilience will change as financial institutions remain to embrace cloud technologies. There will be a transition to less manual recovery tools based on AI and real-time data replication between the geographically dispersed regions of the cloud (de Sousa, 2015). The future may likely provide a need for more predictive analytics and deeper integration of autonomic cloud systems that can adapt and self-correct from threats, and lessen the potential time that a business must go offline.

8. Conclusion

8.1. Key Findings and Insights from the Research

The trends of applying cloud solutions for financial organizations' modernization offers the financial sector many benefits in terms of increasing the efficiency, security, and flexibility of their operations. While engaging in this research, it has been realized that the use of cloud computing is beneficial in these financial institutions. They include: flexibility, reduced cost, data processing in real-time, and dynamic resource utilization. Moreover, disaster recover processes are enhanced on the clouds platforms, making systems more reliable, this helps organizations to continue functioning even in case of an unfortunate incident.

But moving to the cloud doesn't come without its problems. Cultural resistance, information security, regulatory compliance factors, and mainframe integration into cloud are the major challenges faced by the financial institutions. These considerations are frequently made challenging for the adoption of cloud and can therefore result in the slowing down of cloud driven modernization benefits.

The regulatory environment also has a major influence on the plans that the financial sector has for – cloud computing adoption. The growing number of compliance regulations and the consequences of non-compliance with them also dictate relying on a detailed, informed choice of cloud providers. Complacency with legal standards like GDPR, PCI-DSS, or regulating standards most industries have must not be taken since they attract monetary and reputational penalties.

8.2. The Impact of Cloud Modernization on Financial Sector Resilience

Cloud modernization has evidently influenced the recoverability of financial institutions. Therefore, communication between financial and non-financial benefits of leveraging on cloud-based disaster recovery and high availability architectures when aligned with progressive IT structures can be prevented. Multicontext redundancy makes the cloud architectures guarantee backup, security, and availability of data, and means that failures and disruptions can be overcome quickly.

Also, systems can be scaled on-demand, which also improved the access to numerous tools and services in the cloud making the sector even more flexible. This is important as there is growth in uncertainties and financial complexities, which gives the financial institutions the ability to respond to change and incident in the market. The use of multi-Cloud and hybrid Cloud has also helped nay institutions enhance the aspect of resilience as capacities and risks are spread over and across many Clouds to avoid cases of full system failure.

8.3. Strategic Recommendations for Financial Institutions

Based on the findings from this study, the following tactical suggestions can be drawn out for banks signaling a change towards a cloud computing future.

First, financial organizations must recognize that the most important element is to strengthen the formation of cloud strategies. This involves managing expectation, identifying and communicating KPIs and readiness for how the whole affair will affect business processes in the future. It is desirable to conduct a gradual migration, continuously adapting the company's interactions with cloud-based technologies, to avoid disruption of work processes during the change.

Second, institutions should ensure that they dedicate resources to provide people with proper training that practices makes them capable of managing and running their business in a cloud environment. This is even more crucial now since cloud technologies are rapidly growing and staff has to be informed on the latest trends regarding security, compliancy as well as management.

Third, specific attention should be paid to a choice of the cloud providers with high security and compliance standards. Financial institutions should be very selective through conducting adequate research on the solutions provided by their providers with a view of being convinced that offered solutions are standard and correspond to the existing legislation. SLAs should be set and agreed to, to clearly define expectations of the services providing availability, security and backup recovery.

Finally, there is a strong case for financial institutions to investigate the use of AI, machine learning and blockchain to the extension of their cloud solutions. These innovations can enhance capability and capacity and foster better decision making and possibilities for new offerings that meet new customer needs.

8.4. Limitations and Areas for Future Research

Despite these insights, this research has some limitations with regards to its view on the modernization of financial systems by the use of clouds. This is a common problem in research where riders are swift, and some of the trends as well as the technologies that have been featured in the paper might quickly change in development due to the dynamicity of the advance in the technologies and trends. In addition, the effects of particular cloud implementation approaches on financial system transformation was likely to significantly differ between institutions within the sample depending on factors such as the size, geographical location and market niche.

This research could be taken further to examine specific cloud security models and their practice and effectiveness within the sphere of the financial industry paying attention to the level of compliance to international legislation. Further, new analysis of case studies of large scale cloud migration could help the financial institutions understand certain new factors which they need to consider during their large scale cloud migration. Further research into how quantum computing and 5G networks will impact the cloud financial industry and its future also needs to be done.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Zimmerman, D. (2014). Five cloud essentials for the boardroom: What banking and financial markets executives need to know about cloud computing. Journal of Payments Strategy & Systems, 8(2), 135–142.

[2] Nigam, V. K., & Bhatia, S. (2016). Impact of cloud computing on health care. International Research Journal of Engineering and Technology, 3(6), 1351–1355.

[3] Trivedi, H. (2013). Cloud computing adoption model for governments and large enterprises (Unpublished MSc thesis). Massachusetts Institute of Technology.

[4] Trivedi, H. (2013). Cloud adoption model for governments and large enterprises (Unpublished MSc thesis). Massachusetts Institute of Technology.

[5] Kazmi, S. H. A., Abid, M. M., & Iqbal, M. (2016). Impact of cloud services on economic growth. In Proceedings of the IEEE International Conference on Cloud Computing and Intelligence Systems (pp. 220–225). IEEE.

[6] Raj, P. (2012). Cloud enterprise architecture. Wiley.

[7] Turkama, P. (2015). Building inclusive digital societies through the use of open source technologies. EPH-International Journal of Business & Management, 2(1), 45–52.

[8] Hayder, R., & Safiniaynaini, T. (2015). Software as a product versus software as a service. Göteborg University, 5(2), 83–91.

[9] Nodehi, T. (2015). A new MDA-SOA based framework for Intercloud interoperability. ProQuest Dissertations and Theses, 1(1), 101–107.

[10] Peter, K. Y. (2015). Towards the seamless global distribution of cloud content. In Privacy and Legal Issues in Cloud Computing (pp. 145–160). Edward Elgar Publishing.

[11] Palmintier, B., Broderick, R. J., Mather, B., Coddington, M., & others. (2016). On the path to sunshot: Emerging issues and challenges in integrating solar with the distribution system. U.S. Department of Energy, Office of Scientific and Technical Information.

[12] DePalo, M. (2011). Cloud computing—Legal issues in the US & international implications. Georgia State University Reading Room. https://readingroom.law.gsu.edu/

[13] Parsons, B., Hummon, M., Cochran, J., Stoltenberg, B., & others. (2014). Variability of power from large-scale solar photovoltaic scenarios in the state of Gujarat. U.S. Department of Energy, Office of Scientific and Technical Information.

[14] Wang, Z. (2016). Synergetic junction of interregional transit in Shanghai 2030. OhioLINK Electronic Theses and Dissertations Center. https://rave.ohiolink.edu/

[15] Endicott-Popovsky, B., Popovsky, V., Osterli, P., & others. (2015). Conceptual foundation for UW Center of Academic Excellence in Information Assurance Education. CISSE Conference Proceedings.

[16] Palmintier, B., Broderick, R. J., Mather, B., Coddington, M., & others. (2016). On the path to sunshot: Emerging issues and challenges with integrating high levels of solar into the distribution system. U.S. Department of Energy, Office of Scientific and Technical Information.

[17] Scholl, H. J., & AlAwadhi, S. (2016). Smart governance as key to multi-jurisdictional smart city initiatives: The case of the eCityGov Alliance. Social Science Information, 55(1), 41–64. https://journals.sagepub.com/

[18] Hummon, M., Cochran, J., Weekley, A., Lopez, A., Zhang, J., & others. (2014). Variability of photovoltaic power in the state of Gujarat using high resolution solar data. U.S. Department of Energy, Office of Scientific and Technical Information.

[19] de Sousa, M. I. S. (2015). Ericsson: TV is a new game: Diversification strategy for TV & media business. ProQuest Dissertations and Theses. https://search.proquest.com/

[20] Williams, B. G. (2015). Inferno in Chechnya: The Russian-Chechen wars, the Al Qaeda myth, and the Boston Marathon bombings. Potomac Books.