

A Cloud Computing Adoption Challenges in Financial Institution

Nor Elsa Furzanne Mohd Kamil¹, Ganthan Narayana Samy¹, Sundresan Perumal², Pritheega Magalingam¹, Noor Hafizah Hassan¹ and Sivananthan Perumal³

¹*Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, 54100, Malaysia*

²*Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai, 71800, Malaysia*

³*Faculty Accountancy Finance and Business, Tunku Abdul Rahman University College, Kampar, Perak, 31900, Malaysia*

ganthan.kl@utm.my

Abstract. Cloud based technology is constantly on the rise due to its dynamic characteristic. Especially during pandemic, the organizations have invested so much in cloud infrastructure. Moving business strategy to cloud leads to unknown threats and vulnerabilities. These threats are intertwined with the fact that businesses committed to adopt cloud technology without understanding the risks. The absence of consistency has a substantial impact on how financial institutions should execute risk assessment framework based on cloud computing environment. Thus, there is a need for a comprehensive risk assessment framework for highly regulated industries such as financial institutions, which more prone to threats due to these industries hold valuable customers' data that may bring financial gains to the attackers. Therefore, the objective of this paper is to identify and discuss about the existing cloud computing adoption challenges in financial institution to help financial institutions in assessing the risks that they face for adopting cloud computing applications. Moreover, the studies revealed that there are various cloud computing adoption challenges faced by financial institutions include a number of security issues such as breaching sensitive data, tampering with integrity of the data, the issues with ownership of the data, data recovery and loss and involves other legal issues such as regulatory and compliance. In summary, the identified adoption challenges will be used as an element for risk assessment framework for cloud computing applications in financial institutions.

Keywords: Cloud Computing, Financial Institution, Information Security, Risk Assessment Framework

INTRODUCTION

Cloud computing became widely accepted in 2007 as a result of the rapid growth of communication networks and an increase in the geometric evolution of business and the growth of users' demand to extend their information systems [1]. Moreover, the evolution of cloud computing becomes more and more crucial in the when the world was hit by COVID- 19 pandemic. As a precautionary measure to limit the spread of the virus, the majority of businesses have told their workers to operate from home [2]. Furthermore, COVID- 19's rapid spread has increased the amount of data obtained from various sources. Employees who work from home rely heavily on cloud computing tools to complete their tasks rapidly and efficiently. Information Technology (IT) governance organizations saw a thirteen percent decline in on- premises workload post pandemic and five percent increase of workloads stored in cloud infrastructure [3].

While cloud computing technology is gaining traction across a wide range of banking services, there are significant challenges that must be overcome as financial institutions move to cloud computing environment. For example, the confidentiality and protection of commercial and personal information data, as well as high- critical applications, must be prioritised. Financial institutions cannot afford to take the chance of a security breach. Safety remains a major roadblock to cloud adoption, despite market demands to cut costs and reassuring commitments from cloud computing technology providers [4]. Therefore, the objective of this paper is to identify and discuss about the existing cloud computing adoption challenges in financial institution.

LITERATURE REVIEW

Basically, this section will discuss important literature related in this research.

Cloud Computing

Cloud computing is defined as a model for enabling easy, on- demand network access to a configurable computing resource namely servers' resources, network services used in cloud, storages, web applications, and web services that can be immediately provisioned and distributed with little management effort from service provider involvement [5]. Basically, there are three types of cloud computing deployment model namely, Software as a Service (SAAS), Platform as a service (PAAS), and Infrastructure as a Service (IAAS).

Financial Institutions

A financial institution (FI) can be defined as a company that deals with monetary or financial transactions such as cash deposits, lending credit, investment funds, and currency exchange. An FI can be anything from a marketing insurance company to a credit union, banks, a trust company, a finance company, or an investment dealer. There are few types of entities that can be considered as FI which discussed below [6].

Commercial Banks

A commercial bank is a type of financial institution that handles cash deposits, provides regular bank services to individual customers and small businesses, provides corporate business setup, offers mortgage, personal lending, and savings accounts. Unlike an investment bank, most people conduct their banking at a commercial bank. Commercial banks also provide credit cards, wire transfers, and currency exchange services.

Investment Banks

Investment banks specialise in offering specific services to accommodate company daily operations, such as providing Initial Public Offering (IPOs) to the larger corporations, offers financing capital expenditure and equity. Investment banks provide brokerage services for their investors, act as middleman in to manage mergers and acquisition, negotiating stock exchanges, and other corporate reorganization.

Islamic Banking

Islamic banking is a shariah compliant Islamic finance that refers to Islamic law. The sharing of profit- loss margin and the prohibition of riba', excessive rate when the assets are exchanged with another assets. Islamic banking has different types of products such as Ijara, Mudarabah, Musyarakah, Murabahah, and Wadiah. All of these products are catered to the modern Islamic financial institutions.

Insurance Companies

Insurance companies provides insurance, for specific target persons or for large corporations. Asset management and financial risk protection, provided in insurance services, is a critical asset that allows individuals and businesses to make investments that accelerate economic growth.

Brokerage Firms

Mutual funds and exchange- traded funds are available through brokerage firms. Brokerage firms are experts in dealing with wealth management and financial advice. These firms include the services by providing the investors with access to a wider range of investment options, from stocks and bonds to a relatively another alternative services investment such as hedge funds and private equity.

CLOUD COMPUTING ADOPTION CHALLENGES IN FINANCIAL INSTITUTION

Although there are many benefits of cloud computing adoption, there are indeed quite a number of challenges to this adoption. Thus, section will discuss cloud computing adoption challenges or barriers in financial institution.

Data Security Issues

One of the most significant challenges is data security. Data security in this context include issues regarding cyber risk, regulations, data privacy and legal matters [7, 8]. Cloud computing is a relatively new technology computing model, thus, there is a huge problem of the risk's unknown about security of cloud migration at all layers including the network, applications, host, containers and data can be achieved and how applications security is moved to cloud computing. Because of these unknown risks, information executives have consistently stated that security is their top priority when it comes to cloud computing.

Moreover, the characteristic and cloud computing model as a multitenancy system architecture, it gives way an attacker attacking the server computer which can cause concentrated harm, spreading through the technologies based on the cloud distributed systems [9]. The type and severity of the security risks in the cloud may vary from those in traditional IT infrastructure. Through multi-tenancy and virtualization technologies, resource pooling allows multiple users to share the same pool. While the technologies allow rapid elasticity and efficient resource management, the cloud computing technology also open doors to threats and risks into the system [9].

Data Security Law and Regulations Barriers

Other barriers to adopt cloud computing in financial institutions surrounding the law and regulations. Lack of standardization between country's regulation and industry standard lead to discrepancy and confusion in adopting cloud computing. Often, the pre-existing law do not weight in the technology of cloud computing model. Country's national regulatory authorities often demand that data to be held by domestic entities be stored only on servers in that country, and that data access be limited only for that country. Auditors or regulators frequently disagree with information technology security experts in terms of level of protection of cloud services with regulators being more credible on advising of cloud services than information security professionals [10]. Furthermore, internal auditors are rarely tasked with reviewing cloud protection, exacerbating issues and causing uncertainty due to a lack of oversight [11].

Lack of Standardization

Due to cloud infrastructure is usually provided by cloud service provider, a single cloud provider company can hold a huge number of companies' data, it becomes a single point of failure. Even if this cloud provider has numerous data centers throughout the world, the potential of it failing makes it a single point of failure [12]. The best way to avoid this is for clients to seek cloud services from a variety of providers. Using numerous providers in today's cloud, however, poses a data portability difficulty, given that Application Programming Interface (APIs) from multiple providers are still not fully standardized.

Huge Switching Costs

Given that a number of the applications that are planned to be migrated into the cloud and build on a said environment are essential to businesses, it is essential to address common security risks associated with such environments. The implications of not addressing such security risks especially in cloud applications could be of varying nature in the extreme cases banks could lead to reputational damage, loss of operating license and major revenue impact [13].

Latency Problem

Basically, when transferring data to and from the cloud, the latency is higher than when moving data to and from an on-premises data center. Latency is becoming a major concern as applications become more data hungry. Nonetheless, [14] indicates that a viable solution could be found by combining different geographically dispersed data sets. Concerns over security and enforcement are among the top obstacles to cloud computing adoption, as well as barriers to cloud services adoption accessed through the Internet [15]. Many companies are still underprepared for these threats, and if these threats are not addressed, it might expose the vulnerability that the cloud providers and consumers to regulatory violations and data breaches [11].

Network Issues

Another issues of security problem are focused on the operation and implementation of cloud computing models, as well as network issues. In fact, the cloud's network structure is prone to attacks and security threat such as malware injection, browser security issues, flooding attacks, lock-ins, incomplete data deletion, data encryption, and XML signature element wrapping, to name a few. According to [16] has put forward the most suitable categorization to summarize in regard to cloud computing issues classification appropriately.

CONCLUSION

Basically, this study also extends its benefit to the regulatory governing bodies such as Bank Negara Malaysia (BNM), Hong Kong Monetary Authority (HKMA), United Kingdom Prudential Regulations (UK PRA) and Money Authority Singapore (MAS) as a contribution and as an initiative to expand the knowledge bases and capacity in cloud computing adoption. Furthermore, this research will guide on what should be emphasized by management and employees to improve the cloud computing adoption in financial institutions. The findings in this paper contribute to our understanding of the interaction between cloud computing dynamics and the risks in financial institutions. Moreover, the findings from this research also suggests that there are new risk components that are recently discovered when the cloud computing model is integrated with highly regulated environments such as in financial institutions.

REFERENCES

1. Ovidiu Versemen & Peter Friess. (2014). Internet of Things Applications-From Research and Innovation to Market Deployment. River Publishers.
2. Ziyad R. Alashhab, Mohammed Anbar, Manmeet Mahinderjit Singh, Yu-Beng Leau, Zaher Ali Al-Sai, Sami Abu Alhayja'a,. (2021) Impact of coronavirus pandemic crisis on technologies and cloud computing applications, J. Electronic Science and Technology. 19, 1-12.
3. Justina Alexandra Sava. (2022.) Pre & post COVID-19 IT workload location. Retrieved 21 February, 2022 from <https://www.statista.com/statistics/1140721/workloads-preand-post-covid-cloud/>
4. Balanagalakshmi, B & Sujeevan Kumar Bullard (2020). Cloud Computing Technology-Security Issues In Banks-An Overview, European J. of Molecular & Clinical Medicine. 2, 5299-5304.
5. Hogan, M., Liu, F., Sokol, A. and Jin, T. (2011), NIST-SP 500-291, NIST Cloud Computing Standards Roadmap, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD.
6. Smith, Tim. (2019). Disruptive Technology. Retrieved 14 February 2020, from <https://www.investopedia.com/terms/d/disruptive-technology.asp>
7. Mahalle, A, J. Yong, J, Tao, X & Shen, J. (2018). Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure. 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD), 407-413.
8. KPMG. (2020). Key cyber risks for banks during COVID 19: Cyber and anti-fraud controls are paramount for banks during COVID-19 and beyond. Retrieved 10 March 2022, from <https://home.kpmg/lu/en/home/insights/2020/06/key-cyber-risks-for-banksduring-covid-19.html>
9. S. Alatawi, S, Alhasani, S, Alfaidi, S, Albalawi, M & Almutairi, S.M. (2020). A Survey on Cloud Security Issues and Solution. 2020 International Conference on Computing and Information Technology (ICCIT), 1-5.
10. ISACA. (2009). Business Benefits with Security, Governance and Assurance Perspectives. Retrieved 20 February 2022, from <http://www.isaca.org/KnowledgeCenter/Research/Documents/Cloud-Computing-28Oct09-Research.pdf>.
11. Matthew McGee. (2013). University of Maryland Francis King Carey School of Law. Retrieved 12 January 2022, from <https://www.linkedin.com/in/matthew-mcgee7a8901100>.
12. Federal Aviation Administration. (2009). Risk Management Handbook, Retrieved 3rd Dec. 3, 2011 from <http://www.faa.gov/library/manuals/aviation/media/FAA-H-80832.pdf>
13. Cloud Security Alliance. (2019). Cloud Security Alliance's Top Threats to Cloud Computing: Pandemic 11 Report Finds Traditional Cloud Security Issues Becoming Less Concernin. Retrieved 20 April 2022 from

- <https://cloudsecurityalliance.org/pressreleases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computingpandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/>
14. Parekh, D. H., & Sridaran, R. (2013). An Analysis of Security Challenges in Cloud Computing. *Int. J. of Advanced Computer Science and Applications (IJACSA)*. 1, 3846.
 15. North Bridge Venture Partners. (2012) Future of Cloud Computing Survey Exposes Hottest Trends in Cloud Adoption. Retrieved 23 March 2022 from <https://vmblog.com/archive/2012/06/21/2012-future-of-cloud-computing-surveyexposes-hottest-trends-in-cloud-adoption.aspx#.YyYDmnZBzIU>
 16. Tabrizchi, H., Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *J. Supercomput.* 76, 9493–9532.