FINANCIAL DATA SECURITY IN CLOUD COMPUTING

NAVEEN KUNNATHUVALAPPIL HARIHARAN

Sr. Hyperion SME & Department of Information Technology, United States

January 2021

ABSTRACT

KEYWORDS:

Cloud Computing, Cloud Security Financial sector,

Many enterprises have achieved a novel, quick, and low-cost technology to address the concerns of data storage and availability for customers, which is referred to as Cloud Computing. More and more financial service companies and organizations have shifted their offline services to cloud platforms to provide customers with more convenient and accurate services. Working with a cloud services provider offers a wide variety of benefits for banks and financial institutions. This includes greater flexibility and scalability, lower costs, and improved organizational efficiency. However, at the moment, they pose a certain level of data security risk to financial organizations. For financial institutions, keeping data secure is of the utmost importance. Financial information is extremely sensitive, making it valuable and especially vulnerable. The cloud service providers are making significant efforts to develop the cloud industry in order to maintain optimal security. After discussing cloud computing in the financial sector, this research outlined six major security concerns that financial institutions face in cloud computing. They are Information security Business security System Security Host Security Data Security Network Security. We also discussed the major strategies by cloud computing providers to tackle these issues. Once the security challenges can be resolved properly, cloud computing will be further promoted in the finance sector. Financial institutions may leverage cloud computing in the future to develop novel business models and provide customers with an entirely new experience with financial services.

*Copyright © 2021 International Journals of
Multidisciplinary Research Academy. All rights reserved.*

INTRODUCTION

In the present world, data has become an essential part of our daily life. Every day, people deal with a large amount of data as a result of their personal or professional activities. All

of this data requires a significant amount of storage space, as well as consistency in its accessibility around the clock across the numerous devices that users frequently utilize and connect to complete their tasks. However, physical storage space is limited due to the cost.

Many firms have developed a novel, quick, and low-cost solution to address the concerns of data storage and availability for customers, which is recognized around the world as Cloud Computing. Many businesses in the United States have been employing cloud technology to share resources on-demand since the early 2000s (Qian et al. 2009). This technology has begun to acquire traction around the world in the last few years. People must have internet access as well as the cloud domain of the company whose services they wish to employ to keep their data.

It has been predicted that in the coming years, the use of cloud computing services will keep a stable growth rate. For example, more and more financial service companies and organizations, like financial institutions, non-state-owned third-party funds and loan platforms, tax and revenue administration channels have shifted their offline services to cloud platforms to provide customers with more convenient and accurate services (Gill and Cma 2011).

As a result of this emerging trend regarding the usage of cloud-based services, the security issues related to cloud computing have become a massive challenge. The government and the private companies are making a significant joint effort to develop the cloud industry, and they are coming up with plans and policies that are encouraging technological innovations in this field to their maximum. They are also attempting to provide a secure and better service environment. Companies are trying their best to give all kinds of reliable services and ways to prevent and cope with the issues.

However, the most significant challenge for most of the organization is the constant increase in the number of online security threats and the rise in their complexity. The whole process of monitoring and securing a system in an organization becomes complicated because of the widespread use of various devices and platforms by employees to connect to the online world (Amara, Zhiqui, and Ali 2017). Cybercriminals, on the other hand, are also becoming very professional and smarter by using more sophisticated and sometimes readily available online tools to execute attacks. This creates a massive gap between the overall security of an enterprise and the level of potential cyber threats. In addition to the security of cyberspace, the security of the physical space is also paramount. In the last few years, insider threat has become one of the top reasons for an organization to face a massive security breach. Anyone in an organization can become the cause of the breach of data and security by helping the cyber criminals either intentionally or unintentionally (Sabahi 2011).

Cloud computing in the financial sector

Cloud computing has established itself as a component of the next phase of IT transformation in the financial sector as computing technology has advanced and business models have evolved (Oredo, Njihia, and Iraki 2017). With the advent of cloud computing, different industries have embraced its uses, and the financial sector is no exception. At present, more and more financial institutions have begun to consider migrating their traditional IT infrastructures to cloud computing solutions. For financial institutions, cloud computing solutions have made the maintenance and use of information system infrastructures to the greatest degree of simplification (Do and Kim 2018).

Cost savings

When cloud computing is adopted, financial institutions do not need to purchase additional data centers. Through cloud computing solutions, financial institutions don't have to buy any servers, storage devices, and network equipment, and all software, hardware, and technical issues are delivered to a cloud computing service provider. Financial institutions are able to get the most advanced technology applications without being equipped with professional technicians in IT; Financial institutions do not require specialized maintenance and management workers and do not incur additional costs in recruiting such personnel (Nicoletti 2013). By utilizing infrastructure services such as networks, servers, and storage provided by financial clouds, small and medium-sized financial institutions can rapidly build their IT systems at a low cost through the use of IT services, enabling data center outsourcing and on-demand deployment, as well as significantly increasing system flexibility at a low cost.

Reduction of the risk of IT use

Over the years, as buyers of IT technology, financial institutions are massively influenced by IT service providers on many levels, from technical direction to system architecture and application software, resulting in high IT costs and vendor lock-in of IT systems (Bisong, Syed, and Rahman 2011). With cloud computing, financial institutions can acquire infrastructure, development platforms, and even application software via service procurement, eliminating the need for large capital investment.

Enhancement of data processing capability

Through cloud computing technology, financial data can be stored, analyzed, processed, and mined in a short period of time, thus greatly enhancing the bank's data processing ability. As competition grows, financial institutions' marketing efforts should be segmented and customized for different tiers of clients, placing increased demands on financial institutions' data processing capabilities. When dealing with large amounts of data, conventional data analysis methods frequently struggle to produce timely analytical results (Hashem et al. 2015). Cloud computing's distributed design enables a new approach to create data warehouses, with the benefits of huge data mining and analysis. In comparison to a centralized data warehouse, cloud computing significantly enhances data storage capacity and analytical speed. Financial organizations may swiftly extract important information from massive amounts of data by combining data mining techniques and cloud computing, which helps enhance the speed and quality of data analysis and facilitates financial institutions' business choices (Huang et al. 2011).

However, at the moment, they pose some challenges for financial institutions in terms of data security, business continuity, and so on. Once these issues are rectified, cloud computing will be promoted more in the financial sector. Financial institutions may leverage cloud computing in the future to develop new business models and provide customers with an entirely new experience of financial services.

Cloud Security

The term "cloud security" refers to the security policies, controls, and technology used to safeguard cloud computing environments. There are three types of controls

available:

- a) 1) Preventative Controls are a type of control that is used to prevent problems from occurring. These cloud security rules aim to reduce risk and plug security holes in the cloud architecture. Firewalls, encrypting methods, and secure applications use regulations are examples of this. 2)
- b) Controls for Detection identify ongoing or recently completed attacks, allowing automated or manual cleanup to commence. Detection controls include items such (SIEM) systems (which are typically offered via SaaS models), anti-malware detection technologies, and sometimes even controlled network security monitoring.
- c) 3) Controls for co
- d) rection are intended to repair any damage or bad consequences caused by an attack after it has occurred. Corrective controls could include things like distant data backups (to recover corrupted or destroyed files), virus/malware eradication solutions, and controlled security issue response services.

Security issues in the financial sector

Information security

Data is the life of the financial institution. When data leaks, the company has not only economic losses but also has enormous effects on the organization's development prospects. The fundamental goal of cloud computing is to overcome the security issue in order to establish its presence in the banking business. Traditional information security difficulties persist in cloud computing, while new security risks arise as a result of its properties. Some examples are cloud computing data storage and destruction, as well as the appropriate design of security trust systems (Sabahi 2011).

Cloud computing deprives customers of direct control over data management systems and may therefore lead to concerns about the cloud. Of course, financial institutions seek to place more data on "the cloud" in order to consume fewer resources while gaining more benefits. With the storage of data in the "cloud," there is the possibility that it may be misused. Many financial institutions will be hesitant to make a choice because of this difficulty. A financial institution places a high value on data security; moving the workload to a shared architecture will almost certainly increase the danger of unwanted access and data leakage. It will be difficult to acquire financial institutions' faith in cloud computing

if the "security

" hurdle is not overcome as quickly as possible.

Business security

Financial institutions use cloud computing to purchase services from cloud operators using IT resources and pay-per-use models, and computing resources can be scaled up or down at any time to meet business demands. In some ways, cloud computing is a type of information technology socializing service. This technique adapts to the demands of modern society for increased efficiency, but it also exposes the financial institution to potential hazards. External cloud computing providers may not have enough capacity to satisfy the organization's needs, and they may potentially stop services due to financial issues, posing a danger to the organization's ability to provide continuing financial services. Because IT service vendors' lifecycles are impossible to predict at the moment, the sustainability of cloud services will have an impact on the organization's existence (Singh and Chatterjee 2017). Furthermore, because existing cloud companies are still in the early stages of development, they lack confidence. The information processing capability and risk controls of cloud computing platforms may face more hurdles as the complexity of financial services, and the quantity of financial products grows.

System Security

System security consists of many areas, including protection against malicious attacks on cloud users' products and unauthorized access to system data. The mainstream cloud computing companies provide similar solutions because of the nature of similarity in the issues that they all have to deal with. However, many issues are different based on the origin of its domain. For every service provider, the DDoS (distributed denial-of-service) attack is the most significant challenge. A significant amount of DDoS requests occupy the network flow and keep sending a request to the server or the service, forbidding the real clients from getting access to the actual service. All of the cloud providers in the world have very similar ways to avoid or to get rid of this issue, which is to use highly imitative IP addresses. When a user's domain name or source IP is under heavy traffic DDoS attacks, the Anti-DDoS system uses the imitative IP as a proxy for the source IP to hide the source IP and divert the traffic to the imitative IP address. This is where the attacked data will be cleaned and filtered out, and the standard data which is now safe will be resent to the server, ensuring stable access. This process helps in preventing servers from crashing due to the extremely high traffic of requests as a result of the attack (Bisong, Syed, and Rahman 2011; Mell 2012; Carlin and Curran 2013).

Another type of typical attack is DNS change. Each website's IP address is associated with a domain name so that when people want to access that site, they can type the domain name in their browser instead of memorizing the complicated IP address. Hackers can hack and manipulate the actual IP address, tricking the users into visiting other phishing websites. This apparently can reduce the reputation of the original site and harm their business by reducing their customer base. Many leading cloud service providers deal with this situation by setting up a significant amount of stations and server machines in many different areas across the world. Each station will imitate the real users to send the requests

to their cloud users to test if the accessed website is correct (Muttik and Barton 2009; Bates et al. 2018).

Host Security

Attacks on hosts mean hackers target cloud computing service providers' servers or the user's host using the cloud services. The providers have developed products to predict the possible threats, to detect the problems that are happening, and to prevent them from happening again. Most service providers focus on three significant threats, namely, Trojan detection and killing, unauthorized account login detection, and any hacking behavior. To prevent these, the providers start by providing essential services and applications like account security, threat intelligence, and server and host configuration. The system tells the users about the allocated user's permission or that their passwords are very easy to crack and force people to change according to some specific rules and regulations. Some of them allocate limited access to people or force users to change their account password once a week or a month at least (Sethi and Sruti 2017).

Besides, every cloud provider can do real-time scanning to protect both their users and their servers. The cloud providers use threat intelligence techniques on their entire network to detect the potential threat and provide risk evaluation in real-time to prevent it from happening. This real-time scanning can be applied to different risks like web shells and malicious executing files and scripts. Once the files are detected and recognized in real-time, the cloud system can immediately control its user's access and isolate these malicious files to prevent them from causing any damage to the server (Oberheide et al. 2008).

Data Security

The most critical issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. Data security issues are primarily at SPI (SaaS, PaaS, and IaaS) level and the primary challenge in cloud computing is data sharing (Tsai, Bai, and Huang 2014).

Cloud service providers employ several fundamental data security approaches, such as encryption and access control, to safeguard their customers' data from possible data breaches and loss. They also use various techniques to ensure the data privacy of their users, avoid any risk and threat to the data stored on their server, and how to get rid of it in case there is an issue. Most cloud service providers not only apply encryption algorithms to the data stored on their server but also encrypt the data during its transition on the network, as the data on the move is the most vulnerable to an attack (Somani, Lakhani, and Mundra 2010). An advanced method in cryptography can be used to address the issue of confidentiality, and some systems could even monitor how much access people have to the data eliminating the need for users to take any extra precautions to secure their data (F. Zhao, Li, and Liu 2014).

The maintenance staff working for the service providers may also act as an insider threat, especially the ones who have authorized access to the database. They can access, modify and delete data from their customer's accounts, causing severe damage to the reputation of the service provider. Some cloud providers have a system in which the machine for sensitive and private information storage and the maintenance devices are separated. As a result, even the internal operations and maintenance staff are not authorized to access all the data. Some cloud providers also take charge of the access command, which can be used

for the surveillance of staff and user's ultra-right operations. Besides, nearly all the cloud computing companies provide supervision on the database. Each piece of information on the cloud is stored in a database, including the user's business confidential data and government data. Except for essential data cryptography, some cloud providers provide database auditing to supervise all the operations on the database, which can help to trace back the identity and behavior of a user according to their suspicious actions. Cipher machine, server clustering, and load balancing can efficiently solve the problems with data when some of the servers are out of power or destroyed by natural disasters (Y. Zhao and Huang 2009)(Jose, Sajeev, and Suyambulingom 2011).

Network Security

To avoid a data breach, many service providers use data encryption. The transmitted data is separated into several parts using encryption before being transmitted to the cloud server. It is vital to encrypt the data in transit on the network as the data can be easily attacked during that period (Xu, Huang, and Tsai 2014). Some cloud providers handle their clients by making them aware of the reason for the need to update their network transport protocol, like the need to switch from HTTP to HTTPS, without changing the user's server configuration during the request and response exchange (Muttik and Barton 2009). SSL certificate as a controlling service also plays a vital role. SSL helps to establish an information highway to connect the client to the server. It provides client and user authentication and encrypts the transmitted data on the highway.

CONCLUSION

As a result of this emerging trend regarding the usage of cloud-based services, the security issues related to cloud computing have become a massive challenge. The whole financial service industry covers hundreds of different service categories. With the breakneck pace of information development, the traditional service platform database cannot meet the market demand. So, both conventional financial and start-up companies have started to focus their attention on cloud technology due to the massive data increase annually, which is the concept of FinTech (Financial Technology). Traditional financial companies like banks and insurance companies have started to move their stable and closed platforms to open systems to increase their market reach and grow their business. The start-up financial companies are using cloud computing to construct their service platforms. At the same time, retail e-commerce is also developing very fast, and the vast population base in the world that is extremely fond of e-commerce now has caused this business, combined with social media, to move to cloud computing. The commercial business structure gets complicated when it comes to the massive data storage of the users. Thousands of related and irrelevant data have to be stored in the cloud. Due to the existence of many similar companies in the same industry, possible data mixture and confusion might contribute to data loss when the user tries to get their data from the open bank system or, even worse, unauthorized users could access the most critical private data.

Financial organizations that deal with a great deal of data require a large team of operations and maintenance employees to assist them in maintaining the system and responding to any emergencies. However, the operations team with the greatest power can readily access all sensitive data stored in their cloud offering. With the advent of cloud computing, different industries have embraced its uses, and the financial sector is no

exception. At the moment, an increasing number of financial institutions are considering shifting their on-premises IT systems to cloud computing alternatives. Cloud computing solutions have simplified the maintenance and use of information service infrastructures to an unprecedented degree for financial organizations.

However, at the moment, they pose some challenges for financial institutions in terms of data security, business continuity, and so on. Once these issues are rectified, cloud computing will be promoted more in the financial sector. Financial institutions may leverage cloud computing in the future to develop new business models and provide customers with an entirely new experience of financial services.

REFERENCES

- Amara, Naseer, Huang Zhiqui, and Awais Ali. 2017. "Cloud Computing Security Threats and Attacks with Their Mitigation Techniques." In *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 244–51. ieeexplore.ieee.org.
- Bates, Samantha, John Bowers, Shane Greenstein, Jordi Weinstock, Yunhan Xu, and Jonathan Zittrain. 2018. "Evidence of Decreasing Internet Entropy: The Lack of Redundancy in DNS Resolution by Major Websites and Services." Working Paper Series. National Bureau of Economic Research. <https://doi.org/10.3386/w24317>.
- Bisong, Anthony, Syed, and M. Rahman. 2011. "An Overview of the Security Concerns in Enterprise Cloud Computing." *arXiv [cs.CR]*. arXiv. <http://arxiv.org/abs/1101.5613>.
- Carlin, Sean, and Kevin Curran. 2013. "Cloud Computing Security." In *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments*, 12–17. IGI Global.
- Do, Hye-Ji, and In-Seok Kim. 2018. "A Study on Cloud Computing for Financial Sector Limited to Processing System of Non-Critical Information: Policy Suggestion Based on US and UK's Approach." *Journal of Society for E-Business Studies* 22 (4). <http://www.calsec.or.kr/jsebs/index.php/jsebs/article/view/288>.
- Gill, Ron, and Cfm Cma. 2011. "Why Cloud Computing Matters to Finance." *Montvale* 92 (7): 43–47.
- Hashem, Ibrahim AbakerTargio, Ibrar Yaqoob, Nor BadrulAnuar, Salimah Mokhtar, Abdullah Gani, and Samee Ullah Khan. 2015. "The Rise of 'big Data' on Cloud Computing: Review and Open Research Issues." *Information Systems* 47 (January): 98–115.
- Huang, Dijiang, Zhibin Zhou, Le Xu, Tianyi Xing, and Yunji Zhong. 2011. "Secure Data Processing Framework for Mobile Cloud Computing." In *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 614–18. ieeexplore.ieee.org.
- Jose, G. Jai Arul, C. Sajeev, and Dr C. Suyambulingom. 2011. "Implementation of Data Security in Cloud Computing." *International Journal of P2P Network Trends and Technology* 1 (1): 18–22.
- Mell, Peter. 2012. "What's Special about Cloud Security?" *IT Professional* 14 (4): 6–8.
- Muttik, Igor, and Chris Barton. 2009. "Cloud Security Technologies." *Information Security Technical Report* 14 (1): 1–6.
- Nicoletti, Bernardo. 2013. *Cloud Computing in Financial Services*. PDF. 1st ed. Palgrave Macmillan Studies in Banking and Financial Institutions. Basingstoke, England: Palgrave Macmillan. <https://doi.org/10.1057/9781137273642>.

- Oberheide, Jon, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn, and FarnamJahanian. 2008. "Virtualized in-Cloud Security Services for Mobile Devices." In *Proceedings of the First Workshop on Virtualization in Mobile Computing*, 31–35. MobiVirt '08. New York, NY, USA: Association for Computing Machinery.
- Oredo, John, James Njihia, and X. N. Iraki. 2017. "Cloud Computing Adoption in the Kenya's Financial Sector: An Institutional Perspective." In *2017 IST-Africa Week Conference (IST-Africa)*, 1–9. ieeexplore.ieee.org.
- Qian, Ling, Zhiguo Luo, Yujian Du, and Leitao Guo. 2009. "Cloud Computing: An Overview." In *Cloud Computing*, 626–31. Springer Berlin Heidelberg.
- Sabahi, F. 2011. "Cloud Computing Security Threats and Responses." *2011 IEEE 3rd International Conference on*. <https://ieeexplore.ieee.org/abstract/document/6014715/>.
- Sethi, Srinivas, and Sai Sruti. 2017. "Cloud Security Issues and Challenges." In *Resource Management and Efficiency in Cloud Computing Environments*, 89–104. IGI Global.
- Singh, Ashish, and Kakali Chatterjee. 2017. "Cloud Security Issues and Challenges: A Survey." *Journal of Network and Computer Applications* 79 (February): 88–115.
- Somani, Uma, Kanika Lakhani, and Manish Mundra. 2010. "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing." In *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*, 211–16. ieeexplore.ieee.org.
- Tsai, Weitek, Xiaoying Bai, and Yu Huang. 2014. "Software-as-a-Service (SaaS): Perspectives and Challenges." *Science China. Information Sciences* 57 (5): 1–15.
- Xu, Le, Dijiang Huang, and Wei-Tek Tsai. 2014. "Cloud-Based Virtual Laboratory for Network Security Education." *IEEE Transactions on Education* 57 (3): 145–50.
- Zhao, Feng, Chao Li, and Chun Feng Liu. 2014. "A Cloud Computing Security Solution Based on Fully Homomorphic Encryption." In *16th International Conference on Advanced Communication Technology*, 485–88. ieeexplore.ieee.org.
- Zhao, Yi, and Wenlong Huang. 2009. "Adaptive Distributed Load Balancing Algorithm Based on Live Migration of Virtual Machines in Cloud." In *2009 Fifth International Joint Conference on INC, IMS and IDC*, 170–75. ieeexplore.ieee.org.