http://www.jctjournals.com

ISSN(ONLINE):2278 - 3814

Volume-12, Issue-03, March 2023

JOURNAL OF COMPUTING TECHNOLOGIES (JCT)

International Journal

Page Number: 01-04

A REVIEW ON TRENDS IN BANK DATA SECURITY

Louay A. Hussein Al-Nuaimy[1], Mahammad Mastan[2], G. Jai Arul Jose[3]

[1,2]Assistant Professor, Oman College of Management & Technology, Oman

[1]loay.alneimy@omancollege.edu.om, [2]mastan.mohammed@omancollege.edu.om

[3]Associate Professor, St. John's College of Arts and Science, INDIA, jaiaruljose@gmail.com

***Abstract*—Banks and banking jobs have been existed from centuries and the money's history is closely related to the banking industry history. Although the mode we approach banks has reformed dramatically, the basic ideologies remain as it is. Many banks we know have been around us for a longer period than us individuals. The customers are believing the banks not only for keeping the people money safe, but the information about the customers too is also highly protected by the banks. While the banks are having always a large quantity of financial and personal data about their customers, these days it is easy to access every data for anybody with the permission to see and access it. The evolution of fintech has led to more changes and innovations over the past twenty years, such as credit/debit cards, wired transfers, mobile payments and online banking. The Banks had to not only modernize their systems to accommodate these changes but also renovate their operations to ensure sustained security as the new technology has been implemented. In the world of IT, information security plays a vital role. The data security has become one of the today's big and main challenges. This paper aim is to conduct a literature review about the trends which used in banks data security and mark the most important data security practices used in that field and concentrates on the new technologies of data security.**

Keywords— Data Security, Banks Data Security, e-Governance, Information Security and Cloud Computing.

I. INTRODUCTION

The use of information technology (IT) in banking has established significant opportunities for banks and financial techniques. However, this opportunity has come with a range of risk factors. Banking regulators such as central banks provided guidelines on IT governance in the new era. Various researchers suggested the frameworks and principles of IT governance. Many factors need to look at time Implementation of effective IT governance. The used of banking services is growing rapidly and IT governance needs to keep up with[1]. While unrest and new trends, IT risk also takes new forms and unprecedented dimensions. Guidelines and standards, which are generally defined, and the banks are executed for a new range of risk. The implementation of IT governance and multinational banks also differ in their approach and challenges they face. The information technology model adopted by global banks is quite different from one country to another[2].

The IT governance of multinational corporations operating in word wide which differs significantly from typical companies doing business in various countries[3]. The complexities arise from the operating models established within multinational corporations. The environment within multinational companies is highly structured and follows strict operating procedures and this approach poses challenges in terms of roles and responsibilities of local IT management versus global governance[3].Issues like Accountability versus ambiguity in responsibility, use of global versus local tools compatible tools, etc., create a difference in the approaches adopted by multinationals and local companies. Within multinationals companies, control usually tends to gravitate towards global IT governance, which is generally applied as wide word[1]. Also, the well-organized nature of roles and responsibilities within the organization makes it mandatory for local IT administrators to follow standards. This can become a complex issue as global platforms are used within local banks to support businesses in their countries since platforms are mostly built to support global businesses and local is added as an additional user[1]. This complexity affects the decision-making process and business efficiency because key performance indicator (KPIS) for local banks also needs to be consistent with

those of the global entity yet complies with local regulatory standards[4].Certain roles that may be delegated by local regulators are fulfilled by assigning appropriate personnel to coordinate across geographies to ensure local compliance and fulfillment of global mandates. In some cases, local IT personnel play a key role in meeting regulatory requirements[5].

II. RESEARCH QUESTIONNAIRE

This research work will be trying to seek and concentrate on the below questions:

1. What are the most important trends and platforms in bank data security that support the global banks data security?
2. Which data security platform mostly used in multinational banking systems?

The hypothesis of this research has been designed to answer the above questions as follows: "The Cloud computing platform security systems is the most popular used system in multinational banks"[6].

III. METHODS

This work focused on the literature about the banking rules and regulations are continuously changing as per the requirements of modern banking systems and theories. Every banks have at most high legal accountability to keep the customer information safe, secure and protect it from falling into the wrong hands[3]. In this paper, we analyzed how the modernized banks ensure that they fulfill this legal responsibility.

The prove of the hypothesis and finding the results are presented below according:

- First provides an overview checking literature on data security best practices for banks.
- Second by describe the results for approaches of data security platforms used to confirm that a security crack does not take place externally or internally.

IV. THE REVIEW

The criteria that were established for the selection of the articles were:

- Papers relating banks data security.
- Studies analysing the impact of banks IT security.

The following are the most important studies done at the banks data security field which related to IT security. European payment council, Belgium, during 2010 approved an updated version of the document "Using Audit Paths in Security Systems: Guidance for European Banks". These Guidelines support payment service providers to comply with the requirements established to ensure information security, i.e., protect the confidentiality, integrity and availability of the data underlying the payment transaction. Specifically, the revised guidance now includes recommendations regarding the maintenance of so-called audit trails (or audit logs) for payment systems. To develop the skill for employability and the productivity of the young minds.

Abidin et. al [4] suggested the following during 2018: Comparisons between industries such as banking, finance, construction, etc. can also be examined for specific data theft characteristics by industry. Thus, the company can use appropriate standard operating procedures and design internal controls to combat data theft of the nature of its business. The focus of training should also be focused on risks, particularly financial risks, because of poor management of data security and legal risks due to non-compliance with legal and regulatory requirements on customer data protection. In addition, employees need to understand the importance of data security related to their work and what they are required to do, to comply with relevant standard operating policies and procedures.

Kavya Venkatesh and Bhavya Vikas [12] in 2018 suggested the best data security for and the worst security in investment, because the classification of stocks is done based on investment and type of investors. Their study shows that many time markets have collapsed which has not happened before, creating fears for investors to enter the market.

Manoj Kulkarni [1], suggested in their research work "IT Governance in Global Banks: Emerging Models" suggested the following:

- Global banks are streamlining their operations in the wake of unprecedented changes in political, economic, and social domains and the future looks exciting and challenging as well.
- IT governance has taken on greater importance in a world where IT security has become a challenge for global banks.
- Cloud computing technologies have evolved and also enhanced the security of their data, usually to alleviate the concerns of banks.

Igor Kravchuk et al, [13] suggested that banks with high commercial experience (commercial banks) increase the level of their investments in data security compared to other banks (non-commercial banks).Globally the Commission on the Global Financial System identifies shifts in banking business models, advanced economy banks tend to reorient their business away from commercial and more complex activities, towards less capital-intensive activities, including secured commercial banking.

Kanika Tyagi et al [11] suggested the following in their research work:

- As the traditional banking industry has completely changed and now the complete control is in the hands of the customer instead of the bank.
- Cloud computing in the banking industry offers various features, Cost savings, business continuity, business speed and time savings.
- But since the data in the bank is the most important data, so cloud security is the priority of every bank before adopting the cloud.

- Security in the cloud is the biggest obstacle for the banking industry to adopt this popular technology and its services.
- So, there is a need to provide security for the cloud. This paper aims at basic cloud methodology and analysis of some security algorithms and their applicability in cloud banking environment

Deina Kellezi et al [14] suggested that the open banking has received a lot of attention, which Refers to the process of using APIs to open consumers' financial data to third parties .This concept is believed to be secure by assuming that only the customer and the data owner can authorize any communication between the bank and a third-party regulator. Security measures were either handled automatically by components provided by the Technical Kit or were easily avoided by packages included in the Flask Framework.

V. DATA SECURITY MANAGEMENT IN BANKING AND FINANCIAL SERVICES

There is a cyber security department in every Banking and Financial services sector industry. Some security measures are deployed by this cyber security department along with the common security measures to secure the entire banking systems. These security measures include: SSL - Secured Socket Layers (for secure connection), database encryption, Vulnerability and assessment testing of systems, IDS - Intrusion detection systems, Firewalls (to control flow of traffic), NIPS - Network intrusion prevention systems, quarantining unknown systems, password protection mechanism, DNS - Domain Name systems and SMS alerts to customers. All these security systems and devices are to secure cloud architecture infrastructure in banking and financial services, however, there are still vulnerabilities and threats due to external agents or accidental man-made errors by internal staff. So, the data privacy and systems security remain a key concern[7].

Financial services and banks reflect the following measures for information security and privacy while using the cloud computing architecture infrastructure[8].

- **Data Security:** Data security refers to confidentiality, availability, and integrity of data. The data security means – it is accessible, used and processed by authorised users only. Data security ensures it is available, reliable, and accurate. Data security plan ensures collecting only required information, keeping it safe and destroying any information which is no longer needed. Data privacy and Data security are related where former remains an asset for banks and later is the means of protecting it to bring desired end to data collected[9][10].
- **Data Privacy:** Data privacy refers to the desire of individuals to control or have some influence over data about themselves. Information age has led us to four major concerns about the use of information: privacy, accuracy, property and accessibility (PAPA). Clarke (1999) identified four dimensions of privacy – privacy of person, personal behaviour, personal communication, and personal data privacy. Today most communication channels are in digital form through mobile phones and internet, so the personal communication privacy and personal data privacy are merged into information privacy[10].
- **Compliance and Governance:** Compliance and Governance department in banking and financial services sector industry aid to offer over all monitoring, measuring, working and communication framework to keep the cloud architecture safe. Compliance and Governance ensure the strategic alignment of system with customer, business, and employee needs. Cloud security governance is consisting of organization structure, leadership and processes that safeguard information. Compliance is requirements from government regulatory bodies to adhere to rules to function within framework[11].
- **Data Deletion Securely:** Banking and financial services collect relevant data for their use and delete it once the objective is achieved. These data deletion is an operations activity and must be performed to keep free space to store new data. With data storage on cloud and accessed by users, secure deletion of data forms an important part to avoid misuse or manipulation in future. Cloud infrastructure being operated by third party makes it imperative to ensure deletion of data and confirm that it cannot be recovered. If the data is not deleted it can be accessed in future and misuse to create fake identities of customers and their accounts to commit fraudulent activities. This will lead to financial crimes and further issues in creating trust on cloud infrastructure. Secure Data deletion helps maintain data security.
- **Outsourcing and Cloud computing:** For banking and financial services, cloud infrastructure is supposed to within the jurisdiction of the nation. However, the users who are accessing cloud infrastructure are located remotely. Users who are maintaining cloud services and data can be outsourced for cost efficiency. However, these users are required to be managed by identity access management system. These users may changeover the period, so there will be multiple people having access to system and data. Banking and financial corporation's may not have control over these users. In the event of any issues with system, banking and financial services corporation follow the contractual agreements with vendors managing cloud services and takes appropriate action and enforce penalties to enforce stricter security measures.
- **Access Management and Identity (AMI):**In banking and financial services industry, when the personally identifiable information of customer and their financial history is available over cloud architecture, it is very important to identify users who are accessing information. This mechanism helps to authenticate users and services based on credentials

and characteristics. Credentials means "User Identity" (or Unique Network ID and Password)and Characteristics means defined method of running cloud services. An AMI system helps to protect access levels of users by identifying them based on roles and responsibilities.

VI. CONCLUSION

Cloud computing is a combination of several key technologies that have evolved and matured over the years. Cloud computing has a potential for cost savings to the enterprises, but the security risk is also enormous. Enterprise looking into cloud computing technology to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. With banks and financial services having internal IT security team which develops and implements the security framework a constant evaluation of this framework and updating as per changing scenario is required. With several threats being already present in information systems, there will always be chance of attack from outsiders and hence the cloud security continues to be priority for banking and financial institutions. Banks should verify and understand cloud security, carefully analyze the security issues involved and plan for ways to resolve it before implementing the technology. Pilot projects should be setup and good governance should be put in place to effectively deal with security issues and concerns.

References

[1] M. Kulkarni, "IT Governance in Global Banks: Emerging Models.," *Vinimaya*, vol. 39, no. 1, pp. 11–21, 2018, [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=129480222&site=ehost-live&scope=site.

[2] A. D. Giwah, L. Wang, Y. Levy, and I. Hur, "Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory," *J. Intellect. Cap.*, vol. 21, no. 2, pp. 215–233, 2020, doi: 10.1108/JIC-03-2019-0063.

[3] S. HADAD, "Challenges for Banking Services in the Knowledge Economy," *Manag. Dyn. Knowl. Econ.*, vol. 7, no. 3, pp. 337–352, 2013, doi: 10.25019/mdke/7.3.04.

[4] M. A. Z. Abidin, A. Nawawi, and A. S. A. P. Salin, "Customer data security and theft: a Malaysian organization's experience," *Inf. Comput. Secur.*, vol. 27, no. 1, pp. 81–100, 2019, doi: 10.1108/ICS-04-2018-0043.

[5] S. Asadi, M. Nilashi, A. R. C. Husin, and E. Yadegaridehkordi, "Customers perspectives on adoption of cloud computing in banking sector," *Inf. Technol. Manag.*, vol. 18, no. 4, pp. 305–330, 2017, doi: 10.1007/s10799-016-0270-8.

[6] A. A. Abu-Musa, "Investigating the security controls of CAIS in an emerging economy: An empirical study on the Egyptian banking industry," *Manag. Audit. J.*, vol. 19, no. 2, pp. 272–302, 2004, doi: 10.1108/02686900410517867.

[7] M. Zaydi and B. Nassereddine, "A new comprehensive solution to handle information security governance in organizations," *ACM Int. Conf. Proceeding Ser.*, vol. Part F148154, 2019, doi: 10.1145/3320326.3320382.

[8] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Secur. Priv.*, vol. 8, no. 6, pp. 24–31, 2010, doi: 10.1109/MSP.2010.186.

[9] A. B. and S. (Shawon) M. Rahman, "A s c e c c," *Int. J. Netw. Secur. Its Appl. (IJNSA), Vol.3, No.1*, vol. 3, no. 1, pp. 30–45, 2011.

[10] C. L. Philip Chen and C. Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data," *Inf. Sci. (Ny).*, vol. 275, pp. 314–347, Aug. 2014, doi: 10.1016/J.INS.2014.01.015.

[11] K. Tyagi, S. K. Yadav, and M. Singh, "Cloud data security and various security algorithms," *J. Phys. Conf. Ser.*, vol. 1998, no. 1, pp. 1–9, 2021, doi: 10.1088/1742-6596/1998/1/012023.

[12] Kavya Venkatesh, Bhavya Vikas, "A Study on Risk and Return Analysis and Data Envelopment Analysis of Public and Private Sector Banks", Srusti Management Review, Vol -XII, Issue - II, July - Dec. 2018

[13] Igor Kravchuk, Viktoriia Stoika, Business Models of Banks for the Financial Marketsin the EU", European Research Studies Journal, Volume XXIV, Issue 2B, 2021, pp. 371-382

[14] Deina Kellezi, Christian Boegelund, and Weizhi Meng, "Securing Open Banking with Model-View-Controller Architectureand OWASP", Wireless Communications and Mobile Computing, Volume 2021, Article ID 8028073, 13 pages, https://doi.org/10.1155/2021/8028073

