Faster Identification and Resolution of Risk in Mobile and Internet Banking Using CLOUDSHIFT

Rasheed O. Owolewa*, Pritheega Magalingam

Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia

roowolewa@graaduate.utm.my

Article history

Received:
11 Oct 2019

Received in revised form:
5 Nov 2019

Accepted:
4 Dec 2019

Published online:
25 Dec 2019

*Corresponding author:
roowolewa@graaduate.utm.my

Abstract

The security risk report on mobile and internet banking technology has recorded a high-level financial loss globally, while personal data of customers and sensitive bank information are constantly at risk. This research explores the contextual banking technology issues in the financial industry. The study uncovers different security issues in the existing mobile and internet banking technology and proposes a CLOUDSHIFT implementation framework as secure haven. Our CLOUDSHIFT solution evolves a faster cloud technology that can easily investigate, detect and resolve real-time potential failures or breaches within the banking system from any secure web server. CLOUDSHIFT leveraged on where internet-based computing thrive, as such the case of Malaysia was considered. To leverage further on this benefit, banks and financial services need a co-security centric approach in conjunction with cloud providers and third-party solution partners to implement this cyber fraud event management process. The CLOUDSHIFT provides important implications of cloud computing in combating cyber-fraud with better strategic cloud migration framework that addresses the operational challenges of the internet and mobile banking. The framework was evaluated using Gai proposition value chain system and Amazon AWS proof of concept applicable to the financial industry.

Keywords: *Cloud computing; Cloud banking; Internet and Mobile Banking; Cloud migration strategy; Cyber-security*

1. Introduction

Cloud banking is a new technology landscape that provides traditional banking systems with modern and alternative ways to access core banking systems [1],[2]. The spiraling costs of deploying and maintaining complex in-house legacy systems, and the quest to keep up with customers' expectations and improve banking security are leading banks to demand better innovation, flexible and cost-effective. Cloud banking is the future of banking technology as a support technology to scale and analyze growing volumes of transactions and numerous customers across different locations. Banking has a unique formation and structure when it comes to technology; among them are Mobile and Internet banking. Mobile banking and its applications are some of the contemporary banking solutions that have been widely adopted to provide instant financial services to customers [3]. Mobile banking is defined as "a channel for customers to interact with their banks via mobile devices without the internet. But it requires the use of

* *Corresponding author: roowolewa@graaduate.utm.my*

mobile phone or Personal Digital Assistant (PDA), (Barnes & Corbitt, 2003)[4]. While internet banking gives customers access to banking over the internet with a Smartphone or device support, mobile banking gives services to customers on the go without internet, laptop or computer [5].

Consequently, the vulnerability in mobile and internet banking have exposed customers to widespread incidents of fraud and attack in the process of conducting online and offline transaction. Prominent online frauds and attacks on bank customers include credential stealing, client-side and bank server interceptor, content manipulation resulting from man-in-the-middle (MiTM) attack and password guessing attack [6].

Since, 2013, the United States retail banking sector have received extensive media attention surrounding online fraud and attack on banks customer which is carefully executed over mobile banking platform, including point of sale and automated teller machine. Internet fraudsters and hackers have successfully obtained data on over 40 million customers' credit and debit cards from target internet banking and mobile application platform, as well as non-card customer personal data [7]. Similarly, between January and May 2014, financial losses incurred by online retail sector broker eBay has been estimated to about $500 million as a result of cybercriminal's access to customers usernames, email address and phone number which made user credentials to excepted [8].

According to Consumer Bankers Association and the Credit Union National Association, on a survey of 535 banks, it is reported that the banks have lost close to $331 on each customer, while average bank loss stood at about $530 on card transaction [9],[10]. Cyber-attacks have been targeted at bank's customers and eventually resulted in huge revenue loss, business disruption and distort the trust between customers and financial institutions from the customers' perspectives

The advantage of cloud computing in the banking system is the ability to support a complete automated banking system on external organization servers and monitor the large sum of transactions within seconds. According to Gartner, by the year 2020, more than $1 trillion of IT expenditure will be directly or indirectly toward cloud computing technology because of its overwhelming ease of use and cost advantages [11]. Could computing is a modern computing system that provides virtualized resources like Software, Hardware, Storage and Platform to its customers over the internet [12]. Cloud provides different kinds of services such as infrastructure (IaaS), Platform (PaaS), Software (SaaS) and can a combination of all in form of business process as a service (BPaaS) [13]. Cloud computing can be deployed irrespective of the user needs in a public environment (Public cloud), on-premise environment (Private Cloud) or both in form of Hybrid cloud [14].

2. State of application security in the existing banking applications

While most of the mobile and internet banking applications have been discovered to be vulnerable, [15], Chen has assessed 693 banking application across over 80 countries. They unveiled 2,157 vulnerabilities, which many of them can cause serious sensitive data leakage such as access pin, and user name exposure. Another study by [3] followed up to investigate this claim, among over 350 vulnerabilities uncovered; a real vulnerability case was uncovered in one of the famous banking entities in Southeast Asia. Such a mobile application

vulnerability discloses users' credentials and may cause severe financial loss to customers and banks [3].

The vulnerability of internet and mobile banking applications are evident by on Equifax data breach attack, (a major credit bureau in the United States). Online credentials specifically personal data of over 143 million Americans were hacked. JP Morgan experienced the largest data breach in history. Emails and detail of bank customers were swiped off by targeted attack intention to steal customers' valuables [16],[17]. Between 2009-2019 within the commercialization of the Internet and mobile banking, about 1283,747 total vulnerability including DDoS, click fraud, phishing fraud, keylogging, bitcoins fraud, spamming, sniffing traffic and Mobile password theft have been recorded in Malaysia [18]

The attack techniques span across the border as internet and mobile banking are borderless, banks often engaged in third party software which creates some vulnerability loopholes such as Trojan attacks**,** Man-in-the-middle attack, Phishing and sniffer attacks**.** This are all classified as an external attack on banking technology while internet attack attributed to internet and mobile banking includes fraud or theft of payment credentials and devices, back doors or trap doors credentials guessing attack and service negligence or sabotage attack, [6]

To argue further, these threats are applicable to the banking system, hackers identify security flaws in banking applications with respect to customer's negligence. [15] Observed 60 banking applications, and find out that 18 banking entities are vulnerable to both internal and external attack. Most of the internet and mobile applications are vulnerable and are being patched according to [15] vulnerability reports.

The vulnerability in the Mobile and Internet banking platform enables a proxy user's authentication system to be created and approval was passed by the proxy switching system in Bangladesh Bank Heist bank, thereby exploiting the vulnerability in third-party API which most banks often use to promote internet and mobile banking services. Sonali Bank's network security was hijacked and its internet banking websites were controlled by hackers before the service was restored [19].

Cloud computing solutions have attracted much Partnership that has spelled out the need to tackle issues surrounding customer's data, privacy security, and banking across boundaries. Cloud computing has triggered a vision to create a secure environment in which private and public sector organizations can operate their services without or limited fear. Although cloud computing still uses internet for customers to access range of related services on demand. Cloud computing can help meet all the challenges areas of transactions in banking, from cash management, trade and supply chain finance to payments, mobile banking, and business analytics. The key to competitive advantage will lie in the security know-how brought to banks and customers.

2.1. The perspective of cloud banking in Developing Countries (Malaysia and Nigeria)

Cloud banking in Malaysia is relatively low, in fact, one would expect that the Malaysian agile technology moves will have increased the rate of cloud adoption in its banks, however, this has not been. As noted by [20], statistics of

Malaysia's access to banks from the comfort of their home is expected to transform the state of cloud computing in Banking, but on a contrary. Thus, Malaysia households, businesses, and the Government have embraced digitalization between 2005-2019 which make it necessary to establish a linkage between ICT and Cloud technology platform [21]. However, of recent, Malaysia's financial regulator has instigated cloud adoption anticipating how the initiative will drive its digital economy through a procurement notice issued in January 2019, [22].

Nigeria is another country with strong technology potential, cloud banking in Nigeria, as with other countries, has witnessed a slow pace. Interestingly, Nigerian banks have adopted a radical Information Communication Technology drive and are relying on various IT platforms for the provision of faster and more efficient banking solutions to their customers, though, Nigerian banks have identified the significant benefits of cloud services, such as agility, scalability, cyber resilience and secure access, but according to [23], migrating customer's bank data to the cloud giver certain concern over data security and loss of control of its data being stored outside the country. One thing that is common at the point of this study, is that Malaysia and Nigerian banks regulators, BNM and CBN respectively, have acknowledged cloud benefits. They have acknowledged that Cloud is expected to drive a rapid transformation in the financial services sector as more institutions are about to move to the cloud using a reassessment strategy.

Nonetheless, banks are clearly concerned about security, and the privacy of their customer's data, delivery of cloud technologies with effective Security-as-a-service to the banking needs have not been met [24]. Thus, these findings acknowledge the importance of Security, privacy, and trust, it is also a concern than only a few researchers and technology experts have more experience in delivering compliant solutions to financial institutions in Nigeria and other countries.

2.2 Cloud regulatory and security

Malaysia has good internet infrastructures and active collaboration with industries such as 1Gov.Net and IBM Malaysia [23] which have supported the growth of technology usage in government organizations, healthcare and Small, medium enterprises (SMEs). The Malaysian financial services sector has a regulatory limitation just like many other countries. The current financial services industry in Nigeria chaired by the Central Bank of Nigeria (CBN) is characterized by a cohesive regulatory regime, which is particular about banks' customers' data security. However, the regulation does not forbid the use of cloud services in financial institutions, [25].

According to the policy document on Outsourcing involving cloud use, banks regulators have emphasized on security which does not appraise that cloud services are in principle permitted. For instance, the regulatory body (BNM) maintained in section G 11.1 that "Where the outsourcing arrangement involves a cloud service provider, a financial institution should take effective measures to address risks associated with data accessibility, confidentiality, integrity, sovereignty, recoverability, and regulatory compliance" [25]. This, in particular, is important as cloud service providers often operate a geographically dispersed computing infrastructure with the global distribution of cloud customer data.

Hence security is the most essential factor to consider before starting any cloud deployment. There are numerous security regulations that must be followed when moving to the cloud**.** In this case of banks, one of the challenges is working with the third-party service provider, Service Level Agreement (SLA). Another concern is how to ensure cloud architecture complies with government regulations [26]. Most importantly, identity and access management and how to minimize the risk of breaches [27]. Fortunately, many security and identity as aa services have been proposed, but security is still a sensitive issue that needs to be in address.

2.3 Cloud Migration Checklist

Cloud Computing deployment options can be facilitated with trusted and knowledgeable cloud services procurement experts or cloud brokers. Although, there is a provision for self-service migration techniques using lift and shift approach. However, there is a need to establish a cloud migration plan, and employee awareness, return on investment, security and access policy and resource management plan. The wish of banks is to provide services to customers 24/7. This requirement checklist is a basic factor to be considered. Cloud migration plans and security policies are often the biggest challenges of banks and enterprises. computing [28] have recommended in house cloud migration plans (Private cloud) for sensitive organizations like banks. However, the above checklist must still be adhered to.
Banks would typically want to drive new business with cloud adoption experience, public cloud is recommended to sell and promote business virtues to the world. Public cloud banking involves the operation of core banking systems that comprise processing and posting transactions relating to payments, current and savings accounts, loans and securities including deposit and current accounting, loan harmonization, holding securities positions and clearing payments using cloud computing [26].

2.3.1 Case Cloud Migration Strategy adopted by Societe Generale bank of France

A conceptual seamless cloud migration strategy adopted by one of the modern Banks has been presented in figure 2 as a complement to the value chains and main activities a bank can derive from the cloud for a sustainable competitive strategy. In figure 3, we present a surviving cloud migration framework that started with a private cloud. Société Générale (SocGen) bank of France began with the private cloud in 2014, before eventually moving to the public cloud in 2017 [24],[29]. The Banks started its journey through private cloud acceleration leveraging on IaaS then gradually to PaaS and SaaS Public cloud off-premise. As of today, the Banks have seized the opportunity of cloud computing and achieved a 60 % migration framework of its banking infrastructure, currently maintaining agile banking and offers rapid, self-service access to about ten infrastructure services with over one hundred operations. Banking operations are providing simultaneous services through APIs portal shared by all the Group’s business lines. The migration strategy attracted talent and an agile operating model from the conception of opening up to the outside world to exchange ideas with the leading Cloud players and researchers.

2.4 Strategies for moving to the cloud

Cloud Computing deployment options can be facilitated with trusted and knowledgeable cloud services procurement experts or cloud brokers. This study will like to hint banks that there is a provision for self-service migration techniques using lift and shift approach, this gives confidence to banks as adequate security of sensitive data is ensured. However, there is a need to establish a cloud migration architect role to lead the effort. Starting strategy for lift and shift could be initiated firstly with the private cloud, where the entire infrastructure would be meant for a single bank and hosted within the bank's premises. Extensively, banks may need to adopt the public cloud deployment model, where infrastructure would be available to the three main constituencies in the financial environment: i.e., customers, the broader ecosystem of business partners and the banks itself. Authors have envisages that For bank who typically want to drive new business with cloud adoption, must sell its business virtues to the world through public cloud computing [28]. The ultimate wish of every bank is to provide services to customers 24/7. Public cloud banking involves migrating core banking systems that comprise processing and posting transactions relating to payments, current and savings accounts, loans and securities including deposit and current accounting, loan harmonization, holding securities positions and clearing payments [26].

2.4.1 Accelerating cloud strategy adopted by Societe Generale bank of France

A conceptual seamless cloud migration strategy adopted by one of the modern Banks has been presented in figure 2 as a complement to the value chains and main activities a bank can derive from the cloud for a sustainable competitive strategy. In figure 3, we present a surviving cloud migration framework that started with a private cloud. Société Générale (SocGen) bank of France began with the private cloud in 2014, before eventually moving to the public cloud in 2017 [24],[29]. The Banks started its journey through private cloud acceleration leveraging on IaaS then gradually to PaaS and SaaS Public cloud off-premise. As of today, the Banks have seized the opportunity of cloud computing and achieved a 60 % migration framework of its banking infrastructure, currently maintaining agile banking and offers rapid, self-service access to about ten infrastructure services with over one hundred operations. Banking operations are providing simultaneous services through APIs portal shared by all the Group’s business lines. The migration strategy attracted talent and an agile operating model from the initial conception of opening up to the outside world to exchange ideas with the leading Cloud players and researchers.

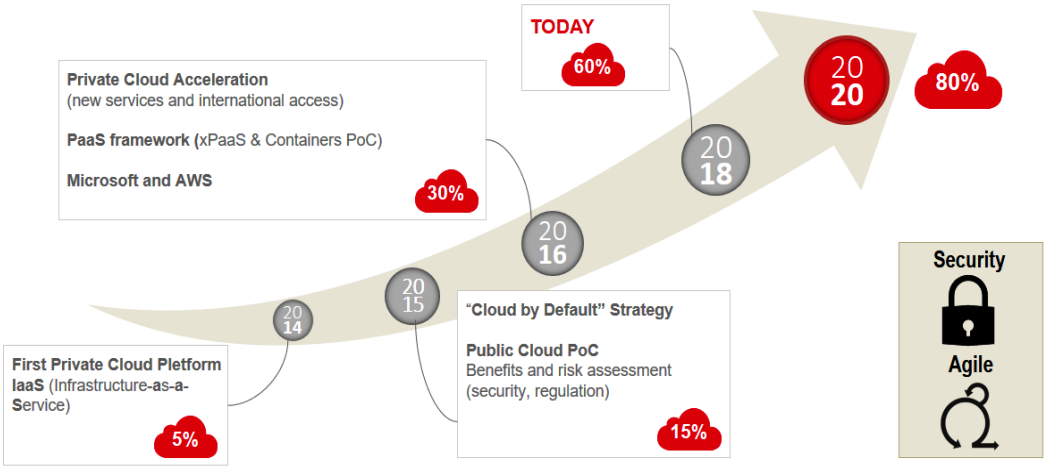

Figure 3. Societe Generale's Cloud Conceptual Strategy (SocGen, 2015)

3. Value chain Cloud propositional framework for cloud migration

Lift and Shift cloud migrating to the private cloud often comes as a wise idea in the cloud migration framework. What makes this move a greater decision is that banks still remain the custodians of customers' most valuable digital assets, the sensitive information is still within the control of the banks. After when security and reliability have been largely met with the rigorous regulatory requirements and compliance, then banks can now take the core banking application which probably will be the last to take the leap. This is to ensure transaction security and operational capability for major strategic decision making which bothers on the banks as the investing party [30]. The cloud computing proposition framework refers to how organizations will *investments* in data *security and* may derive much economic or business benefit from a move to the public cloud. Data security will indeed, create new markets that will attract new customers. To this end [30] has provided a Value chain of how cloud computing can help banks improve and obtain advanced capability through improvement, transformation, and creation.

Figure 4. Value chain of using cloud computing in a financial service institution (Gai, 2014)

3.1 Proposed cloud migration strategy and framework

Cloud migration entails two major concepts, either migrating from organization data centers to the cloud or migrating from one cloud to another cloud: After an exhaustive review of SocGen Bank, we deem Gai Value chain proposition adequate for a financial service institution. Cloud computing will provide better and agile banking services if the Gai framework is considered. In view of this, we propose a migration Plan framework for the financial organizations using Gai propositional value chain. In our framework in figure 4, we advocate cloud migration from a private data center to the cloud by proposing a framework by default called 'WHAT-CREATE-DEPLOYMENT". The following banking applications were considered: (1). Customers service application, (2) Enterprise data/ resource planning, and (3) Core banking functional system as indicated in the lift and shift activity flow diagram. See Figure 4.

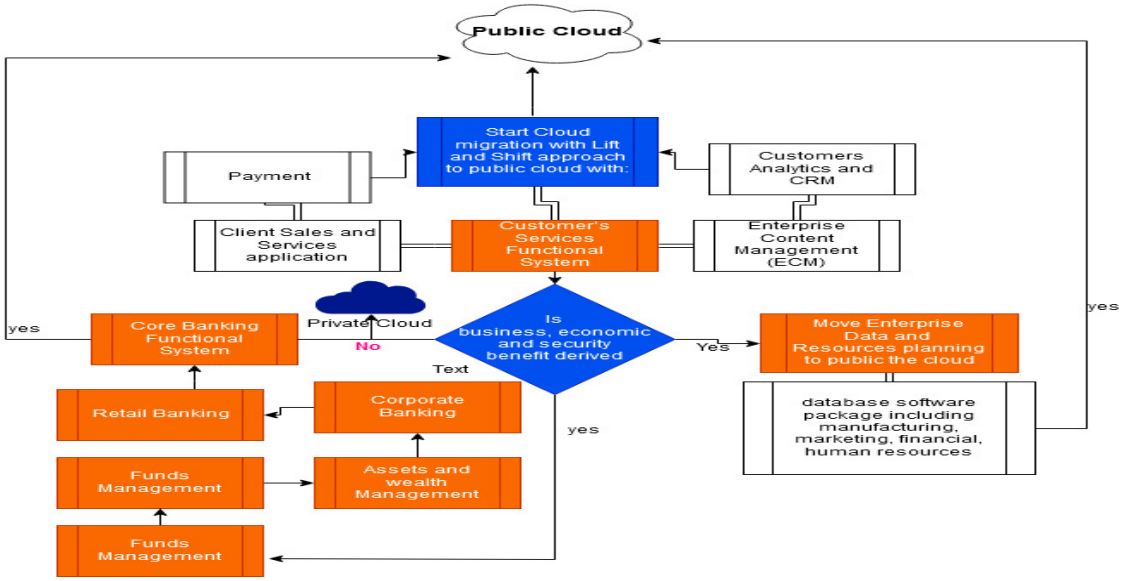

Figure 5. CLOUDSHIFT framework, a Lift, and Shift testing process (Authors defined)

The propose Cloud shift is a Lift and shift migration strategy that provides a novel and secure cloud solution to banks. This enables a business to identify what will be migrated and what will not be, depending on business, economic and security benefit derived. Following is the hypothetical "Create and Deployment model" from our *WHAT-CREATE-DEPLOYMENT* proposed for the lift and shift strategy. See Figure 5.

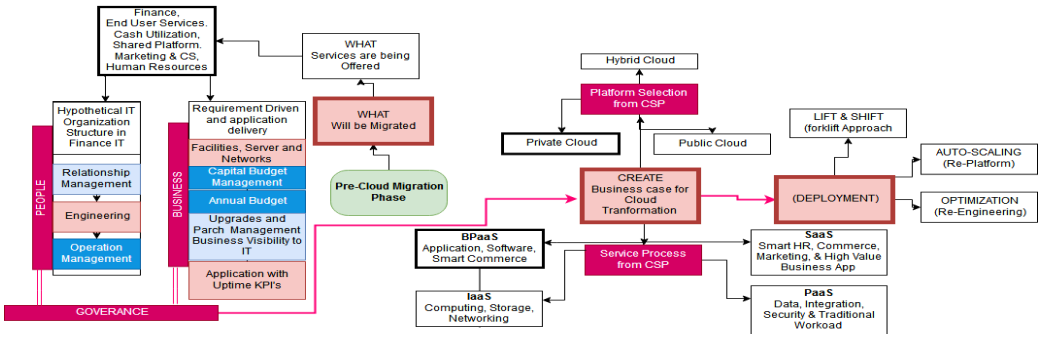

Figure 6. CLOUDSHIFT framework, a Lift and Shift core cloud migration process for Banks and Financial Services. (Authors defined)

3.1.1 Pre cloud migration phase:

Typically the Cloud entails decision making before the migration phase. This includes what banking components will be migrated and who are the stakeholders. Initially, we identified cloud banking stakeholders as the customers, the ecosystem and the bank itself. In this context, stakeholders are who eventually determine what would be migrated and not, i.e., (people, Governance, the Business itself and the Cloud providers). The "PEOPLE" comprises of IT Business Unit, (IT-BU), they decide the needs whether to scale up IT services, they handle security and they are the common determinants of security of data to be moved to the cloud. We have model "BUSINESS" as an entity that will be aligned with IT to support end-user services, marketing, sales, cash Utilization, and customers. In "Governance" there is no way we will model outsourcing management like a cloud without given recourse to the regulators. Governance includes regulatory bodies, legal and compliance. The Cloud services providers (CSP) are an entity whose platform the idea of cloud hosting and deployment is based.

3.1.2 Business case and cloud deployment phase:

Moving services to the cloud need a solid business case management, this includes the type of cloud and the services that will be engaged to deliver the applications. In the cloud deployment phase, we modeled an enterprise as an administrator, i.e. bank can lift and shift services to the private or public cloud with minor code modification. Experience IT administrators can migrate from the existing data center to the cloud. This approach offers a faster, less resource-intensive migration process; however, it may deprive enterprise of the elastic benefit of the cloud. Conveniently, our framework allows an enterprise to leverage the Cloud Service provider who provides an "Auto-scaling" cloud migration plan. Auto-scaling allows enterprise to benefit from the base cloud functionality, cost optimization, harden security and improve productivity.

An enterprise can conveniently migrate using the advanced process optimization labeled" Re-Engineering". This allows users to move other core banking components to the cloud provided the expected benefits are derived. Organizations that migrate using CSP optimization platform can modify their

applications and infrastructure to full native public cloud services. This will maximize operational cost, agility, and availability [31],[32]. Hence, establishing strong security and access management should be considered in the auto-scaling and optimization process. Further proof of concept for the shit and lift approach can be derived from Amazon's "step by step migration strategy" [33]. This demonstrates that our framework is visible.

4. Conclusion

Current banking technologies such as mobile and internet banking applications have been found to be vulnerable to insider and external attacks with such vulnerability effects that can cause more financial loss and result in customer's dissatisfaction. Findings from this study have shown that Cloud computing can help meet all these challenges. The study has *proposed a CLOUDSHIFT for* a reasonable level of data protection even though, cloud computing has its own similar exposure to security threats and privacy breaches. This study has reaffirmed that cloud computing technology can create a secure environment in which private and public sector organizations can use. The CLOUDSHIFT is safer and easy to implement from the existing bank's data center and can be managed at the local banking level. However, this research did not address in detail security model and its implementation, as future work, our proposed cloud migration framework will be integrated with adaptive Identity access management to address security and access control issues.

However, this study can be used to develop a semantically rich ontology to get into the future of cloud computing in the banking environment. The financial industry must work closely with enterprise architects to lay down a framework for starting their cloud journey.

Acknowledgments

This work appreciates UTM IDF Fellowship grant support references: UTM.J.10.01/13.14/1/128 (201902M10117), the effort of the second author was highly helpful.

6. Reference

[1] Bataev, A. V. (2017). Implementation of cloud automated banking systems innovative way of financial institutions.
[2] Bataev, A. V. (2018). Innovative Forms of Financial Institution Management: Cloud Automated Banking Systems.
[3] Chen, S., Su, T., Fan, L., Meng, G., Xue, M., Liu, Y., & Xu, L. (2018). Are mobile banking apps secure? what can be improved? Paper presented at the Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering.
[4] Barnes, S. J., & Corbitt, B. J. (2003). Mobile banking: Concept and potential. IJMC, 1(3), 273-288.
[5] AXISBank. (2017). What is the difference between Internet Banking and Mobile banking? . Retrieved from https://www.axisbank.com/progress-with-us/tech-talk/what-is-the-difference-between-internet-banking-and-mobile-banking
[6] Khrais, L. T. (2015). Highlighting the vulnerabilities of online banking system. The Journal of Internet Banking and Commerce, 20(3).
[7] Freeman, E. (2014). lessons learned from major retailers' cyber breaches, PropertyCasualty360 (2014). In.
[8] Dunnand, E. (2014). Kmart is latest victim of US retail data breach, Bus. Insid.(2014). In.
[9] ABA. (2014). Target Breach Impact Survey. American Bankers Association announced it had been hit by a malicious intrusion that targeted member online purchases and event transactions. Retrieved from https://associationsnow.com/2015/10/american-bankers-association-data-breach/
[10] Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the US retail economy: Restoring confidence in information technology security standards. Technology in Society, 44, 30-38.
[11] Giessmann, A., & Stanoevska-Slabeva, K. (2012). Business models of platform as a service (PaaS) providers: current

state and future directions. JITTA: Journal of Information Technology Theory and Application, 13(4), 31.
[12] Bejju, A. (2014). Cloud Computing for Banking and Investment Services. Paper presented at the Advances in Economics and Business Management (AEBM).
[13] Lynn, T., O'Carroll, N., Mooney, J., Helfert, M., Corcoran, D., Hunt, G., . . . Healy, P. (2014). Towards a framework for defining and categorising business Process-As-A-Service (BPaaS). Paper presented at the 21st International Product Development Management Conference.
[14] Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: issues and challenges. Paper presented at the 2010 24th IEEE international conference on advanced information networking and applications.
[15] Chen, S., Meng, G., Su, T., Fan, L., Xue, M., Xue, Y., Xu, L. (2018). Ausera: Large-scale automated security risk assessment of global mobile banking apps. arXiv preprint arXiv:1805.05236.
[16] Berghel, H. (2017). Equifax and the Latest Round of Identity Theft Roulette. Computer, 50(12), 72-76. doi:10.1109/MC.2017.4451227
[17] Silver-Greenberg, J., Goldstein, M., & Perlroth, N. (2014). Jpmorgan chase hack affects 76 million households. New York Times, 2.
[18] Mycert. (2019). MyCERT - The Malaysian Computer Emergency Response Team Incident Statistics. Retrieved from https://www.mycert.org.my/portal/index#
[19] Karim, S. S. (2016). Cyber-crime scenario in banking sector of Bangladesh: An overview. Vol-44, 12-19.
[20] Cudjoe, A. G., Anim, P. A., & Nyanyofio, J. G. N. T. (2015). Determinants of mobile banking adoption in the Ghanaian banking industry: a case of access bank Ghana limited. Journal of Computer and Communications, 3(02), 1.
[21] Kylasapathy, P., Hwa, T. B., & Zukki, A. H. M. (2018). Unlocking Malaysia's Digital Future: Opportunities, Challenges and Policy Responses. Bank Negara Malaysia Annual Report 2017.
[22] BNM. (2019). Request for Proposal for New Content Management System and Secure Cloud Hosting for Bank Negara Malaysia's Website. Retrieved from http://www.bnm.gov.my/index.php?ch=en_tender&pg=en_tender_rfp&ac=5602.
[23] Abolfazli, S., Sanaei, Z., Tabassi, A., Rosen, S., Gani, A., & Khan, S. U. (2015). Cloud adoption in Malaysia: Trends, opportunities, and challenges. IEEE Cloud Computing. doi:10.1109/MCC.2015.1
[24] Hon, W. K., & Millard, C. (2018). Banking in the cloud: Part 1–banks' use of cloud services. Computer Law & Security Review, 34(1), 4-24.
[25] BNM. (2018). Outsourcing. Central Bank of Malaysia Retrieved from http://www.bnm.gov.my/index.php?ch=57&pg=137&ac=752&bb=file.
[26] Capgemini, E. (2015). World retail banking report. In: Pridobljeno.
[27] Ryan, P., Schneider, S. A., Goldsmith, M., Lowe, G., & Roscoe, B. (2010). The modelling and analysis of security protocols: the csp approach: Addison-Wesley Professional.
[28] Asadi, S., Nilashi, M., Husin, A. R. C., & Yadegaridehkordi, E. (2017). Customers perspectives on adoption of cloud computing in banking sector. Information Technology and Management, 18(4), 305-330. doi:10.1007/s10799-016-0270-8
[29] SocGen. (2015). Societe Generale is accelerating its Cloud strategy. Retrieved from https://www.societegenerale.com/en/newsroom/Societe-Generale-accelerates-its-cloud-strategy
[30] Gai, K. (2014). A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances. Int'l J. of Computer Applications, 95(3), 40-44.
[31] Kim, W., Kim, S. D., Lee, E., & Lee, S. (2009). Adoption issues for cloud computing. Paper presented at the Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia.
[32] Misra, S. C., & Doneria, K. (2018). Application of cloud computing in financial services: an agent-oriented modelling approach. Journal of Modelling in Management. doi:10.1108/JM2-12-2017-0131
[33] Chauhan, S., Jaiswal, M., & Kar, A. K. (2018). The acceptance of electronic voting machines in India: A UTAUT approach. Electronic Government. doi:10.1504/EG.2018.093427