Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure

Abhishek Mahalle

School of Management and Enterprise

University of Southern Queensland
Toowoomba-Australia

u1104050@usq.edu.au

Jianming Yong

School of Management and Enterprise

University of Southern Queensland
Toowoomba-Australia

Jianming.Yong@usq.edu.au

Xiaohui Tao

School of Agricultural, Computational and Environmental Sciences
University of Southern Queensland
Toowoomba-Australia

Xiaohui.tao@usq.edu.au

Jun Shen

School of Computing and Information Technology

University of Wollongong
NSW 2522 Australia

jshen@uow.edu.au

Abstract – Cloud computing architecture and infrastructure has received an acceptance from corporations and governments across the globe. Cloud computing helped to reduce cost of management of physical and technical infrastructure at the same time has made information systems available for locally & globally deployed work force. Cloud computing infrastructure provides access to data and applications from any location and this has made organizations to keep evaluating privacy and security framework. Banking and financial services have data and applications which are internally developed to remain ahead of competition. This data and applications becomes the Intellectual Property (IP) that serves specific business processes and goals. When this data and applications can be accessed from remote locations, there may be a potential risks of data leakages and erosion of IP over a period of time. With an adoption of cloud computing, banking and financial services industry continues to be under strict regulatory and compliance framework to maintain privacy of data and security of systems. Privacy and security of cloud architecture infrastructure continues to be the challenge across the globe. In this paper, various aspects of cloud computing related to data privacy and system security for banking and financial services industry have been introduced.

Key Words – Cloud Computing, Data Privacy, Data security, Systems Security,

I. INTRODUCTION

The term Cloud computing, the word 'cloud' is the metaphor for the internet. The term 'cloud' is derived / inspired from old symbol of cloud often use to represent internet in flow charts [1]. Through cloud computing, information systems resources that include application, data, network, storage devices and servers are made accessible and available for use. The National Institute of Standards and Technology (NIST, U.S.A.) defines cloud computing as *"a model for enabling ubiquitous, convenient, on-demand network access to the shared pool of configurable, resources that can be rapidly provisioned and released with minimal management efforts or service provider interaction"* [2]. Cloud computing is designed using the unique features of Infrastructure as a services (Iaas), Platform as a Service (PaaS) and Software as a Service (SaaS). Cloud computing has deployment models defined based on type of availability of cloud computing resources and accessibility. Main deployment models for Cloud computing are private, public, hybrid, community, inter-cloud and multi cloud.

Banking and financial services industry directly works for economy and so remains matter of national importance and for livelihood of people [19]. As a part of security implementation in bank's technical infrastructure various security checks in the form of digital certificates for devices, one time password token, browser protection policies, transaction monitoring, anti-money laundering and fraud detecting systems are in place [20]. These devices and systems gives robust security measures for the banks at the same time they meet the regulatory requirements to protect data of the customers. With evolution of internet, corporation operating in Banking and financial services started offering their products and services via internet based platform and machines (ATMs) located in remote locations without making customers to visit its branches. These online banking services offers flexibility and convenience in access to banking services [26]. Banks and financial services offer variety of financial products and services to its retail & corporate customers that include internet banking services, mobile banking facility, ATM withdrawals & deposits, Credit card facilities, Debit card facilities, EFTPOS terminals, account maintenance services, stock market and treasury products and forex service. These services can be availed without visiting the actual branch of the bank. These products can be accessed via internet. This helps bank to achieve operational efficiency through faster delivery of services, reduce cost of operation of branch, work with lesser staff, provide competitive services, make faster decision in real time for customers and focus on customer needs to offer personalised services. Through cloud infrastructure banking and financial services also meet

regulatory & compliance of central bank. When the technology infrastructure offering these services is located at secured site and both staff & customers accessing it from various remote locations – data privacy and systems security continues to be the top priority with zero tolerance for risk. [26]

In order to secure cloud computing infrastructure from potential threats and vulnerabilities at the same time to provide seamless accessibility to various users makes it necessary to put additional security, risk management and business continuity framework in place. With emergence of new technologies, interconnection of various devices, increased use of mobile devices, widespread social networks, proliferation of data and different regulatory norms in various countries makes security framework for cloud architecture even more complex and subject to constant evaluation [22].

Banking and financial services industry has cyber security department. This cyber security department deploy some of common security measures in order to secure systems. These security measures include Secured Socket Layers (SSL – for secure connection), vulnerability and assessment testing of systems, database encryption, Firewalls (to control flow of traffic), Intrusion detection systems (IDS), Network intrusion prevention systems (NIPS), quarantining unknown systems, Domain Name systems (DNS), password protection mechanism and SMS alerts to customers. [21] All of these devices and security systems are to secure cloud architecture infrastructure in banking and financial services, however, there are still threats and vulnerabilities due to external agents or accidental errors by internal staff; and so the data privacy and systems security remains a key concern.

II. REVIEW OF LITERATURE

a. *Data Privacy:*

Data privacy refers to appropriate use of data provided to corporations for agreed purposes. Data collected by customers to meet the business requirements and need of customer should be sufficient; it should be accepted by customer and with complete disclosure information being provided to them. Australian Federal Government continues to impose penalty for not providing enough disclosure to customers about data privacy. In banking and financial services industry, the data collected is to ensure identity of customer and it is called as Personally Identifiable Information (PII) [14]

Data Security:

Data security refers to confidentiality, availability and integrity of data [15]. 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 in order to bring desired end to data collected. [13]

b. *Information Privacy:*

Information privacy refers to the desire of individuals to control or have some influence over data about themselves [16]. Information age has lead 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 [16].

d. Systems Security:

Systems security refers to its ability to protect from external attacks (Deliberate or accidental). Secured systems makes them dependable and available when required, thus makes them reliable. Secured systems when function as expected without failures and any delays helps achieve desired objectives for banking and financial services industry.

Damage to systems security will lead to:-

a. **Distributed Denial of services (DDoS)** – Quality of services are degraded or services are unavailable due to failures of multiple infrastructure and network resources. This will lead to unavailability of systems to customers to carry out financial transaction and working staff to perform their operational duties effectively. This will in turn disrupt the normal flow of life and affect economy as a whole. In case of DDoS, the attack may not be detectable as the sources of attack may be from various locations and virtual. This will increase the recovery time required for systems to return to normal business activities.

b. **Corruption (Tampering) of programs and / or data** – Programs and / or data are modified in unauthorised way. Depending upon the type of program corrupted (financial processing, customer data, storage systems, connectivity devices etc.); the impact will be either financial or operational loss or both. In banking and financial services industry, a small introduction of

unacceptable logic in program may not provide the desired outcome from the program and will directly impact both customer and internal working staff. If the website enabling internet banking is updated with informative links and web pages with incorrect scripts, whole internet banking platform may not be available to carry out financial transaction.

c. **Disclosure of Confidential Information** – Information may be exposed to people who are not supposed to access it. The amount of data stored in banking and financial services is huge and has variety due to multiple departments. As this data in stored on shared network drive, access to right users is important to avoid data leakages, tampering and theft.

d. If the unauthorized person deletes this data which cannot be retained or retaining process takes long time then, it will directly impact the work of bank employees.

Any compromise in system security will lead to exposure of risk to assets, loss (monetary or otherwise), vulnerability to future attack or exploitation and loss of control over system.

Systems security includes controlling access to physical system and protecting it against harmful network access, code injections and data corruption.

In order to secure system security, it is important to understand the type of threats. Below are common threats to system:

Backdoor: If someone is able to bypass normal authorization to access system because of poor system configuration, the person may access both personal and financial information. This personal information can be used to open accounts and carry out financial transaction. The nature transaction may look genuine and difficult to detect. Also by the time the transaction is detected as unauthorised the culprits may escape leaving bank with legal and financial implications.

Direct-access attacks: An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, key loggers, covert listening devices or using wireless mice. The unauthorised access may lead to creation of the vulnerabilities in core systems and *tampering of the data which* will lead to constant data leakages and loss of confidential information (personal or financial) on regular basis.

Eavesdropping: Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network (or two parties). If the communication between host and network which involves disclosing personally identifiable details, account numbers, credit card details etc. is accessed by unauthorised person; the information can be used in future to carry out the financial transaction or steal identify of the person. This will lead to loss of customer information and financial penalties to bank and financial services.

SMS Spoofing: Through SMS spoofing a user receives a SMS from unknown source asking to provide account details and credentials in order prevent theft or risk of loss of money; through this customer details can be captured during the process and can be used later to steal money from account.

TCP/IP spoofing: In this type of vulnerability, an email is sent to user (bank's customer) that appears from the genuine source, this technique is powerful as it bypasses the firewall as IP address looks to be external. This method gives access to financial system (server) to external parties which can damage the system as a whole or steal information.

Privilege escalation: Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full unrestricted access to a system.

Phishing: Through phishing, a customer of the bank may be prompted to enter credentials of the account which can be stored in system and used in future to carry out financial transaction. Due to phishing, bank's customer may lose personal information and financial wealth which will look like authentic for both customer & bank and will go undetected.

Vishing: Vishing is use of voice and phishing, in which a person pretends to be calling from bank or financial institution in order to access private and financial information from the public [21]. Once, the person gives details (Account number, card information etc.), they are used to perform financial transaction (theft) from bank account which looks genuine and by the person, which leads to financial loss for person. This act can also be termed as *Social Engineering*.

Cross site scripting (XSS): XSS is the method to include malicious codes in webpages visited by the user. The data entered by user are later used to create fake identifies, open accounts and perform financial transaction which will cause financial losses to actual customer or person [21].

Pharming: Pharming is the technique in which the DNS of the bank or financial institution is attacked towards genuine website to provide personal details (and credit / debit card numbers) and account credential to steal money and information of customer [21].

Insider Threats: Insider threats are when the employee of the bank or financial institution access and modifies data accidentally which interrupts the everyday operations.

Attack on OTP: One time password (OTP) is authentication of the user and its credentials while performing the financial transaction. In this type of vulnerability. [21]

1. Man-In-The-middle (MITM): Information of the user can be stolen when transaction in process and same information can be used to perform financial transaction (Theft) later.

2. Man-In-The-Browser (MITB): Information of the user is captured from website using a fake form and same information is used to create new accounts and financial transaction to steal money.

3. Man-In-The-PC Attack (MITPC): In this, weaknesses of the hardware are exploited in order to secure OTP which may be used to perform financial transaction.

III. INFORMATION SECURITY MANAGEMENT IN BANKING AND FINANCIAL SERVICES

Banking and financial services considers below measures for information security and privacy while using cloud computing architecture infrastructure: [27]

A. Identity Access Management (IDM): 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. 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. An IDM system helps to protect access levels of users by identifying them based on roles and responsibilities.

B. Access Control and Access Logging Mechanism: Cloud services delivery models has complex architecture. This complex architecture needs to be integrated with access control interfaces that demands policy neutral access specification and enforcement framework. In order to control access, Single Sign-On (SSO) method is implemented which gives access to user across multiple applications in banking and financial services. These access method confirms one time identification of user based on "Single User Id / Network Id" and password that meets security policy. Access logging or User Activity monitoring is collecting and storing the logs of users who are using, operating and maintaining cloud infrastructure. User activity monitoring helps to keep record of the all the changes performed on data and applications over cloud infrastructure.

C. Roles Based Access Control and Malicious Insider: Cloud computing is shared infrastructure for employees, customers and third party service providers. Role Based Access control governs the access to information and ensure that users have right level of access as per roles and responsibilities. Role based Access control is importance to avoid exposure of data to user that are not supposed to use it in any form. Malicious insiders is user with access to system at the same time lack of identity, authentication and having control over use of system. With privilege accesses, users can view and use information that may be termed as data theft. In order to maintain confidentiality of business information, access control and control over malicious insider is considered.

D. Governance and Compliance: Cloud security governance consists of leadership, organization structure and processes that safeguard information. Compliance is requirements from government regulatory bodies to adhere to rules in order to function within framework. Governance and compliance ensure the strategic alignment of system with customer, business and employee needs. Governance and Compliance department in banking and financial services industry help to provide over all working, monitoring, measuring and communication framework to keep cloud architecture secure. [26]

E. Service Level Agreements (SLAs) and Contracts with Cloud Service Provider (CSP): Cloud computing infrastructure is availability of computing resources from any remote location at any time. In order to meet these requirements, cloud services should be monitored and maintained well. Cloud service providers are located across geographies, so the contracts is between legal jurisdictions of two nations. These contracts must be in accordance with needs to cloud infrastructure user. These contracts must acknowledge data privacy and data security related aspects to protect sensitive details of various customers. So, SLAs and contractual agreements are considered as important for smooth running of cloud services, which in turn help smooth running of banking operations. SLAs help to define

response time to be met and response steps to be taken when issues are encountered during work and non-work hours. SLAs ensures that services are restored within the stipulated timeframes and in case of failures; appropriate financial penalties are imposed on cloud service providers. This way banking and financial services are able to meet for losses occurred due to down time. In the event of data theft and breaches of data security related policies, contractual agreements helps to ensure necessary actions are in place to ensure further damage or any further data losses are prevented. [26]

F. Secure Deletion of Data: 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 has to be performed in order 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 in order 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. [26]

G. Forensic capabilities: Forensic capabilities involve ability to retain data from system storage devices for deeper level of investigation in case of financial crimes to support investigations and produce those devices to meet legal requirement. With cloud infrastructure being private for bank, accessing logs from storage devices is easier through internal approvals. Also, as part of contractual agreements, cloud services provider accepts to meet these requirements from banking and financial services corporations. [26]

H. Cloud computing and outsourcing: 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 change over the period, so there will be multiple people having access to system and data. Banking and financial corporations 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 (legal, disciplinary or otherwise) and enforce penalties to enforce stricter security measures. [26]

IV. CONCLUSION

Cloud computing has reduced cost required to manage IT infrastructure by developing a robust and secure architecture, however, for institutions like banks and financial services which has financial data of customer and corporations, cloud based model brings long term risks and threats of potential losses due to uncertain or adverse situations which directly impacts profitability and reputation and invites heavy penalties from regulatory bodies. 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.

REFERENCES:

[1] Hassan, Qusay F.; Riad, laa M.; Hassan, Ahmed E. (2012). "Software reuse in the emerging cloud computing era". In Yang, Hongji; Liu, Xiaodong. Understanding Cloud Computing (PDF). Hershey, PA: Information Science Reference. pp. 204–227. ISBN 978-1-4666-0897-9. doi:10.4018/978-1-4666-0897-9.ch009. Retrieved 11 December 2014.

[2] Peter Mell and Timothy Grance (September 2011). The NIST Definition of Cloud Computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce, p2-p3, NIST Special publication, September 2014

[3] Ackermann et. al. / “Perceived IT Security Risk of Cloud Computing, 33rd, p.3, International Conference on Information Systems, 2012

[4] Foley, John. "Private Clouds Take Shape". InformationWeek. Retrieved 2010-08-22, p2-p14

[5] Rouse, Margaret. "What is public cloud?” Definition from Whatis.com. Retrieved 12 October 2014, p1-p13

[6] "Kevin Kelly: A Cloudbook for the Cloud". Kk.org. Retrieved 2010-08-22. http://kk.org/thetechnium/a-cloudbook-for/

[7] "Vint Cerf: Despite Its Age, The Internet is Still Filled with Problems". Readwriteweb.com. Retrieved 2010-08-22.

[8] "Intercloud is a global cloud of clouds". Samj.net. 2009-06-22. Retrieved 2010-08-22. https://samj.net/2009/06/22/the-intercloud-is-a-global-cloud-of-clouds/

[9] "SP360: Service Provider: From India to Intercloud". Blogs.cisco.com. Retrieved 2010-08-22.

[10] Canada (2007-11-29). "Head in the clouds? Welcome to the future". The Globe and Mail. Toronto. Retrieved 2010-08-22

[11] Addressing Cloud computing security issues, Dimitrios Zissis, Dimitrios Lekkas, Future generation computer systems, Volume 8, Issue 3, March 2012, p 583 - p 592

[12] Cloud Security Alliance, The Treacherous 12, Cloud Computing Top threats in 2016, p. 7 – p.35

[13] An overview of the security concern in enterprise cloud computing, Anthony Bisong et. al. , International journal of network security & its applications (IJNSA), Vol.3, No.1, January 2011, P.36

[14] A survey of Cryptographic approaches to securing Big-Data Analytics in Cloud, Sophia, p1-p2, 978-1-4799-6233-4/14,@IEEE, 2014

[15] Privacy in the Digital Age: A review of Information privacy research in Information systems, France Belanger, MIS Quarterly, Vol. 35, No.4, pp 1017-1041/December 2011

[16] Data Intensive Applications, challenges, techniques and technologies: A survey on Big Data, C.L. Phillip Chen, C.-Y. Zhang / Information Sciences, 275, (2014). p 314 – p 347

[17] The Last Line of defence: Motivating Employees to follow corporate security guidelines, Scott R. Boss, Laurie J. Kirsch, Twenty Eighth International Conference on Information Systems, Montreal 2007, p3 – p 6

[18] Cyber security challenges: In brief, Eric A. Fisher, Congressional research services, p2. August 12, 2016

[19] Improving security of interest banking system using three –level security implementation, Emeka Reginald Nwogu, IRACST – International Journal of computer science and information technology & security (IJCSITS), ISSN: 2249-9555, Vol.4, No.6, December 2014, p.168-169

[20] Zarka Zahoor, Jamia Hamdard University, New Delhi, India, International Journal of Computr Applications (0975 – 8887), Volume 144 – No.3, June 2016, p.27-p.28

[21] Mounia Zaydi, Department of computer science, FSTS Hassan 1st University, Settat Morocco, Information systems security governance, Technology intelligence perspective, 978-1-5090-6227-0/16

[22] Alok Gupta and Dmitry Zhdanov, Department of operations and decision sciences, Carlos school of management, University of Minnesota, MIS Quarterly Research Article, vol.36, No.4, page 1109-1130,/ December 2012, Growth and sustainability of managed security services network: An economic perspective

[23] Jorge Uffen, Personality trait and information security management: An imperial study of information security executives, Information systems institute, Leibniz University, Hannover, p1-p3, 2012

[24] Qian Tang et al, Reputation as public policy for internet security: A field study, Thirty third international conference on information systems, p 2– p17, Orlando 2012,

[25] Ioannis Koskosas, Communicating Information system goals: A case in internet banking industry, department of information communication technologies, engineering, university of western Macedonia, Greece, p6-p8, UDC 004.738.5:336.71, 10.2298/CSIS090107K

[26] Secure use of cloud computing in the finance sector, Good Practices and recommendations, European network for network and information security, p.7-p36, December 2015.

[27] Security and privacy challenges in cloud computing environments, Hassan Takabi, Jmaes Joshi, p.5- p.8, IEE Security and privacy magazine, January 2011

[28] Informations systems threats and vulnerabilities, Daniyal M. Algazzawi, Sydem Hamid Hasan, Mohhamad Slim Trigui, p.1-p.7, International Journal of computing applications (-975-8887), Volume 89 – No.03, March 2014,

[29] Security Challenges in Public cloud, Kui Ren, Cong Wang and Qian Wang, Illionis Institute of Technology, January-February 2012, p.4-p.7

[30] An analysis of security issue in cloud computing, Keiko Hashizume, David G Rosado, Eduardo Fernandez Madina, Eduaro B Fernandez, Journal of internet services and application, 2013, p.1-p.13

[31] A role-involved purpose-based access control model, ME Kabir, H Wang, E Bertino, Information Systems Frontiers 14 (3), 809-822, 2012

[32] Special issue on Security, Privacy and Trust in network-based Big Data, H Wang, X Jiang, G Kambourakis, Information Sciences: an International Journal 318 (C), 48-50, 2015