IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 2, February 2016.
www.ijiset.com
ISSN 2348 – 7968

Identifying and Mitigating Against Risks to Privacy of Personal Information in Cloud Computing

Rashid Husain
Lecturer, Department of Mathematics & Computer Science
Umaru Musa Yar'adua Uniersity, Katsina, Nigeria.

ABSTRACT

Cloud computing has brought with it immense possibilities as far as processing of information and the pooling of resources is concerned. Cloud computing has also been noticed by the public sector, as Governments all over the world have undertaken to introduce what has come to be known as e-Government, the provisioning of Government services and communications via Web based applications, rather than the traditional means of in person contact and paper based collection of personal information. While the move to Web based Government has been occurring for the last 25 or so years, a new development in this area is the introduction of Cloud computing and Cloud-based computing platforms, most notably Software-as-a-Service (*SaaS*) in the provisioning of these services. The computing and efficiency potential of this technology cannot be disputed, yet it's important to recognize that taking advantage of this computing power does come at a price. This paper will make it easier for government agencies to make informed decisions about whether or not to migrate data and applications into the cloud. The identification and analysis of potential risks to data security and personal information has drawn together key information from a multitude of both academic and industry sources to make such a decision plausible.

Keywords: Cloud computing, Security, Personal Information, Privacy, Technology, Privacy by Design (PbD).

INTRODUCTION

The National Institute of Science and Technology defines cloud computing as being a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2,4]. One of the ways in which cloud computing is able to compete with traditional modes of computing is to reduce the costs through the pooling and sharing of the available resources. Traditionally, if a corporate entity wanted to deploy a new database, they would acquire the

ISSN 2348 – 7968

hardware, software and staff with technical knowledge to launch and maintain the network. This would generally result in under usage of the network, at least in the initial stages of deployment and operation. In fact, Amazon discovered that their networks were being run at 10% capacity at any given time, to account for occasional spikes in the demand and usage of the network [2,7]. The corporation would have to front 100% of the costs associated with the roll out, even though it would take years to reach anything above the 10% utilization mark, especially since the system would continue to be upgraded and expanded throughout its life to prevent over utilization and account for times of increased demand on the resources. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale.

MITIGATING AGAINST THE RISKS TO PRIVACY

Cloud Computing risks have been identified by many scholars and practitioners in the field of privacy protection [9,10], which has resulted in risk mitigation schemes and best practices having been put forward to assist both corporations and public bodies with the decision to “cloud or not to cloud”. The most widely used tool for risk assessments in the field of privacy are Privacy Impact Assessments (PIA), which are a way for organizations to systematically address and identify privacy issues within information systems, while at the same time taking into account future consequences of a current or proposed action [7, 13].

“Risk management is a process that manages inherent risk, including fraud, non-compliance with laws, regulations, costs, competition and change by identifying: potential risk, potential impact of that risk on organization, controls that reduce the risk, quality of the controls, and possible impact of any residual risk” [18, 19].

One question that often arises is: when should a PIA be undertaken? Meaning, in what circumstances at what stage and does an organization need to complete a PIA? Ten criteria have been identified as warranting the completion of a PIA [14, 19, 21]:

1. Major changes to existing programs
2. New programs
3. New delivery structures and partnerships
4. Changes in the technology
5. Additional systems linkages
6. Enhanced accessibility
7. Service monitoring

ISSN 2348 – 7968

8. Delivery channel management
9. Data warehousing
10. Reengineering business processes

The underlying assumption being of course, that the project or system must be dealing with the collection, use or disclosure of personal information. There are several stages to the PIA process, including [4, 9, 21], [13, 16, 17]:

1. Project initiation is to determine if a PIA is required. Is personal information being collected?
2. Data flow analysis: examine how personal information will be collected, used, disclosed and retained.
3. Privacy analysis: identification of the possible risks to privacy
4. Privacy impact analysis: a discussion of the possible risks, associated implications and possible remedies.

Eight critical principles have been put forward to effectively deal with cross-border privacy impact assessments [11, 13, 14].

1. Organizational responsibility for the ownership of personal information (PI)
2. Identifying the purpose for which the PI is kept
3. Limiting data collection to business objectives
4. Required consent
5. Limitations on the retention of PI information
6. Accuracy of data
7. Data security
8. Training and communication

For each of the principles, a series of questions, which delve progressively deeper into each of the aspects needs to be asked and answered in order to arrive at a fully informed decision as to whether or not the intended cross-border migration of data is fully compliant with jurisdictional and data security requirements. It is imperative that the questions are answered in a comprehensive and truthful manner. As a result of the lack of international standardization for the PIA process, with “critical variations in implementation of PIAs” [16, 17] across various jurisdictions, the principles listed above are of critical importance, to ensure that all issues in the myriad of legislative and jurisdictional differences have been addressed. [15, 16] have proposed the creation of a PIA tool as a kind of “decision support system”, which would rely on the input from subject matter experts. What’s more, the PIA tool would itself be a cloud-based (*SaaS*) application relying on a knowledge base (KB) that would be populated, on an on-going basis by

ISSN 2348 – 7968

subject matter experts from across all of the jurisdictions that utilize PIAs. The tool would be accessed by "end users" via a Web User Interface, where the PIA tool would prompt the user to answer a series of contextually generated questions. Based on the initial questions, the tool would then prepare a project profile with more detailed questions that would form the final PIA.

A different approach that has been characterized as being complimentary to traditional PIAs is the concept of Privacy by Design (PbD), "strongly advocated by the Canadian privacy commissioner (Ontario) Ann Cavoukian. The origins of PbD can be traced back to a 1995 report by the Dutch data protection authority and the Canadian privacy commissioner" [8, 10, 21]. The PbD framework establishes a set of best practices for the implementation of privacy enhancing characteristics into Cloud computing architecture [19].

The original concept of PbD relied heavily on the promotion of the implementation of Privacy Enhancing Technologies (PETs) [11, 12]. PETs have been broken down into four separate functionalities, each with a distinct focus; the aim of all of being protecting personal privacy [10, 11]]:

1. Subject oriented PET: aim to anonymize a data-subject or to offer a pseudo-identity
2. Object-oriented PET: aim to conceal what is exchanged
3. Transaction-oriented PET: aim to conceal occurrence of a transaction
4. System-oriented PET: any combination of the previous three orientations

All of the characteristics and functionalities combined form a more decisive privacy protecting and privacy enhancing mechanism. They are also key players in the strategies and techniques for mitigating privacy risks in cloud computing environments, which have been characterized as being "disruptive innovation which challenges norms and forces out-of-the-box thinking…as individual or enterprise-level consumers shy away due to data security and/or privacy concerns" [9, 13]. It is undoubtedly the case that the implementation of data security and privacy mechanisms, cloud providers can alleviate many of the fears and concerns communicated by both industry and government as the main barriers towards the adoption of the technology.

A recent IBM survey found that 77% of respondents believed that the adoption of cloud computing makes protecting privacy more difficult and 50% expressed concern about data breaches and loss [13]. These perceptions should be clear indicators for the direction that the CSP industry needs to take, in order to ensure greater uptake of the technology and provide "assurance that providers are following sound security practices in mitigating the risk facing both customer and the provider" [7, 9]. Yet that has not been the case, as we see the identification of issues surrounding the adoption of schemes like PbD, which pose serious barriers towards its adoption by CSPs [16, 17].

ISSN 2348 – 7968

TECHNOLOGICAL AND SYSTEMIC SOLUTIONS

A variety of tools and mechanisms have been proposed to ensure that personal information remains secure and protected. None of the solutions alone can stand up to the multitude of risks that have been presented as emerging from the very fabric of cloud computing architecture. Assuming that encryption alone is the answer to a secure solution that will prevent personal information from being breached or otherwise subjected to unauthorized access would be a mistake.

Ten security criteria have been identified to ensure the optimal database security [13, 14, 15]:

1. User identification and authentication – In a safe and unambiguous manner.
2. Identification of robustness and authentication – Making it difficult to usurp or hijack identities.
3. Rights separation – Distinguish types of users and their predefined actions and privileges.
4. Data Access Control – Allowing for various types of access only to authorized users.
5. Integrity and Confidentiality of the stored data – Ensure only authorized users can read or modify the stored data.
6. Communication ciphering – Ensure the integrity and confidentiality of requests and data exchanges between various equipments implementing or using the database.
7. Data concealment- Concealing real data in false data to conceal the actual volume of data.
8. Data masking- Use irreversible processes to replace sensitive data and ensure that the original data cannot be restored.
9. Audit services- Log all events concerning access to the DBMS and ensure integrity of the logs.
10. Certification- Evaluation Assurance Level (EAL) certification that allows for evaluation of IT applications.

There is currently a multitude of technological and some systemic tools that could be leveraged to address the issues raised, to ensure an adequate and optimal level of database security and as a result security of the personal information within those databases. These tools include, but are not limited to [20, 23]:

- Multi-factor Authentication
- Privacy Violation Detection and Monitoring
- Data Encryption
- Privacy Manager

ISSN 2348 – 7968

- Trusted Third Party (TTP)
- Data Concealment
- Data Ambiguity and Preview

Anonymity based method

This method proposes to run all personally identifiable data through an anonimization algorithm, stripping the data of personal QI, which would result in there no longer being a need to protect the anonymized data. It goes further to say that CSPs could freely mine such anonymized data, as there would no longer be a risk to personal privacy [24]. Given the level of information sharing and flow as well as cross referencing of multiple databases, possibly in several jurisdictions, this approach may not prove to be as effective as envisioned.

Perimeter Protection, Trusted Zones and Federated Clouds

As a result of the difficulties of perimeter security in enterprise applications, CSPs need to establish zones of trust, making the virtual machines (VM) "self-defending" thereby moving the location of the perimeter to the VM itself [19, 23]. By organizing Cloud infrastructure into distinctive security domains, it is possible to create a "collection of single clouds that can interoperate i.e. exchange data and computing resources through defined interfaces…each single Cloud remains independent but can also interoperate with other clouds" [17] also referred to as Federated Clouds. Trusted Zones on the other hand can be used to achieve better isolation of data and applications at the network, device or application level [19].

Certificate based authorization and SSL Certificates

Due to the non-traditional relationships between resources and users in a Cloud environment, the management of identities and permissions is more difficult. A scheme that has been developed to make identity and permissions management more attainable is the issuance of certificates by a third party Public Key Infrastructure (PKI) facility that would act as an intermediary in enforcing access control through web portals. The certificates carry with them a combination of attribute-value pairings and information about the principals to whom they apply [22].

SSL Certificates on the other hand are used to provide certification status to portals and services online, thereby communicating to users that their information is being handled by a secure partner, certified by one of the Certificate Authorities (CAs) [14]. The CA is responsible for verifying the identities of partners to whom they grant certification. The SSL encrypted connections help to secure millions of internet transactions daily. While this scheme has provided a certain degree of security as far as trust is concerned in the processing of data, especially financial data over the Web, it is not without weakness. Depending on the level of

ISSN 2348 – 7968

certificate purchased, the identity verification may be severely limited, and require nothing more than a reply to an email to establish administrative privileges [17, 18].

Information Security Management

In order for any of the potential solutions to data integrity and privacy protection listed above to be effective, it's important that organizations identify and implement Information Security Management Systems (ISMS), which are systems that provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets [17, 18, 19]. There are three main phases to the implementation of such systems:

1. Defining security requirements – including identifying security goals/objectives, conducting risk analyses and detailing those risks in the security policies.
2. Enforcing security requirements – identifying security controls to be used and implementing and configuring those controls based on the identified requirements.
3. Monitoring and improving security – including current status, existing issues and improvements to current security controls.

In order for a successful ISMS to be implemented and in order for it to function properly, both the client and CSP must strive for a common understanding and the building of a "quality" relationship and system. Some definite indicators of the lack of quality in such a system have been identified, with the first three having a direct connection to security and privacy concerns [13, 15]:

1. Lack of realism in administering the application of computing.
2. Lack of reliability in the operation of the continuing specific aspects of the organization's investment in computing.
3. Lack of trustworthiness in the performance of the actual application. In the computing environment there is no such thing as acceptable error or relative accuracy. If the data being considered is not absolutely correct then it is absolutely wrong.
4. Lack of well defined profitability in computing activities.

Realism in the administration of the application of computing is critical, otherwise the potential exists for the client and CSP to be agreeing to very different levels of service and protection without taking into account the realities of what is possible and what is merely a wish. The realities and expectations of the security requirements of the client must be presented to the CSP, and adequate "assurance that providers are following sound security practices in mitigating the risk facing both customer and the provider" [11, 18]. CSPs have been urged to adopt newly

ISSN 2348 – 7968

emerging approaches to the security of information systems, which are quite different than traditional security systems.

These include: Security-as-a-Service (SECaaS) and Data protection and privacy-as-a-Service [21, 22]. SECaaS utilizes the provisioning of security resources through the cloud to the infrastructure or software itself or to the customers' own systems [23]. The interest in and uptake of SECaaS appears to be on the rise, with predictions that cloud-based security service will triple in many segments by 2013.

These security management expectations need to be communicated to the CSPs during the negotiation of the Service Level Agreement (SLA) to enable organizations to maximize the security and management of their records in the Cloud [5, 6]. Once these assurances have been secured and documented, CSPs must allow for independent 3rd party audits of their systems to take place, to provide for an unbiased assessment of the security procedures and mechanisms as well as their effectiveness or real life performance [27].

Only this way can we achieve the trustworthiness in the functionality of the application as well as the CSP operating it.

When conducting audits and assessments, it's important to take into account the assessment of the quality of the system that has been designed or implemented, which can be realized using one of the following approaches [25, 26]:

1. Identifying and abandoning any product or service that fails to conform to the applicable measure of its condition or performance.
2. Constructing a product or service development and operation setting in which the lack of quality is not tolerated.

Once an audit or assessment has been completed and if it has identified deficiencies in either the operation or the design of the system, appropriate steps must be undertaken to ensure that personally identifiable information is not being compromised or is not at risk of being compromised. If such a situation is discovered however, the system must be repaired or abandoned to prevent a privacy breach from occurring or continuing, if discovered after the fact. This scenario could prove to be very challenging if the assessment is being done on a Cloud-based system, as abandonment of the application may result in abandonment of some or all data migrated into the cloud as well [14, 15].

CONCLUSION

After examining the security of personal information in a cloud computing environment, I focused on the potential risks to the security and privacy of personally identifiable data in a *SaaS*

architecture platform. I identified potential risks to privacy and security of personal information in the Cloud, and I propose strategies for mitigating against those threats.

I pointed out significant threats to data security and privacy and addressed some shortcomings of the methods currently proposed for identifying and mitigating against the risks to privacy in applications.

The deployment of EAS on the cloud using the SaaS platform does not offer adequate safeguards and does not substantially minimize the risks that are associated with the SaaS platform**.** In fact, such a deployment can actually result in a false sense of security. A sense of security, which cannot be guaranteed or reconciled because of the architecture and inherent weaknesses of that deployment model as it relates to data security and privacy protection.

REFERENCES:

[1] Abu-Nimeh, Saeed & Mead, Nancy, (2010). " Privacy Risk Assessment in Privacy Requirements Engineering", *Second International Workshop on Requirements Engineering and Law*.

[2] Almorsy, Mohamed, Grundy, John & Ibrahim, Amani, (2011). "Collaboration-Based Cloud Computing Security Management Framework", *IEEE 4th International Conference on Cloud Computing*.

[3] Amazon Web Services, (2008). "Overview of Security Processes".

[4] An Oracle White Paper (2011). "Cloud Candidate Selection Tool: Guiding Cloud Adoption".

[5] Andrei, Traian, (2009). Cloud Computing Challenges and Realted Security Issues.WUSTL.

[6] Armburst, Michael, et al., (2009). "Above the Clouds: A Berkley View of Cloud Computing", Technical Report No. UCB/EECS-2009.

[7] Ausloos, Jef., (2012). "The 'Right to be Forgotten' – Worth remembering?", *Computer Law and Security*.

[8] Barnatt, Christopher, (2011). "A Brief Guide to Cloud Computing: An Essential Guide to the Next Computing Revolution", *Constable & Robinson*.

[9] Blandford, Richard, (2011). "Information Security in the Cloud", *Network Security*.

[10] Blauer, Fred, (2009). "Cloud Computing: Are open source business systems and software as a service the next generation of ERP?", *CA Magazine*.

[11] Burns, Michael, (2010). "Work in process: Using Technology to improve the way you do Business", *CA Magazine*.

[12] Calloway, Timothy, (2011). "Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm?", *Duke Law and Technology,* Vol. 11(1).

ISSN 2348 – 7968

[13] Caplan, David, (2010). "Bankruptcy in the Cloud: Effects of bankruptcy by a Cloud Services Provider", *American Bar Association Annual Meeting*.

[14] Catteddu, Daniele & Hogben, Giles, (2009). " Cloud Computing: Benefits, risks and recommendations for information security", *ENISA*.

[15] Cavoukian, (2010). "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach", *NEC Company Ltd. & Information and Privacy Commissioner of Ontario*.

[16] Cloud Security Alliance, (2011). SecaaS: Defined Categories of Service.

[17] Cloud Security Alliance, (2010). Top Threats to Cloud Computing.

[18] Curtis, Sophie, (2012). "New Privacy Laws Could Boost EU Cloud Industry", CSO Security and Risk.

[19] Delettre, Christian, Boudaoud, Karima & Riveill, Michel (2011). "Cloud Computing, Security and Data Concealment", *IEEE*.

[20] Dorey, Paul & Leite, Armando (2011). "Commentary: Cloud computing – A security problem or solution?", *Information Security Technical Report*.

[21] Durbin, Steve (2011). "Information Security without boundaries", *Network Security*.

[22] Esteves, Rui & Rong, Chunming, (2010). "Social Impact of Privacy in Cloud Computing", *2nd IEEE International Conference on Cloud Computing Technology and Science*.

[23] Karadsheh, Louay (2012). "Applying security policies and service level agreement to IaaS service model to enhance security transition". *Computers & Security*.

[]24] O'Malley, Colin (2012). "The EU e-Privacy Directive: don't call it a cookie law", *Econsultancy*.

[25] Parsons, Christopher (2012). "Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies.

[26] Ristov, Sasko, Gusev, Marjan & Kostoska, Magdalena (2012). "Cloud Computing Security in Business Information Systems", *International Journal of Network Security and Its Applications (IJNSA)*,Vol. 4(2).

[27] Whittaker, Zack, (2011). "Google Admits Patriot Act requests; Handed over European data to U.S. authorities", *ZDNet*.

[28] Wright, David *et al.*, (2011). "PIAF: A Privacy Impact Assessment Framework for data protection and privacy rights", *Seventh Framework Programme*.