Cloud Computing Security and Privacy: An Empirical Study

Farid Shirazi[1](✉), Adnan Seddighi[2], and Amna Iqbal[2]

[1] Ted Rogers School of ITM, Ryerson University, Toronto, Canada
f2shiraz@ryersion.ca
[2] Ted Rogers School of Management, Ryerson University, Toronto, Canada
{adnan.seddighi,amna.iqbal}@ryerson.ca

Abstract. Cloud computing allows organizations to deliver better and faster services at reduced cost. Moreover, cloud also enables organizations to expand or contract based on market demand and requirements. Despite many benefits, concerns around security and privacy challenges in cloud are on the rise.

In this paper we have developed a cloud security and privacy taxonomy which is used to capture the traditional security challenges with the divergence cloud technology. The content analysis revealed that cloud security and privacy inherits most of the challenges existing in traditional security, however it also introduces several new challenges around virtualization, trust, legal, privacy and data interoperability issues. The paper identifies also the gaps found in literature around Security as a Service. Finally, it introduces Privacy-by-Design (PbD) framework integrated with cloud security. We developed a control matrix based on the literature review integrated with PbD to offer organizations, developer, business architects, and decision makers a mechanism for assessing security and privacy concerns before adopting a new cloud solution.

Keywords: Cloud computing · Security as a service · Privacy by Design · Control matrix

1 Introduction

In the last two decades, we have witnessed the exponential growth of internet and the emergence of an ever-connected and intertwined world. This has paved the road for the fourth industrial revolution encompassing the cyber-physical era. In such a world, organizations have no choice but to become more agile in order to cater the growing clients' demands. Two decades ago and before the emergence of smart phones, our connectivity to the world through the internet was relatively limited. We communicated with friends primarily via telephone and emails. We worked in physical offices and communicated directly with corporate administration and the physical resources. Fast forward to the present day, it is evident that communication makes heavy use of smart phones and social media platforms. The concept of the office has undergone substantial transformation to the point at which we are able to access resources from anywhere without being physically in the office.

M. Kurosu (Ed.): HCI 2017, Part II, LNCS 10272, pp. 534–549, 2017.
DOI: 10.1007/978-3-319-58077-7_43

The concept of cloud computing is not a new concept. The creation of ARPANET project in 1969, was the first step toward building cloud computing. The ARPANET (Advanced Research Project Agency Network) project was designing and implementing a network through which different kind of computers connect and communicate with each other within cloud known also as Internet. As Internet bandwidth and communication speed grew, more computers were able to connect to each other over a wide area network. Moreover, the advancement of virtualization technologies allowed computers to share their resources more effectively and efficiently. The development of grid computing made it possible for advanced parallel computing and CPU resource sharing. In addition, Web 2.0 technology provided a two-way communication system and paved the way for the rise of social media networks (SMNs). All of this has helped to shape cloud computing technology as we know today. Companies such as Salesforce.com and Amazon Web Services (AWS) were among the first companies to offer commercial cloud services. AWS provides services such as storage and computation via websites allowing a diverse set of devices access cloud resources by the means of a thin client application. Major IT companies such as IBM, Microsoft, Google and VMware among others offer cloud services.

Cloud Computing enables organizations to expand or contract on demand and provide services at reduced cost. By migrating to such solutions, organizations can reduce capital and operational expenditures and at the same time be more efficient. Although cloud solutions provide many advantages there remain serious challenges ahead. As per a survey done by International Data Corporation (IDC) in 2009, security was found to be the main concern that organizations have in adopting a cloud solution [1]. In this paper, we will investigate various privacy and security challenges organizations face in adopting cloud solutions in quest for developing a robust security and privacy framework. Specifically, we intend to identify the main differentiators of a cloud and a traditional security through the lens of Privacy-by-Design (PbD) framework.

Our main research questions are as follow: (a) are there any differences between privacy and security issues in a cloud environment and a non-cloud environment? and (b) how PbD framework can improve the design and implementation of the next generation cloud.

To answer the questions outlined above, we provide an extensive literature review to identify and map the work done by other researchers and practitioners in the field. The output of this research will help organizations focus on the relevant security and privacy concerns when adopting a new cloud solution.

1.1 Research Methodology Overview

The content and data sources of this study come from four main sources as outlined below: (a) peer reviewed articles and literature, (b) reports from industry research organizations such as Gartner, IDC, CSA, SANS, NIST and others, and (c) survey and studies conducted by consulting firms such and Deloitte, EY, PWC among others.

For the sake of content analysis we used NVIVO software (version 11.0). NVIVO provides features such as matrix coding that help researchers to code text documents for further analysis. In total, we've studied 121 documents from the above list in which 84 relevant literature and articles were chosen for further analysis.

2 Cloud Computing Market Overview

Although the concept of cloud computing has been around for some time, mainstream adoption of cloud services did not start until late 1990 and early 2000. Cloud computing first appeared on the Gartner hype cycle in 2008. Hype cycle is a well-known industry graph which presents emerging technologies and estimates time period required for such technologies to mature and become main stream. In 2008, Gartner estimated that it would take 2 to 5 years for cloud computing to be adopted as a mainstream technology. To identify the adoption state of cloud computing, we have tracked the movement of cloud computing on the Gartner hype cycle from the year 2008 to 2014. The graph below shows the way in which cloud computing moved on the hype cycle during these years. It can be seen from the graph that cloud computing has passed the peak of inflated expectation and it is on its way to become a mature technology. However, even in 2014, Gartner expected that the time required for mainstream adoption of cloud computing would be 2 to 5 years. From Gartner's estimation, cloud computing is still not a mature technology and will continue to evolve in the coming years (Fig. 1).

Cloud computing can impact various sections of the IT ecosystem from infrastructure to platforms to services. Moreover, cloud computing can impact various

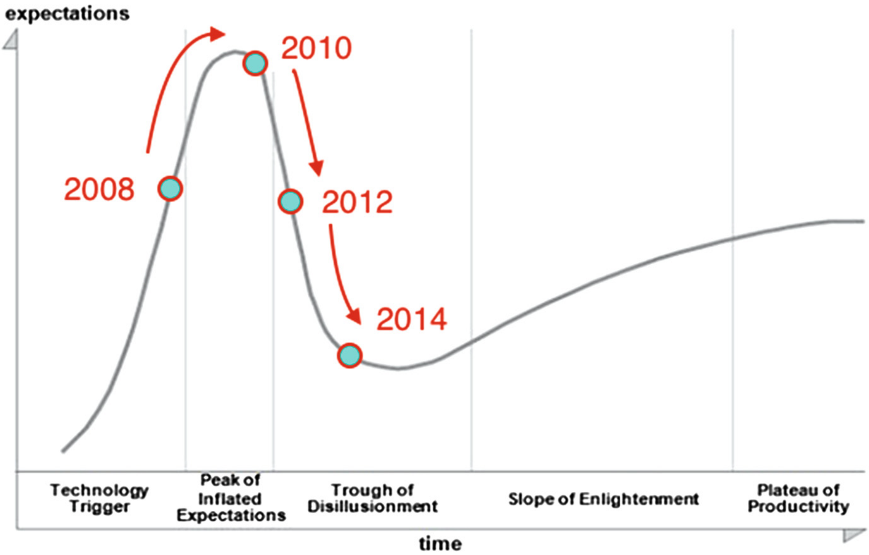

Fig. 1. State of cloud computing on Gartner hype cycle from 2008–2014

organizations and end user based on the type of applications and services they use. When evaluating the market value of cloud computing it is important to understand what aspects of cloud computing are being evaluated. For example, is the evaluation looking at services offered via Software-as-a-Service (SaaS) or Platform-as-a-Service (PaaS) and/or in combination of Infrastructure-as-a-Service (IaaS)? Or is it also taking into consideration other factors such as cloud advertising cost and the cost of cloud management? As per Gartner the public cloud services is forecasted to reach $204 Billion in 2016 [2]. Beside SaaS, PaaS, and IaaS, Gartner also includes among others, cloud business process services, cloud management and security as a service. For example cloud management and security services has shown an increase of 24% from 5.0 billion dollars in year 2015 to 6.2 billion in 2016 [3].

The second source from which market value estimates were collected was IDC. IDC estimated the public IT cloud services at $57.8 billion in 2015 (IDC 2015). If we add up the Gartner market value for SaaS, PaaS, and IaaS for 2015 we get $51.4 billion which is close to IDC's evaluation of $57.8 billion. Hence, it can be concluded that IDC is only including three main cloud services i.e. SaaS, PaaS, and IaaS when estimating the cloud market value. IDC also predicts that the cloud spending will grow to $112 billion in 2019 [4]. Cisco Global Cloud Index (CGI) provides also valuable forecasting data for the future market distribution of cloud services categorized by service models and deployment modes. This index attempts to forecast and map the global cloud-based IP traffic. Table 1 below summarizes CGI's predictions for 2019 [5].

Table 1. Cisco Global Cloud Index 2019

Public vs. Private Cloud (by 2019) Public: 56%, Private: 44%
Global Cloud Traffic (by 2019) Annual Global IP traffic will grow more than quadruple from 2.1 ZB (Zettabyte) per year to 8.6 ZB per year 1 Zettabyte = 10^21 bytes
Cloud Service Delivery Model (by 2019) 59% SaaS, 11% PaaS, 30% IaaS

By looking at the market size estimation and the future prediction of cloud, it is clear that cloud computing is not only here to stay, but will also shape the future of the IT world. Many organizations and businesses have started to embrace cloud solutions. As per a survey done by KPMG in 2011, 81% of businesses were in early or advance stages of experimentation or full implementation of cloud solutions [6]. Among the companies which are adopting cloud solutions, small and medium enterprises (SMEs) are the ones which are realizing the most benefit [33]. This is primarily because smaller companies can adopt cloud solutions faster with fewer hurdles. AMI Partners predicted that SMEs will spend up to $100 billion on cloud computing by 2014 [7].

3 Data Security and Privacy Challenges

Online cybercrime activities are not only increasing day by day, but they are also becoming more sophisticated and targeted. Cyber war does not recognize any borders and cyber criminals are targeting organizations across the globe because of various financial, political, or even personal reasons. In a data breach study conducted by IBM and the Ponemon Institute in 2016, it was estimated that on average the cost of a data breach is estimated $4 USD and that the cost of each stolen record has increased from $154 in 2015 to $158 in 2016 [8].

To demonstrate the financial, privacy and social impact of a data breach, we have provided some examples of the most famous breaches in the recent years. Examples below are just some of many incidents which occur on a daily basis across the world. The aftermath of a data breach can sometime affect individuals and organizations for many years. Organizations affected by data breach lose their trust among their clients which will eventually result in loss of business (Table 2).

Given that many organizations have started to shift their services to cloud, cloud environments have become an attractive target for hackers. Hence, organizations should be extra cautious of the security and privacy measures when moving their services to the cloud.

3.1 Cloud Security and Privacy

As discussed above, the use of cloud computing is on the rise. Organizations have to face the fact that their employees will be using cloud-based services regardless of organizations' policies [9] As per cloud survey done by IDC in 2015, more than 43% of organizations expect that within five years the majority of their IT services will be delivered through cloud. The same report predicts that by 2018 half of the IT spending will be cloud based and that by then industry cloud creation will be seen as a top market entry strategy for IT providers [4]. In addition, a survey conducted by IDC in 2009 indicates that security is among of the main challenges facing the adoption of cloud [10]. Similar concern was echoed by other surveys conducted by Deloitte, Forrester, EY, and KPMG. For example a survey conducted by EY in 2013 shows that 43% of organizations indicate that their information security budgets are on the rise [11].

Within security, issues around trust and privacy are becoming CIOs top concerns. A survey by Deloitte in 2013 revealed that 78% of IT managers considered that the lack of trust in security was the biggest barrier to the adoption of cloud technologies [12]. The same survey showed that insufficient data security and risk of data availability, open compliance and legal issues, and the risk of losing governance or control over data [12] to be the main challenges of cloud adoption. A KPMG survey in 2014 revealed that 53% of organizations believe that data loss and privacy risk are the main challenges of doing business in cloud [13]. The same survey showed that in 2014 security and data privacy was identified to be of greater concern than cost when adopting a cloud solution [13]. Another research survey by Forrester in 2013 indicated that 50% of businesses in Europe and North America view security as the number one

Table 2. Some examples of recent data breaches

Organization	Description
MySpace, 2016	In May 2016, the hacker named Peace (same person who sold the record of more than 164 million LinkedIn users) claimed to have 360 million emails and passwords of MySpace users. This claim was verified by LeakedSource [33]
Anthem, 2015	In February 2015, the giant healthcare provider Anthem was hacked where hackers stole up to 80 million user records. This hack was estimated to be "worth 10 times the amount of credit card data" [36]
AshleyMadison, 2015	In July 2015, the online meeting website Ashly Madison was hacked by a group called The Impact Team. This hack potentially exposed 37 million private records (Krebs on Security 2015). This hack had significant social effects, impacted the personal and private life of many people
Sony, 2014	In December 2014, hackers used phishing techniques to enter Sony network. In this attack, hackers erased data from Sony data bases, stole personal and sensitive information, and released pre-released movies. The financial impact of this attack was estimated at $100 million dollars [36]
JP Morgan Chase, 2014	In this attack more than 83 million household and business account information was compromised. Hackers used this information to perform money laundering and fraud wire transfers through which they made over $100 million [36]
Home Depot, 2014	This attack targeted Home Depot's payment terminal units, which compromised 56 million credit card and debit card numbers. The direct and indirect financial cost of this breach was estimated at $837 million [36]
Yahoo, 2013	In December 2016 Yahoo admitted that one billion of its user account credentials were stolen by an unauthorized third party, in August 2013 [32]. This is one of the biggest breaches of all times. This breach is said to have ripple effects well beyond Yahoo, including hijacking of tens of thousands of other [35] and the $4.8 billion Verizon-Yahoo take over deal [37]
Target, 2013	Similar to Home Depot attack, attackers infected Target's POS (Point of Sale) with a malware through which they got access to identities of 70 million customers and 40 million credit cards [36]
American Banks, 2005–2012	This attack was carried out by Russian and Ukrainian attackers for a period of seven years. During this period the attackers targeted American financial organizations and got access to more than 160 million credit and debit card information. The financial impact of this attack was estimated at $300 million [38]

reason for not adopting a cloud solution [11]. Similarly, EY's global information security survey in 2013 indicates that 25% of organization admit that cloud computing has changed their risk exposure in the last 12 months [11].

3.2 Literature Review and Related Work

A clear majority of reviewed research articles were associated with to the following categories.

1. Threats and vulnerabilities in cloud
2. Issues around privacy, compliance, audit, legal, and trust in cloud
3. Challenges organizations face in adopting a cloud solution
4. Solutions and recommendations for cloud security concerns and issues

A list of all keywords and phrases associated with our literature review has been generated, but due to the page limitation we excluded the list from our appendix.

We could not find any literature during the time of this study (2015–2016) that considered cloud computing design and implementation from the perspectives of the PbD framework. In fact those articles dealing with cloud security have considered privacy as subset of overall cloud security but not as its own specific domain.

4 Data Analysis and Results

In this section we will present the results of our content analysis. In total, we have reviewed over 121 academic and industry reports. For the purpose of content analysis, 84 of the most relevant literature were selected and analyzed by using NVIVO software package. NVIVO software was very helpful in performing thematic analysis and data comparison. Out of 84 papers chosen for this study, 51 focused on cloud security issues, 13 focused on cloud adoption issues, 17 articles focused on cloud security business adoption issues (including the e-commerce), and 3 papers were focused on privacy issues.

4.1 Methodology in Action

In order to perform content analysis, it was crucial to identify the themes which were relevant to this research study. To do so, we needed a well-defined taxonomy presenting a complete anatomy of security issues in cloud computing. The development of such taxonomy was very paramount to this study as it provided a common framework through which we could do the content analysis. Hence, we have used the open coding technique in the first round of literature review for the purpose of building such taxonomy.

Using the keywords generated through relevant industry and academic research studies, initially we ended up with more than 20 categories related to cloud security issues. However, through continuous revision of categories and literature review, we managed to merge and amalgamate relevant categories. As such, we ended up with 11 categories which could not be reduced any further. As per process outlined by [14], we had to continuously sanity check our categories to ensure they addressed this study's security and privacy questions. The categories identified, presents a holistic taxonomy of the cloud security issues based on the reviewed literature. The list of this taxonomy is outlined in table below. The coding agenda table below which was generated using NVIVO tool outlines how coding was done based on each category defined (Table 3).

Table 3. Classification of cloud security domains

Category	Definition	Example
C1: Network and infrastructure security	This category focused on issues related to network and infrastructure security as it related to cloud computing	"Network security: Problems associated with network communications and configurations regarding cloud computing infrastructures" [15]
C2: Software and application security	Any security issue related to software and application, this could be security issues related to web services or any other application used at SaaS layer (like email, photo sharing)	"Security concern #7: Users must keep up to date with application improvements to be sure they are protected" [16]
C3: Virtualization security	Any security issue arising from the virtualization and multi-tenancy technology	"Multi-tenancy issue: this issue poses a challenge to protect user data against unauthorized access from other users running processes on the same physical servers. This is in fact not a new issue taking into consideration the current concern with web hosting services. However, with the widespread use of cloud computing and with the fact that users store more important data in the cloud, this issue needs to be reconsidered seriously." [17]
C4: Data security	Data security category encompasses issues related to confidentiality, integrity, and availability of data	"Confidentiality and integrity of data transmission need to ensure not only between enterprise storage and cloud storage but also between different cloud storage services. In other words, confidentiality and integrity of the entire transfer process of data should be ensured" [18] "Organizations worry about whether Utility Computing services will have adequate availability, and this makes some wary of Cloud Computing" [19]
C5: Data storage, recovery, and backup	Security issues around location of stored data, data isolation, how data is backed up and recovered in an event of disaster	"end-users use the services provided by the cloud providers without knowing exactly where the resources for such services are located" [17] "Another important research area concerns determining apt granularities for isolation." [18]

(*continued*)

Table 3. (*continued*)

Category	Definition	Example
C6: Identity and access control	Security issues around authentication, authorization, identity management, access to data, credentials, privileged user access, etc.	"Security is always a popular topic and there are the following areas of specializations for Clouds: identity management, access control, single sign-on and auditing" [18] "In many application scenarios, such as those in enterprises or organizations, users' access to data is usually selective and highly differentiated. Different users enjoy different access privileges with regard to the data. When data are outsourced to the cloud, enforcing secure, efficient, and reliable data access among a large number of users is thus critical" [17]
C7: Compliance, audit, and legal issues	Issues around data transfer between different jurisdictions, how data can be audited and logged as per various security compliance requirements. Also this category addresses issues related to forensic and investigation shortcomings in cloud	"There is currently no regulation in place to determine how to keep track of the use of the cloud system and what is required to be audited and logged" [20] "Given that cloud computing is a relatively new technology, the current cyber laws do not yet cover the requirements posed by it" [21] "Regulatory compliance: Is the cloud vendor willing to undergo external audits and/or security certifications?" [22] "Legal issues: Aspects related to judicial requirements and law, such as multiple data locations and privilege management." [15]
C8: Privacy and trust	Issues around client's trust with CSPs and handling of users privacy in cloud	"Cloud computing raises new privacy issues that require clear standards for custodians of this information who receive government requests for access to that information." [20] "Lack of consumer trust is commonly recognized as a key inhibitor to moving to Software as a Service (SaaS) cloud models" [18–20]

(*continued*)

Table 3. (*continued*)

Category	Definition	Example
C9: Threat and vulnerabilities	This category relates to any vulnerabilities and threats identified in IaaS, PaaS, and SaaS	"Bugs in Large-Scale Distributed Systems. One of the difficult challenges in Cloud Computing is removing errors in these very large scale distributed systems. A common occurrence is that these bugs cannot be reproduced in smaller configurations, so the debugging must occur at scale in the production datacenters." [19] "Cloud provider vulnerabilities. These could be platform level, such as an SQL-injection or cross-site scripting vulnerability in salesforce.com." [23]
C10: Security governance and risk management	Issues around governance and risk management in cloud	"Governance: Issues related to (losing) administrative and security controls in cloud computing solutions" (Gonzalez et al. 2012)
C11: Standards	Issues around security standards in cloud. Also this category addresses interoperability between CSPs and data lock-ins	"Cloud standards: standards are needed across different standard developing organizations to achieve interoperability among clouds and to increase their stability and security" [15] "there are many general computing standards that may be reused in the cloud, but for the moment, there are to our knowledge no dedicated cloud standards." [17]

4.2 Comparing Traditional and Cloud Security

By taking a closer look at the cloud security taxonomy derived from literature, we can see that nine out of eleven cloud security issues identified are in fact issues which are also addressed by traditional security. The security issues that were uniquely associated to cloud were mainly associated with virtualization, web interface issues and data storage; particularly the issues related to storage locality. This observation alone indicates that cloud security and traditional security have a lot in common.

Although the literature points to the similarities of cloud and traditional security, there are still some major differences. Based on the literature review with argue that due to the complexity of cloud architecture and lack of visibility, traditional security solution cannot address today's cloud security challenges. So although most of the security issues are the same, as mentioned by Chen and Zhao [18] the traditional security mechanisms are no longer suitable for applications and data in cloud. For example, performing some tasks such as forensic investigation in cloud will become much more difficult as investigators might not be able to access system hardware physically [17]. Such differences introduce new challenges and calls for new solutions specific to the cloud.

Another point to note is the differences that exist around the privacy and trust issues in traditional and cloud environments. In traditional computing, since the data resides on clients' premise, there are controls built around securing the data. However, it is assumed that the client is to be trusted with their data as they are the custodian and guardian of that data. In cloud environment however, clients' data is hosted at a third party Cloud Service Provider (CSP). This shift of data storage introduces new challenges around privacy and trust.

The lack of standards and legal issues are two other challenges which should be looked at from a different angle when operating in cloud environments. As discussed above, these issues have much wider impact and expose data to a higher level of risks in cloud environments as opposed to traditional environments.

5 Privacy Concerns in the Cloud

According to [24], privacy is the ability of the persons to decide when, how and to what extent information about themselves is communicated to other people. There are four states of being private: (1) Solitude – physical separation from the group; (2) Intimacy – participation in a small unit that achieves corporate solitude (3) Anonymity – freedom from surveillance (4) Reserve – creation of psychological barrier that protects the individual from unwanted intrusion [24].

As discussed above, the main topics discussed in literature were mainly associated with security threats compromising customers' data. The risk of private data violation is much higher for data stored on the cloud. Cloud providers can deliberately or unintentionally misuse or disclosure sensitive user information that resides within a provider's premises. There are different aspects of the violation of data privacy. For example, the storage location may be a serious data privacy issue. When users start using cloud services, their data is located in cloud. While some providers explicitly specify where the data are located, others do not provide such information. In this case the data can be moved from location to location or even from country to country without a user's knowledge. Because legal regulations may be different in other countries, other privacy laws may apply that users unknowingly have to comply with. In most cases, users do not have full control over their sensitive data once placed in the cloud. According to [25, 26], there are many legal concerns that companies should be worried about. They relate to the privacy and security of the data as well control of the data ownership. Many details depend on the service agreements which still aren't nearly robust enough compared to SLAs in traditional manufacturing industries. Additional issues arise from cloud datacenters being located in different geographical locations which can result in confusion over which law has to be applied. Then there are concerns related to cloud provider declaring bankruptcy – it is not clear what will happen to the data belonging to the companies.

Bowen [25] first looks at data privacy and security issues. There are multiple laws that protect personal data enacted in USA and EU that cloud providers have to comply with. Some laws force cloud providers to notify their users when data breach of personal unencrypted information has occurred. The notable laws are Patriot Act in USA and European Union Data Privacy Directive (EUDPD). The US Patriot Act basically allows government to intercept any electronic information as well as compel any company to disclose such information to the government. The only requirement is government's certification that this information is relevant to the ongoing investigation. This fact is usually used to caution companies about storing their data in clouds located in USA and in promotion of European providers [27]. However, most European countries have analogous anti-terrorism laws as well. There are multiple Mutual Legal Assistance Treaties (MLATs) that require participants to share third-party information upon the formal request. This basically makes actual geographic location of servers storing the data in the cloud immaterial [26, 27]. EUDPD's key feature is its extraterritorial effect – any data from EU can only be sent to countries with compatible data protections.

Next are the jurisdictional issues related to virtualization and data location in which users' data can be stored in multiple countries while in the cloud. One problem is that once EUPDP law is applied to the data it becomes attached to it so from that point it can be sent only to compatible countries as discussed before. This may result in the conflict if initial contract with the cloud provider stipulated that it is done under, say, USA laws which can contradict European Union Directive. In addition, different countries will have different laws regarding government access to the data. As mentioned above the US Patriot Act allows government to access any data it wants. This may not be something that Amazon's customer residing in Europe wants to be exposed to.

A special problem might be with data retention: which policy is in place? how is it implemented? and how long data is retained in the cloud? After the retention period, a user's data have to be destroyed. The cloud provides high data availability by keeping a few copies of the data, sometimes at different locations. The issue here is how to make sure that all copies are destroyed correctly. Cloud users should know and act accordingly, and data privacy regulatory requirements effective data managing policies should be applied to the cloud. While auditing and monitoring cloud service providers it is essential to guarantee that business privacy requirements are not violated, and that sensitive user personal information is not leaked or misused. It is also important to be proactive rather than reactive when it comes to data privacy. To do so we offer a new approach in monitoring and assessing cloud privacy by implementing PbD as a control mechanism in protecting users' private data.

5.1 Privacy by Design

The privacy by design (PbD) framework was originally developed by Cavoukian [28]. This framework contains seven fundamental principles such as: Proactive not Reactive; Privacy as the Default Setting; Full Functionality; End-to-End Security; Visibility; Transparency; and User Privacy and Privacy Embedded into Design. The latter in particular is an important part of this study. The PbD framework offers an approach that is characterized by a proactive privacy measures rather than a reactive ones, it assures that all stakeholders (cloud stakeholder in this case) whether the business practice or technology involved, operate according to the stated promises and objectives and subject to independent verification [28]. Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults. As such we offer a cloud control matrix integrated with PbD to ensure clients' privacy. Figure 2 below was generated based on the eleven security domains discussed above. It integrates PbD as a control mechanism as integral part of cloud design and implementation.

In other words PbD offers a dynamic approach in which the legacy framework of security-privacy-usability triangle [29, 30] is modified so that the user-centric design principle of PbD is fulfilled.

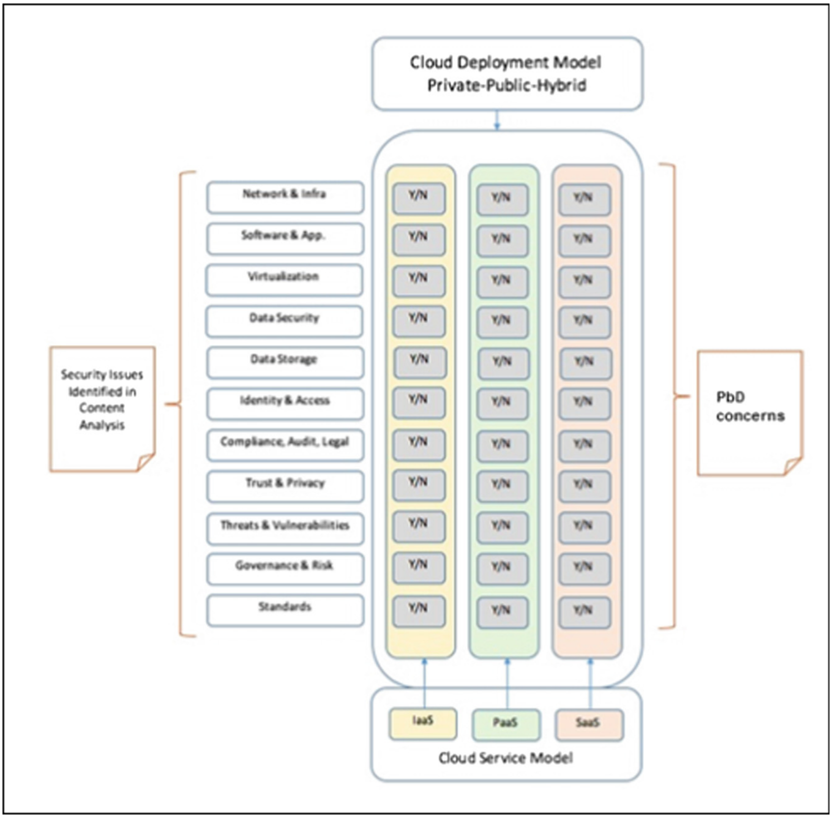

Fig. 2. Cloud security control matrix integrated with PbD

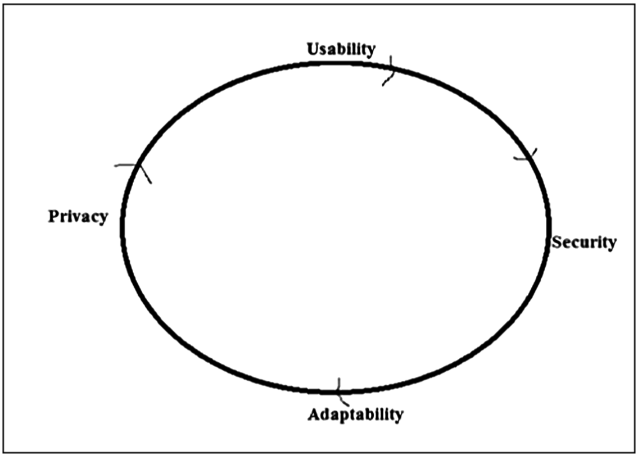

Fig. 3. Privacy, security, usability, and adaptability

As shown in Fig. 3, this integration highlights the vital links between privacy, security and usability in building organization's credibility and trust [31]. The updated model takes into account the dynamic nature of privacy. In addition, it addresses the need for flexibility and adaptability in the process. This paves the way for a richer and smoother user experience.

6 Conclusion

In this study we have focused on identifying differences of cloud and traditional security. Although cloud computing offers many advantages over conventional computing such as reduced cost, elasticity, rapid growth potential, among others, it has several challenges among which security and privacy concerns were the main focus of this study.

Our analysis revealed that cloud computing introduces new challenges on issues around privacy, trust, legal, virtualization and data interoperability. Organizations need to be aware of these new challenges as they move their services to the cloud. The cloud security and privacy taxonomy developed in this paper offers a framework in which the principles of privacy as outlined in PbD has been integrated into the deployment of cloud. Depending on the cloud model being used, organizations can use the matrix offered in this study to ensure whether or not the cloud solution they want to adapt addresses the main concerns associated with cloud privacy and security.

With the current speed of cloud adoption, organizations need to be more vigilant with their data when outsourced to cloud. Organizations should view cloud security and privacy through new lenses and use new frameworks and tools to assess CSPs security.

References

1. Gens, F.: IDC IT Cloud Services Survey: top benefits and challenges, 15 December 2009. http://blogs.idc.com/ie/?p=730. Accessed 27 Sept 2016
2. Stamford, C.: Gartner: Worldwide IT spending, 18 January 2016. http://www.gartner.com/newsroom/id/3186517. Accessed 27 Sept 2016
3. Stamford, C.: Gartner Says Worldwide Public Cloud Services Market Is Forecast to Reach $204 Billion in 2016, 25 January 2016. http://www.gartner.com/newsroom/id/3188817. Accessed 13 Oct 2016
4. IDC. IDC FutureScape: Worldwide Cloud 2016 Predictions—Mastering the Raw Material of Digital Transformation (2015). www.idc.com
5. Cisco. Cisco Global Cloud Index: Forecast and Methodology, 21 April 2016. http://www.cisco.com/. Accessed 13 Oct 2016
6. KPMG. Clarity in the Cloud (2011). www.kpmg.com/SG/en/IssuesAndInsights/Documents/ICE-ClarityInTheCloud.pdf
7. Hickey, A.R.: SMB Cloud Spending To Approach $100 Billion By 2014, 12 August 2010. http://www.crn.com/
8. Ponemon Institute. 2016 Cost of Data Breach Study: Global Analysis, June 2016. http://www-03.ibm.com/security/data-breach/
9. ENISA. Cloud Computing-Benefits, risks and recommendation for information security, 9 November 2009. https://www.enisa.europa.eu/
10. IDC New IDC IT Cloud Services Survey: Top Benefits and Challenges, 15 December 2009. http://blogs.idc.com/ie/?p=730
11. EY. Under cyber attack EY's Global Information Security Survey 2013, October 2013. http://www.ey.com
12. Deloitte. How to ensure control and security when moving to SaaS/cloud applications, October 2013. www.deloitte.com
13. KPMG. Elevating business in the cloud (2014). www.kpmg.com/cloudsolutions
14. Mayring, P.: Qualitative Inhaltsanalyse. Grundlagen und Techniken, 7th edn. Deutscher Studien Verlag, Weinheim (2000). First edition 1983
15. Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., Pourzandi, M.: A quantitative analysis of current security concerns and solutions for cloud computing. J. Cloud Comput.: Adv. Syst. Appl. **1**(1), 11 (2012)
16. Popović, K., Hocenski, Ž.: Cloud computing security issues and challenges. In: Proceedings of the 33rd International Convention, pp. 344–349. IEEE Xplore, Opatija, May 2010
17. Rong, C., Nguyen, S.T., Jaatun, M.G.: Beyond lightning: a survey on security challenges in cloud computing. Comput. Electr. Eng. **39**(1), 47–54 (2013)
18. Chen, D., Zhao, H.: Data security and privacy protection issues in cloud computing. In: 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 1, pp. 647–651, March 2012
19. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Zaharia, M.: A view of cloud computing. Commun. ACM **53**(4), 50–58 (2010)
20. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A.: Cloud computing—the business perspective. Decis. Support Syst. **51**(1), 176–189 (2011)
21. Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M., Inácio, P.R.: Security issues in cloud environments: a survey. Int. J. Inf. Secur. **13**(2), 113–170 (2014)
22. Ramgovind, S., Eloff, M.M., Smith, E.: The management of security in cloud computing. In: 2010 Information Security for South Africa, pp. 1–7. IEEE, August 2010

23. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J.: Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, pp. 85–90. ACM, November 2009
24. Katzan, H.: On the privacy of cloud computing. Int. J. Manag. Inf. Syst. (IJMIS) **24**(2), 1 (2010)
25. Bowen, J.A.: Cloud computing: issues in data privacy/security and commercial considerations. Comput. Lawyer (2011)
26. Bender, D.: Privacy and security issues in cloud computing. Comput. Internet Lawyer (2012)
27. Wolf, C.: Privacy and data security in the cloud: what are the issues? IP Litig.: Devoted Intellect. Prop. Litig. Enforc. **18**(6), 19–28 (2012)
28. Cavoukian, A.: Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. Information and Privacy Commissioner Ontario, Canada (2009)
29. De Cristofaro, E., Wright, M. (eds.): PETS 2013. LNCS, vol. 7981. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39077-7. See also Security and Privacy http://www.parc.com/work/competencies.html
30. Balfanz, D., Durfee, G., Smetters, D.K., Grinter, R.E.: In Search of usable security: five lessons from the field. IEEE Secur. Priv. **2**(5), 19–24 (2004). http://www.parc.com/work/competencies.html
31. Casalo, V.L., Flavian, C., Miguel Guinaliu, M.: The role of security, privacy, usability and reputation in the development of online banking. Online Inf. Rev. **31**(5), 583–603 (2007)
32. Yahoo 2016. Recognize and secure a hacked Yahoo Mail account. https://investor.yahoo.net/releasedetail.cfm?ReleaseID=1004285
33. Tehrani, S.R., Shirazi, F.: Factors influencing the adoption of cloud computing by small and medium size enterprises (SMEs). In: Yamamoto, S. (ed.) HCI 2014. LNCS, vol. 8522, pp. 631–642. Springer, Cham (2014). doi:10.1007/978-3-319-07863-2_60
34. Motherboard.: Hacker Tries To Sell 427 Million Stolen MySpace Passwords For $2,800, 27 May 2016. http://motherboard.vice.com
35. Satter, R.: And this password breach could have ripple effects well beyond Yahoo (2016). http://www.theglobeandmail.com/
36. Sporck, L.: 8 of the Largest Data Breaches of All Time, 17 January 2016. https://www.opswat.com/
37. Leswing, K.: Yahoo confirms major breach—and it could be the largest hack of all time, 22 September 2016. http://uk.businessinsider.com
38. Beekman, D.: Hackers hit Nasdaq, 7-Eleven, others for $300 million: Feds, 26 July 2013. http://www.nydailynews.com