American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

Legal and Privacy Issues with Cloud Computing in Small and Medium Size Enterprises

Regina Ekoa Mbella Mungwe*

Southern University and A&M College, ICITD, Baton Rouge, Louisiana,70813
Email: Mungweregina@gmail.com, Reginaekoa_mungwe01@subr.edu

Abstract

Because of insufficient resources to manage a costly and complex internal information technology infrastructure (local storage computing), cloud computing emerged providing potential benefits to small and medium size enterprises such as rapid access to flexible and low- cost IT resources, enabling payment as per consumption and facilitating productivity for accounting services, for communication customer services and support. It provides simple ways to access servers, database and a broad set of applications over the internet. Cloud computing is a technology paradigm operating on the principle of virtualization, distributed computing, grid computing, and data bases to provide computing services. It provides a simple way of storing, accessing servers, data, program and a broad set of application services over the internet [1]. The product of small and medium size enterprises is now reaching a wider audience using this new Technology (cloud computing). This system of outsourcing however presents many challenges in its different types (public and private cloud). Organizations such as small and medium size enterprises have increased risks by storing sensitive data in the cloud thereby making security, privacy and protection a rising concern to them. In this paper, we will analyze the privacy challenges faced by small and medium sized enterprises with the adoption of cloud. The paper seeks to examine the legal protection provided to secure SMEs who are involved in cloud computing. This paper will address the security challenges cloud computing presents to the local storage computing and provide possible recommendations.

Keywords: Cloud Computing; Data Base; Local Storage Computing.

---

* Corresponding author.

1. Introduction

Cloud computing is a type of outsourcing that provides shared computer processing resources and data to computers and other devices on demand. It is a new system of technology that provides a simple way of storing, accessing servers, data, program and a broad set of application services over the internet.

Small and medium size enterprise tends to use cloud computing because of its outstanding benefits. It provides cost reduction, as cloud hosted servers enable mass-scale computing power and minimize IT requirements and physical storage providing a sufficient savings. As an emerging technology and business trend, small businesses benefit from increasing flexibility and greater integration.

Despite the numerous benefits provided by this new system of technology, cloud users such as small and medium size enterprises (SMEs) face massive privacy and legal challenges which hinders its rapid adoption. In the cloud environment, users outsourcing their data and application can only rely on the cloud service provider (CSP) to provide their security. Many concerns are raised due to the fear of the unknown. Cloud computing provides access to data but the challenge has always been to ensure that only authorized entities have access to this data. The threat of privacy in cloud computing arises from services that deal with different aspects of data such as collecting, transferring, processing, sharing and storing data relating to personal information [3].

The ongoing question today is whether contracts agreement, pro forma documents and other forms of written agreements provides adequate legal protection for the small and medium size enterprises who are tremendously using cloud computing. Privacy, which is, also a big challenge with the use of cloud computing in small and medium size enterprises requires greater data protection policies to ensure that data is not lost or misappropriated.

This paper will discuss in detail the privacy challenges raised with the use of cloud computing in small and medium size enterprises. It will address legal protection provided to SMEs who have adopted the use of cloud computing. Under this examination, this paper will provide possible recommendations that can be adopted to remedy the privacy and security threat posed to SMEs who are engaged in cloud computing.

1.1. Research Methods and Materials

This paper evaluates the challenges faced by SMEs involved with cloud computing, and the regulations that have significant impact on cloud computing environment in SMEs. The research is explanatory in nature adopting qualitative methods. A systematic search was carried out on electronic databases: EBSCO, SCOPUS and Google scholar, trying to identify research work and materials related to the domain. The search terms include: Cloud computing, SMEs, security, privacy and policy.

1.2. Results

The two main issues that exist with security and privacy aspects of cloud computing includes: loss of control over data and total dependence on the cloud computing provider. The ability of cloud computing to store data

remotely and share services in a dynamic environment bring along with it cloud privacy concerns. The challenge for SMEs utilizing, cloud systems is therefore to figure out a way to maintain control and over sight akin to managing the personal data themselves, privacy challenges demands complete protection and the appropriate use of customer's personal information. The frequently asked question regarding protection of cloud computing users such as SMEs has always been:

- Does the legislature provide specific Legal protection laws mandating adequate data security?

1.3. Conclusion

This research work is completed and the findings highlight some of the concerns with security and privacy of the cloud of SMEs. These concerns will form the basis of the design of a framework for future adoption of cloud platforms. A framework evaluation will be carried out using real life scenarios to provide solutions to the issues identified, this will be documented and user experience shared. Our findings, we believe, will aid policy formulation, and draw many SMEs on to the cloud platform.

1.4. Figure 1

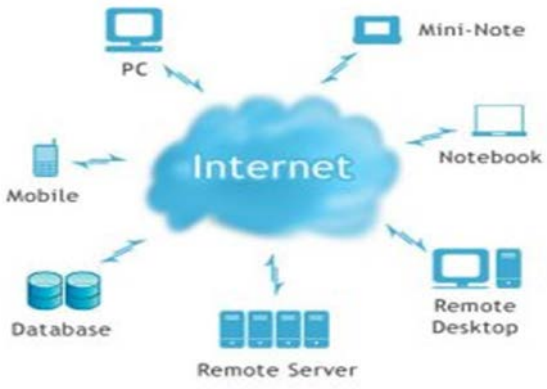

Figure 1: Cloud Computing

In the simplest form cloud computing means storing and accessing data and program over the internet instead of your computer hard drive. Diagram 1.1.1 illustrates the use of cloud computing from different digital tools such as Note Book, PC, Mini Note, Remote Desktop and Mobile phones.

The authors in [8] and [9] provided that cloud computing enables the access of data from anywhere over the internet using these different digital tools. Cloud computing is the delivery of computing services, storage, databases, networking, software, analytics and more over the internet

Many different definitions and meaning of cloud computing has evolved in recent years. According to the NIST (National institute of Standards and Technology), cloud computing is a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example networks, storage,

applications and servers) that can rapidly have provisioned and released with minimal management effort or service provider interaction" [2].

NIST further says that "cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud)" [4].

The Gartner Group defines cloud computing as "a style of computing in which massively scalable IT-related capabilities are provided 'as a service' using Internet technologies to multiple external customers."

The Fast Cloud Group defines cloud computing "as a new style of computing in which dynamically scalable and often virtualized resources are provided as a pay for use service over the Internet or an Intranet network (or both). Users need not have knowledge of, expertise in, or control over the technology infrastructure in the 'cloud' that supports them" [5].

Cloud computing operates on three different cloud service delivery models which include; Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a service. Knowing what these services represent and how they're different makes it easier to accomplish your business goals is important [6].

1.5. Infrastructure as a Service (IaaS)

This is the most basic category of cloud computing services. IaaS enables you rent IT infrastructure-servers and virtual machines (VMs), storage, networks, operating systems from a cloud provider on a pay-as-you-go basis. This service reduces cost and complexity of buying and managing your own physical servers and other datacenter infrastructure. An example of the use of IaaS in a business includes Website hosting. Running websites using IaaS can be less expensive than the traditional web hosting.

2. Platform as a Service (PaaS)

PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development. Like IaaS, PaaS avoid the expense and complexity of buying and managing software licenses, the underlying application infrastructure and middleware or the development tools and other resources.

2.1. Software as a Service (SaaS)

This cloud computing service is a method of delivering software applications over the internet, on demand and typically on subscription bases. With SaaS, cloud providers host and manage the software application and underlying infrastructure, and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their, will ensure the availability and

phone, tablet, or PC. This service provider manages the hardware and software, and with the appropriate service agreement the security of the app and data as well.

2.2. Privacy challenges faced by small and medium size enterprises who have adopted cloud computing

There are four different types of cloud; public cloud, private cloud, hybrid cloud and community cloud, amongst which Private and Public Cloud are the most used.

According to the International Organization for Standardization (ISO), a Public Cloud is a "cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider." It further says that "a public cloud may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. In a public cloud, service is shared and pooled between many customers.

A Private cloud on the other hand is defined as "that which may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. The cloud service customer may also authorize access to other parties for its benefit. Private clouds seek to set a narrowly controlled boundary around the private cloud based on limiting the customers to a single organization." The main aim of private cloud is to share the data, services and resources between the employees inside the organization. In a private cloud, the cloud is dedicated to one customer.

Today, SMEs turn to cloud computing services because of the numerous benefits it provides. Some of the benefits include Scalability (offers unlimited processing and storage capacity), reliability (eliminates the concern of losing valuable data in paper format or through the loss of laptops or hard drives; enables access to applications and documents anywhere in the world through the internet, cost savings. Efficiency, (fear up resources to focus on innovation and product development and access to new technologies. As a result, there has been considerable growth in the provision of cloud-based services and increasingly users are saving their personal data and information on cloud based services.

The ability of cloud computing to store data remotely and share services in a dynamic environment bring along with it cloud security and privacy concerns. The main challenge for data users utilizing, cloud systems is therefore to figure out a way to maintain control and over sight akin to managing the personal data themselves [7]. Some other challenges that arise from the use of the different cloud models include:

- **Technical safe guard for identity management and authentication**. One of the appealing features of the cloud, particularly the public cloud, is its ability to be accessed in the internet from anywhere. Whilst this feature meets the mobility needs of the data users, it also allows easier access for hackers.
- **Proper exit plan, data ensure and portability**. The handling of data after a cloud contract has ended, or after fulfillment of the original purpose of their collection, should be well thought through. Usually there is no formal "exit plan" for personal data upon the completion of contract or mid-term termination. This therefore does not erase previously used data that had been permanently saved.

- **Lack of privacy awareness and legal sanction**. When subcontractors entrusted with the processing of personal data are in jurisdictions without data protection laws they, they could suffer from a lack of knowledge and respect for personal data protection, which poses risks to data users.

2.3. Mandatory Legal protection of Cloud Users (SMEs)

The threat of privacy in cloud computing arises from services that deal with different aspects of data such as (collecting, transferring, processing and storing data) relating to personal information. Privacy demands complete protection and the appropriate use of customer's personal information. The two main issues that exist with security and privacy aspects of cloud computing includes; loss of control over data and total dependence on the cloud computing provider. For example, most customers are aware of the danger of letting data control out of their hands and storing data with an outside cloud computing provider [10]. Data could be compromised by the cloud computing provider itself or other competitive enterprises which are customers with the same cloud computing provider. In this case, there is lack of transparency for customers how, when, why and where their data is processed. In this situation, it is useful to review the requirements of mandatory privacy law in addressing cloud computing issues with SMEs.

The frequently asked questions regarding protection of cloud computing users such as SMEs have always been; Whether the Legislation provides specific Legal protection laws mandating adequate data security? Are absent or vague data security promises inherently unfair to consumers? When contract terms specifically place the burden of security and resulting data loss on consumers, what protections are in place for the consumers?

In the USA, the regulatory approach to data security is generally ex post and there is no single omnibus federal law requiring data security. Stegmaier and Bartnick noted that the focus is instead of "Criminalizing unauthorized access". Each Congressional term brings proposals to standardize laws at a federal level. Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap dovetail and contradict one another. In addition, there are many guidelines, developed by governmental agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered "best practices" [11]. These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators. Security and privacy of personal data relies primarily on the contract terms agreed to by the parties. However even though the legislation does not out rightly provide Federal Privacy Laws for data security; efforts have still been made to provide data security to a certain extent. Some of which include:

- The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorized disclosure of personal data.
- The recently adopted General Data Protection Regulation (GDPR) entering into force in 2018, provides many obligations on cloud computing users (SMEs); Entities processing personal data will have increased accountability and data governance obligations on several fronts. This includes a heightened duty of care on a

controller's selection of processor and ability to demonstrate compliance. In the cloud computing context, the GDPR also places direct obligations on processors, often CSPs. The GDPR limits the ability of processors to add subcontractors without consent from the controller. These direct obligations will require processor to "ensure a level of security appropriate to the risk". The CDPR will generally require entities processing personal data to provide more documentation and in some instances, sharpen the security practices of their operations.

- The Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030) regulate the interception of electronic communications and computer tampering, respectively. A class action complaint filed in late 2008 alleged that internet service providers (ISPs) and a targeted advertising company violated these statutes by intercepting data sent between individuals' computers and ISP servers (known as deep packet inspection). This is the same practice engaged in by Phorm in the UK and several UK telecommunications companies that resulted in an investigation by the European Commission.

2.4. Recommendations

Organizations such as SMEs using cloud computing service must carefully review the cloud provider's terms of service and ensure that the personal information it entrust to the provider will be treated in a manner consistent with its privacy obligations under the relevant privacy legislation. In short, SMEs must use contractual or other means to ensure that personal information is appropriately handled and protected by the cloud provider or better still if they are not comfortable with what a cloud provider is proposing, they should not transfer personal information entrusted to them by their costumer to that provider [12].

Review the Internal Security Policy. Cloud computing requires SMEs to have a complete review of the internal procedures in line with the conclusions of the risk analysis. In fact, the use of cloud introduces new risks related to transmission via the internet or the use of mobile terminals. Special attention must offer a service compatible with these security requirements [13].

Monitor Changes over time. In a spirit of continuous improvement, CNL recommends that SMEs periodically assess cloud computing service considering changes over time in the context, risks, the solutions available on the market, legislation, etc. The recommended risk analysis must be updated as soon as a significant change in the service takes place to adapt the measures or solutions as soon as necessary [14]. These changes may concern the functionalities of the product or the technical provision of the service (new data Centre, change in security policy, change in processing initiated by the customer, etc.

References

[1]. Pearson S. "Privacy, Security and Trust in Cloud Computing" in Privacy and Security for Cloud Computing, Pearson S., Yee G. (eds). Computer Communications and Networks. Springer, London, 2013, pp. 3-42.

[2]. Johndavid K., Kwok T. "Cloud computing: legal and privacy issues". Journal of Legal Issues and Cases in Business.[On-line] Available: http://www.aabri.com/manuscripts/111064.pdf [Jan 2, 2017]

[3]. Tharam D., Chen W. and Elizabeth C. "Cloud Computing: Issues and Challenges", 24th IEEE

International Conference on Advanced Information Networking and Applications, Australia, 2010.

[4]. Peter M. Mell and Timothy G. "The NIST Definition of Cloud Computing". Internet: https://www.nist.gov/publications/nist-definition-cloud-computing, Sep. 28, 2011. [Feb. 3, 2017]

[5]. Dudmesh J. "Cloud Computing for Small- and Medium-Sized Enterprises" Internet: http://www.freshbusinessthinking.com/cloud-computing-for-small-and-medium-sized-enterprises/, Nov. 10, 2009. [Feb. 15, 2017]

[6]. MacArthur H. "How small and midsize enterprises migrate to cloud-based services" Internet: http://www.computerweekly.com/tip/How-small-and-midsize-enterprises-migrate-to-cloud-based-services [Feb. 7, 2017]

[7]. Samer J.A., Abdallah M. A. "Cloud Computing and E-commerce in Small and Medium Enterprises (SME's): the Benefits, Challenges" International Journal of Science and Research, vol 2, pp. 2319-7064, Dec, 2013.

[8]. Eric G. " What is Cloud Computing". Internet: http://www.pcmag.com/article2/0,2817,2372163,00.asp, May, 2016, [Feb. 17, 2017]

[9]. Arnaud R. "25 Definitions of Cloud Computing". Internet: https://www.linkedin.com/pulse/20141117105234-958990-25-definitions-of-cloud-computing, Nov. 17, 2014.[(Feb. 15, 2017]

[10]. Keiko H., David G. R., Eduardo F.M and Eduardo B. F. "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, vol 4, Feb, 2013

[11]. Edgar A., Leslie P. W., and Will V. "Privacy & security in the Cloud", Journal of International Technology and Information Management, vol 22, Nov, 2013.

[12]. MacGillivray K. "A right too far? Requiring cloud service providers to deliver adequate data security to consumers", International Journal of Law and Information Technology, vol 25, pp. 1-25, Sep, 2016.

[13]. Ieuan J. and Loeb L. "Data protection in the United States". Internet: http://us.practicallaw.com/6-502-0467, July. 2017 [August, 20, 2017]

[14]. CNIL "Recommendations for companies planning to use Cloud computing services" Internet: https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf, Jan, 2017, [Aug. 25, 2017]