Ensuring Security and Privacy for Cloud-based E-Services

Khadijah M. Alzhrani
Information Systems Department, Faculty of Computing & Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

Fahd S. Alotaibi
Information Systems Department, Faculty of Computing & Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

ABSTRACT

E-services are becoming more and more a cloud-based with the growth of Cloud Computing and E-society. The aim of this paper is to illustrate those applications and the main challenges that face the adaptation of Cloud Computing, which are mainly privacy and security issues, and what can be done to solve them and prevent problems.

Keywords

Cloud Computing (CC), Mobile Cloud Computing(MCC), Cloud-based E-services, E-health, E-government, E-learning, Privacy, Security, E-government, E-learning, Privacy, Security.

1. INTRODUCTION

Cloud computing (CC) has received a great attention by individuals and societies, the demand for it has been increasing for the last decade [23], [11]. Cloud computing was defined by the National Institute of Standards and Technology (NIST) as 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” [12].

Avram quote from Buyya that the CC can be defined as follow: “Cloud is a parallel and distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLA) established through negotiation between the service provider and consumers”. [11], considered that CC refers to computing services provided within the cloud infrastructure and accessed by customers' demand and needs, without the consideration of details of the service provisioning. While Zissis and Lekkas stated that the CC is empowered by virtualization technology, which provides the critical cloud characteristics of location independence, resource pooling, and rapid elasticity [25]. These virtualized resources such as networks, servers, storages, applications, and services can be dynamically reconfigured to adjust to a mutable load (scale), allowing also for an optimum resource utilization [2], where they can be rapidly conditioned and released with the least management effort or service provider interaction [25]. Also Avram considered that the CC represent a merging of two major points in information technology [2]:

- IT efficiency, where the power of computers is efficiently utilized through dedicated hardware and software resources
- business flexibility, where IT can be used as a competitive tool through rapid deployment, the use of compute-intensive business analytics, and interactive real-time respond mobile applications, through the use of Mobile Cloud Computing (MCC).

Since the increasing of the usage of mobile devices and smartphones platform, MMC aims to upper the level of service's quality through the integration of CC into the mobile environment to enable the users and mobile application providers to use and access the resources of CC on demand [16]. Cloud Services is providing by diverse mobile operators (e.g. AT&T, DT, MT), and technological enterprises (Google, Microsoft, Amazon, Dropbox, Salesforce) based on their network and computing infrastructure [11], where their resources and services are utilized based on customer's demand [23].

According to NIST, the cloud model is composed of three service models and four deployment models (see Figure1), [26].

1.1 Cloud Computing Service Models

Cloud service models are a Service-Oriented Architecture (SOA) that describes services at different levels of abstraction [23], which are:

1.1.1 Software as a Service (SaaS)

The provided ability to the customer is to use the provider's running applications on the cloud by accessing them from various client devices through either a thin client interface, such as a web browser, or a program interface, where the customer does not manage or control the underlying cloud infrastructure e.g. Gmail [12], [11], [16].

1.1.2 Platform as a Service (PaaS)

The provided ability to the customer is to deploy onto the cloud infrastructure to use programming languages, libraries, services, and tools supported by the provider to create or develop applications, where the customer does not manage or control the underlying cloud infrastructure including network, but has control over the deployed applications and possibly configuration settings for the application-hosting environment [12], PaaS provider offers an additional Application Programming Interface (API) to the customer for dynamically adjusting the resources according to the customer needs e.g. Microsoft Azure and Google Application Engine(GAE) [11], [16].

1.1.3 Infrastructure as a Service (IaaS)

The provided ability to the customer is to provision and have total control of processing, storage, networks, and other resources. IaaS provides computation and storage through virtualization using frameworks such as Amazon EC2, where the customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) [12], [11], [16].

And according to 2016 Information and Privacy Commissioner of Ontario (Thinking About Cloud) report, IaaS considered as the basis of all cloud services models as described by the writer (the bottom layer), which provide the major variety of services, with PaaS (the middle layer) structured upon the IaaS, and on top of it SaaS (the top layer) [7].

1.2 Cloud Computing Classifications

CC has been classified into four deployment models, which are:

- **Private cloud**: The cloud infrastructure is provided for exclusive use and owned by a single organization, where It may be managed, and run by the organization, a third party, or some combination of them to serve only the organization needs. Private clouds are considered to be more secure than public clouds since their users are trusted individuals inside the organization [12], [23], [19], [16].
- **Community cloud**: The cloud infrastructure is shared by a specific community of consumers from organizations that have shared concerns. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them e.g. educational cloud used by universities around the world [12], [23], [19].
- **Public cloud**: The cloud infrastructure is open used by the general public. It owned by service provider such as Google and it may be rent parts, managed, and operated by a business, academic, or government organization, or a combination of some of them, where users of it are treated as untrustworthy, security and privacy becomes a big concern about this type of cloud [12], [23], [19].
- **Hybrid cloud:** The cloud infrastructure is a combination of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized technology that enables data and application portability with purpose of providing extra resources in high demand with a medium security level [12], [23], [19].

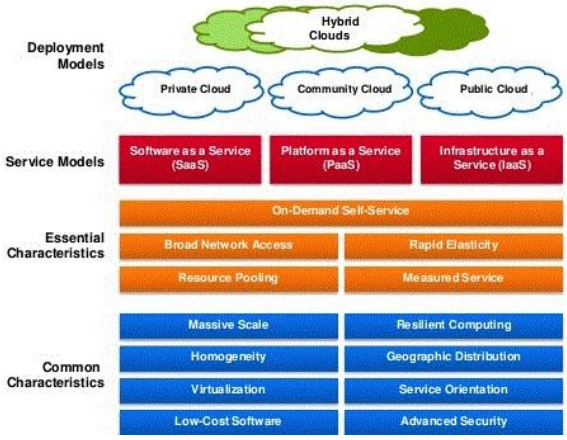


Fig 1: The NIST Cloud definition framework [26].

2. CLOUD-BASED E-SERVICES

CC offers many potentials and services for many E-services, most used Cloud based E-services are E-government, E-learning, and E-health. Youssef research focused on delivering how cloud computing can provide customized, reliable services for E-services. Youssef said that CC is an attractive environment for students, faculty members and researchers, where it can provide universities and research centers with powerful and cost-effective computational infrastructure and where students can connect to campus educational services through their personal mobile devices from anywhere, faculty members can have efficient and flexible access to their course material in their classrooms, and Researchers can find articles, models and share their experiments on the cloud faster [23]. Cloud-based E-learning which are usual provided and controlled by a third party services, can be considered as a method to decrease costs and complexity of data restoring and accessing [10].

According to Intel HealthCare Cloud Computing report, less than one third of healthcare institutions art adopting the cloud with the fast transaction and changing in to electronic systems. Implementing the cloud in E-health offers many potentials for medical insurance institutions including the high quality and speed of processes [8].

In E-government applications, CC can significantly improve the way of governments functions, the provided services to its own citizens and institutions and the cooperating with other governments.

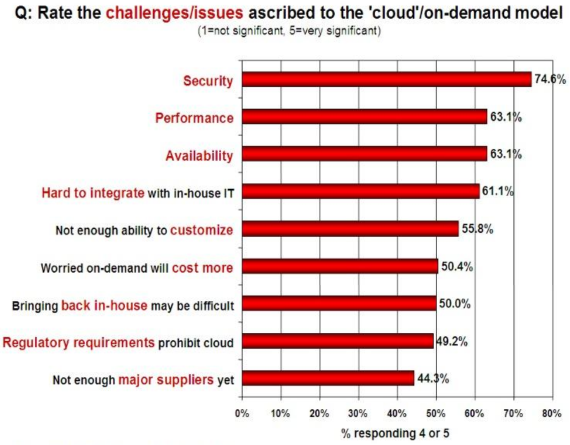
With the lately increased used of different devices with different platform with mobility Rahimi, Ren and Liu added the ability of emerging the MCC in E-learning, and use it through Mobile Learning System (MLE), in E-government in a point of transactions and financial information through M-Commerce, and in E-health through Mobile healthcare and wellness (M-health) [16].

Many information is used in E-services including highly personal information including identification information, financial information and other personal information. That information one way or another are stored and used in the cloud once its implemented.

3. SECURITY AND PRIVACY IN CLOUD-BASED E-SERVICE

Although the distinguish characteristics and benefits of CC, CC and MCC have major challenges and issues that need to be considered. Security and privacy have been the most controversy about cloud computing, which may consider as a barrier to the adaptation of CC and may have a huge effect on the future of the cloud. With the increasing number of cloud users and with the more sensitive information are uploaded in the cloud, security and privacy need to be guaranteed. Also, in MCC; Rahimi, Ren, and Liu noticed that the privacy and security challenges are high priority in all MCC-based E-services, where privacy considered as one of the sensitive issues that had an effect on the deployment of MCC for certain applications where confidential information about users are stored in the cloud [16].

In the International Data Corporation (IDC) Cloud Computing survey, Security had marked as 74.6% (see Figure 2), [5].



Source: IDC Enterprise Panel, August 2008 n=244

Fig 2: IDC's Cloud Computing survey report (2009).

Security and privacy are needed to be ensured not only in data storage but also in computation of CC. Wie, Zhu , Cao, Dong, jia, Chen, and Vasilakos stated that most researchers focused only on data storage security, while they considered that the security needs to be ensured in both data storage and computation, with a taking of consideration of privacy preserving as a critical issue for secure CC by presenting a model for the security problems in CC and proposing and analyzing a basic protocol called SecCloud to attain data storage security and computation [22].

Zissis and Lekkas, considered that security in CC is about defining trust, security identification of threats whether it's inside or outside threats, confidentiality and privacy as a part of security, integrity, and availability. Also, they stated that if a third party is needed and involved, it must be a Trusted Third Party (TTP) to ensure secure interactions between parties through server and client authentication, a creation of security domains, certificate-based authorization and cryptographic separation of data [25].

A mechanism for shared data in the cloud was analyzed by Yu, Yang, MU, and Susilo including privacy-preserving mechanism and distributed storage integrity among other communication issues where they suggested using a secure digital signature scheme to resolve the problems in the original mechanisms [24].

In Cloud-based E-learning Durairaj and Manimaran mentioned in their research, that all SaaS and PaaS and IaaS had security issues, SaaS issues were about the data security including integrity of data, segregation of data, and data breaches and network security, while PaaS issues were about the location of the data and "privileged access", and in IaaS such as Web services attack, and DNS attack that deals with domain name to an IP address. These issues led them to propose a system that consists of a "Cloud-based model to secure E-learning environment" [10].

With the fast transaction and changing to electronic systems and with the government authorization changes for reporting and refunding, led the health-care institutions face more security standers, which make them think again about many electronic approaches and reserves including the adaptation of cloud computing but it also can drive them toward "powerful, cost-efficient, cloud-based IT solution" [8].

Data integrity and confidentiality, and authentication and access control are most worries that need to be under considerations in Cloud-based E-government, where can be prevented by deploying security approaches and techniques [23].

The security and privacy level of cloud computing measured and implemented depending on the kind of E-services work flow and the used information importance, the more highly information and services the more highly worries and protection.

4. METHODOLOGY

Coming to the cloud applications many concerns and question are raised. As mentioned security and privacy consider as the biggest challenges of the cloud computing, which also takes the focus of attention by the public opinion and governments. These questions need to be asked and answered.

- Possession of personal data, who owns personal information and who is trusted with it? Is there a way to ensure that the personal information that has been entrusted to a company, remains only under the seal of the trusted owner?
- Collecting personal information, where can be resulting from impersonal data through applications that can collect and assemble personal information.
- Small data considered as the offender for most usual privacy threats, such as financial information, which may cause huge damage. Is there a way to prevent or limit that?
- Electronic protected health information (e-PHI) and other E-services protected information, though their industry has much to gain from cloud computing and big data, it also has many concerns. e-PHI and other high importance and private E-services information must remain private. Is there a way to gain benefits and maintain e-PHI and other information privacy?
- What about the unauthorized access by snoopers to other corporates? Is there a way to limit the snooping capabilities of corporates, and what about the privacy and security challenges on that?

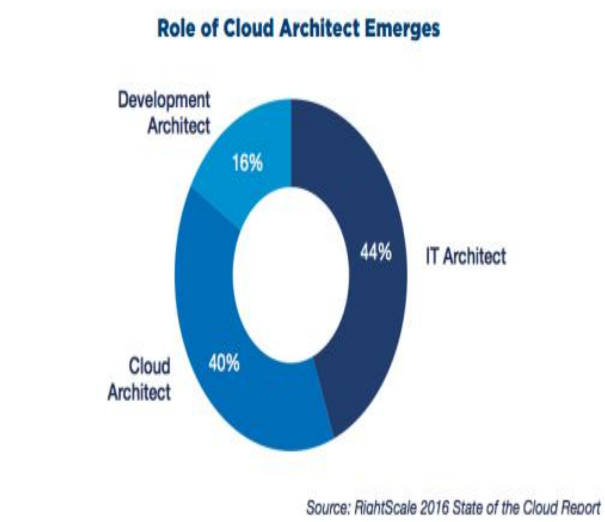
Therefore, many methods need to be applied by all involving parts in the cloud (the cloud provider, third party and stockholders, and E-services and their users), considering all cloud component from head to toe, such as the architecture of the cloud and data storaging. To protect personal information, several methods need to be applied.

Minimizing personal information is a main goal to achieve privacy and security issues in the cloud through:

a. Encryption tools and methods with securely generated and managed encryption and decryption keys that are remain under exclusive control, this can minimize information exposure and risk. Encrypting personal information at breakage and in transportation is the finest way that ensure effective control of information in the cloud, also may be used through the whole processing [7].

b. Tokenization is also a great way to minimize personal information it's a "promising area of security-enhancing technology, where identifiable data is replaced with a random surrogate value, it allows cloud customers to use some cloud computing services, while personal information are held in-house" [7].

According to Right Scale 2016 State of the Cloud report, the role of cloud architect has emerged 40 percent of institutions, as displayed (see Figure 3), [18]. Therefore, architecture security and privacy need to be ensured.



Source: RightScale 2016 State of the Cloud Report

Fig 3: Right Scale 2016 State of the Cloud report 2016

For a secure architecture, security need to be ensured and produced in all CC services models, also there is a need for a secure execution environment for cloud virtual machines (VMs) including networks considering the need for high reliability in the cloud [6].

a. Security as a Service (SaaS) model, need to be considered as a part Software as a Service model to ensure security management to protect and secure data and networks from any threats, consideration about security and privacy also need to ensure in Infrastructure as a Service model for data protection through encryption, authentication and authorization, and monitoring and reporting [6].

b. Current VM-based cloud computing practice does not offer an efficient security execution environment for sensitive applications on cloud end computers. a trusted execution environment (TEE) for VMs need to be engaged such as the suggested one by Jin, Dai, and Zou, which consider as solution to allow multiple customers or VMs on a service cloud-end platform to simultaneously enjoy dynamic root of trust for measurement (DRTM), as in a secure execution environment, without requiring expensive extra hardware [6].

c. Enhancing the reliability of cloud services through approaches such as fault diagnosis and dynamic software updating, when carried out in traditional ways, consumes much time and resources, so to achieve that a software updating need to be consider such as what also Jin, Dai, and Zou suggested to enhance reliability, by presenting two methods of updating: online and offline updating, to update the software of cloud services online and offline through a new automatically offline software update model called UaaS (Update as a Service) [6].

Cloud providers and third party not only should consider the safety of information from being reached, but also they need to ensure privacy of information through having a set of rules and agreements on who have the rights to own, reach the information and use it, considering regulations of IT society and countries such as, "the International Organization for Standardization (ISO), the US National Institute for Standards and Technology (NIST), and some private-sector organizations, such as the American Institute of Chartered Public Accountants (AICPA)".

CC implementations usually contain advanced security technologies, most are available due the implemented architecture and due controlling and managing the [25]. But since the cloud become a base for almost every new technology nowadays and by adopting a cloud architecture with a resource sharing method such as in the public and community cloud, along with the growth of devices and connections many threats are introduced. Trust, knowledge of threats, confidentiality and privacy, and integrity need to be ensured, educate, and obey under countries' legal framework and terms.

Despite the big role of cloud providers' responsibility, customers and users of the cloud also need to be aware of their information security and privacy. Awareness is the best data protection. Each Cloud-based E-Service owners or users should have the full awareness of the Cloud Computing security and privacy issues, what does it need to be ensure, what should the customer do on his behalf to ensure the information safety and what's rights and regulations can he stand for including regulations and standers of other countries that may offer the data storaging, also with the intervention of a third party? better to understand how to integrate federal privacy and security requirements into their practices.

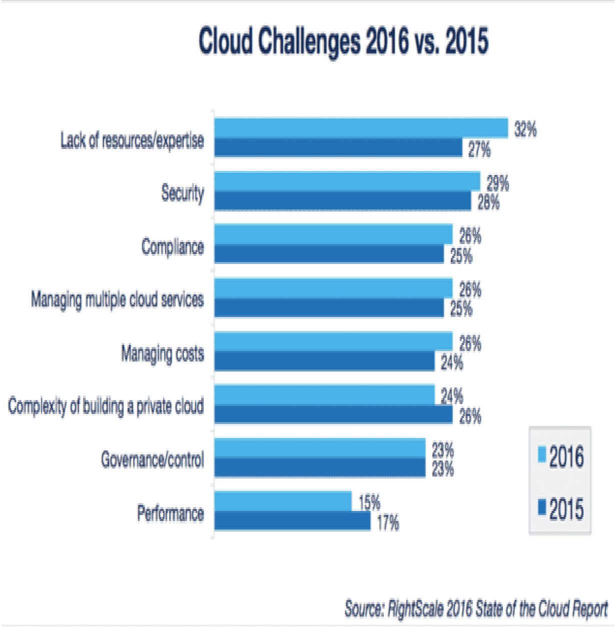
Most Cloud-based E-services share the same security and privacy concerns, but each one of them needs to ensure what is suitable for their own perspective and services, and what kind of information are used and which kind of users they serve.

Also, both cloud provider and cloud customer need to have a plan to attempt the evolutionary in technology also need to attempt if any breach occurred "incident management plan", what is the rescue and recovery plan?

Therefore, to ensure that such issues will not be obstacles for implementing cloud computing, plans and technologies need to be updated. Most new recent security and privacy trends need to be applied in the used cloud architecture, and future developments need to be considered.

Adopting the right privacy and security behaviors, and protection technologies under the seal of regulations and standers will ensure security that will ensure privacy on its behalf, all that together will assure success and conviction for all parts.

As been noticed in the Right Scale Annual Cloud Computing Trends survey (see Figure 4), ensuring security and privacy lately, it's no longer the main issues, but still changes from year to year depending on circumstances and changes in needs and technologies [17].


Cloud Challenges 2016 vs. 2015

Source: RightScale 2016 State of the Cloud Report

Fig 4: Right Scale Cloud Computing trends: 2016 state of the Cloud survey report

One of the main results, since big data is derived by cloud computing, worth to mention ensuring the security and privacy in the cloud should lead to ensuring security and privacy in big data, that’s what has been covered in a report that the white house released on big data called Seizing Opportunities, Preserving Values, discussing big data applications such as into government spending, helping economic recovery, as well as improving education and healthcare, those issues are solvable through Cloud Security Solution for Big Data Applications.

Also, with the enhance of Internet of things (IoT), a new era of opportunities can start to develop new solutions and technologies based on new software and programming models, that may cause so many issues and concerns if an immigration with the cloud happened, especially with the need of collecting and analyzing data.

5. CONCLUSION

Cloud-based E-services has many potentials, but many challenges are stood on it way. The main raised issues were privacy and security issues. These issues need to be considered and solved in view of the highly information that need to be used. Many methods need to be applied but awareness of rights, cloud computing challenges and issues are the main solution to ensure protection and trust at all times. Even though that the CC security and privacy issues are no longer are the main issues, protection and trustworthy behaviors still need to be accrued, and knowledge and awareness need to be increased, especially with the risen of IoT and new IT technologies.

6. REFERENCES

[1] Alshwaier, M., Youssef, Y., and Emam, A. 2012. A new trend for e-learning in ksa using educational clouds.

[2] Avram, M. G. 2014. Advantages and challenges of adopting cloud computing from an enterprise perspective.

[3] Venugopal, S., Broberg, J., Brandic, I., and Buyya, R. 2009. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility.

[4] Gasiorowski-Denis, E. 2015. Trust and confidence in cloud privacy.

[5] Gens, F. 2009. New IDC IT cloud services survey: Top benefits and challenges.

[6] Jin, H., Zou, D. and Dai, W. 2016. Theory and methodology of research on cloud security.

[7] Information and Privacy Commissioner of Ontario.2016. Thinking about clouds? privacy, security and compliance considerations for Ontario public sector institutions.

[8] Intel. How cloud computing can help solve. healthcare's looming it crisis.

[9] Jirasek, V. 2012. Cloud security and security architecture.

[10] Durairaj, M. and Manimaran, A.2015. A study on security issues in cloud based e-learning.

[11] Moura, M. and Hutchison, D. 6016. Review and analysis of networking challenges in cloud computing. Journal of Network and Computer Applications,60:113_129.

[12] NIST. 2011.The NIST definition of cloud computing.

[13] Kumar, S., Kumar, N. K., and Kumar, A.2014. Cloud computing services and its application.

[14] Executive Office of the President. 2014. Big data: Seizing opportunities, preserving values.

[15] The office of the national coordinator for health information technology. 2015. Guide to privacy and security of electronic health information.

[16] Rahimi, R. M., Ren, J., Harold, L. C., Vasilakos, A. V., and Venkatasubramanian, N. 2014. Mobile cloud computing: A survey, state of art and future directions. Mobile Networks and Applications, 19(2):133_143.

[17] Right Scale. 2016. Cloud computing trends: 2016 state of the cloud survey.

[18] Right Scale. 2016. State of the cloud report.

[19] Rong, C., Nguyen, S., and Jaatun, M. G. 2013. Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39(1):47_54.

[20] The office of national coordinator for health information technology. 2015. Guide to privacy and security of electronic health information.

[21] Campo, J. V., Pegueroles, J., Hernández-Serrano, J., and Soriano, M. 2014. Doccloud: A document recommender system on cloud computing with plausible deniability. Information Sciences, 258:387_402.

[22] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., and Vasilakos, A. V. 2014. Security and privacy for storage and computation in cloud computing. Information Sciences, 258:371_386.

[23] Youssef, A. E. 2012. Exploring cloud computing services and applications. Journal of Emerging Trends in Computing and Information Sciences, 3(6):838_847.

[24] Yu, Y., Niu, L., Yang, G., Mu, Y., and Susilo, W. 2014. On the security of auditing mechanisms for secure cloud storage. Future Generation Computer Systems, 30:127_132.

[25] Zissis, D. and Lekkas, D. 2012. Addressing cloud computing security issues. Future Generation computer systems, 28(3):583_592.

[26] WatsoN, A. 2013.Converged Everything, Converged Infrastructure delivering business value and competitive advantage.