Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 110 (2017) 465–472

Procedia Computer Science

www.elsevier.com/locate/procedia

The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017)

A Comprehensive Survey on Security in Cloud Computing

Gururaj Ramachandra[†,‡], Mohsin Iftikhar[†,*], Farrukh Aslam Khan[§]

[†]*School of Computing and Mathematics, Charles Sturt University, Wagga Wagga, NSW, Australia.*
[‡]*Dimension Data Australia, 15 Lancaster place, Majura Park, Canberra ACT 2611, Australia*
[§]*Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia*

E-mail: gururaj.ramachandra@dimensiondata.com, miftikhar@csu.edu.au, fakhan@ksu.edu.sa

Abstract

According to a Forbes' report published in 2015, cloud-based security spending is expected to increase by 42%. According to another research, the IT security expenditure had increased to 79.1% by 2015, showing an increase of more than 10% each year. International Data Corporation (IDC) in 2011 showed that 74.6% of enterprise customers ranked security as a major challenge. This paper summarizes a number of peer-reviewed articles on security threats in cloud computing and the preventive methods. The objective of our research is to understand the cloud components, security issues, and risks, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud. It is a commonly accepted fact that since 2008, cloud is a viable hosting platform; however, the perception with respect to security in the cloud is that it needs significant improvements to realise higher rates of adaption in the enterprise scale. As identified by another research, many of the issues confronting the cloud computing need to be resolved urgently. The industry has made significant advances in combatting threats to cloud computing, but there is more to be done to achieve a level of maturity that currently exists with traditional/on-premise hosting.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Cloud computing; Security in cloud; Security Threats

* Corresponding author. Tel.: +61-2-6933-2048; fax: +61-2-6933-4766.
E-mail address: miftikhar@csu.edu.au

1877-0509
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.06.124

1. Introduction

Cloud computing is increasingly being adapted by a wide range of users starting from commercial entities to consumers. A survey by Right Scale[1] found that an average user runs at least four cloud-based applications and at any point in time is evaluating another four. The survey also found that 41% of commercial entities run significant workload on public clouds. With so much of our workload moving to cloud, security in cloud computing is under increased scrutiny. This assessment is also supported by the 2017 report by Forbes[2], which says that in 15 months, while 80% of all IT budgets will be committed to cloud solution, 49% of the businesses are delaying cloud deployment due to security skills gap and concerns. The problem appears to be multi-dimensional, with lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few. Adaption of cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to cloud from not just average Internet users, but also from most if not all commercial entities. While there are many problems that need identifying, analyzing, and addressing, this document attempts to survey the security in cloud computing and reports on various aspects of security vulnerabilities and solutions. Some questions that need urgent answers are: (a) Privileged User Access Management, (b) Regulatory Compliance, (c) Data Location, (d) Data Segregation, (e) Data Protection and Recovery Support, (f) Investigative Support, and (g) Long-term Viability.

It is highly recommended that these questions, along with other risks, are assessed and addressed. Some of the assessments could be as follows:

a. *Organization capability and maturity*
b. *Technology & data risks*
c. *Application migration and performance risk*
d. *People risks*
e. *Process risks*
f. *Policy risks*
g. *Extended supply chain risks*

This article consolidates various works that address the risks, vulnerabilities, and potential controls in cloud computing. It also provides information on leading cloud architectures and frameworks. Moreover, the article identifies potential future research areas related to security in cloud computing.

The remainder of the paper is organized as follows: The cloud architecture is discussed in section 2. Section 3 discusses the security implications based on deployment and delivery models. General vulnerabilities, attacks, and threats are explained in section 4, whereas section 5 gives insights into countermeasures and controls. Finally, section 6 concludes the paper with potential future directions.

2. Cloud Architecture

Before we dive into the security issues, it is important to understand the cloud definition and architecture. According to Sharma and Trivedi[3], cloud computing is a set of resources that can scale up and down on-demand. It is available over the Internet in a self-service model with little to no interaction required with the service provider. Cloud enables new ways of offering products and services with innovative, technical, and pricing opportunities.

As per NIST's Cloud Computing Reference Architecture[4], there are five major actors that influence and are impacted by cloud computing, along with its security implications. This document focuses on cloud consumer and cloud provider's threat and risk perceptions.

Table 1: Actors in NIST Cloud Computing Reference Architecture[4]

Actor	Definition
Cloud Consumer	A person or Organisation that maintains a business relationship with, and uses service from, *Cloud Provider*
Cloud Provider	A person, organisation, or entity responsible for making a service available to interested parties
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation
Cloud Broker	An Entity that manages the use, performance, and delivery of cloud services and negotiates relationship between *Cloud providers* and *Cloud Consumers*
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*

Figure 1 is a complete reference architecture for cloud computing. It is important to note that the figure represents an end-to-end reference architecture that addresses all the seven layers of the Open Systems Interconnection (OSI) model, and extends to include the business, commercial, and governance aspects. As it is evident, cloud computing is a comprehensive and complex solution with many areas of vulnerabilities.

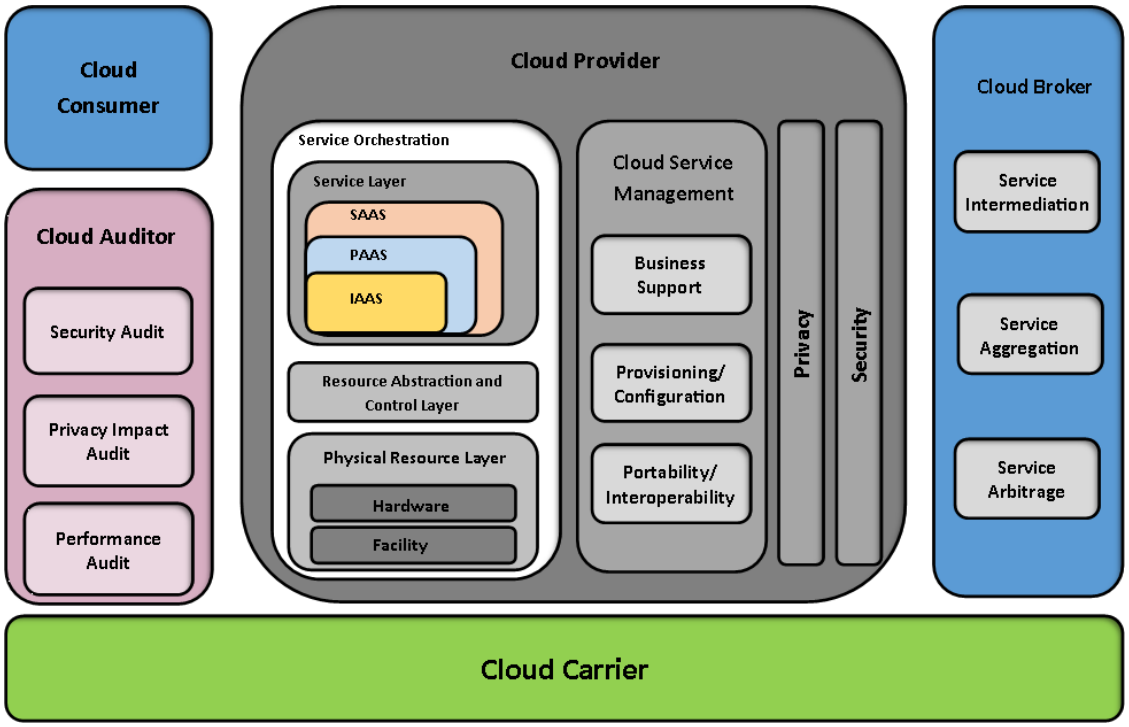

Figure 1: NIST Cloud Computing Reference Architecture[4]

2.1. Advantages of Cloud

According to Avram[5], there are some unique advantages to cloud computing. Some of the key advantages are:

1. Cost of entry for all organizations including small firms
2. Almost immediate access to the resources

3. Reduction in IT barriers to innovation
4. Easy to scale the services
5. Implement and/or offer new class of application and delivery services

3. Security Implications based on Deployment and Delivery Models

The two most important aspects that determine the level of vulnerability in a cloud-computing platform is the choice of deployment and delivery model. According to Modi et al.[6] & NIST[4], there are three deployment and three delivery models that are considered as industry standards. Each of these three deployment and delivery models have unique security implications. The following sub-sections briefly discuss each of these models and their security implications:

3.1. Cloud Deployment Model

The three most common types of cloud deployment models[7] are Private Cloud, Public Cloud, and Hybrid Cloud.

Table 2: Cloud Deployment Model

Deployment Type	Description	Implications	Challenges
Private Cloud	In a private cloud, the cloud service provider pools together scalable resources and virtual applications and makes them available to the cloud consumers. In this deployment model, the resources are dedicated to a single or a set of organizations and treated as an intranet functionality. The billing usually is on a subscription basis with a cloud consumer making minimum commitments.	Positive security implications are relatively high and the organization has significant influence on the architecture, processes, and tools used in the deployment.	Security challenges include high cost of implementation and management, skills requirement, and vulnerability management. In this deployment model, cost and return on investment are key factors and the security implementation is usually based on risk assessment and hence, the security cover is not comprehensive.
Public Cloud	In a public cloud, resources are dynamically committed on a fine-grained, self-service basis over the Internet or a portal[10]. Billing is usually consumption-based and is charged on a pay per use basis.	Positive security implications are that due to a large number of cloud consumers and volumes of transactions involved. The cloud service provider normally has a comprehensive & layered security system, which can potentially provide a high degree of security due to its implement once and use multiple times model, which significantly reduces the cost of security implementation for the consumer.	Security challenges are heightened, as the resources are not committed but leveraged across multiple cloud consumers. This not only adds additional burden of ensuring all applications and data accessed on the public cloud, but also has to manage the multitude of external influences such as legislative, data protection etc.
Hybrid Cloud	Hybrid cloud is a deployment model where a private cloud is linked to one or more external cloud services while being managed centrally. It provides the cloud consumers a flexible and fit-for-purpose solution with a relative ease of operations. The hybrid clouds have a higher degree of complexity in terms of billing and commercials.	Positive security implications are that security can be purpose-built for vulnerabilities, threats, and risks that are assessed. This makes it cost-effective and targeted.	Security challenges are relatively high as the deployment model is complex with heterogeneous environment, multiple orchestration, and automation tools. This will require additional administrative overhead, with any oversight resulting in significant risk exposure.

3.2. Cloud Delivery Model

The three cloud delivery models proposed by NIST and adapted by the industry are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Table 3: Cloud Delivery Model

Delivery Type	Description	Risk and responsibility
Infrastructure as a Service (IaaS)	Infrastructure as a Service is a multi-tenant cloud layer where the cloud service provider dedicated resources are only shared with contracted clients at a pay-per-use fee. This typically means that Operating System is presented to the cloud consumer. The cloud service provider's responsibility ends with the operating system.	This is a great model where the cloud consumer builds the application without worrying about the infrastructure requirements. The security responsibility is equally divided between the cloud service provider and the cloud consumer. In this model, the risk is segregated and layered. It is also a shared risk model.
Platform as a Service (PaaS)	Platform as a Service is one of the more popular delivery services where the cloud provider provisions not just the operating system but also a development stack. It is a common practice for providers in this model to provide database and application administration along with development services. Just as in IaaS, PaaS is a pay-per-use model.	This is an appropriate model, where the cloud consumer brings the application expertise along with licenses, data, and resources, and consumes the platform shell. This model is used by consumers who either lack infrastructure skills or want to save on high capital expenditure (capex) spend required to build the infrastructure. In this delivery model, the security responsibility starts to tilt more towards the cloud provider. Similar to IaaS, this is a shared risk model, however, the service provider bears higher risk than consumer as the provider supports more layers.
Software as a Service (SaaS)	In a Software as a Service model, the complete application stack is hosted by the cloud provider, who provides end-to-end resources, including licensing, application, networking etc., The cloud consumer, typically brings the data and business processes to consumes the services in a web service or software-oriented architecture.	This model is very effective in cases where the cloud consumer does not have the necessary skills, time, or resources to setup an application ecosystem and manage it. This model also provides the best commercial benefit with no upfront capex requirement. The security responsibility is mostly with the cloud provider. The consumer is mainly responsible for securing the client-side vulnerabilities. In this model, the service provider bears most risk.

4. General Vulnerabilities, Threats, and Attacks in Cloud

Cloud computing, like other areas of IT, suffers from a number of security issues, which need to be addressed[8,11,12,13]. These risks pertain to policy and organization risks, technical risks, and legal and other risks[9].

4.1. Vulnerabilities and open issues

Cloud is a set of technology, process, people, and commercial construct. Like all other technology, process, people, and commercial construct, cloud too has vulnerabilities. The following are some of the vulnerabilities in a cloud. Some of the open issues and threats that needs urgent attention are as follows:

a. ***Shared Technology vulnerabilities*** – increased leverage of resources gives the attackers a single point of attack, which can cause damage disproportional to its importance. An example of share technology is a hypervisor or cloud orchestration.
b. ***Data Breach*** – with data protection moving from cloud consumer to cloud service provider, the risk of accidental, malicious, and intentional data breach is high.
c. ***Account of Service traffic hijacking*** – one of the biggest advantages of cloud is access through Internet, but the same is a risk of account compromise. Loosing access to privileged account might mean loss of service.
d. ***Denial of Service (DoS)*** – any denial of service attack on the cloud provider can affect all tenets
e. ***Malicious Insider*** – a determined insider can find more ways to attack and cover the track in a cloud scenario.
f. ***Internet Protocol*** – many vulnerabilities inherent in IP such as IP spoofing, ARP spoofing, DNS Poisoning are real threats.
g. ***Injection Vulnerabilities*** – vulnerabilities such as SQL injection flaw, OS injection, and LDAP injection at the management layer can cause major issues across multiple cloud consumers.
h. ***API & Browser Vulnerabilities*** – Any vulnerability in cloud provider's API or Interface poses a significant risk, when coupled with social engineering or browser based attacks; the damage can be significant.
i. ***Changes to Business Model*** – cloud computing can be a significant change to a cloud consumer's business model. IT department, and business needs to adapt or face exposure to risk.
j. ***Abusive use*** – certain features of cloud computing can be used for malicious attack purposes such as the use of trail period of use to launch zombie or DDoS attacks.
k. ***Malicious Insider*** – a malicious insider is always a major risk, however, a malicious insider at the cloud provider can cause significant damage to multiple consumers.
l. ***Availability*** –the probability that a system will work as required and when required.

4.2. Attack Vectors

According to a recent research[8], the three major vectors of attack are network, hypervisor, and hardware. These vectors are mapped to attacks such as external, internal, and cloud provider or insider attack respectively.

5. Countermeasures & Controls

The vulnerabilities and threats in the cloud are well documented. Each cloud service provider and cloud consumer has to devise countermeasures and controls to mitigate the risks based on their assessment. However, the following are some of the best practices in countermeasures and controls that can be considered:

a. ***End-to-end encryption*** – the data in a cloud delivery model might traverse through many geographical locations; it is imperative to encrypt the data end-to-end.
b. ***Scanning for malicious activities*** – end-to-end encryption while highly recommended, induces new risks, as encrypted data cannot be read by the Firewall or IDS. Therefore, it is important to have appropriate controls and countermeasures to mitigate risks from malicious software passing through encryption.

c. ***Validation of cloud consumer*** – the cloud provider has to take adequate precautions to screen the cloud consumer to prevent important features of cloud being used for malicious attack purposes.
d. ***Secure Interfaces and APIs*** – the interfaces and APIs are important to implement automation, orchestration, and management. The cloud provider has to ensure that any vulnerability is mitigated.
e. ***Insider attacks*** – cloud providers should take precaution to screening employee and contractors, along with strengthening internal security systems to prevent any insider attacks.
f. ***Secure leveraged resources*** – in a shared/multi-tenancy model, the cloud provider has secure shared resources such as hypervisor, orchestration, and monitoring tools.
g. ***Business Continuity plans*** – Business continuity plan is a process of documenting the response of the organization to any incidents that cause unavailability of whole or part of a business-critical process.

6. Conclusion

Security in cloud computing is evolving in step with risks as they are discovered often too late to prevent incidents. Cloud computing due to its disruptive nature, complex architecture, and leveraged-resources pose a unique and severe risk to all actors. It is critical to all stakeholders and actors to understand the risk and mitigate it appropriately. Security needs to be built at every layer in a cloud-computing platform by incorporating best practices and emerging technologies to effectively mitigate the risk. In the cloud, consumer, provider, broker, carrier, auditor, and everyone else has to take the necessary precautions against risks to truly secure the cloud-computing platform or be exposed to significant and sometimes business critical risk. According to a recent survey, the industry recognizes that security engineering provides best practices, methods, and techniques for developing systems and services, which are built for security, sustainability, and resiliency. It is important to take this research forward to provide such best practices to more applications and use cases. It is also essential to conduct further research in systems development life cycle (SDLC) for cloud consumers to incorporate various development and technological advancement models and container systems such as Docker to improve security at a fundamental level. Additionally, there is very limited research on training and people impact on security. Work can be done to understand the challenges, requirements, and impact of effective security training for consumers and other providers.

References

1. State of the Cloud Report. (2017). https://www.rightscale.com/lp/state-of-the-cloud (Retrieved 25 May 2017)
2. State of Cloud Adoption And Security. (2017). https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/ (Retrieved 25 May 2017)
3. Sharma, R. & Trivedi, R. K. (2014). Literature review: Cloud Computing –Security Issues, Solution and Technologies. International Journal of Engineering Research, Vol. 3, Issue 4, pp. 221-225.
4. National Institute of Standards and Technology, (2011). NIST *Cloud Computing Reference Architecture*. https://www.nist.gov/publications/nist-cloud-computing-reference-architecture
5. Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, Vol. 12, pp. 529-534.
6. Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2012). A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing,* Vol. 63, Issue 2, pp. 561–592.
7. Kuyoro S. O., Ibikunle, F., and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks (IJCN),* Vol. 3, Issue 5, pp. 247-255.

8. Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2016). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2016.03.004
9. European network and Information Security Agency. (2009). Cloud Computing: Benefits, risks and recommendations for information security. *https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/*
10. Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M., and Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 2012 1:11. DOI: 10.1186/2192-113X-1-11
11. Ramachandran, M. (2015). Software security requirements management as an emerging cloud computing service. International Journal of Information Management, Vol. 36, Issue 4, pp. 580-590.
12. Roundup of Cloud Computing Forecasts and Market Estimates, 2015. (2015). http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/#56c0b0f0740c (Retrieved 2 May 2016)
13. Wang, C. (2009). Cloud Computing Checklist: How Secure Is Your Cloud? (2009). *Forrester Research*. https://www.forrester.com/report/Cloud+Computing+Checklist+How+Secure+Is+Your+Cloud/-/E-RES55453