International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928| Monthly, Peer Reviewed & Referred Journal|

Volume 3, Issue 7, July 2020 |

A Thorough Examination of Privacy Issues using Self-Service Paradigms in the Cloud Computing Context

Pankit Arora[1*], Sachin Bhardwaj[2]

Sr. Risk Modeling/Analytics Analyst, Mr. Cooper, USA[1]

Assistant Manager (GRC), EXL Service Pvt Ltd. India[2]

ABSTRACT: Spending on cloud-based security is anticipated to rise by 42%, per a 2015 Forbes article. Another study claims that by 2015, IT security spending had risen to 79.1%, indicating an annual increase of more than 10%. According to a 2011 International Data Corporation (IDC) survey, 74.6% of business clients said security was a significant concern. Numerous peer-reviewed publications about cloud computing security concerns and mitigation strategies are compiled in this paper. Our research's goal is to comprehend the threats, security concerns, and components of the cloud as well as new developments that could lessen its vulnerabilities. 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 realize 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 hosting.

KEYWORDS: Cloud computing; Security in cloud; Security Threats.

I. INTRODUCTION

Cloud computing is increasingly being adapted by a wide range of users starting from commercial entities to consumers. A survey by Right Scale 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, 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 [1-12]. 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 [13-27]: (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.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928| Monthly, Peer Reviewed & Referred Journal|

Volume 3, Issue 7, July 2020 |

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.

II. CLOUD ARCHITECTURE

Before we dive into the security issues, it is important to understand the cloud definition and architecture. 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 [28-33]. Cloud enables new ways of offering products and services with innovative, technical, and pricing opportunities.

As per NIST's Cloud Computing Reference Architecture, there are five major factors that influence and are impacted by cloud computing, along with its security implications [34-41]. This document focuses on cloud consumer and cloud provider's threat and risk perceptions.

Table 1: Actors in NIST Cloud Computing Reference Architecture

Factor	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

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928| Monthly, Peer Reviewed & Referred Journal|

Volume 3, Issue 7, July 2020 |

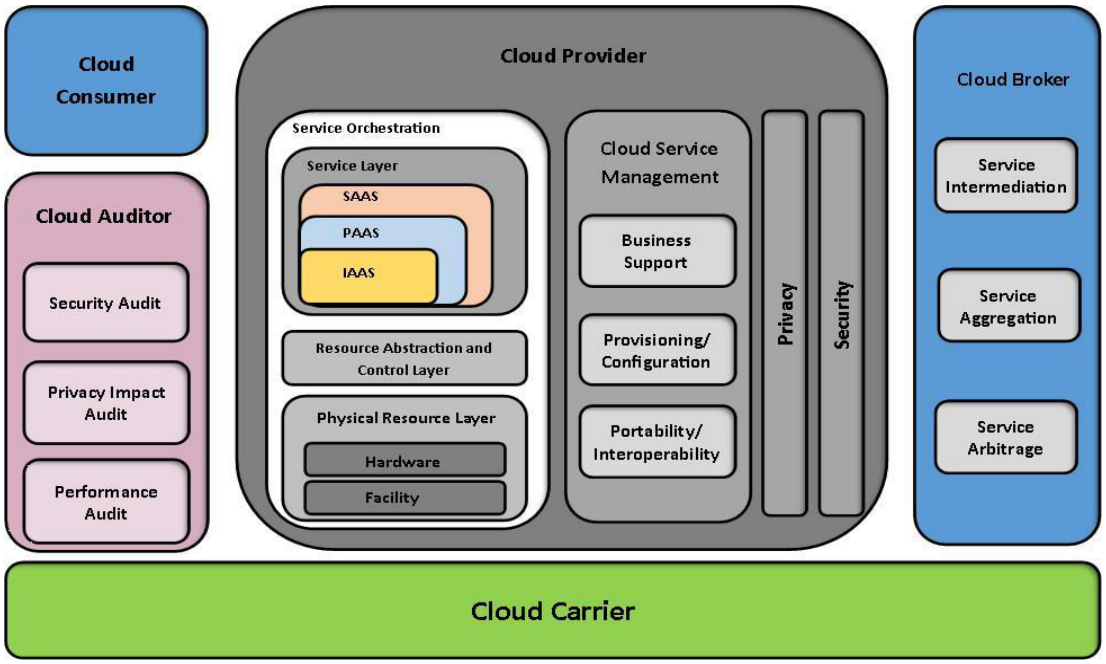

Figure 1: NIST Cloud Computing Reference Architecture

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 [42-47].

2.1. Advantages of Cloud

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

III. 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. 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 are Private Cloud, Public Cloud, and Hybrid Cloud.

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).

IV. 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. These risks pertain to policy and organization risks, technical risks, and legal and other risks.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928| Monthly, Peer Reviewed & Referred Journal|

Volume 3, Issue 7, July 2020 |

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.

V. 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.

VI. 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

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928| Monthly, Peer Reviewed & Referred Journal|

Volume 3, Issue 7, July 2020 |

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) Serageldin, H. Alturkostani, and A. Krings, “On the reliability of DSRC safety applications: a case of jamming,” in International Conference on Connected Vehicles and Expo, 2013, pp. 501–506.
2) B.K. Chaurasia, R.S. Tomar, S. Verma, G.S. Tomar, Suitability of manet routing protocols for vehicular ad hoc networks, in: 2012 International Conference on Communication Systems and Network Technologies, IEEE, 2012, pp.334–338.
3) Laurendeau and M. Barbeau, “Threats to security in DSRC/WAVE,” in Proc. 5th International Conference on Ad-Hoc Networks & Wireless, LNCS 4104, 2006, pp. 266–279.
4) E. Hamida, H. Noura, and W. Znaidi, “Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures,” Connected Vehicles, V2V Communications, and VANET, vol. 4, no. 3, pp. 380–423, 2015.
5) F.K. Karnadi, Z.H. Mo, K.-c. Lan, Rapid generation of realistic mobility models for vanet, in: 2007 IEEE Wireless Communications and Networking Confer-ence, IEEE, 2007, pp.2506–2511.
6) H. Hasbullah, I. Soomro, and J. Ab Manan, “Denial of service (DOS) attack and its possible solutions in VANET,” International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, vol. 4, no. 5, pp. 813–817, 2010.
7) H.-M. Zimmermann, I. Gruber, C. Roman, A Voronoi-based mobility model for urban environments, in: 11th European Wireless Conference 2005-Next Generation Wireless and Mobile Communications and Services, VDE, 2005, pp.1–5.
8) J. Härri, F. Filali, C. Bonnet, M. Fiore, Vanetmobisim: generating realistic mo-bility patterns for vanets, in: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, ACM, 2006, pp.96–97.
9) J. Harri, M. Fiore, Vanetmobisim–vehicular ad hoc network mobility exten-sion to the canumobisim framework, Institut Eurécom Department of Mobile Commu 6904 (2006) 1–19.
10) J. Zhao, G. Zucchelli, and M. Roggero, “Design of FMCW radars for active safety applications,” http://embedded-computing.com/articles/design-fmcw-radars-active-safety-applications/, 2015.
11) L. Bononi, M. Di Felice, M. Bertini, E. Croci, Parallel and distributed simulation of wireless vehicular ad hoc networks, in: Proceedings of the 9th ACM In-ternational Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems, ACM, 2006, pp.28–35.
12) M. Brooker, “Mutual interference of millimeter-wave radar systems,” IEEE Transactions on Electromagnetic Compatibility, vol. 49, pp. 170–181, 2007.
13) M. Piorkowski, M. Raya, A.L. Lugo, P. Papadimitratos, M. Grossglauser, J.-P. Hubaux, TRANS: realistic joint traffic and network simulator for vanets, Mob. Comput. Commun. Rev. 12 (2008) 31–33.
14) N. Li and Y. Zhang, “A survey of radar ECM and ECCM,” IEEE Trans. Aerospace and Electronic Systems, vol. 31, no. 3, pp. 1110–1120, 1995.
15) N. Wisitpongphan, O.K. Tonguz, J.S. Parikh, P. Mudalige, F. Bai, V. Sadekar, Broadcast storm mitigation techniques in vehicular ad hoc networks, IEEE Wirel. Commun. 14 (2007) 84–94.
16) Q. Chen, T. Roth, T. Yuan, J. Breu, F. Kuhnt, M. Zollner, M. Bogdanovic, C.Weiss, J. Hillenbrand, and A. Gern, “DSRC and radar object matching for cooperative driver assistance systems,” in IEEE Intelligent Vehicles Symposium, 2015, pp. 1348–1354.
17) Q. Xu, T. Mak, J. Ko, and R. Sengupta, “Vehicle-to-vehicle safety messaging in DSRC,” in Proceedings of the 1st ACM International Workshop on Vehicular ad hoc Networks, 2004, pp. 19–28.
18) R. Chauhan, “A platform for false data injection in frequency modulated continuous wave radar,” http://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4983&context=etd, 2014.
19) R. Fernandes, P.M. d’Orey, M. Ferreira, Divert for realistic simulation of hetero-geneous vehicular networks, in: The 7th IEEE International Conference on Mo-bile Ad-Hoc and Sensor Systems (IEEE MASS 2010), IEEE, 2010, pp.721–726.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928| Monthly, Peer Reviewed & Referred Journal|

Volume 3, Issue 7, July 2020 |

20) R. Mangharam, D.S. Weller, D.D. Stancil, R. Rajkumar, J.S. Parikh, Groovesim: a topography-accurate simulator for geographic routing in vehicular networks, in: Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks, ACM, 2005, pp.59–68.
21) S. Senthilkumar, R. Nithya, P. Vaishali, R. Valli, G. Vanitha, & L. Ramachanndran, "Autonomous navigation robot", International Research Journal of Engineering and Technology, vol. 4, no. 2, 2017.
22) S. Jaap, M. Bechler, L. Wolf, Evaluation of routing protocols for vehicular ad hoc networks in typical road traffic scenarios, 2005, pp.584–602.
23) S. Maddio, A. Cidronali, M. Passafiume, G. Collodi, and G. Manes, "Interference cancellation for the coexistence of 5.8 GHz DSRC and 5.9 GHz ETSI ITS," in IEEE MTT-S International Conference on Microwaves for Intelligent Mobility, 2015, pp. 1–4.
24) S. Roome, "Digital radio frequency memory," Electronics & Communication Engineering Journal, vol. 2, no. 4, pp. 147–153, 1990.
25) S.-Y. Wang, C.-L. Chou, Nctuns Simulator for Wireless Vehicular Ad Hoc Net-work Research, Ad Hoc Networks: New Research, Nova Science Publishers, 2009.
26) T. Fujiki, M. Kirimura, T. Umedu, T. Higashino, Efficient acquisition of local traffic information using inter-vehicle communication with queries, in: 2007 IEEE Intelligent Transportation Systems Conference, IEEE, 2007, pp.241–246.
27) T. Jeyaprakash, R. Mukesh, A survey of mobility models of vehicular adhoc networks and simulators, Int. J. Electron. Inf. Eng. 2 (2015) 94–101.
28) T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: challenges and a solution framework," IEEE Internet of Things Journal, vol. 1, pp. 10–21, 2014.
29) V. Richard, Millimeter wave radar applications to weapons systems, USA Ballistic Research Laboratories, 1976.
30) V.D. Khairnar, S. Pradhan, Comparative study of simulation for vehicular ad-hoc network, preprint, arXiv:1304 .5181, 2013.
31) W. Zhang, H, Zeng, Y, Li, and X. Wang, "Polarimetric radar performance test of signal processing for anti-active jamming," in IET International Radar Conference, 2009, pp. 1–4.
32) X. Qiao, T. Jin, X. Qi, M. Zhang, S. Yuan, and Q. Zhang, "Anti-millimeter wave polarization agile active jamming," in Proceedings of the International Conference on Microwave and Millimeter Wave Technology, 2007, pp. 1–4.
33) Y.P. Fallah, C. Huang, R. Sengupta, H. Krishnan, Congestion control based on channel occupancy in vehicular broadcast networks, in: 2010 IEEE 72nd Ve-hicular Technology Conference-Fall, IEEE, 2010, pp.1–5.