IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125227

A Survey of the State of Cloud Security

Dipali Vivek Thakre[1], Lovelesh N. Yadav[2], Neehal B. Jiwane[3]

Student, Computer Science & Engineering, Shri Sai College of Engineering &Technology, Bhdrawati, India[1]

Head Of Department, Computer Science & Engineering, Shri Sai College Of Engineering & Technology, Bhdrawati, India[2]

Asst.prof, Computer Science & Engineering, Shri Sai College Of Engineering & Technology, Bhdrawati, India[3]

Abstract: Cloud computing has emerged as an important paradigm in computing today with the potential to offer scalable, fault tolerant services and reduce costs significantly. However, security concerns present significant barriers in its adoption industry wide. The multitenant nature of the cloud and the fact that data is stored in multiple locations compound these security concerns. Confidentiality, authenticity, integrity, availability and auditability are key aspects that need to be accounted for, when dealing with security. Guarantees of secure data and transactions from the service provider will enable more users to migrate to a cloud environment. Employing Intrusion Detection Systems, Cryptographic techniques and Computer Forensic Tools that recover deleted files and collect digital evidence of intruder activities are among some of the guarantees a trustful service provider can provide. This paper presents a survey on some of the common threats and associated risks on cloud platforms along with ways of tackling these threats. We also review data management and security model of some of the leading cloud service providers.

Keywords: cloud computing security, cloud computing, cloud risk assessment

I. INTRODUCTION

Cloud computing was identified by Gartner as one of the top 10 strategic technologies for 2012 with the potential for significant impact on enterprises in the coming years (Gartner, 2011). Applications deployed on the cloud inherit the ability to scale up and down giving the illusion of infinite computing resources being available. This approach allows flexibility while allocating resources and enables a cloud customer to pay only for resources that he consumes thus avoiding costs associated with over provisioning and downtime associated with under provisioning. The pay-as-you-go model is profitable to businesses that do not want to worry about maintaining the hardware or employing administration staff. The new enterprise model of Everything-as-a-Service promotes the idea of making applications, storage and computing power available online through the cloud. Platform, Software and Infrastructure as a service are paradigms well known in computing today. Platform as a service (PaaS) provides a computing platform and environment for building web applications and services. Software as a Service (SaaS) provides business applications as a service eliminating the need for businesses to install and support applications. In the Infrastructure as a service cloud, users are given on-demand access to virtual machines. The user sees a bare bone machine with just an operating system. The user gets full flexibility to install and configure software on this machine. The same concept can be extended to Database-as-a-Service (DaaS). The past few years has seen a gradual change from in-house data management to cloud-hosted data management. Cloud Database-as-a-Service provides on-demand access to database features like data definition, storage and retrieval. It also provides data access and storage services and enables end users to be oblivious of the location and configuration of the system delivering the services.

II. RELATED WORK

Security threats and risks associated with the cloud have been the focal point of many studies. Vaquero et (Vaquero, Rodero-Merino, & Moran, 2011) present some common cloud threats and associate these with different levels in the IaaS cloud architecture: network virtualization domain, machine virtualization domain, and physical domain. S. Subashini et al. (2011) present a survey on the security issues in different service models of the cloud: SaaS, PaaS and IaaS. They identify data security, data integrity, data availability and network security as some of the security concerns in the SaaS model. Attacks on visible code such as code running in user context are identified as an example of security issues faced in the PaaS model. Security holes in the virtualization manager are examples of issues in the IaaS model. Minqi et al. (2010) present issues that accompany multi location of data. Many large cloud providers like Amazon and Google mirror data across geographical regions around the world in order to increase availability. This makes an already bad situation even worse because the privacy laws that apply on customers data now depend on the location of the data. The authors also review some of the privacy protection acts that came into being to protect consumers privacy but hold no ground

DOI: 10.17148/IJARCCE.2023.125227

when applied to the cloud environment. Tsai et al. (2012) discuss security threats from the perspective of virtualization technologies since virtualization is one of the foundations of cloud computing. The authors discuss the implications of virtualization on the different service models (SaaS, PaaS and IaaS). Somani et al. (2010) discuss security issues associated with storing highly sensitive medical data in the cloud. Contractual obligations committed by a service provider do not suffice when it comes to medical data management. The paper stresses on employing Computer Forensics Tools to help uncover issues with cloud.

III. SECURITY THREATS

The Verizon 2011 data breach investigations report (DBIR) presents the categories of security threats that businesses are vulnerable to today (Verizon Business, 2011). The report shows that the greatest security threats stem from external agents (92%). External agents include hackers, organized crime groups and environmental factors such as earthquakes. Insider attacks contribute to 17% of data breaches. Business partner caused breaches contribute less than 1% (Verizon Business, 2011). Business partners include suppliers, vendors, outsourced service support and any third party involved in a business relationship with the organization. The DBIR also presents the most common types of security breaches. Hacking (50%) and malware (49%) take the lead. Physical Attacks (14%) have doubled over the last couple of years. Privilege misuse (17%) like embezzlement and fraud and social tactics (11%) like solicitation and bribery fill up the bottom two positions for types of security breaches. Though the percentages shown above were not tailored specifically to cloud security threats, the report does factor in the loss of control over a company's data and assets. This loss of transparency accompanied with the shared, on-demand nature of the cloud not only introduces new challenges but also amplifies certain existing issues. In this section, we discuss some of the security challenges faced in the cloud.

ACKNOWLEDGMENT

The This research has been supported by the Fidelity National Financial Distinguished Professorship in Computer

REFERENCES

1.Ahmed, S., & Raja, M. Y. A. (2010). Tackling cloud security issues and forensics model. High-Capacity Optical Networks and Enabling Technologies (HONET) (pp. 190-195), 19-21.

2.Amazon. (2011). Amazon Web Services Overview of Security Processes. Retrieved from http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf Amazon. (2012).

3.AWS Risk and Compliance. Retrieved from http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf Amazon Web Services. (2012). Service Health Dashboard. Retrieved from http://status.aws.amazon.com/ Anchises, M. G. de Paula. (2009). Cloud Computing: Enterprise Risks and Mitigation.