International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 6, Issue 1 (JAN-FEB 2018), PP. 07-11

CLOUD SECURITY: A SURVEY ON RECENT DEVELOPMENTS

Rashmi[1], Rahul Dekar [2],
[1]Research Scholar, Bansal Institute of Engineering & Technology
[2]Assistant Professor, Bansal Institute of Engieering &Technology
Lucknow, Uttar Pradesh

***Abstract*— Cloud computing is revolutionizing many ecosystems by providing organizations with computing resources featuring easy deployment, connectivity, configuration, automation and scalability. This paradigm shift raises a broad range of security and privacy issues that must be taken into consideration. Multi-tenancy, loss of control, and trust are key challenges in cloud computing environments. This paper reviews the existing technologies and a wide array of both earlier and state-of-the-art projects on cloud security and privacy. We categorize the existing research according to the cloud reference architecture orchestration, resource control, physical resource, and cloud service management layers, in addition to reviewing the existing developments in privacy-preserving sensitive data approaches in cloud computing such as privacy threat modeling and privacy enhancing protocols and solutions.**

***Index Terms*— Cloud Security, Privacy, Trust, Virtualization, Data Protection**

I. INTRODUCTION

Cloud computing is revolutionizing many of our ecosystems, including healthcare. Compared with earlier methods of processing data, cloud computing environments provide significant benefits, such as the availability of automated tools to assemble, connect, configure and reconfigure virtualized resources on demand. These make it much easier to meet organizational

Goals as organizations can easily deploy cloud services. However, the shift in paradigm that accompanies the adoption of cloud computing is increasingly giving rise to security and privacy considerations relating to facets of cloud computing such as multi-tenancy, trust, loss of control and accountability. Consequently cloud platforms that handle sensitive information are required to deploy technical measures and organizational safeguards to avoid data protection breakdowns that might result in enormous and costly damages.

Sensitive information in the context of cloud computing encompasses data from a wide range of different areas and disciplines. Data concerning health is a typical example of the type of sensitive information handled in cloud computing environments, and it is obvious that most individuals will want information related to their health to be secure. Hence, with the proliferation of these new cloud technologies in recent times, privacy and data protection requirements have been evolving to protect individuals against surveillance and database disclosure. Some examples of such protective legislation are the EU Data Protection Directive (DPD) and the US Health Insurance Portability and Accountability Act (HIPAA), both of which demand privacy preservation for handling personally identifiable information.

This paper presents an overview of the research on security and privacy of sensitive data in cloud computing environments. We identify new developments in the areas of orchestration, resource control, physical hardware, and cloud service management layers of a cloud provider. We also review the state-of-the-art in privacy-preserving sensitive data approaches for handling sensitive data in cloud computing such as privacy threat modeling and privacy enhancing protocols and solutions.

II. KEY CONCEPTS AND TECHNOLOGIES

Over the past few years, major IT vendors (such as Amazon, Microsoft and Google) have provided virtual machines (VMs), via their clouds, that customers could rent. These clouds utilize hardware resources and support live migration of VMs in addition to dynamic load-balancing and on-demand provisioning. This means that, by renting VMs via a cloud, the entire datacenter footprint of a modern enterprise can be reduced from thousands of physical servers to a few hundred (or even just dozens) of hosts.

While it is practical and cost effective to use cloud computing in this way, there can be issues with security when using systems that are not provided in-house. To look into these and find appropriate solutions, there are several key concepts and technologies that are widely used in cloud computing that need to be understood, such as virtualization mechanisms, varieties of cloud services, and "container" technologies.

A. Virtualization Mechanisms

A hypervisor or virtual machine monitor (VMM) is a key component that resides between VMs and hardware to control the virtualized resource. It provides the means to run several isolated virtual machines on the same physical host.

Hypervisors can be categorized into two groups:

1) Type I:

Here the hypervisor runs directly on the real system hardware, and there is no operating system (OS) under it. This approach is efficient as it eliminates any intermediary layers. Another benefit with this type of hypervisor is that security levels can be improved by isolating the guest VMs. That way, if a VM is compromised, it can only affect itself and will not interfere with the hypervisor or other guest VMs.

2) Type II:

The second type of hypervisor runs on a hosted OS that provides virtualization services, such as input/output (IO) device support and memory management. All VM interactions, such as IO requests, network operations and interrupts, are handled by the hypervisor.

B. Cloud Computing

The activities of cloud providers can be divided into five main categories: service deployment, resource abstraction, physical resources, service management, security and privacy [7]. Service deployment consists of delivering services to cloud consumers according to one of the service models (SaaS, PaaS, IasS). Resource abstraction refers to providing interfaces for interacting with networking, storage and compute resources. The physical resources layer includes the physical hardware and facilities that are accessible via the resource abstraction layer. Service management includes providing business support, resource provisioning, configuration management, portability and interoperability to other cloud providers or brokers. The security and privacy responsibilities of cloud providers include integrating solutions to ensure legitimate delivery of cloud services to the cloud consumers. The security and privacy features that are necessary for the activities of cloud providers are described in Table 2 [10].

Security Context	Description
Authentication and Authorization	Authentication and authorization of cloud consumers using pre-defined identification schemes.
Identity and Access Management	Cloud consumer provisioning and deprovisioning via heterogeneous cloud service providers.
Confidentiality, Integrity, Availability	Assuring the confidentiality of the data objects, authorizing data modifications and ensuring that resources are available when needed.
Monitoring and Incident Response	Continuous monitoring of the cloud infrastructure to assure compliance with consumer security policies and auditing requirements.
Policy Management	Defining and enforcing rules for certain actions such as auditing or proof of compliance.
Privacy	Protect personally identifiable information (PII) within the cloud from adversarial attacks that aim to find out the identity of the person that PII relates to.

Table 2: Security and Privacy Factors of the Cloud Providers

The majority of cloud computing infrastructures consist of reliable services delivered through data centers to achieve high availability through redundancy. A data center or computer center is a facility used to house computer systems and associated components, such as storage and network systems. It generally includes redundant or backup power units, redundant network connections, air conditioning, and fire safety controls.

III. CLOUD SECURITY AND PRIVACY CHALLENGES

Cloud computing has raised several security threats such as data breaches, data loss, denial of service, and malicious insiders that have been extensively studied. These threats mainly originate from issues such as multi-tenancy, loss of control over data and trust. (Explanations of these issues follow in the next subsection.) Consequently the majority of cloud providers – including Amazon's Simple Storage Service (S3)13, the Google Compute Engine14 and the Citrix Cloud Platform15 - do not guarantee specific levels of security and privacy in their service level agreements (SLAs) as part of the contractual terms and conditions between cloud

providers and consumers. This means that there are important concerns related to security and privacy that must be taken into consideration in using cloud computing by all parties involved in the cloud computing arena.

A. Security Issues in Cloud Computing 1) Multi-tenancy

Multi-tenancy refers to sharing physical devices and virtualized resources between multiple independent users. Using this kind of arrangement means that an attacker could be on the same physical machine as the target. Cloud providers use multi-tenancy features to build infrastructures that can efficiently scale to meet customers' needs, however the sharing of resources means that it can be easier for an attacker to gain access to the target's data.

2) Loss of Control

Loss of control is another potential breach of security that can occur where consumers' data, applications, and resources are hosted at the cloud provider's owned premises. As the users do not have explicit control over their data, this makes it possible for cloud providers to perform data mining over the users' data, which can lead to security issues. In addition, when the cloud providers backup data at different data centers, the consumers cannot be sure that their data is completely erased everywhere when they delete their data. This has the potential to lead to misuse of the un-erased data.

In these types of situations where the consumers lose control over their data, they see the cloud provider as a black-box where they cannot directly monitor the resources transparently.

3) Trust Chain in Clouds

Trust plays an important role in attracting more consumers by assuring on cloud providers. Due to loss of control (as discussed earlier), cloud users rely on the cloud providers using trust mechanisms as an alternative to giving users transparent control over their data and cloud resources. Therefore cloud providers build confidence amongst their customers by assuring them that the provider's operations are certified in compliance with organizational safeguards and standards.

B. Privacy Considerations of Processing Sensitive Data

The security issues in cloud computing lead to a number of privacy concerns. Privacy is a complex topic that has different interpretations depending on contexts, cultures and communities, and it has been recognized as a fundamental human right by the United Nations. It worth nothing that privacy and security are two distinct topics although security is generally necessary for providing privacy.

Several efforts have been made to conceptualize privacy by jurists, philosophers, researchers, psychologists, and sociologists in order to give us a better understanding of privacy – for example, Alan Westin's research in 1960 is considered to be the first significant work on the problem of consumer data privacy and data protection. Westin [14] defined privacy as follow. "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

The International Association of Privacy Professionals (IAPP)16 glossary 27 refers to privacy as the appropriate use of information under the circumstances. The notion of what constitutes appropriate handling of data handling varies depending on several factors such as individual preferences, the context of the situation, law, collection, how the data would be used and what information would be disclosed.

In jurisdictions such as the US, "privacy" is the term that is used to encompass the relevant laws,

policies and regulations, while in the EU the term "data protection" is more commonly used when referring to privacy laws and regulations. Legislation that aims to protect the privacy of individuals – such as the European Union (EU) DPD, the Gramm-Leach-Bliley Act (GLBA), the Right to Financial Privacy Act (RFPA), and the HIPAA – can become very complicated and have a variety of specific requirements. Organizations collecting and storing data in clouds that are subject to data protection regulations must ensure that the privacy of the data is preserved appropriately to lay the foundations for legal access to sensitive personal data.

The development of a legal definition for cybercrime, the issue of jurisdiction (who is responsible for what information and where are they held responsible for it) and the regulation of data transfers to third countries are among other challenging issues when it comes to security in cloud computing.

IV. SECURITY SOLUTIONS

This section reviews the research on security solution such as authentication, authorization, and identity management that were identified in Table 2.2 as being necessary so that the activities of cloud providers are sufficiently secure.

A. Authentication and Authorization

In the authors propose a credential classification and a framework for analyzing and developing solutions for credential management that include strategies to evaluate the complexity of cloud ecosystems. This study identifies a set of categories relevant for authentication and authorization for the cloud focusing on infrastructural organization which include classifications for credentials, and adapt those categories to the cloud context. The study also summarizes important factors that need to be taken into consideration when adopting or developing a solution for authentication and authorization – for example, identifying the appropriate requirements, categories, services, deployment models, lifecycle, and entities. In other work, a design model for multi-factor authentication in cloud computing environments is proposed in, and this model includes an analysis of the potential security threats in the proposed model.

B. Identity and Access Management

The important functionalities of identity management systems for the success of clouds in relation to consumer satisfaction is an important issue The authors also present an authorization system for cloud federation using Shibboleth - an open source implementation of the security assertion markup language (SAML) for single sign-on with different cloud providers. This solution demonstrates how organizations can outsource authentication and authorization to third party clouds using an identity management system. E-ID authentication and uniform access to cloud storage service providers is an effort to build identity management systems for authenticating Portuguese citizens using national e-identification cards for cloud storage systems.

V. PRIVACY-PRESERVATION FOR SENSITIVE DATA IN CLOUDCOMPUTING

Over the time, organizations have collected valuable information about the individuals in our societies that contain sensitive information, e.g. medical data. Researchers need to access and

analyze such data using big data technologies in cloud computing, while organizations are required to enforce data protection compliance.

There has been considerable progress on privacy preservation for sensitive data in both industry and academia, e.g., solutions that develop protocols and tools for anonymization or encryption of data for confidentiality purposes. This section categorizes work related to this area according to different privacy protection requirements. However, these solutions have not yet been widely adopted by cloud service providers or organizations.

Pearson discusses a range of security and privacy challenges that are raised by cloud computing. Lack of user control, lack of training and expertise, unauthorized secondary usage, complexity of regulatory compliance, transborder data flow restrictions and litigation are among the challenges faced in cloud computing environments. In, the authors describe the privacy challenges of genomic data in the cloud including terms of services of cloud providers that are not developed with a healthcare mindset, awareness of patient to upload their data into the cloud without their consent, multi-tenancy, data monitoring, data security and accountability. The authors also provide recommendations for data owners when aiming to use cloud provider services.

VI. CONCLUSIONS

This paper surveyed recent advances in cloud computing security and privacy research. It described several cloud computing key concepts and technologies, such as virtualization, and containers. The results that are presented in the area of cloud security and privacy are based on cloud provider activities, such as providing orchestration, resource abstraction, physical resource and cloud service management layers. Security and privacy factors that affect the activities of cloud providers in relation to the legal processioning of consumer data were identified and a review of existing research was conducted to summarize the state-of-the-art in the field.

REFERENCES

[1] S. Pearson, “Privacy, security and trust in cloud computing,” in Privacy and Security for Cloud Computing (S. Pearson and G. Yee, eds.), Computer Communications and Networks, pp. 3–42, Springer London, 2013.

[2] E. U. Directive, “95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data,” Official Journal of the EC, vol. 23, 1995.

[3] U. States., “Health insurance portability and accountability act of 1996 [micro form] : conference report (to accompany h.r. 3103).” http://nla.gov.au/nla.catvn4117366, 1996.

[4] “Hypervisors, virtualization, and the cloud: Learn about hypervisors, system virtualization, and how it works in a cloud environment.” Retrieved June 2015.

[5] M. Portnoy, Virtualization Essentials. 1st ed., 2012.Alameda, CA, USA: SYBEX Inc.,

[6] K. Lauter, A. Lopez-Alt, and M. Naehrig, “Private computation on encrypted genomic data,” Tech. Rep. MSRTR-2014-93, June 2014.

[7] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292). USA: CreateSpace Independent Publishing Platform, 2012.

[8] R. Dua, A. Raja, and D. Kakadia, “Virtualization vs containerization to support paas,” in Cloud Engineering (IC2E), 2014 IEEE International Conference on, pp. 610–614, March 2014.

[9] D. Bernstein, "Containers and Cloud: From LXC to Docker to Kubernetes," IEEE Cloud Computing, vol. 1, no. 3, pp. 81-84, 2014.

[10] NIST Special Publication 500–291 version 2, NIST Cloud Computing Standards Roadmap, July 2013, Available at http://www.nist.gov/itl/cloud/publications.cfm.

[11] R. Pike, D. Presotto, K. Thompson, H. Trickey, and P. Winterbottom, “The use of name spaces in plan 9,” SIGOPS Oper. Syst. Rev., vol. 27, pp. 72–76, Apr. 1993. [12] B. Russell, “Realizing Linux Containers (LXC).” http://www.slideshare.net/BodenRussell/linuxcontainersnext-gen- virtualization-for-cloud-atl-summit-ar4-3-copy. Retrieved October 2015.

[13] United Nations, “The Universal Declaration of Human Rights.”

http://www.un.org/en/documents/udhr/index.shtml, 1948. Retrieved August 2015.

[14] A. Westin, Privacy and Freedom. New Jork Atheneum, 1967.

[15] U. States., "Gramm-leach-bliley act." http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf, November 1999.

[16] U. S. F. Law, "Right to financial https://epic.org/privacy/rfpa/, 1978. privacy act of 1978."

[17] D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz, and A. Scherrer, "Fighting cyber crime and protecting privacy in the cloud." European Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs, October 2012. [18] S. Stalla-Bourdillon, "Liability exemptions wanted! internet intermediaries' liability under uk law," Journal of International Commercial Law and Technology, vol. 7, no. 4, 2012.

[19] N. Mimura Gonzalez, M. Torrez Rojas, M. Maciel da Silva, F. Redigolo, T. Melo de Brito Carvalho, C. Miers, M. Naslund, and A. Ahmed, "A framework for authentication and authorization credentials in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 509–516, July 2013.

[20] R. Banyal, P. Jain, and V. Jain, "Multi-factor authentication framework for cloud computing," in Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on, pp. 105–110, Sept 2013.