INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 2002-2007

e-ISSN : 2583-1062

Impact Factor: 5.725

EXPLORING CLOUD USER ROLE IN THE CONTEXT OF INFORMATION SECURITY AND SEMATIC TRACEABILITY

Mr. Mohamed Bahar[1], Dr. Omkar Pattnaik[2], Dr. Mohd Muqeem[3], Dr. Pawan R. Bhhaladhare[4]

[1]M. Tech, Sandip University, Nashik, Maharashtra, India.

[2,3,4]Professor, Sandip University, Nashik, Maharashtra, India.

DOI: https://www.doi.org/10.58257/IJPREMS34523

ABSTRACT

Cloud services are becoming an essential part of many organizations. Cloud providers have to adhere to security and privacy policies to ensure their users' data remains confidential and secure. Though there are some ongoing efforts on developing cloud security standards, most cloud providers are implementing a mish- mash of security and privacy controls. This has led to confusion among cloud consumers as to what security measures they should expect from the cloud services, and whether these measures would comply with their security and compliance requirements. We have conducted a comprehensive study to review the potential threats faced by cloud consumers and have determined the compliance models and security controls that should be in place to manage the risk. Based on this study, we have developed an ontology describing the cloud security controls, threats and compliances. In order to design, build, and provide cloud based solutions that best meet customers' needs, it is essential to understand the skills, goals, primary tasks, and responsibilitiesof the people or organizations involved throughout the cloud service lifecycle.To minimize this risk, cloud applications need to be engineered to adapt their security policies to maintain satisfaction of security requirements despite changes in their usage context. We call such adaptation capability Adaptive Information Security. The paper argues that one of the prerequisites to adaptive information security is the use of traceability as a means to understanding the relationship between security requirements and security policies. Using an example, we motivate the need for improving traceability in the development of cloud applications.

Keywords: Cloud computing, User roles, cloud security, Security compliance models, Cloud security models

1. INTRODUCTION

Information security is about protecting valuable information assets from intentional harm [1]. With the popularity of mobile and ubiquitous uses of computing infrastructures, such as the cloud [2], both technical and social contexts in which software applications operate are increasingly dynamic. By context we mean the properties of the environment in which a cloud application operates that have an effect in its behaviour. User roles describe a set of skills, tasks, and responsibilities that are clustered together. While personas are also commonly used to model users, we have based our framework on developed user roles to makeour artifacts more generalizable, because user roles can be easily used to compose personas to fit a wide variety of products and customer environments of different sizes.

As cloud computing becomes more prevalent in businesses, it has transformed many IT jobs and created new ones. As a result, we may see uncertainty about how responsibilities might be realized in real jobs. The cloud user roles describethe sets of tasks required to create, provide, manage and consume cloud services in a modular way that can be flexibly assembled to accommodate different scenarios. A consistent set of user roles benefits all parties. Understanding the cloud user roles and their business requirements helps IBM deliver the solutions their clients and partners need to effectively and efficiently run their business. Furthermore, the roles provide a vehicle for consistently communicating requirements and business needs. By organizing typical cloud tasks into a set of standard user roles, IBM development teams, vendors, and customers can more readily share experiences throughout the cloud development and operations process. Furthermore, having a complete understanding of the cloud user roles andtheir tasks can enable customers to effectively plan their workloads, resources, and staff for their future cloud applications and environments. The cloud user roles were developed in the context of IBM's Cloud Computing Reference Architecture, as a standard to support IBM's internal as well as external cloudecosystem readiness. We believe these definitions will aid the development of common standards and consistency across many cloud providers. By using similar nomenclatureto define the various tasks related to creating, deploying and managing cloud solutions we reduce the risk of complexityor confusion for those interacting with cloud solutions, and increase the interoperability of cloud services. This work makes three key contributions. First, we have conducted a comprehensive study to review the potential threats. faced by cloud consumers and determined the compliance models and security controls that should be in place to manage the risk. We analyzed more than 20 security standards in cloud computing as well as in IT management.

We also reviewed the security controls implemented by more than 100 cloud providers by studying the security related whitepapers on their websites. Second, based on this study, we have developed an ontology describing the cloud security controls, threats and compliances which is used to capture and store this information from standards and cloud providers in W3C standard semantic web languages. It provides us the capability in ongoing work to reason over it. Finally, we have developed a web-based application that can be used by consumer organization. It suggests, given the threats an organization faces, appropriate cloud security policies and providers that support them. This application classifies the threats faced by cloud users and determines the security and compliance policy controls that have to be activated for each threat. The application also displays the existing cloud providers that support the security policies. The focus of this paper is on the first and third contributions. Challenges

2. LITERATURE SURVEY

Previous studies have attempted to determine cloud security issues. Popović et al.’s study on cloud security controls and standards has been focused primarily at the provider end and concentrated on cloud engineering. Subashini and Kavitha present a survey of the different security risks to the cloud. This study is specific to the security issues due to the cloud service delivery models. Kamongi et. al. have also developed a risk model for the cloud but haven’t tied it with existing compliance standards. How many cloud providers are adapting the cloud security standards in [2], [1] and are capable of handling potential threats remains an open question, and potential source of concerns to consumers who have to select between these providers.

NIST’s cloud computing reference architecture classifies security and privacy policies under the purview of the cloud provider. On the other hand, the security compliance model is applicable across all the roles in the reference architecture. Security controls used to protect a cloud environment are the same for all cloud delivery models. Compliance standards are applied on these security controls.

The IT compliance model focuses on electronic data processing, network and IT infrastructure. Compliance models implement rules and regulations across various components of IT to make them work harmoniously. Organizations often adopt a security control based on these compliance models. Transparency amongst the cloud service model, security controls and the compliance model will help consumers and end users achieve reliable cloud data protection.

The creation and usage of the cloud user roles are governed by three well-defined principles:

A. Governing Principle 1 - Organize roles in a taxonomywith recursive instantiation

While these roles are intended to cover a wide range of scenarios, we have defined a common pattern of three core cloud user roles:

- Cloud Service Provider provides the appropriate hardware and software infrastructure to run the service and the people to manage and maintain this infrastructure.
- Cloud Service Creator creates the individual hardware and software components needed for the service.
- Cloud Service Consumer purchases or obtains the service from the Service Provider and possibly the Cloud Service Creator.

Each role can be filled by a human being or an entire organization. For example, a receptionist at a doctor’s office (the consumer) may use a specialized, multi-tenant application for managing patient insurance claims, which is hosted on the internet (by the provider) and was created by athird partyy vendor (the creator).

Depending on the context, and due to the recursivenature of the roles, a Service Provider may turn into a Service Consumer, and a Service Consumer into a Service Provider, while the Service Creator may be independent or part of either the Consumer or the Provide.

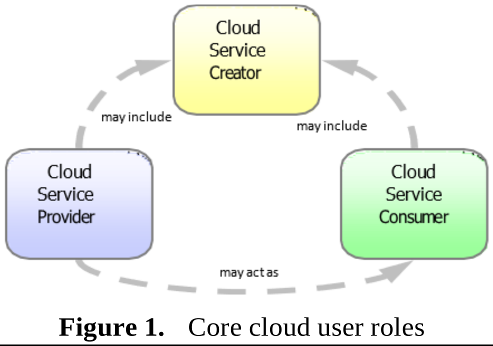

Figure 1. Core cloud user roles

B. Governing Principle 2 - Build roles around mutually-exclusive common task clusters

The cloud roles are not intended to represent every singlecloud scenario. Rather, they are a practical model of the waytasks are commonly organized. We delineate a cloud role bythree criteria:

1. It comprises a distinctive set of typical tasks thatcould be and frequently is performed by one person.
2. The particular set of tasks warrants dedicated cloudservice design decisions.
3. It is mutually exclusive in most circumstances.

C. Governing Principle 3 - Use nesting relationships toorganize roles

While we propose three core roles, in reality, there willbe specializations within each of these core roles, which arecaptured through parent-child relationships (in other contexts, such as outsourcing engagements, you may also find a fourth core Integrator role, which focuses on intermediation and value-add services).

The relationship of child to parent role is an Is-A relationship. Each child node is an instance, or token, of the parent. For example, an operations manager is a specialization of the core Cloud Service Provider role, and a network administrator is a specialization of the operations manager role. The parent role, however, is not necessarily the sum of all the listed child nodes. If instantiated separately, it may assume additional responsibilities and tasks.

3. METHODOLOGY

SECURITY THREAT AND CONTROL MODELS

A. Compliance Standards and cloud security controls.

In this section we discuss the key security controls that affect cloud security. We have referenced the NIST and CSA security documents . We also co-relate them with compliance standards based on the description of controls.

1. **Data encryption, key management**: Data encryption and secure key management provides data confidentiality and integrity. Standards: FIPS, Vaultive.
2. **Media protection:** Media protection includes protection of entertainment content like music, movies and software. Compliance Standards: MPAA.
3. **Identification, authentication and authorization:** Multi-tenancy requires that consumers share common resources in public domain. Identification of correct resources to authorized users is an important aspect of this security control. The users should be identified by key management and passwords. Cloud providers should also provide access controls to users, so that they can give rights to other authorized users. Compliance models: STIG, FedRAMP, Oauth and NIST 800-63. NIST classifies access control as a separate control supported by SOX and Safe Harbor.
4. **Virtualization and resource abstraction**: Virtualization introduce issues like inter virtual machine attacks, hypervisor security etc. Virtual machine setup should include firewall implementation. This security control is only supported by CSA. Compliance standards: DMTF- CADF and PCI-DSS.
5. **Portability and interoperability:** The security standards implemented on cloud system should enable information sharing amongst the other system. Compliance standards: DMTF-CADF and OASIS (SAML).
6. **Application security:** Application security is overall security of the applications running on the cloud. It includes secured SDLC (software development lifecycle), authentication and authorization. Compliance standards: PCI DSS, ISO 27002, **S**OX, HIPAA.
7. **Security risk assessment and management:** Cloud providers should implement the authorization and risk assessment for utilizing shared resources. Standards: STIG [13], ISO27002 [14], FedRAMP [5].
8. **Privacy, electronic discovery and other legal issues**: This focuses on managing the physical location of data and accessing it confidentially. To achieve this security control, documents, terms of services and privacy policies should be reviewed. Compliance model: EDRM- PSRRM [21].
9. **Contingency planning:** The consumer should go over the provider's contingency plans and service level agreements and make sure that provider meets their requirements. Compliance standards: HIPAA [17], NIST 800-34
10. **Data center operations, maintenance:** Security controls for data centers include configuration and personnel background check to allow entry into secured data center location, physical privacy of data center and authentication. Standards: PCIDSS [29], ISO27002 [14], HIPAA [17], NIST 800-16[26] and NIST 800-53 [18].

11. **Incident response:** Cloud providers should develop a response plan in case of any incident like data breaches, data loss etc. Computer forensics has some different tools and techniques for incident response. Compliance standards: NIST 800-61 [30] and ISO 17799 [24].
12. **Compliance, audit and accountability**: After implementing the required compliances, regular audits should be conducted to ensure data security. Compliance standards: DMTF [25].

B. **Awareness and training:** Cloud awareness and training programs, about threats and security controls, should be conducted for cloud consumers. Compliance standards: NIST 800-61[30] and ISO 17799 [24].

C. Threats to cloud computing and how to protect from threats by using security compliance models

We analyzed the security threats, identified in [1], [6] and other public documents from standards bodies, to determine the threats faced by cloud consumers. We related them to the security controls and compliance models that protect from these threats (Table 1). The key threats to cloud security include -

1. **Data breaches:** affect the confidentiality of data and eventually the organization. Data encrypted so that even if it is stolen, the attacker cannot use it.
2. **Data loss:** can happen due to hardware failure or malicious attacks on the system. Data backup policies should be implemented to overcome this type of threats.
3. **Account or service traffic hijacking**: affects the confidentiality and integrity of the users. Hackers can steal users' personal data like bank credentials. Anti-phishing and fraud detection policies should be implemented to reduce these.
4. **Insecure interfaces and APIs:** Users and providers communicate through interfaces and APIs. APIs should be able to encrypt the data and transfer through the interfaces.
5. **Denial of service**: is to prevent valid users from accessing their data. The attacker can change the encryption key or can slow down the system to prevent users from using the service. To prevent this type of attacks, the users and cloud provider should develop a mechanism so that the attackers cannot distinguish the patterns of communications.
6. **Malicious Insiders:** are people within the organization who can access and misuse the data. Legal action is advised for this type of threat.
7. **Abuse of cloud services:** Attackers can misuse the multi- tenancy feature of cloud to hack into other organizational data. Cloud providers should protect against consumers accessing other users' data.
8. **Insufficient due diligence:** Currently many organizations are adopting cloud for cost savings without being aware of the other threats. Awareness programs should be developed so cloud consumers can understand cloud technologies.

Shared Technology vulnerabilities: Cloud providers deliver their service in scalable way by sharing the resources. This sharing strategy should be implemented in every domain in cloud computing and also for monitoring the system

D. Proposed work

Cloud Security and compliance Ontology

We have developed an OWL ontology [31] to capture the concepts of cloud security, threats and compliance controls. In this section we briefly describe this ontology; but it is outside the scope of this paper. The main classes of the ontology are cloud computing security (further divided into cloud security compliance models, cloud security controls and threats to cloud security) and cloud computing providers.

Figure 1 describes the class cloud security compliances and its relation with security control class. The types of cloud security compliances, explained in section III, are represented in our ontology. The the control elements listed in section III A. Each cloud security standard supports a compliance type. The ontology includes the relation between security standards and cloud security compliances listed in Table 1. The threats and its types, detailed in section III, are captured in our ontology. The ontology helped us determine the database design of our recommendation tool.

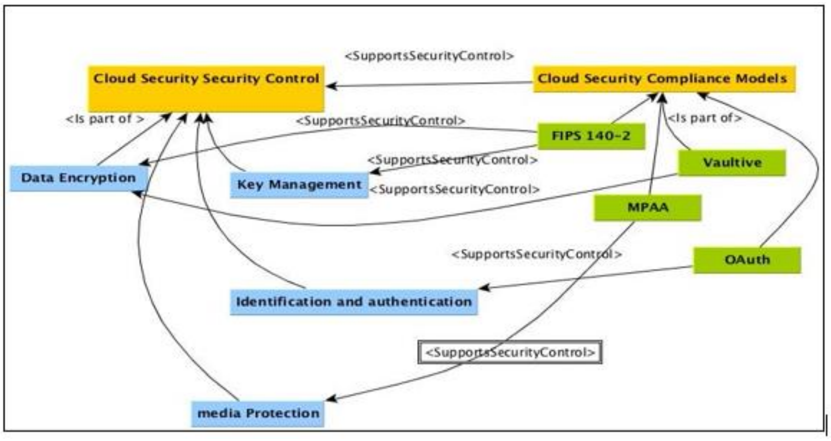
<SupportsSecurityControl>
Cloud Security Security Control
Cloud Security Compliance Models
<Is part of >
<SupportsSecurityControl>
FIPS 140-2
<Is part of>
<SupportsSecurityControl>
Data Encryption
Key Management
<SupportsSecurityControl>
Vaultive
MPAA
<SupportsSecurityControl>
OAuth
Identification and authentication
<SupportsSecurityControl>
media Protection

Figure 1: Ontology describing relationship between Security Controls and security Compliance classes.

4. CLOUD SECURITY POLICY RECOMMENDATION SYSTEM

We have developed an application that can be used by cloud consumers to determine the cloud security and compliance policies that they want to enforce within their organization. This system helps users identify the cloud threats and the security and compliance models that protect against these threats. The application also lists the existing cloud providers who have implemented the standards in their services.

For this application, we analyzed various security compliances, security policies/standards, and threats affecting cloud security. We next related these controls, standards and threats based on parameters like description of the security standards, the requirements of standard fulfillment, compliance description and also analysis of threats that affects the cloud security. This web-based application has been created by using PHP, HTML and AJAX web technology and MySQL database.

5. RESULT AND ANALYSIS

We developed a framework for the definition of a singlecloud user role as well as the taxonomy of the entirety of cloud roles. Expanding from the three core cloud rolesintroduced above, we extended the set of roles to some 30 more detailed creator, provider and consumer roles.

The set of roles will continue to be subject to change. Ascloud computing adoption grows over the coming years, thetasks and responsibilities of people who build and support systems within their businesses will change. The relationships among business partners and resellers will be key influencers on the evolution of the cloud role definitions.At the same time, this framework of cloud user roles transcends these changes, since the roles are defined at a task-level, not at an individual job or functional level.

Comparative study

Comparative studies in cybersecurity can provide valuable insights into various aspects such as Cloud computing, User roles, cloud security, Security compliance models, Cloud security models. Here are some highlights from recent comparative studies: A Semantic Approach to Cloud Security and Compliance, “Cloud User Roles Establishing standards for describing core tasks of cloud creators, providers, and consumers”, ccomparisons of the three areas based on various factors such as efficiency, cost, ease of implementation, etc. Discussion on how these areas interrelate and complement each other in a cloud environment

These studies can support Brief overview of the three areas of study: Cloud User Roles, Adaptive Information Security in the Cloud, and Semantic Approaches to Cloud Security and Compliance.

6. CONCLUSION AND FUTURE SCOPE

We have conducted a comprehensive study to review the potential threats faced by cloud consumers and determined the compliance models and security controls that should be in place to manage the risk. We used this study to develop a semantically rich ontology to model the security threats, cloud security policies and controls and express the provider data in it. We have also developed an easy to use cloud security policy recommendation application for consumers who are planning to move their data to the cloud but are hesitant due to security concerns as they may not be aware of the security controls. As part of our ongoing work, we are further analyzing other IT compliance models that may be applicable in the cloud paradigm and determine if they should be incorporated into our cloud security application. We are also developing rules to reason over the ontology to better match compliant providers.

7. REFERENCES

[1] J.A. Calcaterra, J.H. Bailey, and K.F. Odour, “Multiple people and components: considerations for designing multi- user middleware,” Proceedings of the Symposium Computer Human Interaction for Management of Information Technology (CHIMIT), Nov. 2008. doi: 10.1145/1477973.1477987

[2] E.M. Haber, E. Kandogan, and P.P. Maglio, “Collaboration insystem administration,” Queue, vol. 8, 2010. doi: 10.1145/1898147.1898149

[3] T. Darmohray, Job descriptions for system administrators, 3rded. Berkeley, CA: USENIX Association, 2010.

[4] J.L. Lentz and T.M. Bleizeffer, “IT ecosystems: evolved complexity and unintelligent design,” Proceedings of the Symposium Computer Human Interaction for Management ofInformation Technology (CHIMIT), Nov. 2007. doi: 10.1145/1234772.1234780

[5] J. Elson and J. Howell, “Refactoring human roles solvessystems problems,” Proceedings of the Conference on Hot Topics in Cloud Computing, 2009.

[6] M. Chessell and B. Schmidt-Wesche, “SOA programming model for implementing Web services,Part10:SOAuserroles,”Feb.2006.http://www.ibm.com/developerworks/webservices/library/ws-soa-progmodel10/index.htmlCooper, About Face 3.0: The Essentials of Interaction Design, New York, NY: John Wiley & Sons, Inc., 2007.

[7] V. Hill and V. Bartek, “Telling the User’s Story,” Proceedings of the Symposium Computer Human Interaction for Management of Information Technology (CHIMIT), Nov. 2007. Doi: 10.1145/1234772.1234794.

[8] Getting cloud computing right: the key to business success in a cloud adoption is a robust,provenarchitecture.Armonk,NY:IBMCorporation,2011.http://www.ibm.com/common/ssi/cgi-

[9] bin/ssialias?infotype=SA&subtype=WH&appname=GTSE_CI_CI_USEN&htmlfid=CIW03078USEN&attachment=CIW03 078USEN.PDF

[10] Cloud Security Alliance ,2013, The Notorious Nine: Cloud Computing Top Threats in 2013, p8-p21.

[11] NIST, NIST Cloud Computing Reference Architecture, 2011

[12] Privacy and data protection,Vol 7 Issue 4, IT compliance and IT security-Part 1, Dr. Jörg Hladjk, p 3-4.

[13] SSAE16, The SSAE16 Auditing Standard , http://www.ssae-16.com/

[14] FedRAMP, http://www.gsa.gov/portal/category/102375

[15] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Volume 34, Issue 1, January 2011, Pages 1–11

[16] Ramgovind, S.; Eloff, M.M.; Smith, E., "The management of security in Cloud computing," Information Security for South Africa (ISSA), 2010 , vol., no., pp.1,7, 2-4 Aug. 2010

[17] T. Mather, S.Kumarswamy, S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009

[18] CSA, Diana Kelley ,Understanding Cloud Controls Matrix v1.4.xls

[19] CSA , Nov 14 2014, CSA security Guidance v3,

[20] Mell, P. & Grance, t. (2011) The NIST Definition of Cloud Computing, (Special Publication 800-145).

[21] Vaultive, http://www.vaultive.com/technology/encryption-in-use/

[22] STIG, Application Security and Development STIG, 2014

[23] Introduction to ISO 27002, http://www.standards.bz/iso-27002.html

[24] ISO/IEC 27001, http://www.iso.org/iso/home/standards/management- standards/iso27001.htm

[25] SAFE HARBOR, http://export.gov/safeharbor/eu/eg_main_018476.asp