A Semantic Approach to Cloud Security and Compliance

Amit Hendre and Karuna Pande Joshi
CSEE Department, University of Maryland Baltimore County
Baltimore, MD, USA
{hendre1, karuna.joshi}@umbc.edu}

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. We have also developed an application that classifies the security threats faced by cloud users and automatically determines the high level security and compliance policy controls that have to be activated for each threat. The application also displays existing cloud providers that support these security policies. Cloud consumers can use our system to formulate their security policies and find compliant providers even if they are not familiar with the underlying technology.**

Keywords—Cloud computing, cloud security, Security compliance models, Cloud security models.

I. INTRODUCTION

While cloud based solutions are attractive for their cost savings and rapid provisioning/scaling; privacy and security of cloud data remains a concern for most consumers [8] and a key barrier in adoption of the cloud. In recent years, various cloud security standards have been proposed or are being developed by standards bodies like Cloud Security Alliance (CSA) [9][10], International Organization for Standards (ISO) [14][15], National Institute for Standards and Technology (NIST)[18][19][20], etc. Most cloud providers are implementing a mish-mash of security and privacy controls. This has led to confusion and concern among consumers as to what security measures they should expect from the cloud services and what compliance policies to adopt for their enterprise data on the cloud.

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.

In section III of this paper, we present our analysis of the various cloud security control models, compliance models and threats. The ontology we have developed for cloud security compliances and security standards is very briefly covered in section IV, and is not a focus of this paper. We describe our recommendation application in detail in section V and end with conclusions and future work.

II. RELATED WORK

Previous studies [6][7][8][33] [34] have attempted to determine cloud security issues. Popović et al.'s [34] study on cloud security controls and standards has been focused primarily at the provider end and concentrated on cloud engineering. Subashini and Kavitha [6] 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. [33] 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 [2][11] classifies security and privacy policies under the purview of the

2159-6190/15 $31.00 © 2015 IEEE
DOI 10.1109/CLOUD.2015.157

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 [3] 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.

We used the Web Ontology Language (OWL) [32] to develop our ontology for Cloud security controls, threats and compliances, which is described briefly in section IV.

III. 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 [20][9][10]. 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 140-2 [19], Vaultive [12].
2. **Media protection:** Media protection includes protection of entertainment content like music, movies and software. Compliance Standards: MPAA [28].
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 [13], FedRAMP [5], Oauth and NIST 800-63. NIST classifies access control as a separate control supported by SOX [22] and Safe Harbor [16].
4. **Virtualization and resource abstraction**: Virtualization introduces 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 [25] and PCI-DSS [29].
5. **Portability and interoperability:** The security standards implemented on cloud system should enable information sharing amongst the other system. Compliance standards: DMTF-CADF [25] and OASIS (SAML) [23]
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 [29], ISO 27002 [14], SOX [22], HIPAA [17]
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: PCI DSS [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].
13. **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].

B. 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 providers

should develop a mechanism so that the attackers cannot distinguish the patterns of communications.

Type of threat	Recommended Security Compliance Model
Data breaches	STIG [13], FedRAMP [5], DMTF- CADF[25], ISO-27001[15], FIPS 140-2[19], PCI DSS [29], ISO 27002[14], HIPAA[17], SOX[22]
Data loss	STIG [13], FedRAMP [5], DMTF- CADF [25], FIPS 140-2 [19], PCI DSS [29], ISO 27002[14], HIPAA[17], SOX[22]
Account or service hijacking	STIG [13], FedRAMP [5], DMTF-OVF [25], ISO- 27002[14], FIPS 140-2[19], NIST 800-61[30], ISO 17799[24]
Insecure interfaces/API	OASIS and OVF, DMTF-CADF [25], ISO 27002[14], FIPS 140-2[19]
Denial of services	PCI DSS, ISO 27001[15], HIPAA[17], SOX[22], NIST 800-61[30], ISO 17799[24]
Malicious insiders	ISO 27002[14], FIPS 140-2[19], Vaultive[12], FedRAMP[5]
Abuse of cloud services	NIST 800-61[30], ISO 17799[24], NIST 800-50 [27]
Insufficient due diligence	EDRM[21], NIST 800-61[30]
Shared technology vulnerabilities	ISO 27001[15], FIPS 140-2[19],PCI DSS, ISO 27002[14], HIPAA[17], SOX[22], MPAA [28]

Table 1: Recommendation of Security compliance model based on security threat

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.
9. **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.

IV. 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 subclasses of the Cloud security control class are 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.

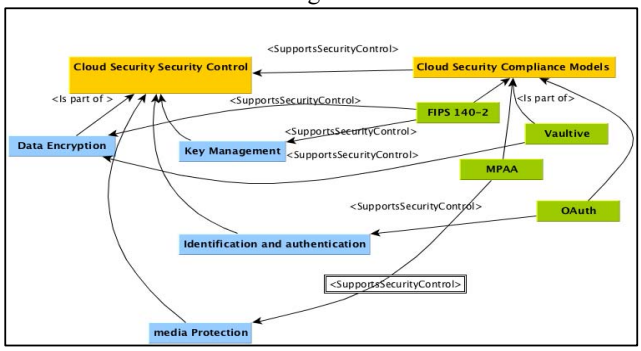

Figure 1: Ontology describing relationship between Security Controls and security Compliance classes.

V. 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. Figure 2 shows the database architecture of the application.

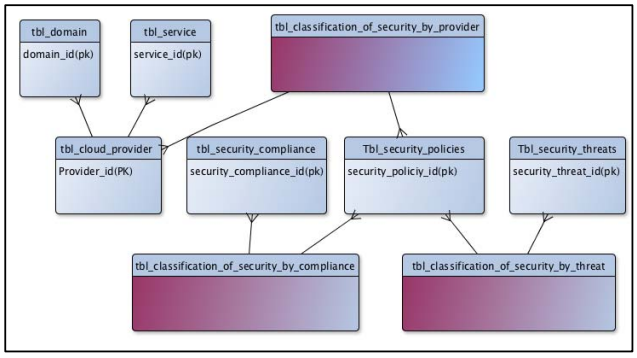

Figure 2: Database architecture for the application

Using our application, cloud consumers can get a list of all providers who support a compliance standard. If the consumers are not sure of the compliance standard to adhere to, they can also search on multiple security controls. When the user selects a particular security control, the system will display the

recommended security compliance model and then recommended cloud providers in the output. (Figure 3).

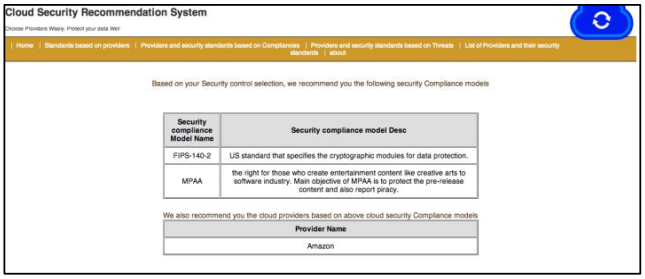

Figure 3: Compliance and providers recommended based on Security Controls selected

This application also allows consumers to find security standards for the corresponding security threats. The system also lists the cloud providers that adhere to the standards, which help users to ensure the data security on cloud (Figure 4). Consumers can also get a list of all security standards supported by a cloud provider selected.

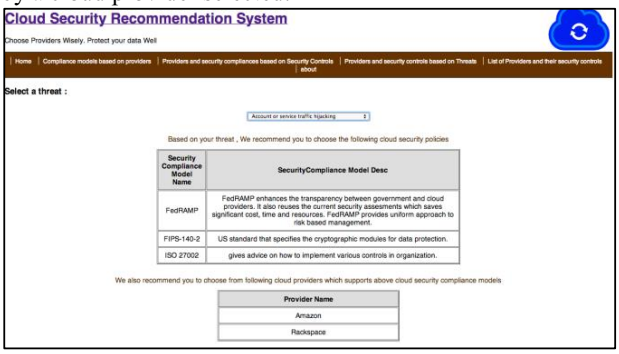

Figure 4: Recommendation of security compliance and Cloud providers based on security threat selected.

VI. Conclusion and Ongoing Work

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.

References

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

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

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

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

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

[6] 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

[7] 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

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

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

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

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

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

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

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

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

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

[17] HIPAA, may 2003,Summary of HIPAA privacy rules. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

[18] NIST SP 800-53 , Information security, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[19] FIPS 140-2, Jan 2011, security requirement for cryptographic models, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[20] NIST Recommended Security Controls for Federal Information Systems and Organizations., http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[21] EDRM-PSRRM, Privacy and Security risk reduction model, http://www.edrm.net/resources/psrrm

[22] SOX , Sarbanes-Oxley Act, http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

[23] Overview of OASIS SAML v2 , https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

[24] ISO 17799, International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf

[25] DMTF CADF, June 2012, Cloud Auditing Data Federation http://www.dmtf.org/sites/default/files/standards/documents/DSP2028_1.0.0a.pdf

[26] NIST 800-16, http://csrc.nist.gov/publications/drafts/800-16-rev1/draft_sp800_16_rev1_2nd-draft.pdf

[27] NIST 800-50, for awareness and training , Oct 2003, program, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[28] MPAA, entertainment content security and protection, http://www.fightfilmtheft.org/docs/2012_Annual_Trending_Report_Final.pdf, 2012

[29] PCI-DSS , oct 2010, requirement and security assessment , https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[30] NIST 800-61, Computer Security Incident Handling Guide, Aug 2012, http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

[31] A. Hendre, T. Finin, K.Joshi, Cloud Security and Compliance Ontology, July 2014, http://ebiquity.umbc.edu/resource/html/id/361/Cloud-Security-and-Compliance-Ontology

[32] D. McGuinness, F. Van Harmelen, et al., OWL web ontology language overview, W3C recommendation, World Wide Web Consortium, 2004.

[33] P Kamongi et. al., Nemesis: Automated Architecture for Threat Modeling and Risk Assessment for Cloud Computing, ASE 2014

[34] Popović, K.; Hocenski, Z., "Cloud computing security issues and challenges," MIPRO, 2010 Proceedings of the 33rd International Convention , vol., no., pp.344,349, 24-28 May 2010