2015 IEEE 16th International Symposium on High Assurance Systems Engineering

Ontology of Secure Service Level Agreement

Chen-Yu Lee
Department of Computer Science and Engineering
University of North Texas
Denton, TX 76203, USA
Email: Chen-Yu.lee@unt.edu

Krishna M. Kavi
Department of Computer Science and Engineering
University of North Texas
Denton, TX 76203, USA
Email: Krishna.Kavi@unt.edu

Raymond A. Paul
Department of Defense, USA
Email: Raymond.Paul@osd.mil

Mahadevan Gomathisankaran
Department of Computer Science and Engineering
University of North Texas
Denton, TX 76203, USA
Email: Mahadevan.Gomathisankaran@unt.edu

***Abstract*—Maintaining security and privacy in the Cloud is a complex task. The task is made even more challenging as the number of vulnerabilities associated with the cloud infrastructure and applications are increasing very rapidly. Understanding the security service level agreements (SSLAs) and privacy policies offered by service and infrastructure providers is critical for consumers to assess the risks of the Cloud before they consider migrating their IT operations to the Cloud. To address these concerns relative to the assessment of security and privacy risks of the Cloud, we have developed ontologies for representing security SLAs (SSLA) in this paper. Our ontologies for SSLAs can be used to understand the security agreements of a provider, to negotiate desired security levels, and to audit the compliance of a provider with respect to federal regulations (such as HIPAA).**

***Keywords*—service level agreement; SLA; security; SSLA; cloud computing;**

I. Introduction

The use of Cloud computing services is becoming the preferred choice for many businesses because of the advantages of Cloud services over in-house IT operations. Cloud computing makes it easier to streamline IT processes and reduce expenditures on technology infrastructure. In addition, it provides the economies of scale and an effective way to monitor project budgets, since the business only pays for the amount of computing and services used. To guarantee the quality of the services, it is necessary to enter the exact usage conditions into contracts which can be specified as a Service Level Agreement (SLA). SLA is described in the Information Technology Infrastructure Library ver. 3: "A service level management negotiates, agrees and documents appropriate IT service targets with representatives of the business, and then monitors and produces reports on the Service Providers ability to deliver the agreed level of service" [1].

Most commercial SLA's regulate the service scopes and the service availability as listed below:

- 99.999% email processing availability
- 100% antivirus filtering
- 99.9% monthly uptime
- SSL/TLS and Service Side Encryption (SSE) support
- 99.999999999% durability of objects over a year
- Versioning support

For Web services, SLA monitoring and enforcement become increasingly important, especially when enterprise applications and services subscribe to cloud resources on-demand. However, natural language based SLA templates lack flexibility in different domains, different organizations, and different definitions for IT parameters. The WSLA framework [2] and Web Services Agreement Specification (WS-Agreement) [3] are XML-based frameworks to formalize the terminology, concepts, and agreement structure used in automatic negotiation, deployment, monitoring and enforcement of SLAs.

The main concern preventing some businesses from adopting Cloud computing is the risk of privacy and security. The security aspects of an SLA are often not taken seriously enough by most cloud computing providers, such as Amazon[1], Google[2],or Microsoft Azure[3]. At best, they mention what security-related services may be provided, or perhaps some recommendations for security maintenance that are described in referenced documents. However, these files are not contracts and are not legally binding. Therefore, this paper proposes the concept of the Security Service Level Agreement (SSLA) to improve the credibility and verifiability of security and privacy commitments made by cloud providers.

Additionally, Service Level Agreements (SLAs) written by a Cloud provider are very difficult to understand, hence quantitatively comparing the SLAs of different providers is even more challenging. To capture and present requirements for both provider and consumer, Modica et al. proposed a SLA ontology to present the definition of a semantic domain of knowledge for the cloud business according to the Cloud

[1]Amazon EC2 Service Level Agreement: http://aws.amazon.com/cn/ec2/sla/

[2]Google Cloud Storage, Google Prediction API, and Google BigQuery SLA, https://developers.google.com/storage/sla

[3]Windows Azure Storage Service Level Agreement, http://www.microsoft.com/en-us/download/details.aspx?id=6656

978-1-4799-8111-3/15 $31.00 © 2015 IEEE
DOI 10.1109/HASE.2015.33

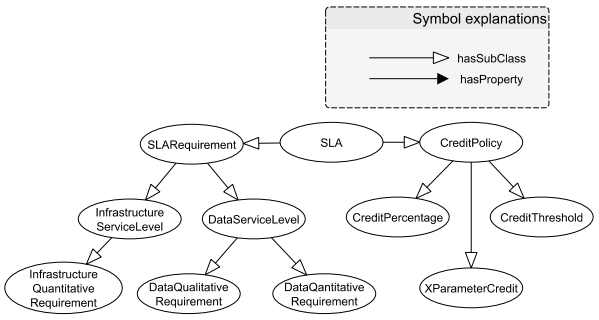

Fig. 1. Ontology for SLA

Standards Consumer Council [4] shown in Figure. 1 [5]. Based on the knowledge base, providers would be able to customize their offers according to their business strategy, and consumers are able to claim the resource requests consistent with their real needs. These works inspired us to develop ontologies for representing our SSLA.

Ontology is a formal framework for representing knowledge. This framework names and defines the types, properties, and interrelationships of the entities in a domain of discourse. We use ontologies to conceptualize our security information for the following reasons:

- The defined ontologies are machine readable vocabularies that are specified with enough precision to allow differing terms to be precisely related.
- The security ontologies could be used by analysts/developers, databases, and applications that need to share domain information.
- Since machines can read and interpret our ontologies, we can instantiate them automatically enabling us to seamlessly and effortlessly generate rich and powerful SSLA knowledge bases/representations.
- We could conduct automatic reasoning on our generated knowledge bases, like the vulnerability knowledge base (OKB) [6].

We use an ontology approach instead of taxonomies for modeling security information since an ontology provides the potential for formal logic inference based on well-defined data and knowledge bases [7]. In general terms, both an ontology and taxonomy can represent the same knowledge domain. However, ontologies are considered to be broader and can be thought of as a number of taxonomies assembled together with more expressive and inter-connective relationships added (with each taxonomy organizing a subject in a particular way). This led to our choice of using ontologies in our modeling because they allow us to take advantage of semantic meaningfulness, and perform automatic reasoning over our domain of knowledge.

In this paper, our ontologies for SSLAs are used to understand the security agreements of a provider, to negotiate desired security levels, and to audit the compliance of a provider with respect to federal regulations, such as HIPAA. The rest of the paper is organized as follows. Section II discusses research that is closely related to ours. The SSLA ontology framework is introduced in Section III. The model design and its implementation are presented in Section III-A, Section III-B respectively. We have discussions of SSLA in Section IV.

II. Related Works

The concept of a Security Service Level Agreement (SSLA) to specify the requirements of security services for an enterprise was first proposed by Henning [8]. Monahan et al. considered the issues of meaningful security SLAs and discussed how a security SLA emobdies certain legal and financial contractual elements to satisfy two basic requirements separation and compartmentalisation [9]. In 2013, the terms "SSLA" and "security service-oriented agreement" were proposed by Takahashi et al. [10]. They proposed a non-repudiatable security service-oriented agreement mechanism which describes security requirements of users and capabilities of service providers. Rong et al. mentioned some cloud security challenges including resource location, the multi-tenancy issue, authentication and trust of acquired information, system monitoring, and cloud standards [11]. Hale et al. built a XML-based compliance vocabulary compatible with the WSLA schema [12].

III. Ontology on SSLA

As an alternative to the traditional SLA written in natural languages, the XML-based SLA is more useful for automated processing. Our ontologies for Security Service Level Agreements (or SSLAs) reference Paul's design concepts of trustworthiness ontology [13] and extend Hales work , which is built as a XML-based compliance vocabulary [12]. To increase the coverage of our SSLA ontology, we take into account the challenges in covering entire control domains specified by the Cloud security alliance (CSA) Cloud control matrix (CCM) v3 [14].

The proposed ontology for SSLAs facilitates understanding of the security concerns in service level agreements, and hopefully matches the security requirements of a consumer with the SSLAs offered by different providers. The SSLA ontology provides the following additional benefits:

- Easier understanding of the security aspects of the SLA.
- During negotiations, a consumer can compare the SLAs offered by many providers and choose the best one.
- It is easier to monitor the security requirements enforced by hosting providers, which is especially important for satisfying some industry compliance requirements.

A. Model Design

Without losing the generality of SSLAs, here we model thirteen classes including `Networking`, `Vulnerability`, `Transparency`, `DisasterDetectionRecovery`, `DataPossession`, `ViabilityOfProvider`, `CryptoSpec`, `AccessControl`, `Processing`, `Compliance`, `Audit`, `Selectable`, and

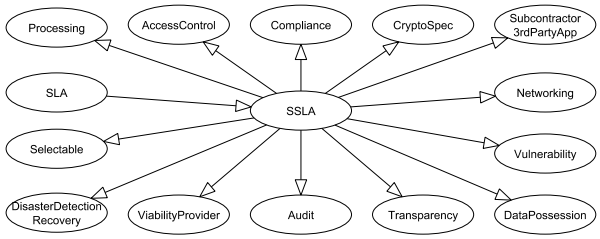

Fig. 2. All classes in SSLA

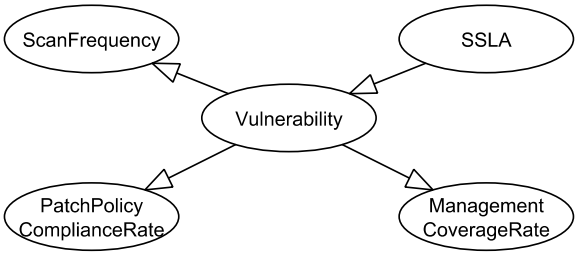

Fig. 3. Vulnerability class in SSLA

`Subcontractor3rdPartyApp` as shown in Figure 2. Each class is described as follows.

- Networking: This class organizes the agreements about the networking environment such as traffic isolation `TrafficIsolation` subclass; individual bandwidth for `IndividualBandwidth` subclass, which defines the guaranteed bandwidth offered to the consumer; and IP address quantity for `IPAddressQuantity` subclass, which defines the max number of IP addresses issued to the consumer.
- Vulnerability: Figure 3 shows the vulnerability class. This class defines assurance in terms of detecting and patching known vulnerabilities, including the use of malware scanners and coverage of services against attacks in `PatchPolicyComplianceRate`, `ScanFrequency`, and `ManagementCoverageRate` subclasses.
- Transparency: This class regulates the transparency of the information related to the security management processes used by the provider. The SSLA should record the responsible office that will provide the information when requested.
- Disaster detection and recovery: This involves the contingency plan and the security incident procedure that describes the regular routines of disaster detection and the recovery steps when the events occur. It also defines the data backup functions because data is usually the most valuable asset for consumers.
- Data possession: This class rules the data storage procedures in Cloud storage, and the data verification method and frequency to ensure data usability.
- Audit: This class requires the architecture, management, and service of providers to be audited by internal auditors, external auditors, and issued certificates (listed in `Certification`) to build consumer trust in the providers. `InternalAudit` and `ExternalAudit` subclasses also define their audit plans and change controls. Log is the most important evidence of behaviors of attackers, consumers, and providers. To protect the security of the log, the `Log` subclass regulates the secure storing procedures and the retention time of the log. The `RiskManagement` subclass describes the risk management and data risk assessment programs. In addition, the class outlines the real time monitoring mechanisms, the acceptable percent and types of security exceptions, security review, and the protection of consumer privacy in `RealtimeMonitor`, `PercentOfSecExcept`, `PercentOfSecReview` and `ConsumerPrivacy` subclasses.
- Subcontractor and third party application: Clarifies the rights and duties with respect to security of the subcontractor and the third party application providers.
- Viability of cloud provider: The system administrators of the providers' systems have the highest level of privilege. They can perform any action on any object. Thus, there is a privacy issue in defining what level of consumer data security is appropriate for a specific person and under what conditions.
- Cryptography specification: Some providers offer cryptography components optimized for their platforms. It is useful to optimize consumer data encryption while also reducing the associated computational complexity.
- Access control: Access control of the instance control panel directly impacts the security of the instance. Therefore, this class defines the access authentication, authorization, accounting schemes and rules of mobile access.
- Processing: This class covers the security demands for building a secure run time environment in a virtual machine migration, queue service capability, virtual firewall, and the isolation, portability, location, and integrity of applications.
- Compliance: Some specific services must be certified as compliant with security and privacy standards and practices as required by law. For example, user services that involve warehousing or mining of electronic Protected Health Information (ePHI), electronic Personally Identifiable Information (ePII), or Health Insurance Portability and Accountability Act (HIPAA) data must comply with any associated federal and local standards [15]. There are many subclasses defined in `Compliance` as shown in Figure 4.

B. Implementation

Our framework can provide a method for determining whether the SSLA satisfies the specific regulations for any given compliance.

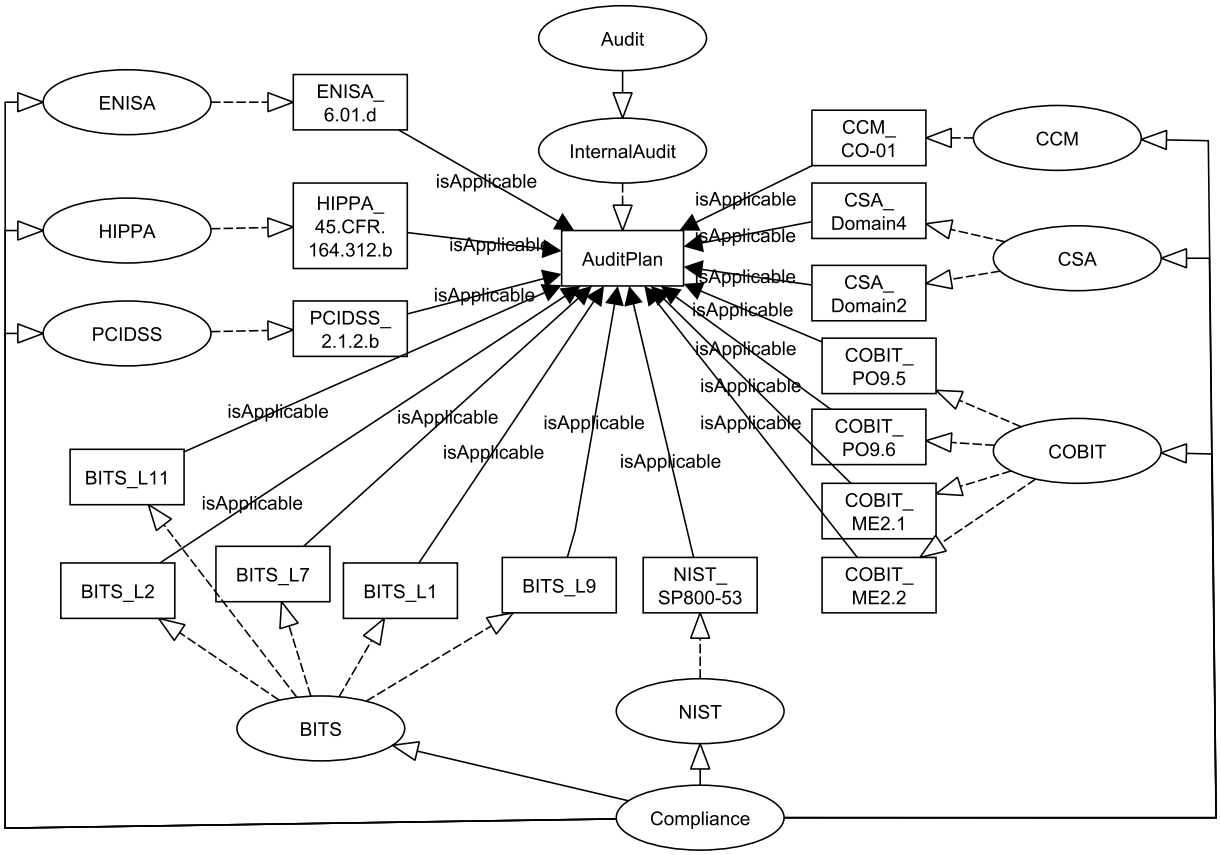

Fig. 6. Audit plan to be in compliance with the standards in CCMv3

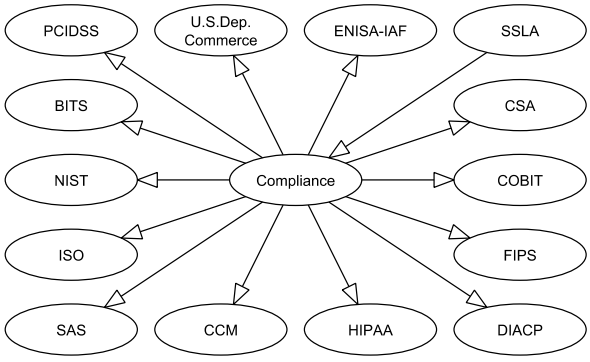

Fig. 4. Compliance class in SSLA

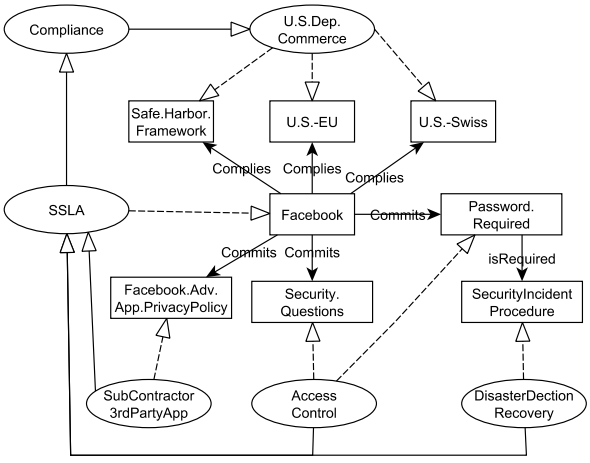

Fig. 5. Facebook privacy guarantee

The following three examples illustrate the `AuditPlan` defined in cloud control matrix v3 [14], the `AccessControl` regulations in the case of HIPAA compliance, and the privacy rules guaranteed by Facebook in our SSLA framework.

1) The design of `AuditPlan`: `AuditPlan` which is an individual of the `InternalAudit` class describes the objectives, methods, and schedules of the provider's internal audit. Figure. 6 shows that such an audit plan is applicable to a number of types of regulatory requirements. For HIPAA, the audit plan should regulate the requirements in HIPAA_45.CFR.164.312.b. Similarly, if the service provider is providing credit card payment systems, the audit plan has to obey PCIDSS_2.1.2.b of Payment Card Industry Data Security

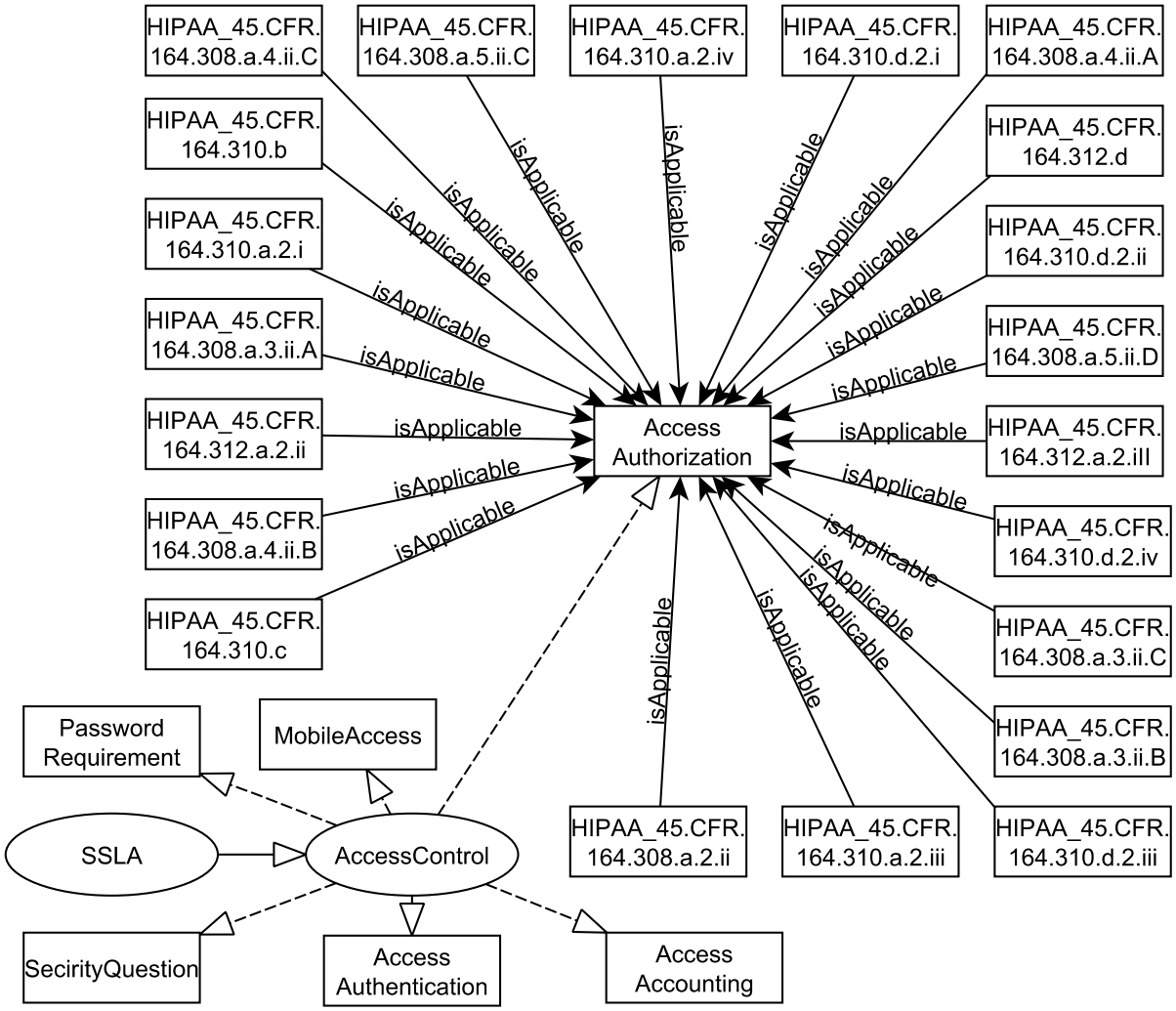

Fig. 7. AccessControl class with HIPAA in SSLA

Standards (PCI DSS) [16].

2) The case of HIPAA compliance: HIPAA compliance regulates the privacy and security of the processing and storing of electronic protected health information (ePHI) and electronic Personally Identifiable Information (ePII). We built the knowledge base for all HIPAA rules. We show two examples here. Figure 7 shows the 21 HIPAA rules that are applicable to `AccessAuthorization` in the `AccessControl` class. Figure. 8 illustrates the rules applicable to secure incident procedures, contingency plans, and data backup storage defined in the `DisasterDetectionRecovery` class.

3) The case of Facebook privacy guarantee: Facebook is a famous social networking service provider which provides some security and privacy guarantees for users listed in its policy page and can be summarized as follows:

- Facebook complies with the U.S.-EU and U.S.-Swiss Safe Harbor frameworks as set forth by the Department of Commerce regarding the collection, use, and retention of data from the European Union[4].
- Password requires at least six digits.
- Secure browsing (HTTPS) is enforced in all the connections.
- A security question helps a user to get back into his/her account if he/she can't log into the Facebook account.
- Facebook doesn't give the advertiser access to any information that identifies any user.

The above five rules can be presented using our SSLA ontology as shown both in Figure 5 and in WS-agreement codes that can be used in automatic requirement matching or negotiations.

```
1: <?xml version="1.0" encoding="UTF-8"?>
```

[4]https://www.facebook.com/full_data_use_policy#otherthings

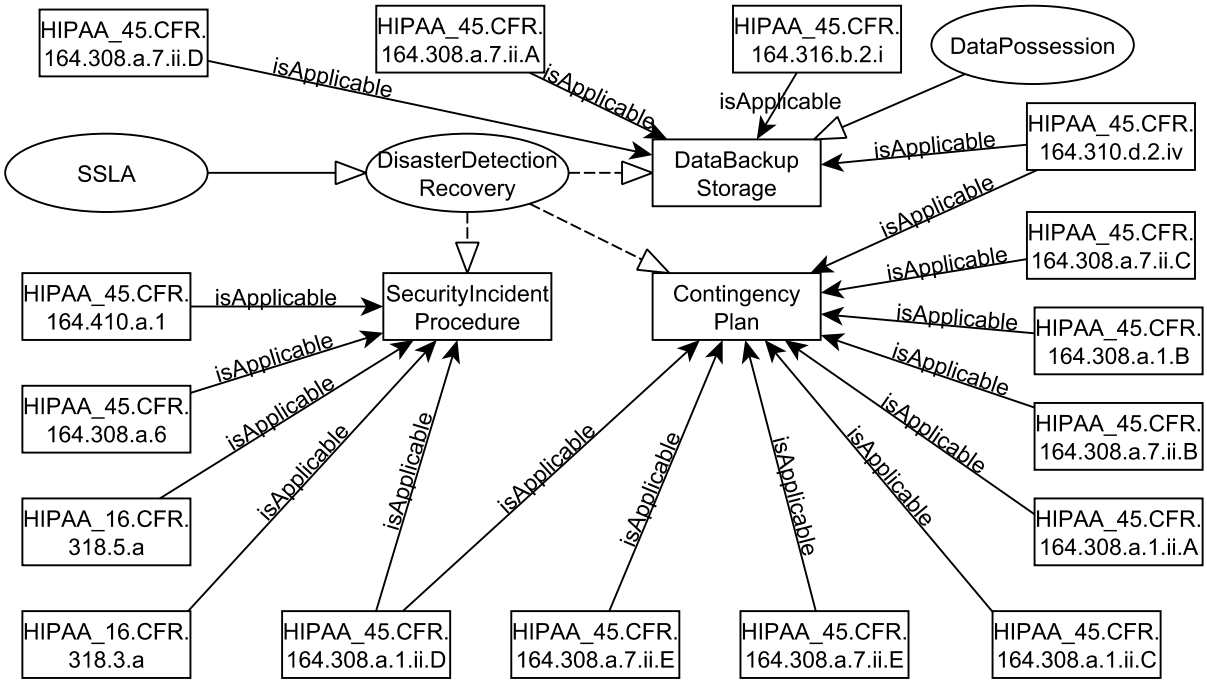

Fig. 8. Disaster Detection & Recovery class with HIPAA in SSLA

```
<wsag:AgreementOffer
...
<wsag:Name>Offer1</wsag:Name>
<wsag:Context/>
<wsag:Terms>
  <wsag:All>
    <wsag:ServiceDescriptionTerm
      wsag:Name="CompliantStandardUS-DoC01"
      wsag:ServiceName="ComputeJob1">
      <job:Compliance>US-EU</job:Compliance>
    </wsag:ServiceDescriptionTerm>
...
    <wsag:ServiceDescriptionTerm
      wsag:Name= "numberofPasswordDigital-Required"
      wsag:ServiceName="ComputeJob1">
      <numberOfMinDigit>6</numberOfMinDigit>
    </wsag:ServiceDescriptionTerm>
...
    <wsag:GuaranteeTerm wsag:Name="ConfigurationPreference"
    wsag:Obligated=ServiceProvider>
      <wsag:ServiceScope>
        <wsag:ServiceName>ComputeJob1</wsag:ServiceName>
      </wsag:ServiceScope>
      <wsag:ServiceLevelObjective xsi:type="sdtc:OpType">
        <SDT>CompliantStandardUS-DoC01</SDT>
...
        <SDT>numberofPasswordDigitalRequired</SDT>
...
      </wsag:ServiceLevelObjective>
    </wsag:GuaranteeTerm>
  </wsag:All>
</wsag:Terms>
</wsag:AgreementOffer>
```

IV. Discussion

A. Benefits for parties

This section discusses the benefits of the SSLA framework for Cloud infrastructure and service providers using HIPAA compliance as an example. It should be noted that both the service provider and the Cloud infrastructure provider are responsible for different aspects if HIPAA compliance.

- For Cloud infrastructure provider: Since an ontology is a good means for describing the knowledge, a Cloud provider could employ our SSLA ontology to present the security levels guaranteed. Additionally, the SSLA ontology also provides for negotiated agreements. With respect to HIPAA, the Cloud infrastructure provider must make sure that the Cloud environment is secure enough at least for known vulnerabilities and can resist known attacks. Moreover, the provider can use some vulnerability evaluation systems (like OKB [6]) to evaluate the security risks of its resources to define the most appropriate security guarantees, or price

different levels of negotiated security agreements.

- For service provider: When service providers employ a Cloud environment, they can utilize our SSLA ontology framework to negotiate better levels of security guarantees from the infrastructure provider. Additionally, the service provider can use our framework to understand the compliance issues pertaining to the services they provide.

B. Data breach

Data breaches are the most frequently occurring security incidents and can lead to lawsuits in some special application areas such as those covered by the HITECH Act [17] and ENISA [18]. When a data breach occurs, the security group then discovers the attack path from the logs in the cloud instances and the logs from the hosting providers according to the SSLA framework. Based on clues that may be found in the logs, the service provider can clarify the responsibility in the face of disaster, and demand compensation.

V. Conclusion

In this paper we have developed a SSLA ontology framework that can be used to understand the security agreements of a provider, to negotiate desired security levels, and to audit the compliance of a provider with respect to federal regulations. For the future, we envision extending the SLA to SSLA in WS-Agreement based WSAG4J[5], a Java implementation of WS-agreement based on our framework. It will be used to design and implement SLAs for specific services and automates SSLA management, offer validation, monitoring, persistence, accounting, and more.

Acknowledgment

This research is supported in part by the NSF Net-centric and Cloud Software and Systems Industry/University Cooperative Research Center and NSF award 1128344. The authors acknowledge the help of David Struble in making this paper more readable.

References

[1] *The Official Introduction to the ITIL Service Lifecycle*. The Stationery Office, 2007.

[2] A. Keller and H. Ludwig, "The wsla framework: Specifying and monitoring service level agreements forweb services," *J. Netw. Syst. Manag*, vol. 11, no. 1, pp. 57–81, Mar. 2003.

[3] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, and M. Xu, "Web services agreement specification (ws-agreement)," Open Grid Forum (OGF), Nov. 2011.

[4] "Practical guide to cloud service level agreements," Cloud Standards Customer Council.

[5] G. D. Modica, G. Petralia, and O. Tomarchio, "A business ontology to enable semantic matchmaking in open cloud markets," in *Proc. SKG2012*, Beijing, China, Oct. 2012, pp. 96–103.

[6] P. Kamongi, S. Kotikela, K. Kavi, M. Gomathisankaran, and A. Singhal, "Vulcan: Vulnerability assessment framework for cloud computing," in *Proc. SERE 2013*, 2013, pp. 218–226.

[7] J. Wang and M. Guo, "Ovm: an ontology for vulnerability management," in *Proc. CSIIRW'09*, 2009, p. 34.

[5]WSAG4J: http://wsag4j.sourceforge.net/site/

[8] R. R. Henning, "Security service level agreements: quantifiable security for the enterprise?" in *Proc. NSPW 1999*, Ontario, Canada, Sep. 1999, pp. 54–60.

[9] B. Monahan and M. Yearworth, "Meaningful security slas," HP Laboratories, Tech. Rep. HPL-2005-218R1, 2008.

[10] T. Takahashi, J. Kannisto, J. Harju, S. Heikkinen, B. Silverajan, M. Helenius, and S. Matsuo, "Tailored security: Building nonrepudiable security service-level agreements," *IEEE VT Mag.*, vol. 8, no. 3, pp. 54–62, Sep. 2013.

[11] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 47–54, 2013.

[12] M. Hale and R. Gamble, "Building a compliance vocabulary to embed security controls in cloud slas," in *Proc. SERVICES 2013*, Jun. 2013, pp. 118–125.

[13] R. Paul, I.-L. Yen, F. Bastani, J. Dong, W.-T. Tsai, K. Kavi, A. Ghafoor, and J. Srivastava, "An ontology-based integrated assessment framework for high-assurance systems," in *Proc. ICSC 2008*, Aug 2008, pp. 386–393.

[14] "Cloud controls matrix version 3.0," Cloud Security Alliance.

[15] *HIPAA Administrative Simplification*, U.S. Department of Health and Human Services Office for Civil Rights Std., Mar. 2013. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/administrative/

[16] *Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures*, PCI Security Standards Council Std., Rev. 3.0, Nov. 2013. [Online]. Available: https://www.pcisecuritystandards.org/security_standards/

[17] *Health Information Technology for Economic and Clinical Health (HITECH) Act*, U.S. Department of Health and Human Services Office for Civil Rights Std., Oct. 2013. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

[18] *Procure Secure: A guide to monitoring of security service levels in cloud contracts*, European Union Agency for Network and Information Security (ENISA) Std.