iaes
Institute of Advanced Engineering and Science

International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.3, No.4, August 2014, pp. 200~210
ISSN: 2089-3337

SecSLA: A Proactive and Secure Service Level Agreement Framework for Cloud Services

Fahad F. Alruwaili, T. Aaron Gulliver
Department of Electrical and Computer Engineering, University of Victoria

Article Info

Article history:

Received Jun 19th, 2014
Accepted Jul 26th, 2014

Keyword:

Service Level Agreement (SLA), Security Operations Center (SOC), Compliance, Monitoring, Trust, Privacy, Cloud Services

ABSTRACT

Cloud customers migrate to cloud services to reduce the operational costs of information technology (IT) and increase organization efficiency. However, ensuring cloud security is very challenging. As a consequence, cloud service providers find it difficult to persuade customers to acquire their services due to security concerns. In terms of outsourcing applications, software, and/or infrastructure services to the cloud, customers are concerned about the availability, integrity, privacy, and legality of the hosted service. In this paper, a secure service level agreement (SecSLA) framework is proposed to alleviate these concerns and provide security control assurance to cloud customers. The framework is proactive in detecting violations of SecSLA parameters based on a cloud security operations center as a service (SOCaaS). In addition, a trusted third party can use this framework to audit and monitor SecSLA compliance.

Corresponding Author:

Fahad F. Alruwaili
Department of Electrical and Computer Engineering
University of Victoria, PO Box 1700, STN CSC
Victoria, BC V8W 2Y2, Canada
Email: fruwaili@uvic.ca

1. INTRODUCTION

Cloud computing services have been the subject of significant recent interest among computing practitioners and researchers. These services are delivered on demand and on a pay-as-you-use basis. Cloud computing is one of the most substantial changes in the history of the information technology (IT) industry. This is because it promises to provide improved functionality, flexibility, and scalability through the delivery of virtualized computing resources. In addition to the agility in providing these resources, cloud customers can reduce costs by acquiring these virtualized resources instead of traditional internal IT resources [1]. Cloud computing services are delivered over the internet and provide scalable processing power and storage [2]. The three main models of delivering these services are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [3].

The major hindrance to the adoption of cloud services has been concerns with regards to security, compliance and information privacy. According to a recent survey by Gartner Inc. [4], a leading information technology research and advisory company, the most sought after cloud security services are email, application, identity, and access management protection. They predict that the market for cloud security services will reach USD 3.1 billion by 2015. The key to providing security assurance to cloud customers is the contractual agreements with cloud service providers. A service level agreement (SLA) is a contract between legal entities ~~t~~hat describes the services expected by cloud customers, the quality of service (QoS), payments for compliance, and penalties in the case of SLA violations [5]. Current SLAs for cloud computing services are typically limited to service availability, performance requirements, and penalties for violations, and thus do not adequately address cloud information security and data privacy issues.

The absence of comprehensive security controls combined with the lack of methods and standards to implement them makes it very difficult for cloud service providers to provide trustworthy virtualized services [6]. This paper presents a secure service level agreement (SecSLA) framework for cloud service environments to address this problem. We previously developed security operations center as a service (SOCaaS) [7] to monitor cloud services and its compliance with customer requirements. The SOCaaS system enables trusted third party entities to manage cloud service provider security appliances, applications, and software to efficiently and effectively detect, analyse, and respond to malicious cloud events. The SOCaaS system does not only collect and analyze events and logs from every security device, but also correlates these logs to identify relationships and proactively detect threats. This improves the response time and accuracy of incident detection. The system event management (SEM) component in the SOCaaS system is utilized in the design of the SecSLA framework. The SEM allows cloud customers to transparently monitor control compliance with their SecSLA parameters and detect violations.

In this paper, the proposed SecSLA framework consists of multiple components including a security controls matrix, log database, compliance and audit checks, and a console for creating and editing SecSLA control parameters. Activity theory is used as the basis for determining the controls for security compliance, and these controls are detailed in the security controls matrix. This taxonomy matrix is based on security controls recommended by the cloud security alliance (CSA), and combines industry accepted security standards, controls and frameworks such as NIST SP800-53, COBIT, ENISA IAF, HIPAA, ISO 27001/27002, NERC CIP, PCI DSS, and FedRAMP [8].

The remainder of this paper is organized as follows. The next section presents the motivation for this work based on customer requirements. In Section 3, the related literature is discussed, and Section 4 outlines the goals of this paper. Section 5 defines service level agreements and describes the construction of the SecSLA framework. Provisioning and negotiation of the cloud security controls workflow process are also outlined. Section 6 provides a discussion of the framework, and finally some conclusions are given in Section 7.

2. MOTIVATION AND CUSTOMER REQUIREMENTS

Organizations wanting to outsource their IT infrastructure, platforms, and applications to cloud service providers should revise their organizational, legal and operational requirements prior to making any decisions. In addition, organizations must assess and document the sensitivity, value, and criticality of their data and information assets. They should also update and document the risks associated with their critical assets. Without this classification and the associated risk assessment, it is not possible to determine the cloud security service requirements and compliance controls. In addition, this exercise will ensure that the security and privacy requirements of cloud customers are properly defined in their initial request for proposal (RFP) and prior to outsourcing to cloud services. This can later be translated into a SecSLA that defines suitable controls provided by the cloud provider. Each SecSLA parameter corresponds to a control or a set of controls. If the acquired cloud services do not conform to the SecSLA parameters, the cloud customer can either accept the risk associated with a failure to protect the services or transfer to a more secure cloud service provider.

3. RELATED WORK

In traditional IT settings, domain specific security controls such as those recommended by the National Institute of Standards and Technology NIST-800-53 standard [9] can be applied. However, new components outside traditional information systems (e.g., cloud computing services) were not designed to be protected by these security controls and policies and therefore are considered insecure [10]. Chaves et al. [11] explored the existing state of security in cloud SLAs. Their survey results indicated the need for improved SLA security specifications and a framework for monitoring and managing secure SLA agreements. This paper addresses these concerns by provides a cloud-specific security controls table and a SecSLA monitoring framework, as well as a control provisioning process.

Bernsmed et al. [6] suggested a monitoring framework for SecSLA through modified web service (WS) agreements. These agreements address security specifications in grid computing and web services, but lack details with regard to cloud security controls, proactive monitoring, and the negotiation process for security controls provisioning. Clark et al. [5] introduced SLA monitoring based on modifications to WS agreements to add the necessary terms and condition to the SLA. Their framework allows trusted third parties to monitor the system and detect SLA violations. However, this approach does not provide security and privacy controls for cloud or traditional IT environments. Further, it cannot be applied to cloud service models (i.e., IaaS, PaaS, SaaS).

In 2003, Keller and Ludwig [12] proposed a web service level agreement (WSLA) framework for specifying and monitoring web enabled service agreements. However, it is not applicable to cloud services and cannot detect security compliance violations. Alhamad et al. [1] proposed a conceptual SLA framework for cloud computing. They defined an SLA framework based on non-functional requirements (e.g., availability, scalability, and response time). While they consider the technical requirements in IaaS, PaaS, and SaaS, the security controls and policy requirements to protect cloud services are not addressed.

In the existing literature on cloud computing services, there is no approach which provides cloud customers comprehensive cloud security and privacy with compliance monitoring and reporting. Given the increasing demand for security and privacy in cloud services and the need to he compliant with regulatory requirements [4], it is very important to implement a suitable framework. The SecSLA framework presented here addresses this problem.

4. OBJECTIVES

The aim of this paper is to develop a secure service level agreement (SecSLA) framework for cloud computing environments. The SecSLA is based on a set of cloud security and privacy controls recommended by the CSA [8]. These controls are defined in a security controls matrix which is presented in Section 5.3. The approach in [7] is used to collect event logs generated by cloud devices and systems. These logs are analysed and the results compared with the SecSLA parameters to ensure compliance and facilitate enforcement. The system can provide cloud customers with both periodic and on demand reports. In addition, customers can add and modify control to provide robust and agile response to changes in security requirements. To achieve this, a control provisioning and negotiation process is provided to facilitate interaction between cloud customers and service providers. The corresponding workflow process is presented in Section 5.4.

It is assumed that cloud service providers will allow not only customers, but also trusted third party agents, to check compliance with SecSLA parameters. These agents are typically hired by cloud customers when they lack the necessary monitoring and auditing capabilities (e.g., auditing experts and auditing systems). In addition, hiring a professional third party promotes accuracy, transparency, and compliance with SecSLAs.

5. THE SECURE SERVICE LEVEL AGREEMENT (SecSLA)

This section provides the SLA and SecSLA definitions, as well as the theory used to develop the SecSLA cloud security controls matrix. The SecSLA control negotiation and provisioning workflow process is also presented as well as the system for monitoring and enforcing the SecSLA.

5.1. SLA and SecSLA Definitions

An SLA is a contractual document between a cloud customer and a cloud service provider. It describes the required services, service parameters, service guarantees, and the actions required in case of SLA violations. Typically these actions include the penalties service providers have to pay to their customers if the SLA parameters (e.g., service performance metrics), are not satisfied [1], [13]. Conversely, the SecSLA specifies security and privacy control policies. It describes the availability, confidentiality, integrity, and privacy parameters and the associated controls needed to protect cloud services. While the SecSLA can be a component of the SLA, it is a separate document. In this paper, a controls matrix, control provisioning and negotiation workflow process, and monitoring system are proposed to ensure proper security service levels and compliance and enforcement of SecSLA parameters.

5.2. The SecSLA Concept

The SecSLA framework (shown in Figure 1 and described in detail in Section 5.5), is based on activity theory as introduced by Engestrom [14],[15]. The application of this theory to the objectives in Section 4 provides a basis for determining actions for security noncompliance and violations. It provides means of addressing complex cloud security requirements by allowing technical or non-technical personnel to apply the necessary rules and policies to achieve a given outcome. According to Figure 1, the object (applying security and privacy controls to each SecSLA parameter) is achieved by involving subjects (cloud customers, providers, and auditors) who use tools or mediating artifacts (e.g., SecSLA framework, SOCaaS [7], and event management) to perform the necessary tasks to meet the SecSLA requirements. The tasks are accomplished through a division of labour (e.g., between the cloud provider and compliance auditor). The subject functions within the respective community (i.e., service provider and external parties) through rules (i.e., information security and privacy policies, legal obligations and mandates, organizational goals) to determine the basis for the required set of security and privacy requirements (i.e., SecSLA parameters).

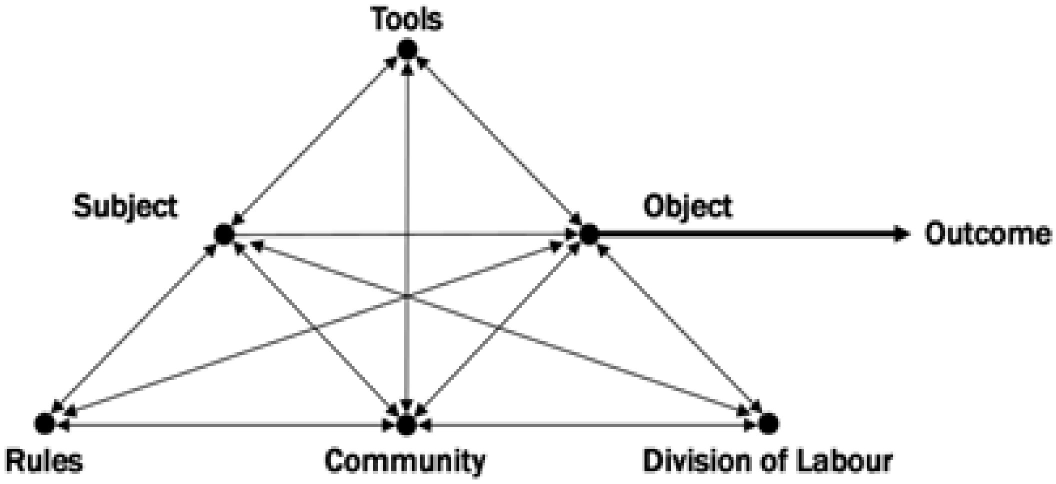

Figure 1. The activity theory system model [15].

5.3. The SecSLA Taxonomy Matrix for Cloud Security and Privacy Controls

The cloud security and privacy controls are identified in this section with respect to four main domains: confidentiality, integrity, availability, and privacy. Table 1 shows the domain, relevant control name, and its application to the cloud service models, i.e., IaaS, PaaS, and SaaS. Note that the service criticality and control priority criteria for a control can vary depending on the customer. Typically, criticality is classified as low, medium or high, and control priority from P0 to P3 (P0 indicates no control, P3 indicates a higher priority than P1 and P2). Therefore, if a cloud service is marked as highly classified, the priority can be set to P3 indicating that a set of security controls must be applied.

Table 1 gives a sample of the most critical cloud security controls. In an actual implementation a longer list would be required. The goal is to provide cloud customers with tailored security controls. If after the SecSLA is defined a new control is required by the cloud customer, negotiations can be conducted with the cloud provider to discuss its feasibility and applicability.

Table 1. The cloud security controls matrix [15].

Control Domain	Control Name	Control Description	Application to Cloud Service Model		
			SaaS	PaaS	IaaS
Privacy	**Data Retention**	The policies and procedures for storing cloud data for compliance and/or other reasons as defined in the SecSLA. The storage location (country) is an important element of the SecSLA.	✓	✓	
Confidentiality	**Data Leakage**	The security mechanisms employed to prevent data leakage. These include the access control policy, user account management/identity management, and access enforcement for cloud assets. For example, a cloud user may require dual authorization (two forms of approval) to access cloud services and/or data.	✓	✓	✓
Privacy and Confidentiality	**Secure Disposal of Data**	The policies and mechanisms for the complete removal of customer data from the cloud without any possible recovery. These may include media sanitization to release cloud provider control media for reuse. If the media cannot be sanitized, then it must be physically destroyed.	✓	✓	

Confidentiality	**Classified Data Protection**	The encryption mechanisms and protocols employed to protect cloud data in storage, processing, and transmission according to the customer SecSLA data classification. The cryptographic module is installed within supervisory engine to protect against data disclosure to another virtual machine (cloud tenant). In the network layer, cloud customer sessions are encrypted to protect against disclosure.	✓	✓	✓
Confidentiality	**Cloud Storage**	The encryption employed by the cloud service providers. Typically they are required to employ strong encryption (e.g., 256 bit AES), but only the data owners (cloud customers) have access to the keys. Therefore, cloud customer must adopt a secure key management system.	✓	✓	
Confidentiality, Availability, Integrity, and Privacy	**Incident & Vulnerability Management**	The intrusion detection and prevention systems implemented in the layers of the cloud model. This prevents cloud services from viruses, cyber-attacks, and other known or zero day attacks. In addition, cloud service providers must perform periodic penetration testing and vulnerability scans to detect system/application weaknesses and take necessary corrective actions (e.g., system patches). Antivirus software is mandatory to protect cloud servers, customers and virtual machines. Service providers must make incident and vulnerability information available to all affected customers.	✓	✓	✓
Confidentiality, Availability, Integrity, and Privacy	**Trusted Third Party Assessment**	The cloud service providers must allow access to external trusted third parties to audit and assess compliance with the SecSLA. This can be both prior to cloud service acquisition and during service operations. All cloud systems are assessed, e.g. physical, procedural, technical, legal, and compliance controls. It can be conducted at planned intervals or on demand as required to maintain SecSLA compliance.	✓	✓	✓
Confidentiality	**Virtualization (Hypervisor) Security**	The cloud service provider must implement isolation controls to shield critical cloud assets and sensitive data from other tenants. Sessions that need stronger controls should be segregated from machines that implement insufficient security controls. In addition, access to the hypervisor must be restricted and strong authentication employed, e.g. two-factor authentication.		✓	✓

5.4. The SecSLA Control Provisioning and Negotiation Process

Security and privacy control request changes can originate from different locations. For example, a cloud customer may call, email, or web request a service provider to add or edit security controls in the SecSLA. The cloud customer can hire a trusted third party cloud agent or an expert to monitor SecSLA compliance. While a cloud customer can choose from an existing security controls matrix, they can also request a new control, which for example can result from a new security or privacy mandate. These requests typically originate from the chief security officer (CSO) and/or chief privacy officer (CPO) or their delegates.

Figure 2 shows the security and privacy control request negotiation workflow. The steps in this process are outlined below.

1. The CSO and/or CPO receive a new regulatory compliance request or an update to a security and/or privacy policy.
2. The cloud security agent (CSA) receives the request, assigns a tracking number, informs the initiator, and forwards the request to the security and privacy control personnel of the cloud service provider. The CSA is an automated service that manages the requests received electronically via emails, online forms, and automated phone answering agents. It assigns the necessary request information (e.g., initiator information and request parameter information), and forwards the request to control personnel for request revision and assessment. This process can also be executed manually if the CSA administrator receives the request in person or via a voice call. The request information is then sent to the control provisioning and negotiation system.

3. The control personnel review the request and assign it to the appropriate control based on the existing controls matrix.
4. The request is forwarded to the cloud operations personnel to check compatibility with the customer cloud services. If there are no issues, the control is applied to the customer services and this is reported back to the cloud agent. The cloud agent updates the SecSLA and informs the customer of the successful change and request completion.
5. If an issue occurs that prevents completing the request, for example when there is a conflict between the SecSLA and the original SLA. For instance, when applying the new security or privacy control, the CPU time and memory usage can be degraded such that it affects the functionality of a cloud service. This must be resolved prior to applying the security control. In this case, the solution may be to increase the allocated CPU time and memory, which will result in additional costs to the customer. Once the issue has been resolved, the control personnel will instruct the cloud security agent to update the SecSLA and inform the CSP/CPO of request completion.

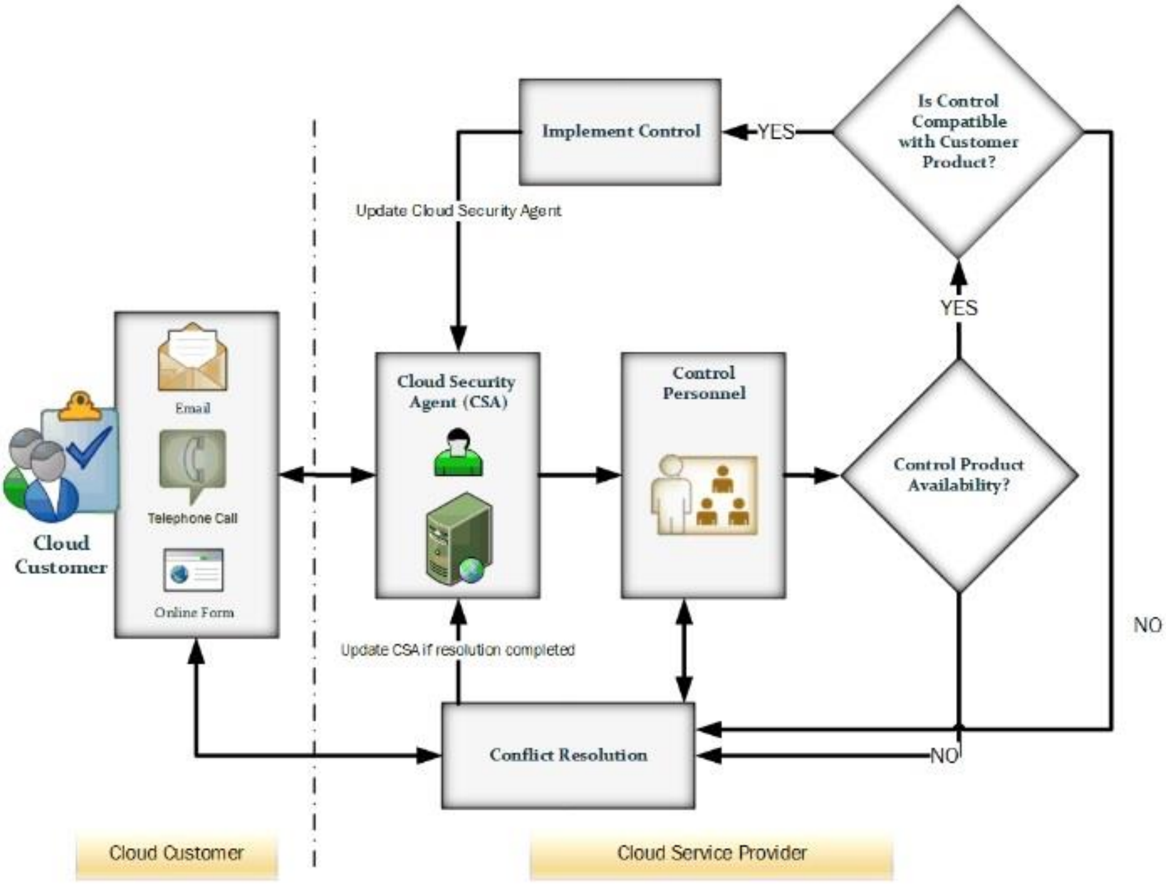
Implement Control
YES
Is Control Compatible with Customer Product?
Update Cloud Security Agent
YES
Cloud Customer
Email
Telephone Call
Online Form
Cloud Security Agent (CSA)
Control Personnel
Control Product Availability?
NO
Update CSA if resolution completed
Conflict Resolution
NO
Cloud Customer
Cloud Service Provider

Figure 2. The security and privacy control request negotiation workflow.

5.5. The SecSLA Framework

The SecSLA framework is presented in Figure 3. It is a standalone system to minimize the impact on the performance of virtualized services, yet it interacts with many components of the cloud system. For example, the SecSLA system checks with security devices (e.g., firewalls, antivirus applications, intrusion detection and prevention systems, identity and management and access control systems), to ensure SecSLA polices are enforced.

The framework consists of the following main components:

5.5.1 Log Database (LD)

The LD is responsible for collecting and storing logs from security devices, policy profiles, event management, and the hypervisor in real time. The LD provides a taxonomy for these logs. For example, the LD classifies logs as logs collected:

- *from firewall devices in the IaaS layer*
- *form user activities in the PaaS layer*
- *from virtual machine (VM) sessions*
- *from the event management system*

The LD also reports if it fails to collect from or reach a device to a system administrator or analyst who will assess the cause and take the necessary steps to recover from the failure. The LD as the main repository for logs, it requires online backup in case of failure.

5.5.2 Compliance Monitoring Engine (CME)

The CME continuously checks the LD database for any deviation between the applied security controls and security controls matrix (SCM) parameters. Any deviation triggers a violation to the customer SecSLA. The CME performs advanced analysis to detect security control violations. For example, if a cloud customer requests incident and vulnerability management control to protect their virtual resources, the control is granted and listed as active in their profile. Now, if logs collected from the event management system indicate that this control is not listed as active, a SecSLA violation is triggered. As another example, suppose a customer requests control of secure web service activities. The service provider will perform the following controls and apply them to the customer web service:

# Disable HTTP – TCP port 80, <egress=1, ingress=1>
# Disable HTTP – UDP port 80, <egress=1, ingress=1>
# Disable HTTP – TCP 8080, <egress=1, ingress=1>
# Enable HTTPS – TCP port 443, <egress=1, ingress=1>
# Enable HTTPS – UDP port 443, <egress=1, ingress=1>

If a TCP service request on port 80 is then found to be open or TCP/UDP HTTP connection establishment is acknowledged, a SecSLA violation is triggered.

5.5.3 Security Controls Matrix (SCM)

The SCM provides a control profile for each cloud customer. From Section 5.3, each profile consists of security and privacy parameters for each service. Each parameter corresponds to a security control or a set of security controls in the service provider domain. For example, if a parameter is to provide protection against incidents, the control is to place the customer service under the supervision of the incident and vulnerability management system. As another example, if a customer wants a certain service to be classified as public and highly available, then the corresponding security controls will be set to P0 (no controls) and the availability set to 1 which represents 100% service availability (0.5=50% of the time the service is available). In practice it is hard to achieve 100% availability due to, for example, routine maintenance. However, the five nines (99.999%) is commonly taken to indicate high availability and reliability of computing services.

5.5.4 Cloud Customer Console (CCC)

The CCC enables cloud customers to negotiate SecSLA parameters. The negotiation process was described in Section 5.4.

.

5.5.5 Reporting and Notification

This component provides involved parties (i.e., customers, service providers, and trusted third party compliance auditors), with detailed compliance reports and notification of violations. The report lists the customer SCM parameters and the corresponding controls. It also indicates either compliant or non-compliant for each SecSLA parameter. A justification is given if non-compliance is indicated. Notifications are quickly sent to all involved parties in the form of email and/or text messages if a violation is detected (e.g., customers unable to reach services, customer data unencrypted, an incident that affects customer services is not reported). These reports can be scheduled weekly and also delivered on demand depending on the circumstances. Generating the reports and notifications requires that logs be processed and checked for compliance in real time.

In Figure 3, the left side of the framework consists of the cloud service provider domain which contains security systems, devices, policies, and controls. These work together and exist on each cloud service model (IaaS, PaaS, and SaaS). The logs generated from these systems are examined by the LD for control compliance by checking against the customer profiles in the SCM. It is important for cloud providers to ensure that all logs are collected by the LD in a timely manner, otherwise false or missed violations may occur which will result in erroneous notifications and reports.

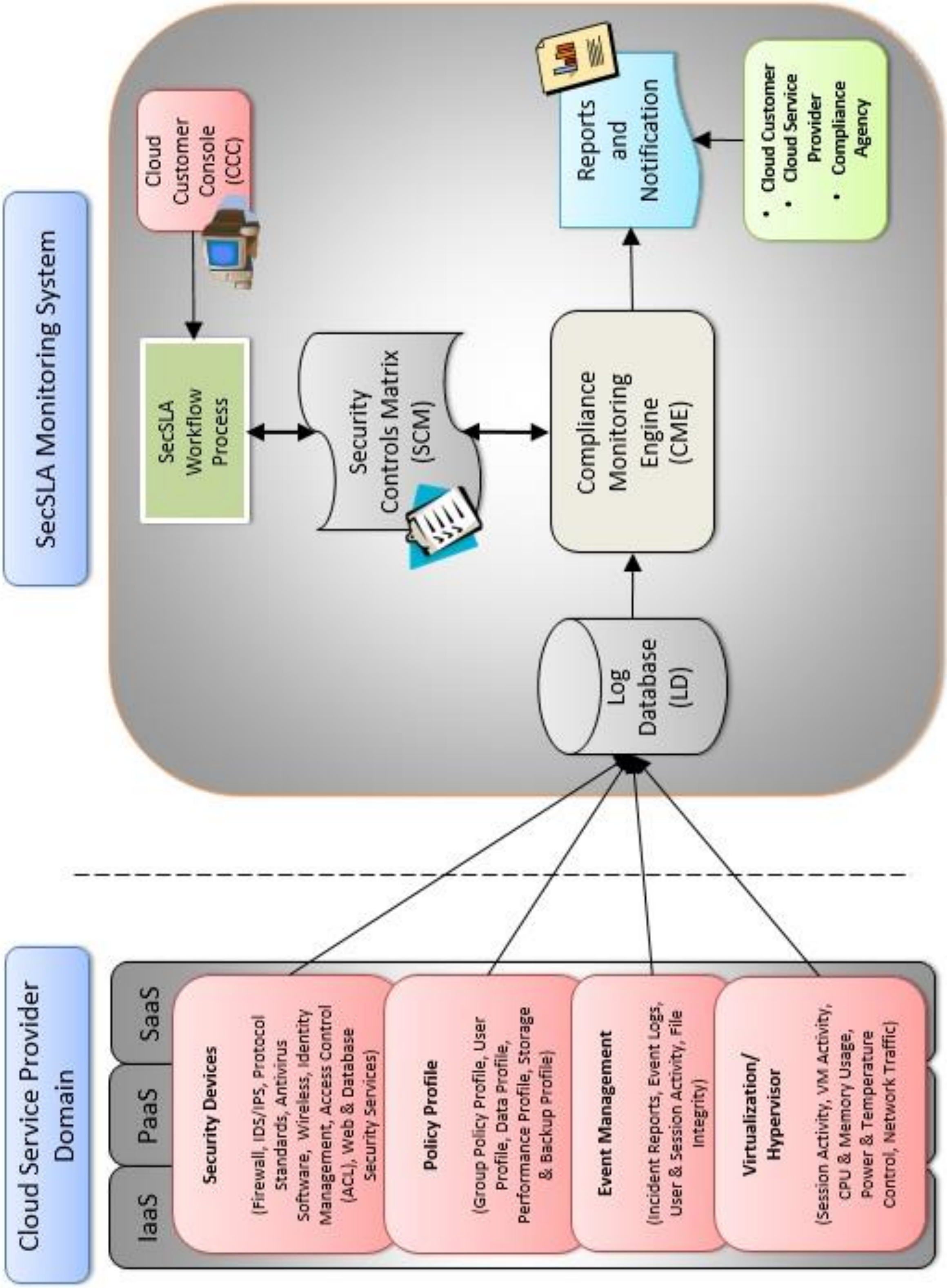
SecSLA Monitoring System
Cloud Customer Console (CCC)
SecSLA Workflow Process
Security Controls Matrix (SCM)
Compliance Monitoring Engine (CME)
Log Database (LD)
Reports and Notification
Cloud Customer
Cloud Service Provider
Compliance Agency
Cloud Service Provider Domain
IaaS
PaaS
SaaS
Security Devices
(Firewall, IDS/IPS, Protocol Standards, Antivirus Software, Wireless, Identity Management, Access Control (ACL), Web & Database Security Services)
Policy Profile
(Group Policy Profile, User Profile, Data Profile, Performance Profile, Storage & Backup Profile)
Event Management
(Incident Reports, Event Logs, User & Session Activity, File Integrity)
Virtualization/ Hypervisor
(Session Activity, VM Activity, CPU & Memory Usage, Power & Temperature Control, Network Traffic)

Figure 3. The SecSLA system framework.

6. DISCUSSION

In this section, the advantages of the proposed SecSLA framework are discussed based on the objectives given in Section 4. The SecSLA framework was developed according to cloud security controls recommended by CSA and implemented using a cloud security matrix (CCM Version 3) [8]. While cloud customers receive periodic reports from cloud providers regarding SecSLA compliance, transparency will be greatly improved if cloud customers employ a trusted third party as a compliance agent to monitor and verify that the SecSLA is not violated. Continuous verification and monitoring also increase customer trust and acceptance of cloud services. The monitoring component in the SecSLA framework is an extension of the SOCaaS approach presented in [7] which provides comprehensive security monitoring and event management for cloud services. The SecSLA monitoring system detects any deviations from the agreed upon terms and proactively alerts cloud customers and providers of violations via email and text notifications.

The security and privacy controls are the key component of the SecSLA framework as they alleviates the majority of cloud customer security and privacy concerns. Each control corresponds to a parameter in the SecSLA and these are typically defined in the early stages of the negotiation process. This framework also provides a negotiation system for cloud customers to request, edit, or remove security controls on their cloud services. A conflict resolution process is included for situations where a requested control is not viable or is not listed as an option in the controls table.

The SecSLA is a set of contractual requirements that addresses the four main security concerns, confidentiality, integrity, availability, and privacy of cloud information. Functional and business process requirements are not included since most cloud providers have reached a sufficient level of maturity in these areas. However, security and privacy controls must be improved, which will require significant investment by service providers. The proposed SecSLA framework motivates these investments as it will increase the trust, compliance transparency and enforcement of cloud providers.

7. CONCLUSION

Current cloud service level agreements (SLAs) have parameters for availability, quality of service and penalties for violations, but few are provided for security and privacy [6]. Further, cloud service providers do not offer detailed security and privacy SLA parameters. In addition, there is a shortage of tools for cloud customers to provision, monitor, and enforce security and privacy controls. A recent survey by the European network and information security agency (ENISA) indicates that while SLAs are often used to address service availability, security parameters are poorly covered. Moreover, many cloud customers often do not monitor SLA security on a continuous basis which leaves them unaware of security violations [16], [17]. Section 2 stressed the importance of cloud customers performing a risk assessment and data classification of their information assets prior to outsourcing their assets to the cloud.

In this paper, a new security SLA (SecSLA) framework was proposed to address the shortcomings of current SLAs in terms of cloud confidentiality, integrity, availability and security and privacy controls. The framework components are compliance monitoring of the SecSLA parameters, provisioning and negotiation of cloud security controls, security controls matrix, and reports and notifications. The monitoring system was developed based on a recently proposed approach to collecting, analysing, and responding to events via data logs [7]. The SecSLA framework enables cloud customers and trusted third party auditors to monitor SecSLA compliance and the efficiency and effectiveness of controls on customer services. The main goal of this work is to promote the adoption of cloud services by cloud customers. The proactive control monitoring promotes trust, increases transparency, and emphasizes information security and data privacy controls.

ACKNOWLEDGEMENTS

The research work of the first author was sponsored by Shaqra University, Shaqra, Saudi Arabia

REFERENCES

[1] M. Alhamad, T. Dillon, and E. Chang, "Conceptual SLA Framework for Cloud Computing," *IEEE International Conference on Digital Ecosystems and Technologies*, pp. 606-610, April 2010.

[2] E. Badidi, “A Cloud Service Broker for SLA-Based SaaS Provisioning,” *IEEE International Conference on Information Society*, pp. 61-66, June 2013.

[3] M. Peter and T. Grance, "The NIST definition of cloud computing (draft)." *NIST special publication (800-145)*, January 2011.

[4] Stamford, and Conn., “Gartner Says Cloud-Based Security Services Market to Reach $2.1 Billion in 2013,” *Gartner Inc.*, http://www.gartner.com/newsroom/id/2616115, October 2013.

[5] K. P. Clark, M. E. Warnier, F. M. Brazier, and T. B. Quillinan, “Secure monitoring of service level agreements,” *IEEE International Conference on Availability, Reliability, and Security*, pp. 454-461, February 2010.

[6] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim,”Security SLAs for federated cloud services,” *IEEE International Conference on Availability, Reliability and Security*, pp. 202-209, August 2011.

[7] F. F. Alruwaili, and T. A. Gulliver, "SOCaaS: Security Operations Center as a Service for Cloud Computing Environments," *submitted for publication on International Journal of Cloud Computing and Services Science*, May 2014.

[8] Cloud Security Alliance Research, "Cloud Controls Matrix v3.0," *Cloud Security Alliance,* https://cloudsecurityalliance.org/research/ccm/, September 2013.

[9] J. T. Force, "Security and Privacy Controls for Federal Information Systems and Organization," *NIST Special Publication (800-53),* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, April 2013.

[10] M. L. Hale, and R. Gamble, "SecAgreement: Advancing Security Risk Calculations in Cloud Services," *In Proceedings of the IEEE World Congress on Services*, pp. 133-140, June 2012.

[11] D. Chaves, S. Aparecida, C. B. Westphall, and F. R. Lamin, "SLA Perspective in Security Management for Cloud Computing," *IEEE International Conference on Networking and Services*, pp. 212-217, March 2010.

[12] A. Keller, and H. Ludwig, "The WSLA Framework: Specifying and Monitoring Service Level Agreements for Web Services," *Journal of Network and Systems Management*, Vol. 11, No. 1, pp. 57-81, March 2003.

[13] Y. Chi, H. J. Moon, H. Hacigümüş, and J. Tatemura, "SLA-tree: a framework for efficiently supporting SLA-based decisions in cloud computing," *International Conference on Extending Database Technology*, pp. 129-140, March 2011.

[14] J. Show, "Information Security in Practice from an Activity-Theoretic Perspective," *In Proceedings of the Annual Security Conference*, pp. 241-248, April 2007.

[15] Y. Engestrom, "Activity Theory and Individual and Social Transformation," *Perspectives on activity theory*, pp. 19-38, 1999.

[16] J. Luna Garcia, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," *In Proceedings of ACM Workshop on Cloud computing security,* pp. 103-112, October 2012.

[17] M. Dekker, and G. Hogben, "Survey and Analysis of Security Parameters in Cloud SLAs Across the European Public Sector," *European Network and Information Security Agency (ENISA),* http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector, December 2011.

BIOGRAPHY OF AUTHORS

Fahad F. Alruwaili is a faculty member at computer science department at University of Shaqra, Saudi Arabia. He works as information security and computer networks consultant with over nine years of practical experience and research development. He earned his BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he achieved his MS degree in Computer, Information, and Network Security with first class honour from DePaul University, Chicago USA. In 2011, he received his second MS degree in Information Systems and Technology from Claremont Graduate University, Los Angeles USA with first class honour. He is currently working towards achieving Ph.D. degree in University of Victoria, the Department of Electrical and Computer Engineering, Canada. His research interests are in the technical and theoretical views of information security and data privacy.

T. Aaron Gulliver received the Ph.D. degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.