Understanding Trustworthy Service Level Agreements: Open Problems and Existing Solutions

Yudhistira Nugraha, Andrew Martin

Understanding Trustworthy Service Level Agreements: Open Problems and Existing Solutions

Yudhistira Nugraha[1,2] and Andrew Martin[1]

[1] Centre for Doctoral Training in Cyber Security,
Department of Computer Science, University of Oxford, UK,
yudhistira.nugraha, andrew.martin@cs.ox.ac.uk,
[2] Directorate of Information Security, Indonesia,
yudhistira.nugraha@kominfo.go.id

Abstract. Security has been considered for decades as a possible attribute in service level agreements (SLAs). However, the formulation of security properties has not been expressed in such concrete terms in SLA contexts because security is a process, not a product. Consequently, security properties, such as data confidentiality, integrity and availability have been overlooked in SLA contexts. This paper aims to identify open problems and existing solutions in the context of incorporating security properties into SLA contexts. First, we provide an overview of system assurance of which trustworthy SLAs can be considered as alternative assurance technique in the context of service provisioning. Then, we describe the notion of trustworthy SLAs and discuss possible security properties that can be potentially used in SLA contexts. Finally, we present some open research problems for the incorporation of security capabilities into SLA contexts to establish trust between the customer and service provider. This study identifies needs for developing a trustworthy SLA capability framework to formulate discrete levels of assurance which are believed to be capable of preserving data confidentiality, integrity and availability in SLAs as trust-enhancing instruments.

Keywords: security, assurance, trust, trustworthiness,
security capability, service level agreement

1 Introduction

Security and assurance have recently been the focus of attention for customers (e.g. government agencies) when using external information system services from third-party services providers. The relationships with the service providers are usually established through service level agreements (SLAs), which have been used for many years in various outsourcing scenarios to regulate multiple service dimensions. However, there is a concern that existing SLAs are typically limited to defining and monitoring the system availability and performance aspects [1–4].

In fact, such SLAs overlook key security aspects (i.e. data confidentiality, integrity and availability). It is not rare the case that many service providers only offer non-binding security mechanisms that are non-negotiable and not incorporated in SLA contexts. Additionally, most service providers will not include in their contract liabilities for assuring the security of any data that is processed, stored and transmitted through their information system services. Such contracts strictly limit service providers' responsibilities for the impact of any security breach.

It is apparent that the perception of SLAs is focused on the system availability aspects, without considering security aspects [1–3]. In this paper, the term of a trustworthy service level agreement [5] is introduced to help ensure discrete levels of assurance can be incorporated into an SLA between a customer and service provider.

The idea of trustworthy SLAs as trust-enhancing instruments is presented in this paper as one of the assurance approaches used in the context of service provisioning. It is intended as a means of quantifying and guaranteeing SLA-based on discrete levels of assurance. Each level is distinct from another. It is expected that each discrete level of assurance offers an increase in quality of protection over the previous level.

Furthermore, in this context, the level of trust can be specified in SLAs regarding a specific security capability offered by service providers according to each discrete level of assurance. However, security is one of the unmeasurable quantities that cannot be measured automatically [6] because security is a process, not a product [7]. Additionally, it is merely hard to measure security without knowing possible risks and threats [8].

Although many service providers have claimed that the information system services they deliver are secure, customers have not received adequate assurance regarding security capabilities from service providers. In fact, such claims fail to address one necessary component: Secure against what? [9] Hence, a threat model and perceived risk, such as spoofing, tampering and information disclosure need be considered in making such claims [10].

This paper seeks to give an overview of concepts, approaches and open problems of expressing security considerations (i.e. data confidentiality, integrity and availability), using discrete levels of assurance into SLA contexts. As far as our knowledge goes, this is the first survey with such goals. The paper shows that there is a need for framework supporting security considerations specified in SLA contexts to enhance the level of trust between customers and service providers. Therefore, this work can be used in future research as foundations for developing a trustworthy SLA capability framework in the context of service provisioning as a means of incorporating discrete levels of assurance into SLA contexts.

The rest of the paper is structured as follows. Section 2 introduces the background. Section 3 presents the notion of trustworthy SLAs. Section 4 presents

open research problems and existing solutions. We conclude our study in Section 5.

2 Background

The terms trust and trustworthiness are used interchangeably, but these are different meanings depending on the context in which they are used. According to NIST SP800-53 [11], *Trust* can be defined as '*the belief that an entity will behave predictably while performing specific functions, in specific environments, and under specified conditions or circumstances*'. In this definition, the entity can be a person, a process, information systems, system components, a system of a system or any combination thereof [11].

In particular, from a security perspective, '*trust is the belief that a security-relevant entity will behave in a predictable manner when satisfying a defined set of security requirements under specified conditions or circumstances and while subjected to disruptions, human errors, component faults and failures, and purposeful attacks that may occur in the environment of operation*' [11]. In other words, *trust* is the belief that a security-related entity will behave as expected, according to the required security requirements, which defined based on a risk tolerance level. Therefore, this definition implies that trust can be determined by a specific security capability, which is a combination of security controls to be applied to a particular risk. Such security controls are implemented by technical means, physical means and individuals [11].

Whereas, trustworthiness concerning information systems '*expresses the degree to expresses the degree to which the systems can be expected to preserve with some degree of confidence, the confidentiality, integrity, and availability of the information that is being processed, stored, or transmitted by the systems across a range of threats*' [11]. RFC 4949 (2007) defines '*a trustworthy system as one that not only is trusted, but also warrants that trust because the systems behaviour can be validated in some convincing way, such as through formal analysis or code review*' [12]. In broad terms, Avizienis et al. (2004) define trustworthiness as '*assurance that a system will perform as expected*' [13].

The term of assurance is a much broader notion than security, which is defined as the protection of information and information systems from unauthorised access, disclosure, modification, disruption or destruction [11]. Assurance properties are aspects of the systems that can be established evidence provided by the system or a third party [14]. These elements may include security requirements, capabilities or functionality of the systems involved [11]. In the context of a remote service environment, it is possible to have good security and poor assurance, while poor assurance is closely associated with poor security [15]. Consequently, inadequate assurance proves that security properties are not well implemented according to laws and regulation.

2.1 System Assurance: An Overview

Many assurance approaches have been used to verify the security of a product, service or system. Some methods are often used to evaluate whether a service is trustworthy. Those approaches are testing, monitoring, certification, audit/compliance, and SLA [15].

Testing The first class of approaches to product, software or service validation and verification is based on testing. In the context of software testing, according to ISTQB glossary, software testing is "a process of executing a program or application with the intent of finding the software bugs". In a remote service environment, such as cloud-based services, testing usually can be group into four main categories, namely functional testing, performance testing, interoperability testing and security testing [16].

However, security testing presents a unique problem [17]. Most software or application flows and vulnerabilities are not associated with security functionality, but because of an intentional or unintentional misuse of the application posed by an attacker [17]. In this case, penetration testing is the most common approach for software security of which it is a form of security testing performed by a group of experts who attack a target system, using a defined set of attack scenarios [17, 18].

Such testing is commonly used to measure software security, especially when it is fully integrated into the development process in such a way that findings can help to identify and fix the development problems [18]. The main problem with the penetration testing is frequent failure to devise mitigation strategies to address the identified vulnerabilities in the analysed systems [18].

Monitoring The second class of approaches to measuring remote services is based on monitoring measurements. Monitoring can help to increase the level of transparency in a remote service environment. According to NIST SP 800-94 on Guide to Intrusion Detection and Prevention Systems [19], monitoring can be performed, as follows:

- Network-Based, which monitors network traffic flows or devices and performs network analysis to identify suspicious activities.
- Wireless, which monitors wireless network traffic flows and analyses it to identify suspicious activities.
- Network Behavior Analysis (NBA), which identifies unusual traffic flows, such as distributed denial of service (DDoS) attacks, malware, and policy violations.
- Host-Based, which monitors features of a single host and the events occurring within that host for suspicious activities.

Focusing on cloud environments, service monitoring can be performed through different layers, namely facility, network, OS, middleware, application and the user [20]. These layers can be controlled and monitored by either the cloud customer or the cloud provider [20, 21]. For example, the cloud provider controls under the three service models (i.e. Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS)).

However, not all layers of monitoring can be controlled by the cloud provider. In SaaS model, the cloud provider can access all layers except the user layer. Similarly, the PaaS provider does not have access to the application layer and the user layer. Whereas, the IaaS provider only has access to facility, network and hardware layers.

Any SLA should describe these line of responsibility. Such SLAs must include robust auditing and monitoring capability for the customer [20, 21]. It is clear that contracts and SLAs are the primary instruments of customer control [20]

Certification The third class of approaches to evaluating and certifying security properties of product or software, in general, is based on certification schemes. Such certifications aim to provide enough evidence that product, software or service holds some security properties and behaves as expected [15, 22]. Many certification schemes have been proposed in past and today, and have been widespread and become essential in outsourcing and remote service environments.

Such certifications are very commonly used for public procurement to help identify the security level of information systems, such as the Common Criteria (CC) and ISO 27001 [14, 23]. For instance, CC is often used as the basis for a government-driven certification scheme and security evaluation for information technology products, software, services or systems, especially those focused on high-assurance systems [24].

However, the security evaluation process is known to be slow-moving, and such certifications cause substantial costs of security services to the suppliers or service providers [23]. Interestingly, according to Anisetti et al. [25], existing certification schemes are not well-suited to the service scenario, such as cloud-based services. In fact, the certification schemes do not ensure better security [26] and cannot contribute to addressing emerging threats and vulnerabilities [23].

Audit and Compliance The fourth important aspect of assurance systems is the capability of observing the product, software or service behaviour and evaluating its compliance requirements and regulations [15]. In other words, this aims to increase the level of trustworthiness between the service provider and its customers. In the context of cloud computing, Pearson [27] claims the need of an accountable cloud, which helps increase the level of trust between service

providers and customer, and support in the identification of responsibilities in case of disputes.

Doelitzcher [28] identified three auditing categories, which are security audit, privacy audit and legal audit. Each of categories has different requirements to be fulfilled. The security audit includes requirements regarding Malware protection, preventing undesirable software, service misconfiguration, unwanted service combination, account and login requirements, access rights and password strength. The privacy audit includes mostly requirements which help prevent metadata and unintentional data disclosure, such as browser caches, log files, history files and insecurely deleted files. Whereas, the legal audit includes all set of compliance requirements, such as customer specific requirements and illegal contents.

It is acknowledged that cloud audit is challenging than non-cloud systems, which have been seen as a potential barrier to procuring cloud-based services [29]. Whereas, the approaches to IT audit and financial audit are well-established. Armbrust et al. [29] point out that lack of cloud audit capability presents some questions, such as compliance with new legislation, such as the Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX) [30]. Consequently, there is a need for a robust approach to cloud audit that helps ensure compliance with all related legislation, regulations and standards [31].

Another issue with standard compliance is that it is not mandatory, but purely a voluntary basis and practice. The importance of having compliance is to assure all customers even though there is no legal or regulatory obligation to do so. Interestingly, according to Duncan and Whittington, compliance with security standards, such ISO 27000, NIST and Cloud Security Alliance [32] is more likely to ensure compliance with a particular security standard, rather than achieve a significant level of security. This argument is also supported by Anderson [26].

Service Level Agreement Another type of assurance systems is based on Service Level Agreements (SLAs). The use of SLA as trust enhancing instruments is to establish contracts between customers and service providers regulating their interactions, and formulating their agreement regarding both functional and nonfunctional requirements. In other words, an SLA can be seen as a binding agreement between the service provider and customer to establish the obligation of the service provider to deliver service capabilities (e.g. security capabilities) according to service requirements (e.g. security requirements) elicited from the customer side [1, 15].

Such SLAs typically include the responsibilities of both parties of the services delivered, and the legal remedies to be applied by the customer or the service provider in case of the agreed terms are not respected [1, 33]. Such SLAs also include quality of service attributes (e.g. throughput, response times, resolution times and service availability)

Debate continues about the appropriate assurance approach in service provisioning. So far, the use of assurance approaches based on SLAs is becoming increasingly important in procuring such remote services. However, the perception of SLAs is mainly focused on the system availability and performance aspects, without considering security aspects [1–3]. Security is often overlooked when expressing such attributes in SLAs [1,2] because of lack of linkage between discrete levels of assurance and SLAs.

It seems that the idea of a trustworthy SLA capability as trust-enhancing instruments can be considered as alternative assurance technique in the context of service provisioning, which aims to establish discrete levels of assurance expressed in SLA contexts between contracting parties. Lack of trustworthiness and security in SLAs, in fact, makes the service provider's liabilities for the impact of any security threats not clear to the customer. By using the concept of trustworthy SLAs, the service offerings are evaluated according to the discrete level of assurance required.

3 The Notion of Trustworthy Service Level Agreements

The term *security property* is widely used in information security literature (i.e. confidentiality, integrity and availability). In addition to this, according to ITU-T Rec. X.805 [34], the security properties can include access control, authentication, non-repudiation, communication security and privacy, as shown in Figure 1. The formulation of security properties (i.e. data confidentiality, integrity and availability) has not been expressed in such measurable terms in SLA contexts, because security is a process and not a product [7].

In fact, the perception of SLAs is focused on the performance and system availability aspects, without considering security aspects [1–3]. Thus, in this paper, the term of a trustworthy service level agreement is introduced to help ensure discrete levels of assurance that are believed to be capable of preserving data confidentiality, integrity and availability in SLA contexts.

Furthermore, according to Chan et al. (2004), such security properties or dimensions (i.e. availability, data confidentiality, data integrity, access control, authentication, non-repudiation, communication security and privacy) can be potentially used as security SLA attributes [35], as follows.

Availability Service providers place a significant importance on the system availability and performance aspects [3, 6]. These aspects seem to be the major attribute specified in SLAs, including response times and resolution times. However, from a security perspective, availability is intended to ensure there is no denial of authorised access to network and service elements [34]. The SLA attributes are measured by metrics, such as % of downtime due to security incidents (e.g. DDoS attacks) [35].

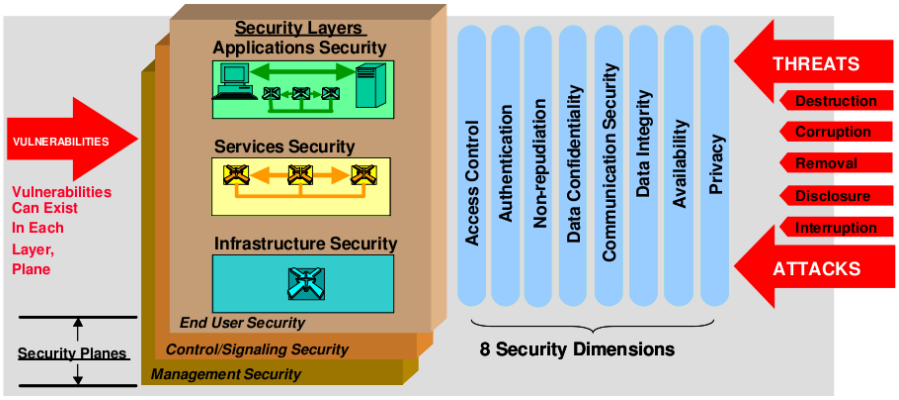

Fig. 1: ITU-T X.805: Security Architecture for Systems Providing End-to-End Communications [34]

Data Confidentiality Confidentiality is one of the security properties that can be potentially used as a security SLA attribute [35]. This attribute is intended to preserve sensitive data from unauthorised access or disclosure. This SLA attribute can be measured by examining whether confidentiality is preserved or confidentiality is lost [36]. However, it seems not useful to use the metrics since little attention has been paid to specify the assured levels of confidentiality against information disclosure threats [10]. Hence, there is a need to develop confidentiality capabilities specified in the formulation of security-related SLAs [3].

Data Integrity Chan et al. [35] named the integrity is one of the security properties that can be specified in security-related SLAs [35, 36]. This property aims to ensure the correctness of data against unauthorised modification (e.g. Tampering) [10, 34]. According to Chan et al. [35], this SLA attribute can be measured by metrics, such as percentage attack occurred due to lack of integrity checks. However, there is a present little knowledge how to define key metrics for data integrity, which can be understood and accepted by customers and service providers [36]

Access Control According to Chan et al. [35], access control can be potentially used as a security SLA attribute to ensure only authorised personnel or devices are allowed to access network elements, services, applications as well as information stored, transmitted and processed within systems [34]. However, this property does not receive the same degree of attention as availability for which metrics are not well established, such as the percentage of unauthorised access detected in sys log [35].

Authentication Authentication is one of the key elements of security properties, which apply to the use of information system services to confirm the

Table 1: Concepts Of Security-related SLAs, based on Risks [10, 34, 35]

Risk	Description	Properties
Denial of Service	It allows an attacker to take action that prevents legitimate users from accessing targeted systems or devices.	Availability
Information Disclosure	It allows an attacker to gain valuable information about a system and reveal it to unauthorised users.	Data Confidentiality
Tampering with Data	It allows an attacker to make unauthorised modification, deletion and replication.	Data Integrity
Unauthorised Access	It allows an attacker to access network elements, services, applications, and data stored, transmitted and processed within systems.	Access Control
Spoofing Identity	It allows an attacker to pretend to be another person, which claims identity of communication entities.	Authentication
Repudiation	It allows an attacker to deny that the attacker performed specific actions or transactions.	Non-repudiation
Interception	It allows an attacker to divert, listen or intercept information flows between the authorised endpoints.	Communication Security
Observation	It allows an attacker to discover network activities or information associated with users.	Privacy

identities of communication entities against spoofing [10, 34, 35]. Although it is possible to formulate authentication into SLA metrics, such as the percentage of systems that require authentication [35], there is little material published on key metrics for authentication.

Non-repudiation According to Chan et al. [35], non-repudiation property is concerned with the ability to provide proof of the origin of data or the cause of an event or an action [34]. Although this property can be potentially used as a security SLA attribute, which defines metrics (e.g. % use of digital signature) [35], little attention has been paid to define measurable metrics against specified threats (e.g. repudiation) [10].

Communication security Chan et al. [35] pointed out that communication security will be possible security attribute in SLAs. This attribute is intended to ensure that information flows only between the authorised endpoints [34,35]. According to Chan et al. [35], this SLA attribute can be measured by metrics, such as the percentage of time sessions are hijacked. However, the SLA metrics depend on security capabilities of the service providers (e.g. IPSec, TLS, encryption method, authentication, VPN Software, Firewalls, IDS and filters) [10,35].

Privacy Another security property highlighted by Chan et al. [35] that potentially be used as a security SLA attribute is privacy. This property is concerned with the system's ability to provide the protection of information that might be derived from the observation of network activities run by the service providers [34,35]. However, little attention has been paid to validating measures of its metrics, such as the percentage of time masquerading attacks occurred [35].

4 Open Problems and Existing Solutions

Many open research problems are still not well investigated and need to be addressed by future research. In this section, we discuss some of the most important open research issued to incorporate security properties into SLA context.

4.1 Quantifying security properties in SLA contexts

Open Problem One of the greatest challenges in expressing security properties in SLA contexts is measuring security capabilities that can be quantified and guaranteed with a reasonable risk for SLA contexts. Security capability is a combination of mutually-reinforcing security controls that can be implemented to mitigate risks and demonstrate compliance with the customer's security requirements [11]. However, it is simply hard to measure security capabilities for which a threat model and risk assessment is not defined. Consequently, the same services that provide an adequate level of security precaution for one customer might provide an inadequate level of security for other customers [8].

Existing Solutions The concept of security-related SLAs was first proposed by Henning [4], who pointed out that security-related SLAs have a lack of tangible and measurable services because security is not quantifiable and has not been expressed in such concrete terms in SLAs. This view is supported by Monahan and Yearworthy [37] who argue that statistical measures need to be captured and understood by customers and service providers to develop meaningful security-related SLAs.

Similarly, Bernsmed et al. [1] asserted that existing security mechanisms should be formalised in explicit agreements or SLAs. Another question has been raised by Luna et al. in [38] about the lack of assurance techniques to quantify security

properties. The authors noted that it is difficult to understand what security capabilities (e.g. specific security controls that will be provided by the service provider) the customers have been paying for, when considering particulars services.

Such previous studies have outlined the importance of considering the formulation of security-related SLAs [1,2,4,37,39]. However, they have primarily served to highlight unresolved issues in defining guarantees and regulations regarding security properties specified in SLA contexts. It is interesting to note that most studies have addressed common ground on lack of tangible and measurable security capabilities in SLA contexts.

Future Research Although quantifying security capabilities is difficult, the formulation and classification of security capabilities according to perceived risks are still open problems in the research area where existing solutions do not achieve adequate results. So far, there has been little, or no discussion of the security capabilities can be quantified and addressed in SLA contexts according to a defined risk tolerance level. The fact that the formulation and classification of security capabilities according to threats are essential to assess what is being claimed and achieved by service providers [24]. In so doing, a customer can understand security capabilities offered and guaranteed by the service provider.

Overall, there is a pressing need to develop discrete levels of security precautions, which can be used to negotiate the best possible formulation of security-related SLAs between customers and service providers. With this in mind, this paper is a logical step in the research into foundations for developing a trustworthy SLA capability framework that represents the interplay of risks, security requirements, and security capabilities according to data classification in SLA contexts.

4.2 Specifying security capabilities in SLA contexts

Open Problem The main challenge faced by customers and service providers is the lack of trust established and retained in SLA contexts concerning specific security capabilities offered and guaranteed by the service providers.

Many certifications have been proposed and become important in a cloud computing and outsourcing environment. However, such certification schemes are largely unsuitable in the context of service provisioning and do not ensure better security [26]. To achieve the application of SLAs as trust-enhancing instruments, it is necessary to incorporate security capabilities into SLA contexts to help ensure an adequate level of trust between the customer and service provider.

Existing Solution According to Jaatun et al. [2], security-related SLAs are necessary for Internet services to help ensure that customers and service providers

have a shared understanding of security capabilities expressed in SLAs for which customers receive the required level of assurance. Furthermore, Guesmi and Clemente in [40] noted that the service providers should be able to describe what they can supply regarding security capabilities specified in SLAs according to security requirements (e.g. the level of confidentiality, integrity and availability a customer requires), which help the providers to convince the customers regarding their security capabilities.

Some previous research [39, 41, 42] have initiated to address the notion of security attributes specified in SLAs, particularly in cloud computing [43, 44]. Additionally, some well-established auditing and certification schemes for service provisioning (e.g. EuroCloud, StarAudit and CSA Certification) typically use a level-based approach to certify service providers to ensure a particular security level. The existence of such certification schemes are typically incorporated into contractual agreements, thus, indirectly constituting security-related SLAs. However, some contracts limit the service provider's liability for the impact of any security breach and incidents.

Future Research Although extensive research has been carried out on specifying security properties in SLA contexts, little or no study exists which adequately demonstrates well-established approaches for sufficiently security capabilities in SLA contexts. Moreover, while it is acknowledged that such existing research is important in the context of service provisioning, they do not provide a coherent approach to incorporate the interplay of risks, requirements and capabilities into SLA context according to data classification when handling sensitive government data or corporate data. Significantly, there has been little studies on the problem of incorporating security capabilities into SLAs when using external information system services provided by service providers. Of course, there is still active research conducted in the field to reach and guarantee a discrete level of assurance that can satisfy the real requirements of customers.

4.3 Evaluating security capabilities specified in SLA contexts

Problem A key issue is how to check compliance with such security capabilities incorporated into SLAs as trust-enhancing instruments. In the context of SLAs, compliance of security-related SLAs can be measured and tracked by using metrics. However, metrics for security-related SLAs are not well-established. The existing SLA metrics are typically defined and measured based on statistics and implemented with proper requirements and capabilities related customers and service providers. Hence, developing effective security metrics for SLAs has proven to be very challenging.

Many service providers typically offer SLAs for well-established metrics, such as response times, resolution times, availability, throughput, delay and jitters [1,2]. The concept of security-related SLAs has been researched for a while. However,

the security metrics for SLAs are not well established [8, 39]. Many researchers have been attempting to measure security to demonstrate compliance with security requirements. For example, it is of interest whether data confidentiality and integrity are preserved and whether services will remain available for unauthorised users [8].

In fact, measuring security is difficult because security is not an event or an object, but it is a process [7]. However, such reasons do not imply that measuring security is impossible, as such measurement is essential to enhancing security measures; according to Lord Kelvin[3] '*If you can not measure it, you can not improve it*'. Many researchers suggest that effective security metrics implement quantitative scales (e.g. numbers) rather than qualitative scales (e.g. high-low-medium ratings) [45].

However, Mateski et al. [45] argue that most organisations continue to implement qualitative scales for measuring 'intangible' factors, such as the characteristics of a threat. Thus, qualitative scales, such as discrete levels of assurance, are practical ways of classifying security requirements and capabilities according to perceived threats for data classification. In this context, assurance levels of security precautions play an important role in support of defining and enforcing trustworthy SLA capabilities.

Existing Solution Takahashi et al. [46] introduced security-related SLAs and defined it as the security level of a service agreed between a customer and a service provider. In this case, the formulation of security-related SLAs is built through matching and negotiating the security requirements and capabilities of both the customer and the service provider. Furthermore, Lee et al. [47] developed ontologies for security-related SLAs to understand the security agreements of providers, to negotiate desired security levels, and to audit the compliance of providers concerning such regulations. The authors pointed out that it is necessary to incorporate the exact usage conditions for security considerations in SLAs to guarantee the quality of protection against a range of threats.

However, a few amount of literature has been studied to address security considerations in outsourcing arrangements, particularly in cloud computing and service provisioning [43,44]. For example, SPECS is intended to provide security-as-a-service, by expressing the notion of security framework in SLA contexts [39]. Similarly, the MUSA framework is developed to support the security-intelligent lifecycle management of distributed multi-could applications [41]. In the same way, the SLA-Ready framework is proposed to support a reference model for supporting and developing cloud SLAs [42].

Several attempts have been made to propose monitoring and compliance mechanisms in outsourcing-based services, particularly in cloud computing [39, 41, 42].

[3] Lord Kelvin, PLA, Vol. 1, Electrical Units of Measurement, 1883-05-03

However, such approaches failed to check its compliance with such security capabilities. Also, existing research recognises the critical role played by external service providers in any compliance mechanism and audits of security-related SLAs. It is clear that cloud audit is challenging than non-cloud systems, which have been seen as a potential barrier to procuring cloud-based services [29].

Another issue with audit and compliance is that such compliance with security standards, such ISO 27000, NIST and Cloud Security Alliance [32] is more likely to ensure compliance with a particular security standard, rather than achieve a significant level of confidentiality, integrity and availability of data a customer requires [23, 26, 32].

Future Research The problem is still open, and there is at present little knowledge on how compliance will be checked and monitored. Although many monitoring and compliance mechanisms have been proposed in outsourcing-based services, this topic has not been well researched in the context of service provisioning. Therefore, SLA-based on discrete levels of assurance can be evaluated based on the degree of compliance with the applicable laws, regulations, policies, standards, procedures, business needs and actual security requirements of customers.

5 Conclusion

In this paper, we have provided a review of the state of the art covering concepts, approaches and open problems to contextualise the evident growing interest in building trustworthy SLAs as trust-enhancing instruments. Considering all of the existing approaches, it seems that the literature still lacks insights into the question of incorporating security capabilities into SLAs according to a reasonable risk for each data classification. It is interesting to note that little attention has been paid to the underlying discrete levels of assurance according to defined risks for data classification in the existing approaches [39, 41, 42]. Thus, there is a pressing need to develop a trustworthy SLA capability framework, which can be used to negotiate the best possible formulation of SLA-based on discrete levels of assurance when procuring external information system services, such as cloud-based services.

The main contribution of this study is to point out existing research gaps in incorporating security capabilities into SLA contexts using discrete levels of assurance. Each level is distinct from another and has different threat models. Furthermore, this study can be used as a means to transfer knowledge to customers (e.g. government agencies) and service providers about another class of assurance techniques-based SLAs. This study is still active research on how to quantify, specify and evaluate security capabilities according to perceived risks for data classification.

6 Acknowledgements

This work was supported in part by the Indonesian Ministry of Communications and Information Technology under the Directorate of Information Security, and the Indonesia Endowment Fund for Education Scholarship (LPDP).

References

1. Bernsmed, K., Jaatun, M., Meland, P., Undheim, A.: Security SLAs for federated cloud services. In: Availability, Reliability and Security (ARES), 2011 Sixth International Conference on, IEEE (2011) 202–209
2. Jaatun, M., Bernsmed, K., Undheim, A.: Security slas–an idea whose time has come? In: International Conference on Availability, Reliability, and Security, Springer (2012) 123–130
3. Hamilton, H.: An examination of service level agreement attributes that influence cloud computing adoption. (2015)
4. Henning, R.: Security service level agreements: quantifiable security for the enterprise? In: Proceedings of the 1999 workshop on New security paradigms, ACM (1999) 54–60
5. Nugraha, Y.: Security assurance requirements engineering (stare) for trustworthy service level agreements. In: 2015 IEEE 23rd International Requirements Engineering Conference (RE). (Aug 2015) 398–399
6. Bianco, P., Lewis, G., Merson, P.: Service level agreements in service-oriented architecture environments. Technical report, DTIC Document (2008)
7. Schneier, B.: Secrets and lies: digital security in a networked world. John Wiley & Sons (2011)
8. Pfleeger, S., Cunningham, R.: Why measuring security is hard. IEEE Security & Privacy **8**(4) (2010) 46–54
9. Benenson, Z., Kühn, U., Lucks, S.: Cryptographic attack metrics. In: Dependability metrics. Springer (2008) 133–156
10. Shostack, A.: Threat modeling: Designing for security. John Wiley & Sons (2014)
11. of Standards, N.I., Technology: NIST sp 800-53: Security and privacy controls for federal information systems and organizations (2013)
12. Shirey, R.: Internet security glossary, version 2. (2007)
13. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing **1**(1) (Jan 2004) 11–33
14. Lyle, J.: Trustworthy services through attestation. PhD thesis, University of Oxford (2011)
15. Ardagna, C., Asal, R., Damiani, E., Vu, Q.: From security to assurance in the cloud: A survey. ACM Comput. Surv. **48**(1) (July 2015) 2:1–2:50
16. Inki, K., Ari, I., Szer, H.: A survey of software testing in the cloud. In: 2012 IEEE Sixth International Conference on Software Security and Reliability Companion. (June 2012) 18–23
17. Arkin, B., Stender, S., McGraw, G.: Software penetration testing. IEEE Security & Privacy **3**(1) (2005) 84–87
18. Lindskog, S.: Modeling and tuning security from a quality of service perspective. Chalmers University of Technology (2005)

19. Scarfone, K., Mell, P.: Guide to intrusion detection and prevention systems (idps). NIST special publication **800**(2007) (2007) 94
20. Spring, J.: Monitoring cloud computing by layer, part 1. IEEE Security Privacy **9**(2) (March 2011) 66–68
21. Spring, J.: Monitoring cloud computing by layer, part 2. IEEE Security Privacy **9**(3) (May 2011) 52–55
22. Damiani, E., Manã, A.: Toward ws-certificate. In: Proceedings of the 2009 ACM Workshop on Secure Web Services. SWS '09, New York, NY, USA, ACM (2009) 1–2
23. Böhme, R.: Security audits revisited. In: International Conference on Financial Cryptography and Data Security, Springer (2012) 129–147
24. Martin, A., Davies, J., Harris, S.: Towards a framework for security in escience. In: IEEE Sixth International Conference on e-Science, IEEE (2010) 230–237
25. Anisetti, M., Ardagna, C., Damiani, E., Saonara, F.: A test-based security certification scheme for web services. ACM Trans. Web **7**(2) (May 2013) 5:1–5:41
26. Anderson, R.: Security engineering. John Wiley & Sons (2008)
27. Pearson, S.: Toward accountability in the cloud. IEEE Internet Computing **15**(4) (July 2011) 64–69
28. Doelitzscher, F.: Security audit compliance for cloud computing. (2014)
29. Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A view of cloud computing. Commun. ACM **53**(4) (April 2010) 50–58
30. Duncan, R.A.K.and Whittington, M.: Enhancing cloud security and privacy: the power and the weakness of the audit trail. Cloud Computing 2016 (2016)
31. Chen, Z., Yoon, J.: It auditing to assure a secure cloud computing. In: 2010 6th World Congress on Services. (July 2010) 253–259
32. Duncan, B., Whittington, M.: Compliance with standards, assurance and audit: Does this equal security? In: Proceedings of the 7th International Conference on Security of Information and Networks. SIN '14, New York, NY, USA, ACM (2014) 77:77–77:84
33. Casola, V., De Benedictis, A., Rak, M.: On the adoption of security SLAs in the cloud. In: Accountability and Security in the Cloud. (2015) 45–62
34. Union, I.T.: Itu-t rec. x.805 on security architecture for systems providing end-to-end communications (October, 2003)
35. Chan, C.K., Chandrashekhar, U., Richman, S.H., Vasireddy, S.R.: The role of slas in reducing vulnerabilities and recovering from disasters. Bell Labs Technical Journal **9**(2) (2004) 189–203
36. Gelbstein, E.: Data integrityinformation security's poor relation. ISACA Journal **6** (2011) 20
37. Monahan, B., Yearworth, M.: Meaningful security SLAs. HP Labs (2008)
38. Luna, J., Taha, A., Trapero, R., Suri, N.: Quantitative reasoning about cloud security using service level agreements. IEEE Transactions on Cloud Computing **PP**(99) (2015) 1–1
39. Rak, M., Suri, N., Luna, J., Petcu, D., Casola, V., Villano, U.: Security as a service using an sla-based approach via specs. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science. Volume 2. (Dec 2013) 1–6
40. Guesmi, A., Clemente, P.: Access control and security properties requirements specification for clouds' seclas. In: Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on. Volume 1., IEEE (2013) 723–729

41. Rios, E., Iturbe, E., Orue-Echevarria, L., Rak, M., Casola, V.: Towards self-protective multi-cloud applications: Musa–a holistic framework to support the security-intelligent lifecycle management of multi-cloud applications. (2015)
42. Ready Consortium, S.: The SLA ready project website (2015)
43. Benedictis, A.D., Casola, V., Rak, M., Villano, U.: Cloud security: From per-provider to per-service security slas. In: 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS). (Sept 2016) 469–474
44. Casola, V., Castiglione, A., Choo, K.K.R., Esposito, C.: Healthcare-related data in the cloud: Challenges and opportunities. IEEE Cloud Computing **3**(6) (Nov 2016) 10–14
45. Mateski, M., Trevino, C., Veitch, C., Michalski, J., Harris, J., Maruoka, S., Frye, J.: Cyber threat metrics. Sandia National Laboratories (2012)
46. Takahashi, T., Kannisto, J., Harju, J., Heikkinen, S., Silverajan, B., Helenius, M., Matsuo, S.: Tailored security: Building nonrepudiable security service-level agreements. IEEE Vehicular Technology Magazine **8**(3) (Sept 2013) 54–62
47. Lee, C.Y., Kavi, K.M., Paul, R.A., Gomathisankaran, M.: Ontology of secure service level agreement. In: 2015 IEEE 16th International Symposium on High Assurance Systems Engineering. (Jan 2015) 166–172