Towards the Classification of Confidentiality Capabilities in Trustworthy Service Level Agreements

Yudhistira Nugraha*†, Andrew Martin*
*Department of Computer Science, University of Oxford, UK
†Directorate of Information Security, Ministry of ICT, Indonesia
yudhistira.nugraha, andrew.martin@cs.ox.ac.uk

***Abstract*—Many governments are increasingly reliant on external service providers to process, store or transmit sensitive data on behalf of the government. This study is motivated by the problem of preserving the confidentiality of sensitive government data, particularly following Edward Snowden's revelations of alleged pervasive surveillance; a problem posed by foreign intelligence services to the Indonesian government in 2013.**

In this paper, we discuss the idea of proposing *Trustworthy Service Level Agreements* (TSLA) as a means of incorporating security considerations (considering confidentiality) into a Service Level Agreement (SLA) between a service provider and the customer (e.g. government). In particular, we classify confidentiality requirements and capabilities according to a typical threat profile for government data classification, by describing five discrete levels of security precautions that can be negotiated between the government and service providers to ensure the confidentiality of sensitive data handled by the providers. It further provides an evaluation framework for assessing and clarifying security considerations in SLAs. The levels of assurance should serve as a foundation for expressing security considerations (including threats, requirements, and capabilities) in SLAs as well as for designing information system services regarding security. The contribution of this paper is in developing five distinctive levels of increasing assurance that can be applied to the formulation of security-related SLAs, as well as in discussing the discrete levels, using the context of a government cloud.

***Index Terms*—Trustworthy service level agreement, data security, data confidentiality, levels of assurance, government cloud**

I. Introduction

Today, many governments have become the most targeted organisations for a wide range of attacks, from script kiddies to well-funded state actors. According to data from BAE Systems, 85% of the attacks have targeted high-profile organisations, such as government ministries (55%), embassies (15%), and public organisations (12%).[1] It is not surprising, as government agencies (GAs) generate, collect and store far more sensitive data than the private sectors and often keep them with more vulnerable systems. For example, several misconfigured servers run by GAs could allow external attackers to access internal government systems [27]. It is also becoming apparent that the greatest threats to organisational security stem from insider threats [28], from those who routinely work with GAs (including employees, contractors, business partners and service providers).

In particular, many government organisations are increasingly reliant on information system services (e.g. cloud-based services and data centres) provided by external service providers (SPs). However, there is an absence of coherent approaches for preserving confidentiality of government data or services when using external information system services. This situation contrasts with well-established norms for systems, such as the Common Criteria (CC), which is often used as the basis for a government-driven certification scheme and security evaluation for information technology products and systems [3]. However, the security evaluation process is known to be slow-moving, which is problematic and unlikely to be appropriate in the context of service provision.

Furthermore, our empirical investigation[2] of 'real-world' SLAs in terms of security guarantees found that the major SPs in Indonesia, which provide information system services (e.g. cloud-based services) to the Indonesian GAs place a significant importance on availability. We also observed that most of the SPs find difficulties in addressing other security requirements (e.g. data confidentiality) in SLAs. Thus, this paper begins to classify confidentiality requirements and capabilities according to a typical threat profile for data classification, by defining levels of increasing assurance that are intended to be applied in the formulation of security-related SLAs, using the *Trustworthy Service Level Agreement* (TSLA) Framework [1].

We adopted an approach from the *NIST Electronic Authentication Guideline SP800-63* [4] as a key inspiration to the formulation and classification of security requirements and capabilities according to a typical threat profile for government data classification into five levels of increasing assurance from one level to the next following, in which skipping a level is not permitted. For instance, Level 1 is the lowest assurance level (least resistant to threats), and Level 5 is the highest (most resistant to threats). As *trust* is often determined in relation to specific security capabilities provided by external SPs [13], the defined levels for data confidentiality can be viewed as a set of discrete criteria that describe the characteristics of effective confidentiality capabilities implemented by technical, physical and human elements. Additionally, each level has a set of minimum technical requirements that must be satisfied in

[1]Data was gathered from the slides presented to the Indonesian government, see https://goo.gl/vumsm2, (Accessed February 2017).

[2]Investigations were carried out with five major SPs in Indonesia that provide Internet access, cloud-based services and data centre services to the Indonesian GAs, see https://goo.gl/5LhWun, (Accessed February 2017).

the areas of data security, which is the protection of data from unauthorised access or disclosure (*confidentiality*), unauthorised modification (*integrity*), and denial of authorised access (*availability*) [21]. Our main contribution is in developing a set of discrete levels for preserving the confidentiality of government data against unauthorised access or disclosure and discussing the defined assurance levels for data confidentiality, using the context of a government cloud.

The remainder of this paper is structured as follows. Section 2 discusses related work. Section 3 presents the methodology. Section 4 presents a set of discrete levels of increasing assurance, based on perceived threats to data classification. In Section 5, we discusses the defined levels for data confidentiality, using the context of the government cloud. Finally, we conclude the paper and outline our ongoing work.

II. Background and Related work

Many SPs have claimed that the information system services they deliver are '*secure*'. However, threat models must be considered when making such a claim; hence, this claim lacks one necessary component: *secure against what?* Also, in most cases, SPs will not include liability for security of any data that is processed, stored and transmitted through their information system services in their contracts. In other words, the contracts strictly limit the provider's liability for the impact of any security breach. In fact, relationships with external SPs are usually established through SLAs as trust-enhancing instruments, despite the fact that most SPs do not adequately express security considerations (particularly for threats, requirements, and capabilities) in their SLAs. Thus, there is an absence of a clear direction for incorporating security considerations in SLAs between GAs and SPs.

In this section, we review the related work in the formulation of security-related SLAs. An SLA is a binding agreement between a service provider and a customer that is widely used in a variety of information system services (e.g. cloud-based services) to claim the obligation of the SPs [5] to deliver service capabilities (e.g. security capabilities) according to service requirements (e.g. security requirements). However, little attention has been paid to expressing security requirements adequately in SLAs, particularly with regards to data confidentiality [5] [6] [25]. The concept of a security SLA was first proposed by Henning [7], who found that it was not easy to measure and quantify security. Similarly, Bernsmed et al. [5] asserted that existing security properties (i.e. confidentiality, integrity, availability) should be incorporated into an SLA. The authors pointed out that the absence of security considerations in the SLAs makes it impractical for the SPs to offer trustworthy services to their customers. However, previous work in [5] [6] [25] reported that existing SLAs are limited to defining guarantees in terms of service availability and performance. Of course, the lack of assurance of confidentiality and integrity of handled sensitive government data is a major drawback. For instance, Guesmi and Clemente [9] pointed out that existing cloud SPs do not express service provisions in terms of data protection and data security in their SLAs.

We acknowledge that several projects have been initiated to address security considerations in outsourcing arrangements, particularly in cloud computing, such as the *Secure Provisioning of Cloud Services based on SLA Management* (SPECS),[3] the Confidential and Compliant Clouds (COCO Cloud),[4] SLA-Ready,[5] and SLALOM.[6] In particular, our study is related to Takahashi et al. [10], who developed a security SLA that is built through matching and negotiating the security requirements and capabilities of both the customer and the SP. Another is SPECS that mentioned before [11]. The project was aimed at developing and implementing a framework to provide Security-as-a-Service, using the notion of security parameters specified in the SLAs.

Questions have been raised about the lack of assurance and techniques to quantify security [12], as well as how to classify confidentiality considerations according to a typical threat profile for data classification expressed in SLAs. Although measuring security is difficult, the formulation and classification of security requirements and capabilities according to threats is essential to avoid what is being claimed and achieved [3]. By doing this, GAs can understand the service capabilities regarding security that are provided by SPs. So far, there has been no discussion of the formulation and classification of confidentiality considerations that might be addressed in SLAs. Thus, 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 GAs and SPs.

III. Systematisation Methodology

This paper attempts to formulate and classify confidentiality considerations according to typical perceived threats for government data classification. First, we introduce a conceptual TSLA framework as an approach to address the interplay of threats, security requirements and security capabilities according to data classification in SLAs, as shown in Figure. 1.

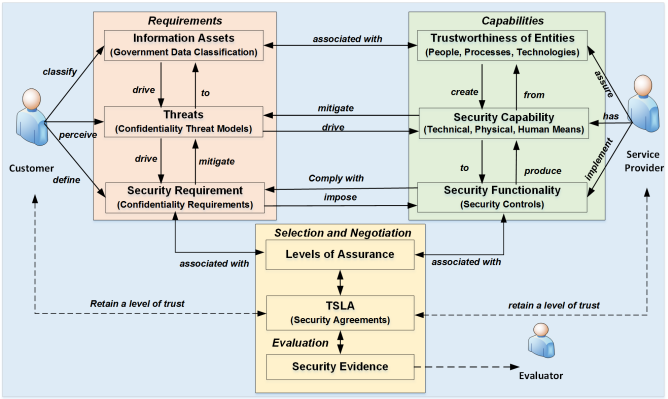

Fig. 1: Conceptual TSLA Framework [1]

[3] www.specs-project.eu, (Accessed February 2017).
[4] www.coco-cloud.eu, (Accessed February 2017).
[5] www.sla-ready.eu/, (Accessed February 2017).
[6] www.slalom-project.eu, (Accessed February 2017).

To classify confidentiality requirements and capabilities according to a typical threat profile for government data classification, we adopted an approach from the *NIST Electronic Authentication Guideline SP800-63* [4] by describing discrete levels of assurance, based on particular threat profiles. We then extracted technical requirements and capabilities from the literature and publicly available solutions [3] [15] [16] [17] [18] [21] [20], focusing on the formulation and classification of confidentiality considerations (including threats, requirements, and capabilities) according to data classification.

The discrete levels of security precautions play an important role in supporting the definition and enforcement security-related SLAs. Many authors suggest that good metrics implement quantitative scales (e.g. numbers) rather than qualitative scale (e.g. high-low-medium ratings) [24]. However, Mateski et al. [24] 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 confidentiality requirements and capabilities according to threats. We will now explain our precise methodology.

A. Scope of the study

This paper focuses on the problem of preserving government data security, especially when `GAs` are using external information system services. The growing use of external `SPs` to operate information systems across government data and services on behalf of the government present challenges, especially in the area of data security. Relationships with external entities are usually established through SLAs as trust-enhancing instruments, which can be done or associated with various interacting entities (i.e. customers, end-users, provider, suppliers, integrator, standards body and accreditation body). Thus, we introduce and discuss a five-level classification of security precautions for data confidentiality that can be incorporated into an SLA between the government and provider.

B. Threat Model

We need to consider threats when expressing security considerations in SLAs. Our potential adversaries include active or passive adversaries, adversaries from an external or internal entity to the system, adversaries from a single entity or a well-funded nation-state. Our threat model, which is adopted from [14] [22] [23], aims to obtain sensitive information from data that is processed, stored, or transmitted, as follows:

1) `Interception` allows an adversary to intercept communications in an attempt to read sensitive government data, because there is no cryptography tool used.
2) `Observe(Channel)` allows an adversary to collect credentials directly from communications in an attempt to read sensitive government data.
3) `Brute-force` allows an adversary to check all possible keys to access or read sensitive government data.
4) `Sniffing` allows an adversary to monitor network traffic in an attempt to capture sensitive data.
5) `Decrypt` allows an adversary to decrypt a ciphertext in an attempt to read sensitive government data because it is encrypted with non-standard cryptographic tools.
6) `Transmit(Data)` allows an adversary to exfiltrate sensitive government data or information deliberately or unwittingly from a collaborator (e.g. a service provider).
7) `Transmit(Key)` allows an adversary to exfiltrate cryptographic keys from a collaborator (e.g. a service provider) deliberately or unwittingly.
8) `Inject` allows an adversary to manipulate and inject data in transit onto the target network.
9) `Install` allows an adversary to install a malicious program on the endpoint, such as a website or email, in an attempt to obtain sensitive data or information.
10) `Extract(File)` allows an adversary to obtain data or sensitive information from logs, temporary files, or error messages.

We consider that the adversary models presented in this paper provides general attacker capabilities, which can be performed by script kiddies, hackers, insiders and advanced persistent threat (APT) or state-sponsored attacks. These threat models are not necessarily exclusive. However, the threat models can be applied to an area preserving the confidentiality of government data against unauthorised access or disclosure. Note that the defined levels for data confidentiality protect against increasing sophistication of cyber-attacks, but the levels of assurance cannot truly 'prevent' particular threats as listed above. Nevertheless, the use of levels of assurance taken by `SPs` makes those threat models less feasible in practice.

C. Security Objective

Trustworthiness of information system services is composed of two fundamental components, namely *security functionality* and *security assurance* [13]. We recognise that the TSLA framework [1] is intended to express the degree to which the system can be expected to preserve, with some degree of assurance, *confidentiality*, *integrity* and *availability* of data processed, stored, or transmitted by a information system service across a range of threats [13]. However, this paper will examine assurance of data confidentiality as a basic security requirement for protecting sensitive government data. Other security requirements, such as data integrity and data availability, are not included in this paper.

D. Classifications of Confidentiality

We formulate and classify minimum technical requirements and capabilities for preserving the confidentiality of government data against unauthorised access or disclosure by describing a five-level classification of security precautions that can be used by `GAs` and `SPs` to negotiate the formulation of security-related SLAs. Level 1 is the lowest (least resistant to threats) and Level 5 is the highest (most resistant to threats), which is perhaps an 'unreachable level' for a period of time.

We adopted the elements of confidentiality from the Information Assurance Technical Framework [21] and expanded them to (1) cryptographic selection and key management, (2) physical security, (3) isolation, and (4) metadata protection.

Each level is composed of four key elements of confidentiality. These five levels of increasing assurance allow for cost-effective solutions that are appropriate for different degrees of data classifications and different information system services. The SPs that provide such services to GAs should ensure whether their security capabilities provide an acceptable level of assurance, based on the government's security requirements.

IV. Levels of Assurance in Trustworthy SLA

In this section, we describe five discrete levels of security precautions that are intended to be applied in the formulation of security-related SLA, as well as involved in the design of information system services regarding security, as follows:

A. *Level 1*

This level provides the lowest level of confidentiality protection measures, which is intended for information system services handling public data transmitted across untrusted channels and stored in public cloud services.

There is no encryption requirement at this level to protect the transmission of data (over the network), or data at rest (in file systems, databases, and servers), or data in use (in memory, and operating system).

At this level, data is allowed to be managed in remote services and stored in a public cloud. Data or network isolation is not required to prevent an adversary from obtaining public data or information. Furthermore, there is no security requirement at this level to protect metadata of communications.

B. *Level 2*

This level is intended for information system services handling internal data or information that is commonly shared within organisations and is not intended for public distribution. Level 2 provides encryption for protecting data in transit and a wide range of available access control mechanisms are required for protecting remote connections. At level 2, a service provider is allowed to generate keys for access. Furthermore, basic physical security is required to protect unauthorised attempts at physical access.

Data and network isolation (e.g. secure routing protocol) is required to prevent data from reaching unclassified networks [21]. This level also provides data padding to prevent an adversary from knowing metadata of communications. Furthermore, obfuscation of identifying data is required to prevent accidental data disclosure [3]. Additionally, metadata protection mechanisms are required to hide the actual characteristics of data, such as data frequency, and message size [21].

C. *Level 3*

This level is intended for information system services handling sensitive data with restricted uses, such as personal health information. Level 3 enables the use of standard cryptographic functions and libraries, with standardised key sizes [15]. This level is intended to provide encryption for secrecy, timestamped signatures for authenticity, and strong authentication and authorisation for protecting data at rest. At this level, data is stored on the local server, or in private clouds. Keys for access are negotiated between an end-user and a SP.

Furthermore, a physical security mechanism is required to detect and respond to unauthorised attempts at physical access [16]. Also, this level enables the employment of the sandboxed execution model [18] to offer protection against rogue processes that could interfere with user processes and data. Level 3 allows the application of a stateful packet filter to examine the content of the packet [17]. Moreover, such isolation mechanisms are required to prevent unauthorised disclosure, such as process-level isolation, OS-level virtualization, hypervisors, network segmentation and trust boundaries.

Level 3 requires that all metadata are not identifiable within a set of subjects. It also requires reversible mapping techniques of identifying data, but the mapping must be keyed in which the key is controlled tightly [3].

D. *Level 4*

This level is intended for information system services handling very sensitive information (e.g. government secrets). Level 4 provides strong cryptography with associated key management processes, such as securing generation, storage, distribution and destruction of keys. This level further enables the use of cryptography with hardware-backed key store implementation and hardware key random number generation for encryption data in use [3].

This level requires that data is managed locally and keys are encrypted by end-users, and enables the use of cryptographic tools to protect data in transit, data at rest and data in use.

Level 4 allows the use trusted computing technologies to provide a strong isolation mechanism at hardware and a guarantee of which virtual machine is in use [19]. It further requires the isolation for the endpoint and allows the implementation of a set of firewall protections to manage incoming packets from an unclassified network.

Furthermore, this level aims to enhance the physical security mechanisms of Level 3 by adding robust mechanisms that detect and respond to all unauthorised attempts at physical access [16]. Also, zeroization is enabled to prevent data disclosure when the system is attached [16]. The use of anti-tamper devices (e.g. tamper detection and tamper response) is required. In addition, this level provides an 'air-gap' approach [20], which is physically isolated from the Internet.

Regarding metadata protection, Level 4 provides approaches to substitute the identifying data with genuinely random keys, and to perform mapping from the identifying data to the new keys, which is held by a trusted entity as a lookup table [3].

E. *Level 5*

This level is intended for information system services handling the most sensitive data (e.g. government top-secrets). Level 5 is designed to provide the highest level of security precautions defined in this paper, which is considered to be unreachable for a period of time. It enables the use of 'hard' cryptographic tools for all sensitive data and communications transmitted among parties using specialist cipher suites, for very long term (exceeding 30 years) protection [3].

TABLE I: Summary of Assurance Levels for Data Confidentiality

Consideration	Level 1	Level 2	Level 3	Level 4	Level 5
Data Classification	Services aim for handling *public data* transmitted and stored in *public cloud services*.	Services aim for handling *internal data* that is commonly shared within the organisations.	Services aim for handling *sensitive data with restricted uses* (e.g. personal health information).	Services aim for handling *very sensitive data* (e.g. government secret).	Services aim for handling *the most sensitive data* (e.g. government top secrets).
Trustworthiness of Service Providers	SPs are required to implement basic security capabilities against common cyber threats (e.g. virus)	SPs are required to implement the same security capabilities, along with external evaluation.	SPs are required to hold 'vendor certification' to process, store or transmit sensitive data.	SPs are required to prove such level of trust for handling government secrets. Trustworthiness of entities are required (e.g. SPs)	Only Trustworthiness of entities (e.g. people, process, technology) are required for handling government top secrets.
Perceived Threats	This level of security aims to defend against unauthorised access or disclosure by unsophisticated attackers (script kiddies)	This level of security aims to mitigate unauthorised access by attackers with limited capabilities and resources, including unintentional insider threats.	This level of security anticipates to defend against unauthorised access by attackers with moderate capabilities and resources (e.g. corporate insiders)	This level of security aims to mitigate unauthorised access by attackers with high capabilities and resources (e.g. state sponsored hackers/insiders)	This level of security aims to mitigate unauthorised access by attackers with abundant capabilities and resources (e.g. state sponsored hackers/insiders)
Crypto selection and key management	No cryptographic tools to protect the transmission of data, or data at rest, or data in use.	Access control is required for protecting remote connections in which keys is generated by providers.	Standard cryptography is required for the secrecy of data at rest, authenticity and authentication.	Strong cryptography is required for encryption data in use, using a hardware-backed keystore.	Advanced cryptography is required for the protection of all sensitive data transmitted among parties
Physical Security	Physical security mechanisms are limited or nonexistent.	Basic physical security is required to protect attempts at physical access.	Threat detection and response to unauthorised attempts at physical access.	Threat detection and response to all attempts at physical access.	Robust Threat detection and response to all attempts at physical access.
Isolation	Data or network isolation is not required to prevent an attacker from obtaining public data	Data and network isolation is required to prevent internal data from reaching unclassified networks	Make use of isolation techniques, such as sandbox security, virtualization and trust boundaries.	In addition to firewalls, trusted computing is required to provide the isolation for the endpoint.	Provide an entirely isolated network ('air-gap'), which is physically isolated from the Internet.
Metadata Protection	No require specific technical requirements to protect metadata.	Obfuscation of identifying data is required to prevent accidental data disclosure.	Reversible keyed mapping techniques required to protect metadata.	Identifying data with genuinely random keys is required to protect metadata.	Genuinely irreversible mapping of identifying data is required.

Level 1 is the lowest (least resistant to threats) and Level 5 is the most stringent (most resistant to threats). Security requirements and capabilities are primarily cumulative by level, Security requirements include the level of security protection one party requires, while the security capabilities specify the countermeasures that will be provided

Data is managed locally and physically isolated from the Internet. Only trustworthy entities (e.g. people, processes and technologies) are required for handling government secrets.

Level 5 provides the highest practical methods of data hiding techniques, using genuinely irreversible mapping of identifying data. This level necessitates a set of requirements for complete anonymity, unlinkability and unobservability.

We summarise the defined levels for data confidentiality in Table I. Note that the discrete levels are not necessarily exclusive. The levels can be adjusted to cope with increasing sophistication of cyber-attacks.

V. Analysis and Discussion

In this section, we discuss the defined levels for data confidentiality, using the context of government cloud environment. Some governments are currently redefining their businesses to deliver improved citizen services using government cloud computing, such as the AWS GovCloud (US) and the UK Government Cloud (G-Cloud). Of course, governments would require scalable platforms, such as cloud infrastructure services for their large amount of data and computation. However, cloud SPs might not meet some security requirements, as they suffer from some challenges and security threats. The fact that cloud-based services are increasingly used in public sectors. Such services are comprised of tens of thousands of servers and perform the processing for many sensitive government data (e.g. citizen's data). For instance, the data centre has become their most critical assets. Thus, most governments require data centres which are located locally in order to have direct access to government data or services. From a security perspective, at least two data centres are in different geographical locations under the same jurisdiction. It is expected that the implementation of the defined levels for data confidentiality may help to protect against unauthorised parties access to raw data through cloud SPs. In this section, we discuss four key elements of confidentiality considerations that may be addressed in the formulation of security-related SLAs, namely cryptographic technologies and key management, physical security and location, isolation, and metadata protection.

A. *Cryptographic Selection and Key Management*

Increasing amounts of sensitive government data require cryptographic tools for ensuring data confidentiality or data integrity. In fact, the use of cryptographic technologies appears to be of limited interest as it is reliant on standard solutions. Thus, GAs should understand which sensitive information needs to be protected so as to decide whether the cryptographic technologies will be deployed (in-house or out-sourced) at the application level, file system level, network level, or device level. Also, GAs would need to ensure that the cryptographic tools are properly configured, as the accurate implementations of cryptographic technologies are extremely critical to their effectiveness against unauthorised disclosure of sensitive government data. Thus, it is necessary to understand whether data is managed locally, or on the server, or in remote services when one defines security attributes in contracts or SLAs.

Regarding key management, when GAs decide to use cloud-based services from external SPs, it is important to understand whether data is encrypted by the providers or by end-users or keys for access negotiated between a user and a service provider. It is clearly evident that the absence of attributes for cryptographic key management in the formulation of security-related SLAs makes it impossible for cloud SPs to meet the increasing demand for data protection and data security as well as to offer trustworthy services to their customers.

Of course, key management is critical and challenging in a cloud environment. Cloud-based services can provide a secure connection using TLS or SSH. Like traditional data centres, cloud data centres also have the ability to store application data in an encrypted form. If a strong government expectation of data confidentiality is required, cloud SPs can provide end-to-end encryption. In this case, SPs are required to provide evidence to demonstrate that they do not have access to the encryption keys or they would not be able to hold those keys over unauthorised entities. Thus, the need for third-party vendor protection requirements would be required to be built into contracts or SLAs, as most services or applications store data in cloud data centres. One also needs to look at the entire data supply chain when data is stored in multiple locations and in what country the data is stored. Overall, in the context of a government cloud, the specified levels of assurance will be appropriate at **Level 3** protection.

B. Physical Security and Location

It is necessary to include physical security attributes in the formulation of security-related SLAs. In practice, many SPs claim that they have 24 x 7 x 365 services on-site physical security, which can be checked through security audits to help build the trust and confidence between a customer and a service provider [25]. Physical security controls can include security guards, physical access control devices (e.g. locks), physical intrusion alarms, and surveillance equipment [13].

Furthermore, the physical location of cloud data centres has been highlighted as a major concern since the Edward Snowden revelations in 2013. Although data security does not only depend on its geographical location, many governments are not allowed to store citizen's data under other jurisdictions. For instance, according to Article 17 of the Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012, mentioning that Electronic System Operators have obligations to locate data centres within the borders of national jurisdictions, especially for the purpose of law enforcement and protecting citizen's data against force majeure (e.g. earthquakes, floods and wars) [26]. In particular, localised data centres may help to get access, as well as to apply digital forensics to cloud-based services for law enforcement. Thus, it is important to include the physical location of data centres in the formulation of security-related SLAs when using cloud-based services provided by external SPs, especially for handling or storing sensitive government data. In the context of a government cloud in general, this corresponds to **Level 3** protection.

C. Isolation

If a government's network infrastructure has been leased from external SPs, government organisations would need to ensure that the network segmentation and segregation meets the minimum security requirements, which can be specified in SLAs. To defend against the most serious threats, some potential SLA attributes for isolation mechanisms, such as whitelisting, Virtual LANs, traffic flow filters for web and email, and 'air-gap', should be specified in the formulation of security-related SLAs. Although a true 'air-gap' seems to be used in an environment that sensitive government data is not connected to a network, it is of course unrealistic to represent the approach when using cloud-based services.

It is acknowledged that cloud-based services remove the concept of the 'air-gap' approach. However, data and network isolation needs to be considered carefully to achieve as much of a security requirement as possible in SLAs. For example, most virtual machines run on the same physical hardware that leads to sharing the underlying infrastructure with untrusted customers. However, access control and security policies are not sufficient to assure isolation in cloud data centre services.

Isolated networks at Level 3 may provide an acceptable level of protection against unauthorised data disclosure from trusted to untrusted cloud-based services. Overall, **Level 3** protection may be suitable for this case. It is expected that this level of security precautions can mitigate the threats at least to increase the efforts required to access sensitive government data.

D. Metadata Protection

Security features to protect metadata are limited. However, security approaches to address metadata protection need to be specified in the formulation of security-related SLAs. One of the common methods to protect metadata, particularly for protecting the actual communications or communication headers is to make use of a mixed network, onion routing, proxies, and virtual private networks (VPN) [22] [29].

Protecting metadata includes to increase the efforts required by adversaries (e.g. SPs or foreign intelligence services) to collect government's metadata and turn the metadata collected into useful information. Thus, the most sensitive information would set confidentiality requirements for completely anonymous data when data is shared with other entities.

Data flow protection is required to provide confidentiality. It is possible that cloud-based services are well suited for anonymous traffic (e.g. Tor Cloud). Anonymity can be achieved when combined with anonymous cloud with Tor. However, most SPs must comply with lawful interception. Thus, metadata protection, especially for data anonymity can provide only **Level 3** protection. Level 3 protection will also be appropriate to protect against any reasonably anticipated uses or disclosures of such sensitive data that are not permitted.

It seems that a cloud SP could provide security capabilities required at Level 2 or Level 3. We acknowledge that it is becoming increasingly difficult to establish level of trust between GAs and SPs when using cloud-based services. In other words, Level 4 and Level 5 seem to be impossible to

fully achieve for a cloud service provider. However, a cloud SP could aim for Level 4 or Level 5, especially for some security capabilities (e.g. physical security and location, cryptographic selection and key management).

Overall, the discrete levels of security precautions are designed to protect against increasing sophistication of cyber-attacks. We also acknowledge that it is difficult to determine whether the defined levels for data confidentiality could protect against unauthorised disclosure of sensitive government data, as described above in Section 3. However, the levels of assurance would help GAs to list the threat resistance requirements per assurance level, as well as to select appropriate requirements and capabilities for data confidentiality that meet each of the five levels of assurance. Note that the elements of security considerations described in this paper are needed for further elaboration.

VI. Conclusion and Ongoing Work

Thus far, we have presented five discrete levels of security precautions, based on perceived threats for government data classification and discussed the implementation of the assurance levels, using the context of a government cloud. The distinctive levels of increasing assurance are intended to be applied in the formulation of security-related SLA within a framework developed in this research, called a *Trustworthy Service Level Agreement* Framework. The intended discrete assurance levels can also be used in the design of service capabilities regarding security. We believe that the formulation and classification of discrete levels is essential to avoid ambiguity regarding what is being stated and performed by service providers. Also, this would help GAs to select an appropriate level for preserving the confidentiality of sensitive data. However, there are a few challenges to the use of the defined levels for data confidentiality in the formulation of security-related SLAs. For example, the provider's liability is strictly limited, with the particular level of confidentiality capabilities expressed in SLAs. Also, the total costs associated with security considerations expressed in SLAs become a more difficult calculation since it compasses liability and compensation. These challenges sketch many avenues for future work.

Furthermore, the discrete levels of security protection are clearly in need of further development and field validation. We plan to elaborate on the levels of security precautions, using the results of a grounded Delphi study, by asking government experts to classify confidentiality considerations according to data classifications, and by conducting a grounded theory analysis of the Delphi study data to reveal a theory on how to classify confidentiality considerations according to data classifications, using Indonesia as a case study. In light of the significant challenges with validating such a set of discrete levels of assurance in a representative situation, our study will conduct expert reviews of the assurance levels, with a wide variety of stakeholders, such as government employees, external service providers, and SLA contract experts (lawyers). In addition, we aim to provide examples of how the defined discrete levels for data confidentiality can be applied in real-world cases of government cloud computing, such as the AWS GovCloud (US) and the UK Government Cloud (G-Cloud). It will also be interesting to discuss how the defined levels of assurance are compliant with the national legislation.

VII. Acknowledgments

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] Nugraha, Y, Martin, A,"Trustworthy Service Level Agreements: An Approach for Protecting Government Data Secrecy", In 10th Layered Assurance Workshop, Works in Progress, ACSAC-32, 2016.
[2] Nugraha, Y, Brown, I, Sastrosubroto, AS, "An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements", IEEE Transactions on Emerging Topics in Computing 4, no. 1, pp.47-59, 2016.
[3] Martin et al., "Towards a framework for security in e-Science", In Sixth International Conference on e-Science, pp.230-237, IEEE, 2010.
[4] Burr et al., "Electronic Authentication Guideline", NIST, 2015.
[5] Bernsmed et al., "Security SLAs for federated cloud services", In Availability, Reliability and Security, pp.202-209, IEEE, 2011.
[6] Jaatun, et al., "Security SLA - An idea whose time has come?", In Multidisciplinary Research and Practice for Information Systems, pp. 123-130, Springer Berlin Heidelberg, 2012.
[7] Henning, RR, "Security service level agreements: quantifiable security for the enterprise?", Workshop on New security paradigms, ACM, 1999.
[8] Monahan, B, Yearworth, M, "Meaningful security SLAs", TR, 2008.
[9] Guesmi at al.,"Access control and security properties requirements specification for clouds' SECLAS", CloudCom, pp.723-729, IEEE, 2013.
[10] Takahashi, et al., "Tailored security: Building nonrepudiable security service-level agreements", IEEE Vehicular Technology, pp.54-62, 2013.
[11] Rak et al., "Security as a service using an SLA-based approach via SPECS", In Cloud Computing Technology and Science, IEEE, 2013.
[12] Luna et al.,"Quantitative Reasoning About Cloud Security Using Service Level Agreements", In Transactions on Cloud Computing, IEEE, 2015.
[13] NIST 800-53. Security and privacy controls for federal information systems and organizations, 2013
[14] Do, Q., Martini, B., Choo, K. K. R.,"Exfiltrating data from Android devices", Computers Security, 2015.
[15] Barker, E, "NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management Part 1: General", NIST, 2016
[16] FIPS PUB 140-2, "Security requirements for cryptographic modules", Information Technology Laboratory, NIST, 2001.
[17] Van Rooij, G,"Real stateful TCP packet filtering in ...", USENIX, 2001.
[18] Backes et al., "Boxify: Full-fledged app sandboxing for stock Android" In 24th USENIX Security Symposium, pp. 691-706, 2015.
[19] Cooper et al.,"Towards a secure, tamper-proof grid platform", In International Symposium on Cluster Computing and the Grid, IEEE, 2006.
[20] Horowitz, M,"Defending a network from the NSA",Computer, 2016.
[21] U.S NSA, "Information assurance technical framework", TR, 2000.
[22] Shostack, A, "Threat modeling: Designing for security", Wiley, 2014.
[23] Barnes et al.,"Confidentiality in the face of pervasive surveillance: A threat model and problem statement", IETF, 2015.
[24] Mateski et al.,"Cyber threat metrics", Sandia National Lab, 2012.
[25] Hamilton, HG, "An Examination of Service Level Agreement Attributes that Influence Cloud Computing Adoption", 2015.
[26] Nugraha et al., "Towards data sovereignty in cyberspace", In International Conference on ICT, IEEE, 2015.
[27] Whittaker, Z, "Security flaws in Pentagon systems 'easily' exploited by hackers", ZDNet, Online at http://www.zdnet.com/article/pentagon-system-flaws-likely-under-attack-by-foreign-hackers/, 2017
[28] Lord, N, "Insiders vs. Outsiders: What's the Greater Cybersecurity Threat?". Digital Guardian, Online at https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic, 2017, Accessed 2 February 2017
[29] Privacy International, "What is metadata?", Online at https://www.privacyinternational.org/node/53, Accessed 2 February 2017