CHAPTER - V
AN EXTENDED CLOUD SECURITY MODEL FOR THE
PROVISIONING OF SLA BASED ON USER FEED BACK
SESSION

5.1 INTRODUCTION

In previous chapters, the proposed cloud security model with the inclusion
of trusted third party auditing and data displacement strategies have been
extensively discussed and implemented proposal is also shown with the proposed
architecture and algorithms. The result obtained through cloud simulator also
shows the efficiency of the proposed algorithm by comparing the results.

Service Level Agreements are always the key for the success of any sort of
cloud service. Various SLA principles and factors play a pre-dominant factor. This
chapter extends our cloud security model further provisioning of SLA where user
satisfaction has been designated as a primary goal of SLA. Various cloud service
SLA principles are studied and user feedback session based SLA mechanism is
presented and using –Cloudsim, certain user feedback sessions have been created
and tested for the fulfillment desired SLA.

5.2 CLOUD SERVICE LEVEL AGREEMENT

Cloud Service Level Agreements (Cloud SLAs) [28][29] form an important
component of the contractual relationship between a cloud service customer and a
cloud service provider of a cloud service. Given the global nature of the cloud,
SLAs usually span many jurisdictions, with often varying applicable legal
requirements, in particular with respect to the protection of the personal data
hosted in the cloud service. Furthermore different cloud services and deployment
models will require different approaches to SLAs, adding to the complexity of
SLAs. Finally, SLA terminology today often differs from one cloud service
provider to another, making it difficult for cloud service customers to compare
cloud services. For the avoidance of doubt, this document does not address
consumers as being cloud service customers.
Standardizing aspects of SLAs improves the clarity and increases the understanding of SLAs for cloud services in the market, in particular by highlighting and providing information on the concepts usually covered by SLAs.

In that context, under the second key action, the Cloud Computing Strategy calls for the development of standardization guidelines for cloud computing service level agreements for contracts between cloud service providers and cloud service customers (not being consumers). In February 2013 the European Commission, DG CONNECT set up the Cloud Select Industry Group – Subgroup on Service Level Agreement (C-SIG-SLA) to work on this aspects. The C-SIG SLA subgroup, an industry group facilitated by the European Commission DG Connect, has prepared this document to provide a set of SLA standardization guidelines for cloud service providers and professional cloud service customers, while ensuring the specific needs of the European cloud market and industry are taken into account.

5.2.1 Desirable Requirements of SLA

5.2.1.1 Availability

Availability is the property of being accessible and usable upon demand by an authorized entity. Availability is usually covered by certification at a general level. Availability is a key service level objective, since it describes whether the cloud service can actually be used, and it is typically necessary to specify numeric values for availability to make meaningful statements that are useful for cloud service customers.

The question of what "usable" means is a complex matter, which depends on the cloud service concerned. A service can be up and available, but perform so poorly that it is effectively unusable. Similarly, the service can be up, but respond with errors for valid requests. It can be valuable for the SLA to provide clear information on these aspects of service availability.
5.2.1.2 Response Time

Response time is the time interval between a cloud service customer initiated event (stimulus) and a cloud service provider initiated event in response to that stimulus. The response time SLOs can vary depending on the point at which the customer stimulus is measured. For example, the measurement may start from when the customer initiates the stimulus on their device, or it may start from the point where when the request from the customer arrives at the cloud service provider's endpoint – the difference being the network transit time, which may be outside the control of the cloud service provider. Similarly, the point at which the response is measured can vary.

5.2.1.3 Support

Support is an interface made available by the cloud service provider to handle issues and queries raised by the cloud service customer.

5.2.1.4 Reversibility and the Termination Process

The termination process takes place when a cloud service customer or a cloud service provider elect to terminate the agreement. The termination process includes a series of steps which enable the customer to retrieve their cloud service customer data within a stated period of time before the cloud service provider deletes the cloud service customer data from the provider's systems (including backup copies, which may be done possibly on a different schedule). The cloud service provider can potentially delete or aggregate any cloud service derived data (this is limited to derived data related to operations) that relates to the customer and their use of the cloud service, although such deletion may be limited in scope.

5.2.2 Security Service Level Objectives Overview

Specifying measurable security level objectives in SLAs is useful to improve both assurance and transparency. At the same time, it allows for establishing a common semantics in order to manage cloud security from two perspectives, namely (i) the security level being offered by a cloud service provider and, (ii) the security level requested by a cloud service customer.
The approach used in this section consists of analyzing security controls from well-known frameworks into one or more security SLOs, when appropriate. These SLOs can be either quantitative or qualitative. This section focuses on the definition of possible security SLOs. Eight categories are provided, each with one or more SLOs. The categories are representative of some important security requirements. However not all security requirement categories are reflected below, as relevant SLOs may not exist for each of them. For example resilience, business continuity and disaster recovery are important aspects of security, specific controls and measures are usually put in place by CSPs, but no SLO has been derived for these security aspects.

For each category, the SLOs are meant to provide more quantitative and qualitative information relevant to a specific control, in addition to what is usually assessed in the context of an audit for a certification. It should be noted that the list of SLOs is not meant to be considered as exhaustive and that the SLOs proposed are not meant to be considered as applicable in all individual cases. The applicability of a particular SLO can depend on the type of service offered (in terms of both of service functionally and service model) and pricing of it (free service, paid, premium). It is important to understand that some of the SLOs relevant to security also have relevance in the areas of Data Management, Performance and Data Privacy and those SLOs are found in those sections.

### 5.2.2.1 Security Incident management and reporting

An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. Information security incident management are the processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.
5.2.2.2 Logging and Monitoring

Logging is the recording of data related to the operation and use of a cloud service. Monitoring means determining the status of one or more parameters of a cloud service. Logging and monitoring are ordinarily the responsibility of the cloud service provider.

5.2.2.3 Auditing and security verification

Auditing is the systematic, independent and documented process for obtaining audit evidence about a cloud service and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. The audit evidence required and the audit criteria are usually determined by the audit scheme or certification scheme which is used to perform the audit. Certification is one of many ways to address audits.

5.2.2.4 Vulnerability

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat. Management of vulnerabilities means that information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

5.3 EXTENDED SECURITY MODEL FOR THE PROVISIONING OF SLA

5.3.1 Data Management Service Level Objectives Overview

As companies transition to cloud computing, the traditional methods of securing and managing data are challenged by cloud-based architectures. Elasticity, multi-tenancy, new physical and logical architectures, and abstracted controls require new data security strategies. Managing data and information in the era of cloud computing can affect all organizations. It begins with managing internal data and cloud migrations and extends to securing information in diffuse, cross-organization applications and services.
The data management SLOs presented in this section cope with important quantitative and qualitative indicators related with data life cycle management, and can be considered as complementary to existing and applicable security and data protection certifications offered by the cloud service provider.

Presented data management SLOs are subdivided in four (4) different top-level categories covering all aspects of the identified data life-cycle. Each category is subdivided in one of more SLOs that are applicable to that specific category. Not all SLOs may be relevant for each cloud service, in particular depending on the type of cloud service such as IaaS, PaaS or SaaS.

5.3.2 Data classification

5.3.2.1 Description of the context or of the requirement

Data classification is a description of the classes of data which are associated with the cloud service:

- cloud service customer data
- cloud service provider data
- cloud service derived data

Cloud service customer data is a class of data objects under the control of the cloud service customer. Cloud service customer data includes data input into the cloud service by the cloud service customer and the results of the cloud service customer's use of the cloud service, unless the master service agreement specifically defines a different scope.

5.3.2.2 Personal Data Protection Service Level Objectives Overview

This paragraph focuses on the definition of appropriate SLOs with reference to the cases where the cloud service provider acts as a data processor, on behalf of its customer (data controller), which typically applies to B2B services. Providers that act as data controllers or joint controllers (notably by processing personal data for their own purposes, outside of an explicit mandate from the
customer) may still make reference to this document, but they and their customers need to ensure compliance with legal obligations that may derive from their controller role.

Besides, this paragraph concentrates on data protection measures that are suitable for being translated into SLOs, i.e. into objectives that must be achieved by the provider. Other data protection measures and obligations can be better managed through other instruments, such as adherence to a code of conduct, certification against an approved standard and the relevant contract and/or service agreement and applicable law.

5.4 CODES OF CONDUCT, STANDARDS AND CERTIFICATION MECHANISMS

The cloud service customer, as data controller, must accept responsibility for abiding by the applicable data protection legislation. Notably, the cloud service customer has an obligation to assess the lawfulness of the processing of personal data in the cloud and to select a cloud service provider that facilitates compliance with the applicable legislation. In this regard, the cloud service provider should make available all the necessary information, also in adherence to the principle of transparency, as described hereinafter. Such information includes information that may assist in the assessment of the service, such as the data protection codes of conduct, standards or certification schemes that the service complies with.

5.4.1 Openness, transparency and notice

Only if the provider informs the customer about all relevant issues, the cloud service customer is capable of fulfilling its obligation as data controller to assess the lawfulness of the processing of personal data in the cloud. Moreover, the cloud service provider shall make available the information that enable the customer to provide the data subjects with an adequate notice about the processing of their personal data, as required by law. Notably, transparency in the cloud means it is necessary for the cloud service customer to be made aware of cloud service providers’ subcontractors contributing to the provision of the respective cloud service.
5.4.2 Accountability

In the field of data protection, accountability often takes a broad meaning and describes the ability of parties to demonstrate that they took appropriate steps to ensure that data protection principles have been implemented. In this context, IT accountability is particularly important in order to investigate personal data breaches; to this end, the cloud platform should provide reliable monitoring and logging mechanisms, as described in the relevant sections of these Guidelines.

Moreover, cloud service providers should provide documentary evidence of appropriate and effective measures that are designed to deliver the outcomes of the data protection principles (e.g. procedures designed to ensure the identification of all data processing operations, to respond to access requests, designation of data protection officers, etc.). In addition, cloud service customers, as data controllers, should ensure that they are prepared to demonstrate the setting up of the necessary measures to the competent supervisory authority, upon request.

5.4.3 Geographical location of cloud service customer data

Personal data processed in the cloud may be transferred, also by subcontracting, to third countries, whose legislation do not guarantee an adequate level of data protection. This also implies that personal data may be disclosed to foreign law enforcement agency, without a valid EU legal basis. To minimize these risks, the cloud service customer should verify that the provider guarantees lawfulness of cross-border data transfers, e.g. by framing such transfers with safe harbor arrangements, EC model clauses or binding corporate rules, as appropriate.

To this end, the cloud service customer shall be made aware of the location of data processed in the cloud, as required also by the above-mentioned principles of openness and transparency.
5.5 IMPROVED SERVICE LEVEL AGREEMENT REQUIREMENTS

The Internet and other advances in computing have spawned a global digital economy and the continuing evolution of cloud computing has added a new and rapidly growing dynamic. While cloud computing is increasing in maturity, it is still in its nascent stages and the related technologies, business models and polices will undoubtedly evolve over a number of years. There are a number of efforts underway to facilitate adoption of cloud computing by adding clarity to the agreements between cloud service customers and cloud service providers, thus making them more comparable and comprehensible. These efforts are valuable but at the same time it is important to not constrain the technical and business innovation of cloud computing. The following is a set of principles that can assist organizations, through the development of standards and guidelines for cloud SLAs and other governing documents. These principles are not intended to be limiting nor to even set model terms.

Essential hallmarks of cloud computing are flexibility and extensibility for which technology neutrality is a necessary foundation. Cloud services can be built using any number of technologies and a particular technology stack should not be assumed.

For example, many cloud services expose REST interfaces or APIs but they can also use technologies such as Web Services to receive data and interoperate with other services. In another example being technology neutral is important because cloud services commonly run on virtualized hardware platforms but virtualization should not be assumed. Continuous improvement to deliver increasing value is critical to the future of cloud computing and the freedom to innovate technically is key to that. Cloud services are built on open source software and proprietary software alike. There can also be a variety of hardware platforms underlying cloud services.

A particular business model for cloud services should not be assumed. Cloud services may be funded by any number of methods such as pay per use, long term contracts, advertising, public funds and others. Remedies for failure to achieve cloud service level objectives (SLOs) stated in the SLA can also take different forms such as refunds on charges, free services or other forms of compensation.
5.5.1 Unambiguous definitions

Keeping the definition of service level objectives well-defined and unambiguous is important to ensure the effective standardization of cloud SLAs and to enable clear communication between cloud service providers and cloud service customers. As technology develops and new terminology is developed it will also be important to ensure definitions are up-to-date and consistent with an evolving cloud services landscape.

5.5.2 Comparable Service Level Objectives

Service Level objectives (SLO) are often quantitative and have related measurements. For cloud service customers to make informed decisions when choosing cloud services, it is best if the service level objectives offered by each cloud service provider for similar services can be easily compared. Measurements should also be comparable since reduced comparability impedes adoption. However, from case to case reviewing less-quantitative or qualitative SLOs and comparing different services may provide extra insights for making such informed decision. To be comparable, service level objectives need not be determined by identical means but sufficient information about the SLO needs to be provided by cloud service providers. Standardized terminology, metrics and templates can be helpful in documenting how a particular SLO is determined. Service level objectives are often associated with metrics. A metric is a defined measurement method and measurement scale, which is used in relation to a quantitative service level objective.

Metrics are used to set the boundaries and margins of errors which apply to the behavior of the cloud service and any limitations. Metrics may be used at runtime for service monitoring, balancing, or remediation. Using a standard set of metrics or metric templates in the cloud SLA makes it easier and faster to define a cloud SLA and service level objectives, and simplifies the task of comparing one cloud SLA to another. It is often true that a given SLO may have multiple different metrics which can be used. It is important that an SLA makes it clear which metric(s) are being used for each quantitative SLO.
5.5.3 Standards and Guidelines which span customer types

Cloud services are valuable to both enterprises with thousands of users as well as small businesses with just a few users. In many cases, the cloud service is a highly standardized offering that relies heavily on uniformity to enable economies of scale and offer customers benefits, such as low prices. In some cases, the cloud SLA and other governing documents may be negotiated between the cloud service customer and the cloud service provider but such a negotiation cannot be assumed by default. In many cases, cloud service customers are offered a fixed standard agreement by the cloud service provider, which they can either choose to accept, or they can choose a different cloud service provider that offers different terms and conditions.

Standards and guidelines for cloud SLAs must be able to span from the smallest cloud service customer to the largest. Useful standards and guidelines exist, produced by organizations such as ENISA, NIST or ISO/IEC. For example, in the field of security, relevant work is using the approach to analyze and refine an individual control into one of more security SLOs, which are then associated with metrics and measurements that can be either quantitative or qualitative.

However, it is not possible to list exhaustively relevant standards, guidelines or certifications and many other useful specification initiatives exist.

5.5.4 Securing Infrastructure as a Service

The IaaS model lets users lease compute, storage, network, and other resources in a virtualized environment. The user doesn’t manage or control the underlying cloud infrastructure but has control over the OS, storage, deployed applications, and possibly certain networking components. Amazon’s Elastic Compute Cloud (EC2) is a good example of IaaS. At the cloud infrastructure level, CSPs can enforce network security with intrusion-detection systems (IDSs), firewalls, antivirus programs, distributed denial-of-service (DDoS) defenses, and so on.
5.5.5 Securing Platform as a Service

Cloud platforms are built on top of IaaS with system integration and virtualization middleware support. Such platforms let users deploy user-built software applications onto the cloud infrastructure using provider-supported programming languages and software tools (such as Java, Python, or .NET). The user doesn’t manage the underlying cloud infrastructure. Popular PaaS platforms include the Google App Engine (GAE) or Microsoft Windows Azure. This level requires securing the provisioned VMs, enforcing security compliance, managing potential risk, and establishing trust among all cloud users and providers.

5.5.6 Securing Software as a Service

SaaS employs browser-initiated application software to serve thousands of cloud customers, who make no upfront investment in servers or software licensing. From the provider’s perspective, costs are rather low compared with conventional application hosting. SaaS — as heavily pushed by Google, Microsoft, Sales-force.com, and so on — requires that data be protected from loss, distortion, or theft. Transactional security and copyright compliance are designed to protect all intellectual property rights at this level. Data encryption and coloring offer options for upholding data integrity and user privacy.

5.6 A SLA COMPONENT FOR THE PROVISIONING OF CUSTOMER FEEDBACK

The proposed security model is simulated using –CloudSim Simulator and users are encouraged to furnish feedback about the proposed security model. The parameters have been classified under Functionality and usability. The parameters such Easy to use, Quick to Lean, Likeable, Achieving users goal, Time consumption have been taken under Usability criteria. The parameters such as Split and store, Security, View of Particular data, Fulfilling the user’s requirements and user renewal are accounted under functionality. Customers are encouraged to evaluate their opinion as sample prototypes which are shown below.
Fig 5.1 Customer Feed Back Form
Fig 5.2 Feed Back Form with Ranking after customer Feed back
5.7 IMPROVING THE QUALITY OF SERVICE (QoS) BASED ON CUSTOMER FEED BACK

On the basis of the feedback session, the Quality of Service (QoS) is being focused for further improvements. The goal of QoS provisioning is to achieve a more deterministic network behavior, so that information carried by the network can be better delivered and network resources can be better utilized. A network or a service provider can offer different kinds of services to the users. Here, a service can be characterized by a set of measurable pre specified service requirements such as minimum bandwidth, maximum delay, maximum delay variance (jitter), and minimum packet loss rate. After accepting a service request from the user, the network has to ensure that the service requirements of the user’s flow are met, as per the agreement, throughout the duration of the flow (a packet stream from the source to the destination). In other words, the network has to provide a set of service guarantees while transporting a flow. QoS in traditional networks can generally be obtained via the over-provisioning of resources or traffic engineering. With the method of over provisioning, network providers add abundant resources in the networks so that it can provide satisfactory services to bandwidth hungry applications. This method is easy to realize and all the users are served in the same service class. But services may become unpredictable during peak traffic. In that case, two approaches based on traffic engineering are used to achieve QoS; i.e., reservation-based and reservation-less approaches. In the reservation based approach, network resources are assigned according to an application’s QoS request and subject to bandwidth management policy. In the reservation-less approach, no reservation is required. QoS is achieved via some strategies such as admission control, policy management, traffic classes, and queuing mechanisms. The admission control strategy decides if a node can access the network and guarantees that once the node obtains the permission, it will be served with the QoS it requests. Policy management ensures that no node will violate the type of services it is pre-assigned. Traffic classes differentiate the priority of data packets and they thereby achieve a particular per-hop behavior at each intermediate node. Queuing mechanisms are responsible for dropping the packets with lower priority in the case of congestion.
Some of the popular and important QoS parameters can be classified into conventional and modern. Conventional QoS parameters are used in the case of multimedia and regular applications. Those are bandwidth, jitter, delay, throughput and latency. Modern applications like military, industrial, emergency and research, use availability, sensing coverage, accuracy, load balancing, security, reliability, and energy efficient routing as their QoS parameters. Some short definitions of important QoS parameters in WSN are narrated below in a chronological order from conventional to modern.

The proposed security model on the basis of Usability and Functionality criterias are evaluated in cloud simulator and the results are shown below in Figure Fig 5.3. It shows that the proposed security model scores better and provide considerable user satisfaction for the provisioning of SLA.

![Graph for Usability and Functionality](image)

Fig 5.3 Test Results of Usability and Functionality with Current and Existing System