future internet

MDPI

Article

A Framework for Security Transparency in Cloud Computing

Umar Mukhtar Ismail [1], Shareeful Islam [1,*], Moussa Ouedraogo [2] and Edgar Weippl [3]

[1] School of Architecture, Computing and Engineering, University of East London, London E162RD, UK; u0852138@uel.ac.uk

[2] Luxembourg Institute of Science and Technology, L-4362 Esch-sur-Alzette, Luxembourg; moussa.ouedraogo@list.lu

[3] Secure Business Austria, Sommerpalais Harrach, Favoritenstrasse 16, 1040 Wien, Austria; eweippl@sba-research.org

* Correspondence: shareeful@uel.ac.uk; Tel.: +44-208-223-7273

Academic Editors: David G. Rosado and Stefanos Gritzalis
Received: 31 October 2015; Accepted: 22 January 2016; Published: 17 February 2016

Abstract: Individuals and corporate users are persistently considering cloud adoption due to its significant benefits compared to traditional computing environments. The data and applications in the cloud are stored in an environment that is separated, managed and maintained externally to the organisation. Therefore, it is essential for cloud providers to demonstrate and implement adequate security practices to protect the data and processes put under their stewardship. Security transparency in the cloud is likely to become the core theme that underpins the systematic disclosure of security designs and practices that enhance customer confidence in using cloud service and deployment models. In this paper, we present a framework that enables a detailed analysis of security transparency for cloud based systems. In particular, we consider security transparency from three different levels of abstraction, *i.e.*, conceptual, organisation and technical levels, and identify the relevant concepts within these levels. This allows us to provide an elaboration of the essential concepts at the core of transparency and analyse the means for implementing them from a technical perspective. Finally, an example from a real world migration context is given to provide a solid discussion on the applicability of the proposed framework.

Keywords: cloud computing; security transparency; cloud service provider; cloud service user

1. Introduction

Cloud computing (CC) provides numerous benefits such as cost reduction and a scalable environment that stimulate organisations for wider cloud adoption. Nevertheless, as more and more mission critical data and applications are migrated to the cloud, it is critical to protect them from potential risks [1]. Concerns are constantly raised by Cloud Service Customers (CSCs) about Cloud Service Providers' (CSPs) capability to protect their critical assets. Security transparency is an essential means that provides sufficient visibility of security operations and practices implemented by a CSP to protect users' data and applications [2,3]. Recently, it has received a lot of attention by both industry and research communities. For instance, virtual machine monitoring and Service Level Agreement (SLA) management are considered transparency related activities as indicated in the work of [4,5]. However, efforts related to virtual machines monitoring mainly focus on security management of CSP services rather than serving as a means of providing transparency to the CSCs. Service Level Agreements (SLA) monitoring is mainly CSP-centric as it mainly emphasizes areas where CSPs feel more confident to render such as service performance rather than overall view of the user migrated assets. Leveraging the benefits of CC requires a detailed understanding of CSP controls for

adequate protection of CSC critical data and applications. It is therefore crucial to develop a systematic framework for analysing cloud transparency needs based on CSCs' context as well as devising means for meeting such needs.

Within the above context, the novel contribution of this paper is a framework that supports the analysis of security transparency in CC from three different levels of abstraction; namely, conceptual level, organisational level and technical level. The approach of using different levels of abstraction is aimed at supporting users in the understanding and alignment of security transparency needs in accordance with CSP offerings for supporting such needs. The presented framework is based on basic transparency principles. It uses concepts from the existing requirements engineering domain and combines them with concepts relating to transparency principles so that the framework can support extraction of user needs, identification of requirements to support these needs and checking of CSP offerings to address these requirements. To demonstrate the applicability of our work, we consider a real migration use case to analyse security transparency using our framework.

The paper is structured as follows: Section 2 covers a description of related works. Section 3 outlines transparency basics, while Section 4 covers security transparency. Section 5 describes the proposed security transparency framework, while Section 6 demonstrates the approach through a real work migration use case. Finally, Section 7 concludes the paper and provides a direction for future research.

2. Related Works

There are a number of efforts that consider transparency for the cloud based context. Most of the works by academia unravel the challenges by offering solutions through SLA management and virtual machine monitoring, while industry experts have developed acceptable initiatives such as audit and compliance programmes, and self-assessments [6]. This section outlines some of these essential works.

Ouedraogo *et al.* in [6,7] proposed one of the first solutions for promoting security transparency in the cloud realm. Their proposal which is event-driven allows both CSC and CSP to make specifications to represent patterns of events of which their occurrence can be evidence of a security anomaly or breach or simply a sign of a nefarious use of the cloud infrastructure by some of its users. Dedicated algorithms for the detection of composite events coalesced with the definition of primitive events structure based on XCCDF format is meant to ensure the reuse and interoperability with security audit tools based on the Security Content and Automation Protocol-SCAP.

In literature related to the SLA based-approach, Casola *et al.* in [8] presented a monitoring architecture that integrates different security-related monitoring tools to provide continuous monitoring capabilities for SLA security parameters. The monitoring architecture put forward by the authors is built on and integrated with monitoring components belonging to SPECS framework, which also aims at designing and implementing a management framework of the SLA lifecycle. The validity of the approach was demonstrated through a case study related to the detection and management of vulnerabilities, where an open source monitoring system (OpenVAS) was integrated into the architecture in order to prove how open source and commercial monitoring tools can be flexibly mapped to enable automatic monitoring according to security SLOs.

Rak *et al.* in [4] discussed a preliminary design and implementation of a security solution for PaaS based on SLA approach with the aim of addressing the issues related to the management of security requirements in the cloud. The work adopts a dedicated cloudware platform that is deployed over infrastructure resources. The platform supports end-users and CSPs to specify their security requirements by means of SLAs, evaluate security features offered by remote cloud security brokers, management of SLA lifecycle as well as the development and deployment of security services. The preliminary architectural design of the platform involves three service layers, namely: application layer, services and platform layer, each with a distinctive function.

Happe *et al.* in [9] also proposed SLA@SOI management framework for service oriented architectures and CC. The authors advanced the idea of monitoring SLA by translating them into

operational monitoring specifications that can be checked by a low level monitor. The foundation of the SLA@SOI is built on a universal monitoring engine used for monitoring quality and behavioural properties of distributed systems based on events captured from them during the operation of systems at run time. The engine is called EVEREST and the properties that can be monitored by this machine are expressed in a language based on Event-Calculus.

For virtual machine monitoring, Krautheim [10] offered Private Virtual Infrastructure for the pre-measurement of cloud security properties, secure provisioning of cloud data, and provision of situational awareness enforced through continuous monitoring. The initiative uses a concept based on combination of Trusted Platform Module and a Locator Bot as a channel to support cloud service monitoring. Through this approach, the author argued that security remains a common responsibility between a CSP and a CSC, thereby making an SLA a critical tool for defining roles and responsibilities of both actors.

Theilman *et al.* in [11] discussed multi-level approach to SLA management for service-oriented infrastructure (SOI). In their work, SLAs are consistently specified and managed within SOI. They presented the run-time functional view of the conceptual architecture, applied and discussed the concepts to real case studies including Enterprise Resource Planning. Koller *et al.* in [12] proposed an autonomous QoS management that uses a proxy-like approach, which is implemented based on WS-Agreement. The work suggested that SLAs can be exploited to define certain QoS parameters that a service must maintain during its interaction with customers.

In compliance, assurance programs such as Security, Trust & Assurance Registry (STAR) dominate the scene and they have developed assurance schemes for promoting cloud security transparency [13]. CSPs subscribe to this initiative by adequately and satisfactorily implementing the security objectives specified by such bodies for enhancing security transparency. Also, ISO/IE27001 provides a certification framework for demonstrating best practice information security routines exercised by CSPs. The objective is to assist CSPs in improving the performance and effectiveness of Information Security Management Systems (ISMS) and help CSCs implement controls to address risks and understand their security needs. CSA STAR Self-Assessment is also a free initiative that allows CSPs to submit self-assessment reports documenting compliance to CSA's published best practices through a report [12]. The report involves a Consensus Assessments Initiative Questionnaire (CAIQ) that provides a set of questions a CSC would naturally wish to ask and CSPs may decide to submit completed answers to the questions.

The approaches discussed above have made tremendous and important contributions but they also demonstrate a number of limitations. Some of the limitations associated with an SLA based approach include the enormity of areas in cloud security that ought to be covered and the works are mainly rationalised to address transparency from the position of a CSP. Furthermore, other works evolve around the integration of vulnerability management for checking the actual enforcement of SLA related metrics. This implies that the security transparency expectations of cloud users are not appropriately considered, thus making the initiatives appear as CSP-centred.

The current efforts in virtual machines monitoring are mainly steered by the need to strengthen the management of security from a CSP perspective rather than providing an all-encompassing solution that unravels multi-party trust and mutual auditability complexities from CSCs' side. This direction thereby makes virtual machine monitoring CSP-centred. Compliance through certifications by security standards only provide a periodic assessment for a timespan, but do not provide additional feedback for intervals between assessments. Self-assessments prepared by CSPs are self-proclaimed declarations that are usually tilted in their favour, thus susceptible to bias, subjectivity, and failing to capture an accurate impression of the authentic state of affairs within the environment. Conversely, third-party customer audit has its own setbacks as a CSP may conceivably decline to consent to a physical audit of its infrastructure, and likely attempt to limit customer audit scope in protecting the confidential security processes of its services.

Our work attempts to complete the shortfall in preceding literatures by providing the basics of cloud security transparency by elaborating on what constitutes transparency, its deployment types and practices. Given the scarcity of initiatives for practically implementing and overseeing security transparency requirements, this work's contribution could improve state of the art knowledge of the concepts surrounding it and the means to enforcing it. A distinguishing contribution of our work is that it adopts a multi-tiered approach to security transparency through three levels of abstraction, namely: conceptual level, organisational level and technical level. These levels are connected with the essential concepts that are used for attaining transparency, how they are implemented within an organisational context and identify the practical means of fulfilling them. In general, the approach supports users to (i) identify and refine the essential security transparency needs pertinent to their operating goals (ii) place the focus of security transparency on the areas that are most significant to their requirements; (iii) identify the means for continuous visibility.

3. Transparency Basics

Transparency in the past few years has received considerable attention across several domains as a result of the surge to access information [14]. It is often considered as a universal remedy for all sorts of socioeconomic, sociocultural, socio-political and civic problems. Institutions gain the confidence of the public by ensuring that the demand and supply of information continue to flow and also by promoting mechanisms that assure the accessibility of information by the public [15]. Several denominators across different domains have offered various definitions and interpretations of transparency. However, there is no commonly concurred definition across different areas, except for a universal consensus that transparency is associated with the public access to information [16]. One way to understand the meaning is to review a few broad general definitions of transparency. For example, in fiscal economic terms, transparency is defined as governments being open towards the public about structures and functions, policy intentions, public sector accounts, and projections [17]. In social sciences, transparency connotes the ability of interested parties to see through otherwise private information. Moreover, within the area of information technology, transparency is viewed differently and considered as implying to the actions of openness and accountability [18]. The practice of transparency comes in many different forms of varying commitments, engagements and obligations; thus, it is crucial to identify the categories of adopted institutional practices that are intended to promote transparent operations and the manner in which they are deployed. In the upcoming sections of this paper, the pivotal transparency categories (such as proactive and reactive) and the deployment types (opaque and explicit) will be covered while emphasising the context of CST.

4. Cloud Security Transparency

Transparency is an essential means for strengthening information disclosure and enhances users' trust in using cloud services. It is one of the fundamental aspects of operations that ensure visibility regarding some important areas such as performance, configuration, billing, and workload [19,20]. Transparency in the past was particularly used to imply CSCs' need for visibility on matters such as pricing models, but a broad range of interests such as security, service delivery and performance are now associated with the term. Security transparency among all other spectrums has prevailed as the most censorious necessity due to the complex chain of interactions between multiple actors, which fundamentally calls for the need to know how security and compliance measures are being applied to protect sensitive assets [21,22]. Considering the apparent definitions and connotations of transparency as attempted by researchers from different spheres of activities, for the purpose of this research, we define security transparency as:

> The disclosure of information related to security practices and controls used in the protection of customer data and applications hosted in the cloud environment. It also entails providing synchronous and asynchronous information to events pertaining customer

data and applications in order to enable them to obtain sufficient visibility of incidents concerning their assets while in the custody of a cloud service provider.

Moreover, a key integral direction in this aspect is the need to elaborately dissect what constitutes transparency in the cloud through the identification of categories, deployment types and the formulation of a conceptual model that entails necessary attributes.

4.1. Why do We Need Security Transparency in Cloud?

One of the most considerable obstacles to successful cloud migration is the management of security that is relatively aggravated by the non-transparent nature of CSP to disclose security related information associated with their offerings [23]. Users are driven by the fear of unrevealed occurrences cognate to ongoing CSP control procedures, and they always endeavour to make informed decisions by relying on CSP disclosures to achieve optimum security goals and operate in compliance with necessary requirements. A successful adoption of cloud technology by corporate users, businesses and organisations requires a clear-cut disclosure of the security policies, designs and practices of CSPs, including ongoing visibility of relevant security measures. These requisites for transparency constitute the pathway for users to assess the possible risks of CC and its potential impact on assets. For example, a CSP may choose to outline the policies and procedures being employed to ensure the availability of user data by disclosing information on the architectural setup of backup plans, business continuity and redundancy strategies that ensure continuous data availability. Security transparency in public clouds is considered as demanding a substantial magnitude of interest in comparison to other deployment models, due to its characteristics of being open to the public and serving a broad customer base. In contrast, other deployment models such as private clouds are specifically designed for individual organisations thereby offering customised functionalities that do not necessitate transparent operations.

4.2. Principles of Security Transparency in Cloud

It is necessary to provide some guiding principles that are imperative for understanding transparency. A justification for these principles is to establish the fundamental norms that represent what is desirable and affirmative in the general sense of information disclosure within the sphere of CC. In other words, they are meant to govern the action of providing visibility and to inform cloud actors about the precepts they can be expected to uphold in the delivery of transparency. These considerations impact the accessibility and quality of information released under a transparency initiative. According to Kosack *et al.*, in [24], there are some generic guiding principles for transparency. Our research will adopt these principles and tailor them according to cloud based systems.

- **Availability**. Availability means that information relating to occurrences regarding migrated assets should be available to the users. A monitoring system should be configured to stream real-time or near-real time status information regarding customer assets and every action performed to those assets.
- **Clarity**. Implies that information should be clear and precise for easy understanding. In other terms, clarity eliminates all elements of ambiguity so that information is delivered precisely, in a coherent and intelligible manner. The benefit of clarity is about helping CSCs utilise information to reduce complexity and uncertainty so that analysis can be applied to identify a clear path forward. An example to this is represented by a scenario where a shared responsibility model for security provisioning is adopted. The CSP should clarify their responsibility in securing a cloud infrastructure, while CSCs should take on the responsibility of securing data or applications integrated into that infrastructure.
- **Current**. Means that the information should be up-to-date. Information should be regularly streamed to CSCs in a real-time or near real-time flow for enabling the evaluation of actions pertaining to their assets in the cloud. Also, the information should clearly state the timestamp

and occurrences of actions in relation to cloud-hosted assets. For example, anomaly detection in the cloud environment greatly depends upon current or real time information.

- **Relevance**. Information should be relevant to the context. Cloud systems consist of numerous virtual machines, hardware, operating systems and applications that provide valuable information. Information must be relevant to provide information from a variety of platforms. For example, if a CSC subscribes to information feed on cloud resource availability, the usage data of the cloud resource being considered should be particularly streamed to CSCs.
- **Notification**. Information relating to security incidents, events, deviations, or occurrences that affect customer assets in the cloud should be appropriately disseminated to concerned customers so that they can evaluate the occurrences and optionally take action. For example, the presence of dedicated monitoring systems that detect security phenomenon and notify CSCs to take remedial actions or invoke an autonomous action.
- **Free of Charge or at Low Cost**. Information should be automatically compiled, organised collocated and streamed to concerned cloud actors that subscribe information feed for free of charge or at a low cost.

4.3. Categories of Cloud Security Transparency

Security transparency shows three different types as shown in Figure 1.

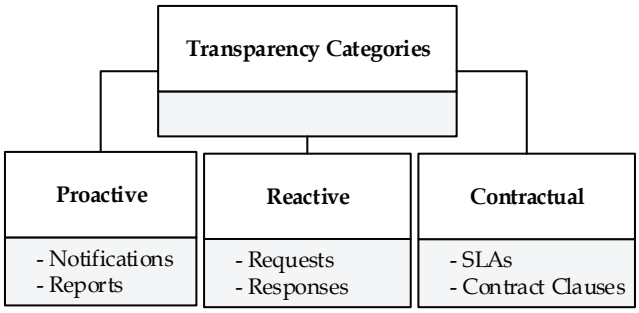

Figure 1. Categorisation of cloud security transparency.

- **Proactive Transparency (Voluntary)**. Proactive transparency involves voluntary disclosure of information, meaning that the CSP voluntarily provide information to the users by means of autonomous agents or manual process. It stems from CSPs initiatives to make security information of their offerings available to all without a request being filed. It can be generated through various methods such as notifications or reports (such as websites and portals, benchmarks, whitepapers, *etc.*). This disclosure is generally intended to improve customer trust and confidence, assist customers evaluate basic CSP control environments, demonstrate CSP certification to regulatory or industry requirements, and also help customers address some specific questions around general practices. It does not reveal information that could jeopardise the security posture of a CSP or expose them to harm's way. For instance, when a CSC's data falls under restrictions emanating from regulatory or compliance requirements, the choice of a CSP hinges on the contentment that they are fully compliant to a regulatory body, otherwise there is the risk of violating regulatory, legal or other privacy requirements [25]. The benefits that accrue from CSPs initiative to proactively disclose information include the availability of information that ensures timely access to information to help all CSCs including small, large and medium enterprises without the need to file special request, which is indeed associated with various sorts of commitments.
- **Reactive Transparency (Necessary)**. Reactive transparency involves a request-driven approach where a CSP is expected to respond to a user's specific request. It emerges from a request-response routine between a CSC and a CSP for the latter to provide additional information. Through the

request-response regime, a prospective user files a request and receives information from an existing CSP or for an incident notification to be sent to the CSC. Generally, the contents of a CSP response represent the actual settings, offerings or security status of CSC assets rather than a meagre attempt to beat competition from other vendors, which indeed increases transparency on how individual requirements are distinctly addressed. The advantage of the request-response driven approach is its ability to enable users to exclusively specify their security requirements and the identification of suitable controls by the CSP. However, it could be argued that it has become a traditional practice for CSPs to frequently publish information in public domains so that future cloud users do not have to file a request, saving time for both the CSP and the customers.

- **Contractual Transparency (Statutory)**. This implies that a CSP is legally mandated by the law to provide transparency while rendering services to CSCs. It involves a valid written agreement where the CSP observes utmost disclosure of all essential security services on an individual basis, while refraining from divulging information that could compromise the privacy of other users. SLAs are useful tools widely used by both CSPs and CSCs for ensuring transparency and establishing a common pact in order to manage the security requirements requested by a CSC and the security levels being offered by a CSP. Also, the SLA forms the basis for defining responsibilities and the remedies available for customers in case of a contract breach. Fundamental aspects of the SLA are the representation of the contexts shared by the two parties, and how each actor utilises the contexts in its own operations throughout the SLA. In order words, the SLA provides a comprehensive description and transparent security processes for both the CSP and customer to avoid uncertainty, apprehension and disputes. Conventional SLAs generally provide clarity on CSP service offers, unambiguous definition of expectations and obligations on both sides, and the boundaries of liability. Nevertheless, a notable limitation to this class of transparency is that essential security properties of a customer may not be captured.

4.4. Cloud Security Transparency Deployment Practices

Information that is disclosed through transparency takes different dimensions. Some information disclosure eminently supports the CSC in decision making while, in some cases, certain disclosures present inessential information that perhaps creates ambivalence. It particularly falls into two categories: opaque and explicit transparency, as illustrated in Figure 2.

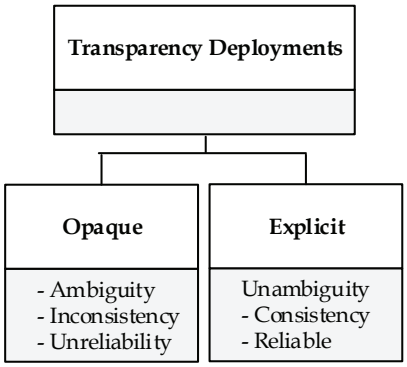

Figure 2. Cloud security transparency deployment practices.

- **Opaque Transparency**. Opaque transparency means that information is not well clarified. It involves CSPs disclosing information that either partially represent its actual operational values or provides equivocal statements. It may also involve inconsistent or unreliable information in terms of how controls are actualised in the cloud environment. For example, a CSP might claim to operate a service with security as a key principle through the implementation of reasonable technical network security routines, but then fails to genuinely demonstrate the application

or actual implementation of significant secure network architectures and security devices that monitor and control communications at the key boundaries within their environment. This would mean that transparent service is provided with virtually futile effects.

- **Explicit Transparency**. This refers to the disclosure and dissemination of information that represents a realistic implementation of CSP security control that precisely outlines the processes and procedures of how operations are securely managed. It provides a comprehensible elucidation on CSP's approach to ensuring the protection of CSC assets while in their control. This type of transparency is considered as most effectively attracting customer trust and confidence, as well as supporting accountability in the cloud. An example of explicit transparency would involve a CSP supporting a system that collects data related to the state or behaviour of customer assets and sends such data for onward analysis and evaluation by the concerned customer.

4.5. Relationship between Categories of Transparency and Deployment Practices

An overlapping relationship could be identified as existing between the transparency categories and its deployment practices. It could be argued that some CSPs provide the actual information that corresponds to their environment, while a proportion plausibly opt to provide spurious information so as to keep step with market competition, and others may attempt to conceal certain damaging information that could affect their reputation.

Figure 3 illustrates how each security transparency category is associated with one of the two deployment practices. For instance, a CSP may proactively provide transparency through security whitepapers regarding the security and compliance measures they have in place to protect customer assets. The CSP, nonetheless, may deploy an explicit security transparency practice to provide detailed information into their existing monitoring and prevention controls that prevent attacks, malware and other unauthorized activities while refraining from disclosures that expose them to risks. However, it may choose to deploy an opaque transparency practice to state the existence of security controls that either fail to capture the actual state of controls or are presented in an ambiguous form. Moreover, contention in this regard upholds the opinion that contractual security transparency is mainly associated with explicit deployment practice. This argument is supported by the fact that contracts are enforced by law and become legally bound once an agreement is reached between the CSP and user. Thus, a CSP is less likely to provide non-transparent or ambiguous disclosures that could result in ramifications and consequently lead to indemnifying its customers.

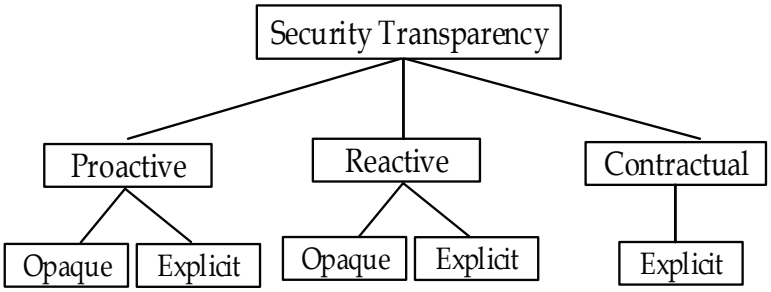

Figure 3. Relationship between transparency categories and deployment practices.

5. Cloud Security Transparency Framework

Our framework allows a comprehensive understanding of security transparency for the cloud based system context. It includes three different levels of abstraction along with associated concepts within these levels. These levels build the bridge from the concepts necessary for transparency with the organisational settings and technical means for the purpose of implementation. This section provides a detailed description of our framework.

5.1. Levels of Abstractions

The proposed approach views transparency from three different levels of abstraction—a conceptual view, at the organisational level, and finally at a technical level, as illustrated in Figure 4. Sitting at the top level of abstraction is the conceptual view that constitutes the concepts necessary for security transparency. The aim of this layer is to develop the foundation concepts for the transparency principles that are valuable for a comprehensive introduction of how security transparency is achieved at the subsequent levels. At the middle layer lies the organisational level, which is triggered by the concepts developed at the conceptual level and how they can be mapped to an organisational setting. In other words, organisational level describes how the conceptual view of cloud security transparency is integrated with other concepts for enabling security transparency to CSC. Finally, the bottom layer deals with the technical level that supports the implementation of the conceptual view and the concepts at an organisational level in a technical sense. The layer specifies the technical outlook in terms of the practicality to achieve security transparency, for example, how SLA based monitoring can be used to help organisations ensure their requirements are continuously fulfilled. The levels of abstraction influence each other and they are related in a way that supports the mapping of all the concepts at each level.

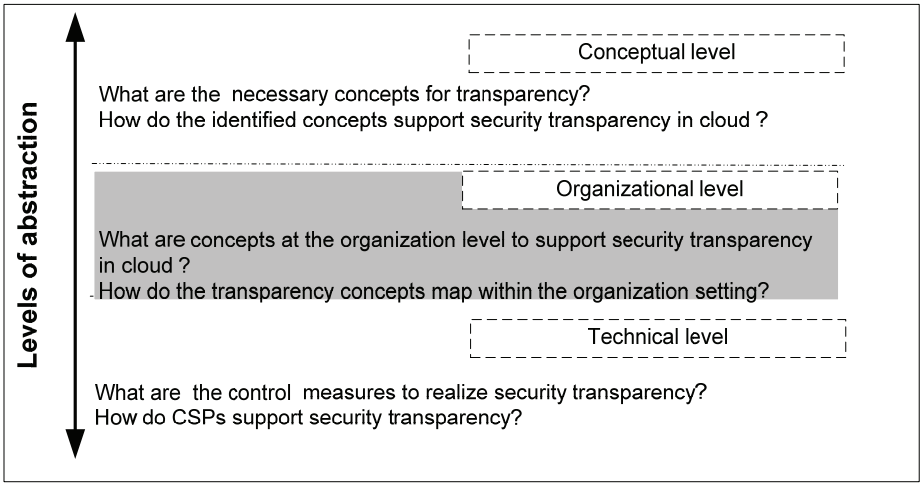

Figure 4. Levels of abstraction for security transparency in cloud.

5.2. Conceptual View

This section provides the essential foundation concepts that are used for the development of security transparency at organisational and technical levels. Regardless of the category at which it is articulated and the deployment practice being followed, it is paramount that security transparency encompasses other concepts that support its development and delivery between cloud actors. The identified concepts are given below:

- **Actor**. An actor represents an entity, partiularly a CSP, a system, an organisation, a user, or a process that carries out actions to generate transparency or become the recipient of transparency generated by another actor.
- **Transparency Request**. The purpose of a transparency request is to allow a CSC to collect information about the capabilities of a CSP and the occurrences of incidents that affect their migrated assets within the cloud environment. It is initiated by the CSC seeking real-time or recorded information being held by a CSP, particularly information that discloses how requirements can be fulfilled and how operations are being executed on migrated assets. The core of this concept is enabling the CSC to wholly specify the information required to support their operations, thereby constituting the need for an explicit rather than opaque transparency. A way

for a CSC to request transparency is achieved by way of reactive or contractual transparency, largely due to the fact that both categories support actors in their requests for additional disclosures relevant to their needs. In most cases, CSPs exclusively deploy explicit transparency in response to the transparency requests in order to avoid misinterpretation of legal liabilities. It is noteworthy to highlight the distinction between transparency requests and the requirements concept (at an organisational level). Transparency requests do not independently support the description of CSC requirements, it rather solicit details on how requirements are fulfilled and how occurrences are reported. Whereas, the requirement concept aims at enabling the specification of the most pertinent security requirements to the assets of a CSC.

- **Mechanism**. A mechanism is defined as a high level or low level solution being adopted for the disclosure of relevant security information pertaining to an actor's operational processes. The term is used to imply an actor making use of proactive, reactive or contractual transparency initiatives to make operational information available and respond to transparency requests by detailing how it conforms to governing rules and providing security protections. Furthermore, a mechanism is predominantly the fore attribute that triggers the conceptualisation of other concepts because it presents first-hand information in areas of common security practices and management.
- **Evidence**. Evidences represent disclosures in a specific format that provide collective information about transparency mechanisms. The aim is to enable an actor to provide to other actors a status report on the general security condition of its environment. Another important aspect of the evidence is to support actors to perform a check and verification of disclosures against their transparency needs in order to purposefully determine the integrity of an actor's response to their requests.
- **Accessibility**. Encompasses the credence for an actor's transparency mechanism and emerging evidences to be requisitely made available, accessible and affordable to all other actors through various initiatives. It contains initiatives regarding information disclosure such as autonomous reporting systems, websites, policies, compliance, SLA *etc*.
- **Liability**. This is the state of being legally responsible for security transparency *i.e.*, an actor becomes legally answerable for the contents of a disclosure. An actor that is held liable for a disclosure becomes legally responsible to render agreed redress in non-fulfilment or misstatement of information. For example, if contractual agreements have been reached between a CSP and a customer for the former to provide 99% service availability, they become legally liable to ensure such and redress the latter in the event of a failure.
- **Monitoring**. This is the ability to observe and check the quality of information provided. In order to substantiate the accuracy of a disclosure, it must be observable by other actors. This may be achieved through analysing evidences generated by a transparency mechanism being supported by an actor. In other words, monitoring is a function of processes that can be used to establish the effectiveness of the internal operations of an actor by observing the content in evidence.
- **Verifiability**. This is the degree to which a disclosure can be confirmed to be existent and to establishing its accuracy. This concept allows other actors to validate whether observable properties comply with agreed expectations or requirements. It is concerned with ensuring that materials presented are made truthfully and reflect genuine credibility about perceived quality.

The concepts in Figure 5 provide an insight into the conceptual view of security transparency. An actor (CSC) initiates a transparency request to another actor (CSP) soliciting for transparency in their operational environment and actions relating to their assets. The CSP actor, on the other hand, supports mechanisms for transparency to make available vital information regarding its operational processes. The mechanism is characterised by various means for information disclosure, which is literally used to disclose customary security practices and the status of customer assets within its environment. The responsibility to support a mechanism may either be one-sided or shared amongst the two actors. This is commonly noticeable *in situ*ations, for instance, public clouds where a CSP is responsible for

supporting mechanisms of transparency, whereas in certain setups such as private clouds the CSC is solely responsible for security administration and control of information. Additionally, the mechanism generates evidences in order to provide status reports on the condition of the CSP environment and assets belonging to an actor. For the evidence to essentially yield significance, it must possess the qualities of being monitorable and verifiable for establishing the genuineness or truthfulness of disseminated information according to perceived quality and expectations of an actor. Therefore, the CSC verifies the transparency mechanism through monitoring, hence providing the avenue to verify disclosed information.

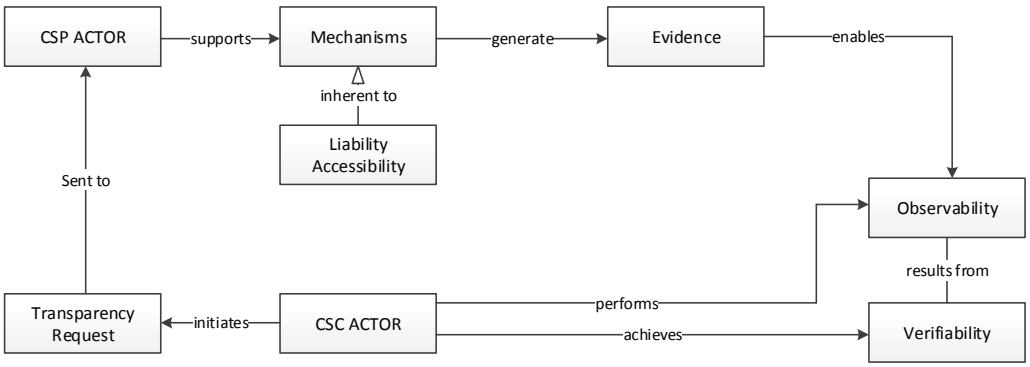

Figure 5. Conceptual Model of Cloud Security Transparency.

5.3. Organisational Level and Modelling Concepts for the Framework

The organisational level concepts are based on the conceptual level foundation concepts to ease the implementation of transparency at the technical level. For example, a CSC at the conceptual view sends a Request for Transparency to a CSP demanding additional security information while the CSP responds to such a request by disclosing information through mechanisms for transparency. Before the request for information is sent, the CSC ought to apply some essential analytical steps for identifying their goals, assets and security transparency. This level allows for such processes to be applied. Therefore, the following are the necessary concepts at an organisational level while focusing on the conceptual view.

- **Cloud Strategy**. This supports the CSC to make sense of adopting or the reasons cloud services have been adopted. In other words, it allows CSCs to conduct an internal analysis of their goals and the readiness to adopt cloud services, and how security transparency can be realised. The cloud strategy is characterised by two attributes:
    - Goals. Represent the aims and objectives of a CSC's intention of migrating to the cloud. The goals could be cost reduction, flexibility and scalability, improved accessibility, and security *etc*.
    - Cloud Readiness. This analyses the integration of locally hosted applications, data, or processes with cloud services in terms of standardisation, format, portability, interoperability, *etc*. Also, cloud readiness identifies the potential benefits associated with fulfilling goals.
- **Assets**. This involves the identification of CSC assets, those assets that are outsourced to the cloud environment and those that are hosted locally. Selected assets are classified according to category and criticality to the operations of the CSC. The relevance of this is to allow for the identification of the essential security requirements that are put around the assets to help the CSC maintain a track record of the assets. Asset has two attributes:

  - Category. Assets are classified according to different tiers of sensitivity and security requirements such as public, open or confidential. Public means asset is accessible to the general public, open means available to every company user, confidential limits access to only authorised company users.
  - Criticality. Criticality is the major indicator used by the CSC to determine the importance of the asset to the business. Criticality is not dependent upon category, however, the criticality of any asset category can be high, medium or low. Assets with a high rating are the most valuable to CSC, a medium rating represents a moderate value; while low means little value to the CSC.

- **Risk**. Risks are the potential consequences inherent to a CSP control environment that could potentially compromise the security of assets in the cloud. A risk could fall under one or more of areas of cloud such as: security, operational, technical, nontechnical, regulatory, governance *etc*.
- **Controls**. Controls are sets of security safeguards or countermeasures to avoid, counteract or minimise security risks in a CSP operating environment. Controls may also represent the mechanisms used by CSPs for providing transparency. They are supported by a CSP and characterised by a combination of technical and non-technical controls that describe the essential components assembled and actions taken to protect assets.
- **Evidences**. Are affirmations from the CSP specifying the existence of acclaimed security controls and providing a transparent overview of their implementation/management. In other words, evidences are exclusively generated by a CSP in connection with supported controls to CSCs assets. They provide a detailed representation of the actual security controls in the areas of technical, human, physical and operational safeguards adopted by a CSP to sustain security, and reveal the actions, functions and steps taken in order to provide transparency and meet CSC security expectations. They are provided through attested sources such as automated evidence collection tools, websites, security whitepapers, *etc*.
- **Requirements**. Requirements imply vital security needs for safeguarding CSC assets and enabling security transparency. In some scenarios of service negotiation, a CSC may be wholly satisfied with CSP offerings while in other scenarios the CSC may identify some inadequacies between CSP offerings and their needs. In both circumstances, the CSC identifies and clearly defines the essential security requirements that safeguard assets and which are worthy of tracking to ensure continuous transparency. Put differently, requirements represent the crucial CSC security needs that are continuously monitored for transparency once assets are outsourced to the cloud. It is important to mention that requirements' extraction considers the identified goals from the cloud strategy, risks, security best practice and assets. For ensuring the extraction of appropriate requirements, best security practice guide such as Cloud Security Alliance's Cloud Control Matrix (CSA CCM, 2011) should be taken into consideration.
- **SLA**. The pertinent CSC security needs identified through the requirements concept are stipulated as requisite clauses in the SLA. The clauses are transformed to form the subject of security transparency that deliver visibility into the security occurrences on assets migrated to the cloud.
- **Monitoring**. Monitoring involves the tracking of security events pertaining to CSC security requirements as specified in the SLA. It also tracks CSP controls in order to check their operational status. It consolidates several services that are supported by the CSP to enable CSCs to collect evidences on the status of their assets.
- **Events**. Events deal with information provided to show the incidents, or activities performed on CSC assets and the resulting status of the assets. They are the occurrences that take place in the cloud services relevant for CSC assets. Events send a status report generated by the monitoring concept to provide accurate and timely information relating to the operating conditions that are of interest to CSC requirements. This will generate evidence-based trust between cloud actors

that all expectations are being met and that everything claimed to be happening in the cloud is indeed happening.

The metamodel in Figure 6 shows an overall view of the concepts and their relationships. A CSC actor could be a corporate or individual user interested in cloud services offered by a CSP. At the preliminary stages of cloud adoption, the CSC performs an appraisal of cloud strategy designed to (i) identify the goals for cloud adoption such as cost reduction and security; (ii) and analyze the readiness for cloud technology in terms of security, portability, integration *etc*. The cloud strategy allows the CSC to comprehensively identify their critical assets so as to determine what assets are put into the cloud and to also recognize the security specificities that could protect the assets while in the cloud. CSPs, on the other hand, implement the necessary technical and non-technical controls for safeguarding CSC assets, as well as transparency mechanisms for providing information to such security services. They also adopt proactive and reactive transparency mechanisms to generate evidence in various forms to disclose how CSC needs are supported. Moreover, the CSC may require more security services. Therefore, the CSC defines the desirable and essential requirements for the protection of its assets. The security requirements become the major points of attention to the CSC that ought to be monitored in the cloud, and therefore, they are enumerated and specified in SLA. The SLA serves as a powerful tool for the CSC because it creates a legally bound agreement with the CSP and it becomes the subject of monitoring. The primary role of the monitoring concept is to track the status of the security requirements and the efficiency of CSP supported security controls. Lastly, in the case of an unspecified event, (*i.e.*, breach to properties or manifestation of risks), evidence is generated by the monitoring tool describing the event that took place and the state of an asset after the event. These details are collectively sent to the CSC using a notification system.

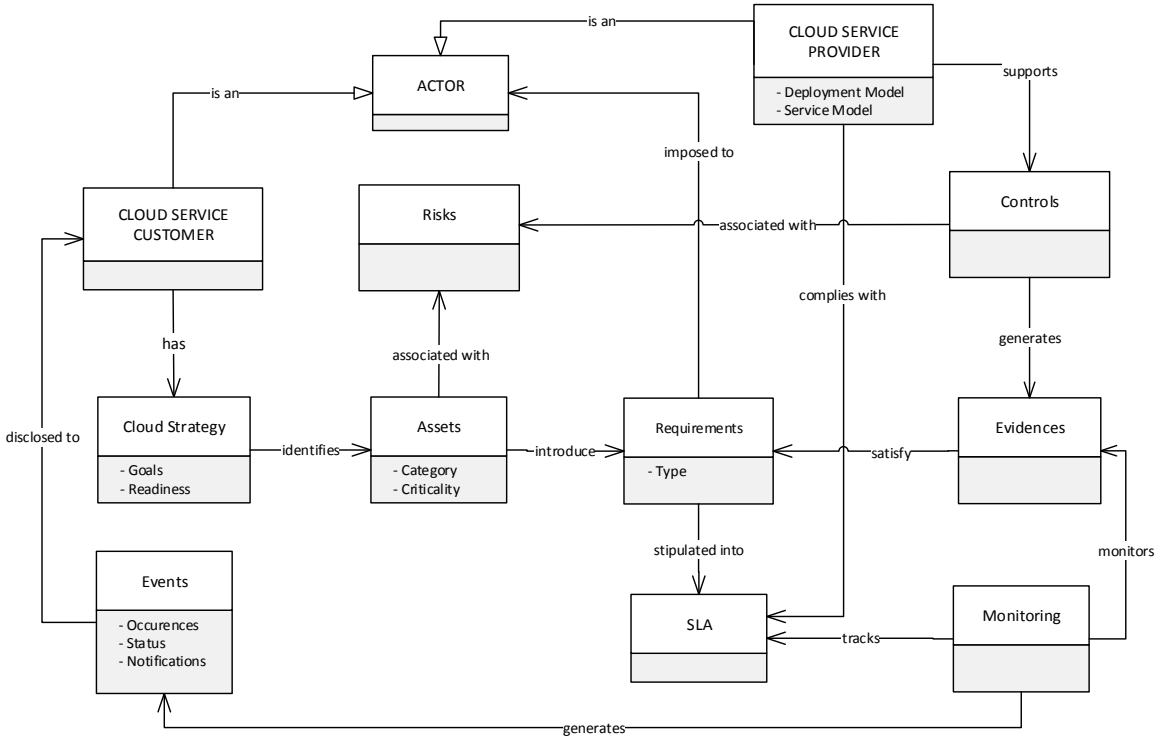

Figure 6. A metamodel for security transparency at the organisational level.

5.4. Technical Level

This level is influenced by the organisational level because concepts at the organisational level support the understanding of what type of technical means are needed to ensure security transparency. The primary emphasis of the technical level focuses on the technicalities for realizing continuous

transparency and generating security event notifications through SLA based monitoring as identified at the organisational level. This further illustrates the interdependence or interlinking of the three levels of abstraction that can be viewed from a conceptual view, at the organisational level down to the technical level. However, it is relatively important to identify the most commonly used conventional transparency mechanisms adopted by CSPs to provide customers with detailed and useful information. The mechanisms include:

- **Compliance Programs:** CSPs are increasingly using compliance programs as mechanisms for demonstrating transparency through conformity with multiple traditional standards that predominantly focus on certifying the composition and management of security practices in CSP environments. Consequently, CSPs earmark a significant sum of budget for ensuring security, and spend sizeable amount of resources and time into compliance with security standards such as ISO 27001/27002, Payment Card Industry Data Security Standards (PCI DSS), and other relevant standards.
- **Self-assessments:** CSPs have realised the obligation to provide satisfactory transparency of their services to CSCs. CSPs often conduct a discretional self-assessment of their services by employing control objectives specified in frameworks that document and certify best security practice within CSP environment in order to provide transparency to their customers. Self-assessments are usually free and open to all CSPs. One such framework is CSA STAR Certification that embarks on a three-levelled certification scheme to certify CSP's compliance to its set of security guidance and control objectives.
- **Third-Party Customer Audit:** This is another type of transparency mechanism that materialises in the form of a systematic and objective evidence gathering process initiated by an independent auditor appointed by a CSC to physically appraise the CSP environment. Also, a CSP may be mutually obliged to fill-out a questionnaire and complete a detailed checklist prepared by a CSC about areas that are of concern to them.
- **Security Policies:** CSPs usually enforce security transparency policies that make them committed to making information available to the public upon demand. CSPs consider access to information a key component of effective participation of all CSCs. Transparency policies are often enforced through an Information Disclosure Policy, which is guided by the underlying principles of accountability and openness concerning operational programmes and customer related aspects.
- **Service Level Agreements (SLAs):** Another important technique for ensuring adequate disclosure of information involves the use of SLA. The SLA is a binding contract between the CSP and a customer, which specifies customer security requirements and the CSP's commitment to fulfilling them. It clearly describes the security responsibilities and liabilities between the two parties, states the service performance and delivery, problem management, legal compliance, *etc*.

We advocate SLA specifications as a part of contractual transparency because it is a common practice by CSPs to provide service offers with adjustable SLAs for allowing their customers negotiate the terms of offers. This provides an added opportunity that enables potential CSCs to request additional services on top of CSP offerings through the specification of their security expectations and the collection of evidences. CSCs achieve this by including most refined security needs that require frequent visibility as part of SLA security guarantees. It will facilitate the balancing and negotiating of security requirements from the onset of cloud contracts, all the way to forming the basis upon which continuous security transparency is delivered by the CSP. Therefore, the SLA based monitoring allows CSCs to define what is followed-up for realising transparency on a continuous basis with the aim of monitoring whether an actual service delivery complies with the agreed CSC expectations. The security requirements are selected on analysis of a CSC's foremost areas of operations. This method is important, as shown in Figure 7, because it follows a sequence of activities in cloud procurement that progresses through all the categories of security transparency identified at the abstraction level (proactive, reactive and contractual), which indeed results in achieving organisational transparency goals.

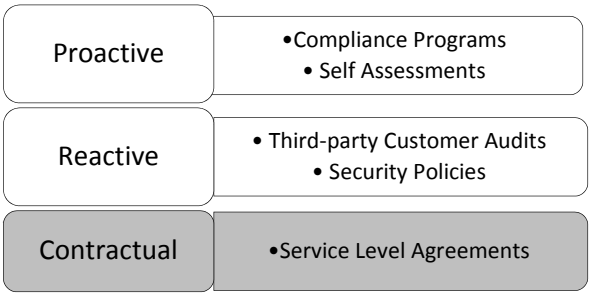

Figure 7. Mechanisms for cloud security transparency.

6. Example

To demonstrate the applicability of our approach, we present a migration scenario from a real organisation context. The goal is to understand the transparency related issues and requirements from the context based on the concepts introduced by the framework, as well as providing solutions to realise security transparency.

6.1. Use Case Scenario

The migration use case adopts a London based open-access publishing company. Due to confidentiality reasons, we are restrained from using the publisher's real name. The organisation provides affordable open access publishing services of peer-reviewed academic journals, books and data through a network of independent university and society presses. The publishing services provided by the company include anti-plagiarism checking, rigorous peer review, indexing and archiving.

The underlying technology for the open access publication is using a code repository with Python and PHP for storing and archiving documents. The code repository is currently used by 25 users. The business process includes: receiving articles from potential researchers, assigning reviewers for the papers, proofreading of the selected papers and final publication. The existing in-house systems use three web servers, and 20 Mbps of bandwidth. Generally, there are thousands of articles published every month. The company has recently decided to adopt public cloud for performing existing operations within tight budget constraints. Top of the priority list is the company's obligation to ensuring acceptable security of its assets through satisfactory security transparency of CSP services, and it also strives to realize the provisioning of cloud services that enables storage, integration and deployment of the codes to the cloud.

An attempt was made by the company to define their primary service expectations at the early stages of the cloud transition with the aim of receiving a significant degree of commitment on how they can be fulfilled by a potential CSP. The expectations reflect most essential desideratum desired for enabling a favorable outsourcing that include: (i) the provision of robust code management tools that encompasses security integrity enabling capabilities as well as service availability procedures for continuous availability of the repository code (ii) and the presence of dedicated transparency mechanisms that support monitoring capabilities for gathering, storing and generating security information related to occurrences in the code repository. Various CSPs were considered for meeting these expectations and a renowned CSP that specialses in the delivery of PaaS was approached where they vehemently pledged the ability to meet all the expectations. The CSP has also acceded to accommodate additional expectations should the company identify any before contracts are agreed. However, in apprehension of the CSP's non-fulfillment of promises and the incapacity to deliver commitments, the company's management resolved to administer a systematic process that allows them to comprehensively identify all fundamental requirements that form the focus of the SLA contracts. One of the coauthors through his personal contacts granted us the opportunity to apply the framework accordingly.

6.2. Implementation of the Security Transparency Framework

6.2.1. Actors

Users including *the programmer* and *admin staffs* of the anonymous printing company are identified as the CSC actors who require the services provided by another actor to achieve specific goals. A CSP is another actor who specializes in the delivery and provisioning of cloud services to the public, and therefore, supports services that assist the company in achieving its goals. We use a pseudonym "*TransparentCloud*" to imply the prospective CSP actor in the example in order to be more specific and to also avoid employing a generic terminology for this actor.

6.2.2. Cloud Strategy

It is important that the level of security services provided by a potential CSP correlates with their internal IT environment, the reason being an oversight to appropriately ensure consistency could potentially result in operational uncertainty.

a **Goals**. The company has identified some goals as the motivating factors for outsourcing to the cloud. They are: (i) cost minimization; (ii) continuous availability of the code repository and published articles; (iii) the integrity of published articles (iv) and the portability of supporting a specified number of company users to access the codes across diverse platforms.

b **Cloud Readiness**. Platform as-a-Service (PaaS) was identified as being suitable service offering that provides basic computing resources for users to run applications and store data relevant for Python and PHP in terms of compatibility, portability and interoperability. Cloud services could support the CSCs to avoid large capital expenditures associated with infrastructure and software license procurement, real time application support. The main aspect for selecting PaaS is the provision of development options that support the portability, interoperability and compatibility of various applications including Python and PHP. It also supports multiple platforms such as mobile and browser platforms, which serves as an advantage in achieving the company's aspiration to support a platform for an unlimited number of researchers that can be accessed from multiple platforms.

6.2.3. Assets

IT assets owned by the company are classified according to data and tangible assets. The data assets entail the code repository that allows the company to provide open access publication services, store and archive journals online. The data assets are the potential candidates outsourced to the cloud environment because it forms the main substructure that facilitates company activities. The Table 1 below shows the asset category and criticality.

Table 1. Asset categorisation and criticality.

Asset Name	Category	Criticality
Code repository	Confidential	High
Online published papers	Public	High

6.2.4. Risks

The risks based on the scenario are categorised according to:

a **Loss of Integrity:** This refers to unauthorised changes to the source code or intellectual property of the articles either intentionally, maliciously or by accidental acts of a legitimate user.

b **Loss of Availability:** This arises if the mission-critical source code repository and published articles become unavailable to the target users. Other issues deal with loss of essential

functionalities and operational effectiveness such as impeding the end users' to perform their basic functions in supporting the company's goals.

c **Loss of Confidentiality:** This refers to the inability of *TransparentCloud* to protect the data asset from unauthorised disclosure. The impact of this is jeopardising the disclosure of mission-critical tools and private data of publishers. It could result in legal action against the company, public embarrassment as well as compliance issues.

d **Loss of transparency:** Outsourcing the data asset means total loss of control and management of security controls. Lack of transparency and monitoring tools for security operations may hinder the company from observing internal regulatory compliance and security due diligence.

6.2.5. Requirements

The practices that could provide sufficient protection if the source code repository was hosted locally may have included configuration and management of in-house source control server to include security practices such as secure file stores, reduced access rights/level of privileges, password protection, *etc*. However, the potential cloud transition changes this landscape and requires a more robust approach. Table 2 shows the identified requirements from the study context based on the security practice, goals defined in the cloud strategy and control actions for the protection of risks. The domains of CSA's CCM were used as the basis for extracting the requirements owing the fact that CCM provides a clear direction for security in the cloud.

Table 2. List of requirements.

Requirements (Req.)	Controls
Req1: Secure access control, data encryption, vulnerability scans.	Data encryption and integrity checks Secure access controls Vulnerability scans
Req2: Disclosure of all security activities related to the data asset.	Access logs Event notification Audit reports
Req3: Scalability to accommodate a significant and frequency of users.	Scalable platforms
Req4: Backup and redundancy plans, BCP & DRP for continuous availability.	Business continuity management Disaster recovery plans Backup capabilities
Req5: PCI DSS, EU & UK Data Privacy Laws and ISO27001	PCI DSS Compliance EU and UK Data Privacy laws ISO27001

6.2.6. Controls

The examination of security controls explores the basic transparency mechanisms being supported by *TransparentCloud* to disclose security practices. The idea behind this measure is founded on the consideration that CSPs tend to use proactive transparency to provide an overview of their security practices to the general public without having to individually address customer requests before cloud contracts are reached. This form of disclosure makes it almost impossible to ascertain the candid set of controls that safeguard assets specific to the need of the company. Therefore, the security controls of *TransparentCloud* were closely inspected to ensure their existence for which evidences must be provided to support genuine claims. A stimulating facet of this is the ability to collect evidences for identifying variations between the company's requirements and *TransparentCloud's* security offerings so that vital requirements are identified, negotiated and enforced through SLA.

6.2.7. Evidences

We were able to perform an evaluation routine for gathering valuable evidences on how the security controls from *TransparentCloud* are sustained as well as how requirements could be satisfied. Evidences were collected from them providing clear and detailed information on how their security controls are being implemented. It is interesting to note that the evidences were collected from *TransparentCloud's* security whitepapers. Thus, the evidences are categorised in association with the conditions as illustrated in Table 3.

6.2.8. Monitoring

Monitoring activity is very paramount for both fostering and enforcing security transparency principles. Conducting monitoring for the purpose of security transparency requires a number of specifications related to: the targeted controls, the description of the verification to conduct, the means of verification (probe, manual, *etc.*), the reference against which the verification ought to be conducted and, sometimes, the frequency of the verification as depicted in Table 4.

The target of the verification may include the set of controls put by the CSP. For the monitor to be able to perform the required verifications, a base measure is used, that is the set of information related to what would need to be vetted within the controls to make an informed account of its status. Furthermore, a reference or the desired status of the controls would be used by the monitor to detect any mismatch between the controls actual posture and the desirable one. In the context of security transparency, references may be extracted from the SLA clauses, CSP published document, and existing policies. As for the frequency of verification, it is used to determine how often security transparency related information should be relay back to the CSC. Monitoring itself could be done manually by a human auditor on behalf of the CSC or, conducted by software probes that could be an existing security management tool (such as firewall tester, IDS, system vulnerability scanner and so forth) or self-developed programs to audit the operational status of those controls (namely their correctness and existence). Upon the comparison between the reference and the actual posture of the controls, or through direct analysis of the set of evidence available such as logs, the monitor would infer some outcome or derived measure under the form of alert in case of mismatch with what is expected.

Within the context of the company's data assets, it is worth mentioning that not all requirements can be the subject of automated monitoring. In cases where this is not possible, the CSC would be expected to be shown evidence that support the claims of the CSP (e.g., for claim of Data encryption and integrity checks, secure access, vulnerability scan , data backup). Other requirements such as the need for vulnerability scans and integrity checks could be monitored by respectively checking the availability and operational status of tools such as Nessus and by setting up programs that could check the hash of documents with their originals.

Table 3. Evidences of *TransparentCloud's* security controls.

CSC Requirements	CSP Controls	CSP Evidences
Req1	Data encryption and integrity checks	Assets are stored using Advanced Encryption Standard (AES). Customers are supported to use preferred encryption mechanisms to encrypt data before moving assets to *TransparentCloud's* environment. Data integrity checks can be performed by CSCs to protect data using Hashed Message Authentication Codes (HMACs) digital signatures, and Authenticated Encryption (AES-GCM).
	Secure access controls	Advanced data access controls provided to ensure limited access to assets. A multi-factor authentication that uses a combination of name and password credentials for access is provided as an additional layer of security using a device that generates single-use authentication code.
	Vulnerability scans	Regular vulnerability scans are performed on the host operating system, web applications and databases using a variety of tools. Vulnerability patches are regularly fetched from applicable vendors. The environment is regularly assessed for new and existing vulnerabilities and attack vectors by external and internal penetration testers.
Req2	Access logs	Systems are configured to log access to data assets. The access log contains details about each access request type, the requested source, the requestor's IP, time and date of the request.
	Notification	Event notifications relating instances are sent to customers. An email notification service is provided to notify customers when an application status changes or application servers are removed or added.
	Audits	An audit log service feature is maintained that provide valuable insight into who has accessed which asset. The features enable customers to directly view logs in order to verify who has accessed what data and what was done with it. Controls are put in place to support customers' access to the audit logs for dealing with security incidents and investigations.
Req3	Scalability	Load balancers are used to distribute workloads between cloud servers with identical configuration and data. In addition, horizontal and vertical scalability are adopted to support scalability. Horizontal (out) and vertical (up) scaling are used depending on the nature of customer needs as well as resource constraints. More resources are added to the same computing pool that host customer asset through vertical scaling, such as adding more virtual CPU, RAM or disk to handle increased application workload. Also, in some cases, horizontal scaling is used to add more machines or devices to the computing platform in order to accommodate increased customer demand.
Req4	Disaster recovery plan	Various techniques are used for disaster recovery. One of such involves the continuous replication of assets in order to maintain a second version of it. These replicas are transparently backed up off-site in the form of snapshots on multiple devices across multiple facilities. Availability zones are created and dispersed across multiple geographical regions and, in case of failure, automated processes divert traffic away from the affected area to another availability zone.
	Business continuity management	Data redundancy techniques such as image and file-based backups, and automated system failover are implemented at multiple levels. It also includes redundant disks that guard against local disk failure to full data replication across geographically dispersed data centres.
	Data backup	Customers are allowed to perform their own backup using their own backup service provider, and they can also specify which physical region their data will be located in.
Req5	PCI DSS	Certified compliance to the standard.
	EU & UK Privacy Laws	Received broad validation from the European and UK data protection authorities.
	ISO27001	Certified compliance to the standard.

Table 4. Monitoring specification.

Target of Verification	Verifications to Perform			Means of Verification	Derived Measures
	Base Measures Description	**Reference**	**Frequency of Verification**	**Description of Mean of Verification**	**Description of the Verification Outcome**
Data encryption & integrity	Encryption & hash functions	SLA, CSP document	Periodic	Integrity-based remote data auditing	Validate the proof of data intactness in the possession of the CSP.
Secure access	User account authentication & authorisation	SLA, access control policy	Regularly	Automated auditing and logging reports relating to VM and service usage	Verifying legitimate users access and perform authorised changes/modifications.
Vulnerability scans	Internal & external security weaknesses	SLA	Regularly	Cloud security vulnerability scan reports	Address security threats and receive notifications on emerging threats that could harm assets.
Data backup	Backup data, policy	SLA , backup policy	Frequently	Manual review of CSP historical data backup activities and comparison of original data and backed up data.	Verify the frequency at which data is backed up.
PCI DSS, ISO27001 compliance	Relevant control objectives	Compliance report	Demand driven	Periodic review of compliance documents by requesting CSP certificates.	Ensuring conformance to the standards.

6.2.9. Events

The event notification types that are required for receiving notifications when certain security events occur regarding the company's data access pertain to areas relating to data integrity that include:

- Unauthorized access, additions, modifications or deletion of published articles.
- Unauthorized system or application activities to source code repository.
- Audit trail of authorized changes or modifications to data assets.

7. Conclusions

Security transparency is becoming an increasingly important concern for users to entrust CSP for using cloud services while supporting and managing business critical data and applications. Our approach attempts to systematically analyse transparency from an organisational perspective based on fundamental security transparency concepts. In particular, the framework allows users to identify their needs for transparency based on a cloud migration strategy and checks how these needs can be satisfied through the CSP offerings.

To demonstrate the applicability of our framework, we applied it to a real use case scenario. The example shows that the framework sufficiently supports the organisation to analyse their transparency issues based on the cloud migration strategy and checks the CSP offerings for supporting transparency. The example also follows a sequential order according to the levels of abstraction. The importance of addressing the transparency according to levels of abstraction is that it enables us to use a step-by-step process in identifying the crucial concepts that can be used to formulate the basics of security transparency, how those basics are linked to helping users attain transparency requirements in organisational settings, and finally how the concepts can be integrated into a technical process for cloud security transparency.

However, the framework does not outline a detailed process on how to technically translate the requirements into SLA-based monitorable properties for continuous transparency. We are currently working on process development to achieve this, which could also be used to assists users in understanding their transparency needs based on a specific migration context. Moreover, we would like to apply the framework to other use case studies so that we can generalise our findings.

Acknowledgment: This work is partly financed by the Austrian Science Fund (FWF) project No. P26289-N23.

Author Contributions: Umar Mukhtar Ismail and Shareeful Islam contributed to the design and development of the proposed framework, three different level of abstraction, concepts within the levels, and model. Moussa Ouedraogo initiated the idea of the transparency related concepts within the existing organizational settings and then contributed to refinement of the framework and evaluation of case study results. Edgar Weippl contributed to setup the case study and review the whole paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Agarwal, A.; Agarwal, A. The Security Risks Associated with Cloud Computing. *Int. J. Comput. Appl. Eng. Sci.* **2011**, *1*, 257–259.
2. Islam, S.; Ouedraogo, M.; Kalloniatis, C.; Mouratidis, H.; Gritzalis, S. Assurance of Security and Privacy Requirements for Cloud Deployment Model SI: Security and privacy protection on cloud. *IEEE Trans. Cloud Comput.* **2015**. [CrossRef]
3. Ouedraogo, M.; Shareeful, I. Towards the integration of Security Transparency in the Modelling and Design of Cloud Based Systems. In Proceedings of the Advanced Information Systems Engineering Worships, Stockholm, Sweden, 8–12 June 2015.
4. Rak, M.; Casola, V.; Beneditics, A.; Villano, U. Preliminary design of a platform-as-a-service to provide security in cloud. In Proceedings of the 4th International Conference on Cloud Computing and Services Science, Barcelona, Spain, 3–5 April 2014.

5. Santos, N.; Gummadi, K.P.; Rodrigues, R. Towards Trusted Cloud Computing. In Proceedings of the 2009 Conference on Hot Topics in Cloud Computing (Hotcloud), San Diego, CA, USA, 14–19 June 2009.
6. Ouedraogo, M.; Severine, M.; Herve, C.; Steven, F.; Eric, D. Security Transparency: The Next Frontier for Security Research in the Cloud. *J. Cloud Comput.* **2015**. [CrossRef]
7. Ouedraogo, M.; Dubois, E.; Khadraoui, D.; Poggi, S.; Chenal, B. Adopting an agent and event driven approach for enabling mutual auditability and security transparency in cloud based services. In Proceedings of the International Conference on Cloud Computing and Services Science, Lisbon, Portugal, 20–22 May 2015; pp. 565–572.
8. Casola, V.; Benedictis, A.; Rak, M. Security monitoring in the Cloud: An SLA-based approach. In Proceedings of the 10th IEEE International Conference on Availability, Reliability and Security (ARES), Toulouse, France, 24–27 August 2015.
9. Happe, J.; Theilmann, W.; Edmonds, A.; Kearney, K. A reference architecture for multi-level SLA management. In *Service Level Agreements for Cloud Computing*; Springer Service-Business Media: New York, NY, USA, 2011.
10. Krautheim, J.F. Private Virtual Infrastructure for Cloud Computing. In Proceedings of the Hotcloud Conference 2009, San Diego, CA, USA, 14–19 June 2009.
11. Theilman, W.; Yahyapour, R.; Butler, J. Multi-level SLA management for service oriented infrastructures. In Proceedings of the 1st European Conference on Towards a Service-Based Internet, Madrid, Spain, 10–13 December 2008.
12. Koller, B.; Schubert, L. Towards Autonomous SLA Management using a Proxy-Like Approach. *Multiagent Grid Syst.* **2007**, *3*, 313–325.
13. Cloud Security Alliance CloudAudit Security, Trust & Assurance Registry (STAR). Available online: https://cloudsecurityalliance.org/star/certification/ (accessed on 29 August 2015).
14. Jaydip, S. Security and privacy issues in cloud computing. In *Architectures and Protocols for Secure Information Technology*; Information Science Reference: Hershey, PA, USA, 2013.
15. Granados, N.; Gupta, A.; Kauffman, R. The impact of IT on Market Information and Transparency: A Unified Theoretical Framework. *J. Assoc. Inf. Syst.* **2006**, *7*, 148–178.
16. Bushman, R.; Piotroski, J.; Smith, A. What Determines Corporate Transparency? *J. Account. Res.* **2004**, *2*, 207–252. [CrossRef]
17. Kopits, G.; Jon, C. *Transparency in Government Operation*; IMF Occasional Paper, No. 158; International Monetary Fund: Washington, DC, USA, 1998.
18. Andrews, S. What is Security Transparency? Available online: http://www.zdnet.com/article/ what-is-security-transparency/ (accessed on 25 August 2015).
19. Aslam, M. Bringing Visibility in the Clouds. Ph.D. Thesis, Swedish Institute of Computer Science, Stokholm, Sweeden, 2014.
20. Kalloniatis, C.; Mouratidis, H.; Islam, S. Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements. *Requirements Eng.* **2013**, *18*, 299–319. [CrossRef]
21. Kalloniatis, C.; Mouratidis, H.; Vassilisc, M.; Islam, S.; Gritzalis, S.; Kavaklif, E. Towards the Design of Secure and Privacy-Oriented Information Systems in the Cloud: Identifying the major concepts. *Comput. Stand. Interfaces* **2014**, *36*, 759–775. [CrossRef]
22. Pauley, W. Cloud Provider Transaprency: An Empirical Evaluation. *IEEE Secur. Priv.* **2010**, *8*, 32–39. [CrossRef]
23. Doelitzscher, F.; Reich, C.; Knahl, M.; Clark, N. Understanding cloud audits. In *Computer Communications and Networks*; Springer: London, UK, 2013; Chapter Privacy and Security for Cloud Computing.
24. Kosack, S.; Fung, A. Does transparency improve governance? *Annu. Rev. Political Sci.* **2014**, *17*, 65–87. [CrossRef]
25. Islam, S.; Mouratidis, H.; Weippl, E. An Empirical Study on the Implementation and Evaluation of a Goal-driven Software Development Risk Management Model. *J. Inf. Softw. Technol.* **2014**, *56*, 117–133. [CrossRef]