https://doi.org/10.1007/s10207-023-00709-8

REGULAR CONTRIBUTION

A quantitative framework for security assurance evaluation and selection of cloud services: a case study

Ankur Shukla[1] · Basel Katt[1] · Muhammad Mudassar Yamin[1]

Published online: 19 June 2023

Abstract

Due to the high adoption of cloud services, the protection of data and information is critical. Cloud service customers (CSCs) need help to obtain the authoritative assurances required for the cloud services and negotiate the cloud service contract based on the terms and conditions set by cloud service providers (CSPs). Several standards and guidelines are available for assessing cloud security. However, most of these standards and guidelines are complex and time-consuming to select a service or make an informed decision for CSCs. Moreover, the existing methods are insufficient to solve this problem because they are process-oriented, neglect the importance of stakeholder requirements, and lack a comprehensive and rigid analytic method that can aid decision-makers in making the right decisions. In this paper, we developed two evaluation techniques: (i) a quantitative cloud security assurance method to assess the security level of cloud services by measuring the critical security properties and (ii) a novel and rigid categorical analytical method that enables CSPs to identify the major problems in the system and assess how much gain can be achieved by solving each of them. The cloud security assurance method is based on two important metrics: *security requirement* and *vulnerability*. It assists CSCs in avoiding severe mistakes and making informed decisions while selecting a cloud service. Moreover, these methods support CSPs in improving the security level of cloud services and meet customer requirements. The proposed methods are validated using different case scenarios on a private cloud platform.

Keywords Security assurance · Cloud computing services · Security requirements · Security vulnerability · Security testing · Decision making

1 Introduction

With time, software systems become more complex, connected, and dynamic. Cloud computing services provide economic and technological advantages in the smooth operation of these software systems. However, it comes with some disadvantages. Security is a significant concern of organizations, and general customers are looking to move to the cloud or use cloud services. According to a cloud survey report, 82% of respondents consider security the most critical attribute to the organization seeking a cloud solution. This survey also concludes that security and data privacy have become more significant concerns in comparison to cost-efficiency [1]. The CSCs need assurance from CSPs with their data and threats related to integrity, confidentiality, and availability. Therefore, CSPs need to ensure that the security level of the cloud services is acceptable, which requires evaluating the security assurance level continuously and acting upon it.

It is difficult for CSCs to obtain authoritative security assurances they need primarily to protect their data [2, 3]. Standard cloud services from CSPs are designed to meet high-volume needs at affordable prices on shared infrastructure. CSCs face difficulties while negotiating cloud service contracts based on the standard terms and conditions set by the CSPs. It is also a very common trend that CSPs offer services on a take-it-or-leave-it basis. The negotiation also depends on the type of service offered; for example, SaaS services are generally offered without negotiations, whereas negotiation is possible in IaaS services if additional storage or processing capabilities are required. Many security standards and control frameworks such as ISO/IEC 27002 [4], the CSA's Cloud Control Matrix (CCM) [5], and the NIST's SP 800-53 [6] are present to guide CSPs and assist CSCs

✉ Ankur Shukla
shukla395@gmail.com

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), Gjøvik, Norway

in assessing the security assurance and overall security risk. However, these security standards and control frameworks are generally time-consuming to implement, require security expertise, and require considerable effort to prepare evolution evidence [7]. Although they try to bring transparency to clouds, however, results make customers' actions uncertain [8]. The contract terms are also often vague and do not cater to the set of characteristics of clouds [9]. Therefore, it is important to have an easy and flexible method that enables CSCs to compare the services contracts offered by CSPs to avoid making major mistakes. CSPs also need these methods for evaluating and improving the cloud service's security.

There have been several security assurance procedures developed in the past to assess cloud security [10–18]. These contemporary cloud security assessment approaches consider the general cloud security standards, policies, and guidelines that are complex and time-consuming for CSCs. Moreover, the existing methods are insufficient to provide authoritative assurance because they are process-oriented, neglect the importance of stakeholders' requirements, and lack a comprehensive and rigid analytic method that can aid decision-makers in making the right decisions. Therefore, these approaches are not helpful for CSCs to avoid severe mistakes and make informed decisions while selecting a cloud service. Moreover, these methods do not support CSPs in improving the security level of offering cloud service and meeting customer requirements.

This paper presents a quantitative approach to measure the security assurance of cloud services in order to solve this problem. The proposed approach is an extension of our previously developed framework in which two security metrics: Security requirements and vulnerabilities are used to evaluate the security assurance level of REST APIs developed by Statistics Norway [19, 20], and a web discussion forum that was developed [21]. It is not possible to directly apply the existing security assurance framework to the cloud services because cloud services have different security requirements and vulnerabilities. It is also noteworthy that the existing method does not take into account both customer and provider perspectives on security assurance. Moreover, existing security assurance methods are unable to provide insights into the level of security of different components and the action that needs to be taken. Taking these facts into consideration, we developed a security assurance framework for cloud services based on two key metrics: security requirements and vulnerabilities. Risk estimation has been attached to the VM, while importance has been attached to the RM as a weight factor. In addition, a novel rigid and categorical analytical method is developed to enable CSPs to identify the major problems in the system and assess how much gain can be achieved by solving them. The proposed approach allows CSPs to measure and improve the level of security of their service offerings to meet customer requirements.

The rest of the paper is organized as follows: The background and related work on security assurance is discussed in Sect. 2. In Sect. 3, we discuss and develop a security assurance framework for cloud services. A case study is conducted in Sect. 4 on a private cloud platform considering different scenarios. Section 5 analyzes and assesses categorical risks, while Sect. 6 concludes the paper.

2 Background and related works

Security assurance provides the confidence that the system has met and continues to meet its required security objectives. Security assurance is an activity that goes throughout the development life cycle of a system, starting from the initiation phase to the target of evaluation certification. The assurance activities are also important during the operational and maintenance phases to ensure the assurance level of a certified system is maintained [22, 23].

There are some standards developed by the ISO for the cloud computing system and technologies, for example, the cloud computing reference architecture (ISO/IEC 17789: 2014) [24], ISO/IEC 19944-1:2020 [25] for cloud computing and distributed platforms, common technologies, and techniques used in conjunction with cloud computing (ISO/IEC TS 23167:2020) [26], and protection of personally identifiable information (PII) in public clouds (ISO/IEC 27018:2019) [27]. There are several frameworks and benchmarks for ensuring cloud security; for example, Cloud Controls Matrix (CCM) developed by the Cloud Security Alliance (CSA) [28] is designed to assist cloud vendors and prospective customers in assessing cloud security risks. CIS Benchmarks [29] provide cybersecurity practitioners with globally recognized and consensus-driven best practices for implementing and managing cybersecurity defenses. CIS foundation benchmarks deal with the leading cloud service providers, including Oracle Cloud Infrastructure, IBM Cloud, Amazon Web Services, Microsoft Azure, and Google Cloud Platform, for securely configuring cloud environments. These security standards and best practices can be adhered to even when an organization's workloads expand in cloud environments; however, most CSPs are implementing a combination of privacy and security measures. This has caused confusion among users regarding the security measures they expect from their service providers. Due to this, SINTEF [30] has compiled a set of security requirements organized into eight categories based on industry standards and best practices and incorporating requirements from European data protection legislation. Additionally, security issues identified in recent research on Cloud security have been taken into account.

There have been different models and frameworks developed to measure system security assurance in various application domains and operating environments [22, 31–37]. Lan and Han [38] proposed a security assurance development process model for developing the NeoKylin operating system. Such et al. [39] studied different characteristics of assurance techniques such as expertise required, person required, completion time, effectiveness, and cost from the perspective of industry stockholders. Ardagna et al. [40] discussed the need, design, and challenges of assurance methods for IoT-based services. Katt and Prasher [19] developed a quantitative framework of security assurance based on the security requirement and VM. Zhi et al. [41] also developed a quantitative approach to evaluate security assurance. Ardagnan et al. [40] developed continuous security assurance methods for IoT services. Khan and Khan [42] developed a software security assurance model to support organizations in measuring the readiness for the development of secure software. Sakthivel [43] analyzed the advantages of machine learning and deep learning approaches in the security assurance of cyber systems. Wen et al. [44] developed an approach for modeling, calculating, and analyzing security assurance metrics to enhance quantitative security assurance evaluation.

There have been some efforts made in the past on cloud computing security assurance evaluations [11, 45], security controls [12], security transparency and auditing [17], and monitoring and analysis [40, 46]. However, some of these methods are conceptual or do not provide concrete security requirements. These methods also do not focus on evaluating overall security and component-based analysis. A conceptual model framework was developed by Duncan [47] for cloud security assurance, monitoring how effectively the operational layer meets the declarative layer's goals and confirming the whole system is working and reaching its objectives. Islam et al. [48] discussed a conceptual framework to elicit security and privacy requirements. They introduced assurance as evidence for satisfying the security and privacy requirements in terms of completeness and reportable of a security incident through the audit. Using this method, cloud users can define their assurance requirements and select the suitable cloud model for the situation at hand. The proposed approach focused on selecting the security and privacy requirements. Kumar and Goyal [49] developed a three-dimensional cloud security model that combines security solutions, operations, and compliance. The proposed model is conceptual and does not provide a concrete method. A comparison of the proposed work and some related works is given in Table 1.

The existing cloud security methods are also focused on some specific challenges such as transparency [15], portability [15], encryption time, decryption time, total authentication time [18], authentication level, level of uptime, logs retention period, third party authentication support, and certifications and compliances [50]. Rizvi et al. [15] discussed the challenges related to the data security and privacy of cloud service users. They developed a method that helps CSCs to select services based on their security requirements. They proposed a framework to evaluate the security of the service provided by the CSPs according to the user's requirements. However, this work mainly focused on security auditing. Pachala et al. [18] proposed a hybrid approach for security and privacy of cloud in a distributed environment to avoid un-trusted service providers of the cloud to protect private or essential data. They mainly focused on security issues like encryption, decryption, total authentication, and memory utilization. Maroc and Zhang et al. [50] proposed a framework for evaluating multi-tenant cloud services that consider the different quality of service classes. This framework considers the preferences and requirements of the tenants, as well as their importance level. They do not focus on the systematic method of security assurance and defining concrete AMs or how to assist CSPs in improving the security level of their cloud offerings.

A few quantitative cloud security assurance methods have also been developed based on several security requirements. Rios et al. [45, 51] considered the security assurance challenges of multi-cloud applications that consume and orchestrate services from multiple independent Cloud Service Providers. As a result, they introduced a MUSA DevOps approach for securing multi-cloud applications early in their lifecycle, allowing developers to take corrective actions as soon as possible, whenever necessary. This paper does not focus primarily on evaluating the overall security assurance level quantitatively and supporting CSCs and CSPs in making decisions. Halabi et al. [52] developed a methodology that helps CSPs perform security self-assessments and assess the level of their security services to identify their limitations and improve them. The proposed methodology uses a set of quantitative metrics to evaluate cloud security services. However, the paper does not focus on evaluating the overall security assurance level, component-based analysis, and supporting CSCs and CSPs in making decisions. Ismail and Islam [17] developed a framework for cloud security transparency and audit tool that enables users to gather and analyze cloud providers' evidence to determine compliance with requirements and specify remedies. Despite this, they do not focus on assessing the level of security assurance provided by CSPs and the level of security assurance based on the customer's preferences. However, these methods have considered a minimal set of security requirements, do not provide a security assurance level, component-based analysis, or focus on either CSCs or CSPs.

Table 1 Comparison of the proposed framework with some related works

Paper	Security assurance	Security requirements/ Threats profile	Summary	Standards/ Guidelines	Quantitative	Assurance level	Component based analysis	CSPs support	CSCs support	Other limitations
[45, 51]	SLA-security assurance	Different security controls including Information input validation Penetration testing Vulnerability scanning Least privilege Process isolation DoS protection Separation of duties	A methodology was developed to detect non-compliance with CSP's and components' SLAs so that corrective actions could be taken	The NIST Control Framework	No	No	No	Yes	No	This paper does not focus on quantitatively evaluating the overall security assurance level and supporting CSCs and CSPs in making decisions.
[52]	Quantitative evaluation of security of CSPs	Authentication Authorization and access control Web application security Network security Data and storage security Virtualization security Physical security Data and computing integrity Data availability Service availability Security auditing and testing	Evaluation methodology for cloud security services that can assist CSPs in self-evaluation	NIST	Yes	No	No	Yes	No	This paper does not focus primarily on evaluating the overall security assurance level, and the control questions regarding security requirements are detailed.

Table 1 continued

Paper	Security assurance	Security requirements/ Threats profile	Summary	Standards/ Guidelines	Quantitative	Assurance level	Component based analysis	CSPs support	CSCs support	Other limitations
[17]	Cloud security transparency and audit	-Data breach Weak identity, credential and access management Insecure APIs System and application vulnerabilities Malicious insiders Advanced persistent threats (APIs) Data loss Insufficient due diligence Abuse and nefarious use of cloud services DoS Shared technology vulnerabilities	Provide support for achieving security transparency, which can potentially improve businesses' trust in cloud computing.	CSA CCM	Partial	No	No	Yes	No	This paper does not focus primarily on evaluating the overall security assurance level, the security requirements are limited, and control questions are not detailed.
Proposed framework	Quantitative security assurance	-Data storage: Back-up, encryption, location, isolation, ownership -Data processing: Isolation, monitoring, location, migration, encryption data transfer: Encryption, integrity, non-repudiation, isolation, location, monitoring -Access control: Management access control, user access control, Physical access control Security procedure: Auditing, classification, countermeasures, testing, detection, notification, recovery Event management: Response, logging, reporting, forensics Privacy: nondisclosure, anonymity, data minimization, data processing agreement Third-party services	A quantitative cloud security assurance method to assess the security level of cloud services, and (ii) a novel and rigid categorical analytical method to support CSPs in decision making.	Different industry standards and best practices including ISO, NIST, CSA CCM [30] Requirements from European data protection legislation, Security issues identified in recent research on cloud security	Yes	Yes	Yes	Yes	Yes	

3 Cloud security assurance framework

In this section, we developed a general security assurance framework for cloud computing services. This framework is designed to measure the level of security of cloud services offered by CSPs.

In this paper, we developed a security assurance framework for cloud computing services by extending our framework [19, 20]. Furthermore, a novel categorical analytical method is proposed to allow CSPs to identify the system's primary problems and determine how much gain may be realized by solving each of them. The developed framework utilizes the security requirements and vulnerabilities to determine the level of security assurance for a cloud. It helps CSCs analyze and compare the security levels of cloud services and their different components and make the appropriate decision. It also allows CSPs to offer a secure product that fulfills the requirements of the customers. The developed framework has the following basic components:

3.1 Security assurance profile

An assurance profile is a description that contains the security objectives of the system to be analyzed based on the expected level of security of the system. The framework contains the following set of security objectives:

(i) security requirements and compliance with set of conditions, and
(ii) potential vulnerabilities, threats and their conditions of existence.

In this paper, we have considered two security metrics as a part of the assurance profile (i) security requirements and (ii) vulnerabilities. The assurance profile includes the terms of security requirements and their fulfillment, as well as potential vulnerabilities and their existing conditions for cloud computing services. It also suggests a way to check the conditions of security requirements and vulnerabilities. A detailed discussion of these two security metrics is given as follows:

(i) Security requirements:

The CSCs or organizations that are using cloud computing services or planning to move to the cloud are concerned about the security of the services. The contracts for cloud services are typically drafted according to the provider's standard terms and conditions, and many CSCs face difficulties in negotiating the terms of their contracts. The standards and guidelines for cloud security services are very complex, time-consuming, and challenging to comprehend by a customer. On the other hand, CSPs need to evaluate the security of their service and provide evidence to the customer so that they can compare the security level of the services and make a relevant decision.

The cloud security requirements checklist that an organization or CSCs should consider when dealing with cloud services has been identified by SINTEF [30]. Several other security requirements for cloud services such as OpenStack [53], Amazon [54], Microsoft Azure [55], and SINTEF [30] have been reviewed, and the security requirements of SINTEF has been selected because it covers and impose conditions on several aspects of the cloud security. The content has been collected from established industry standards and best practices such as NIST, Cloud Security Alliance, FedRAMP, and ENISA, supplemented with requirements from European data protection legislation, and considering security issues identified in recent research on Cloud security. The requirements in the document have been organized in terms of whether they are related to data storage, data processing, data transfer, access control, security procedures, incident management, privacy, or third-party services. The details of these security requirements with their goal and control questions are given as follows

(a) *Data storage requirements* The data storage requirements are about how the user's data is handled and ensure that backup, storage, isolation, and secure data removal are appropriately performed. The details of control questions for this category of security requirement are given in Table 2.
(b) *Requirements for data processing* In data processing requirements, it has been ensured that data in use are not mixed with the memory so that users can only access their data and cannot be accessed or overwritten by others. This is important for maintaining the confidentiality and integrity of all users' data. The details of control questions for the requirements for data processing are given in Table 3.
(c) *Data transfer requirements* The data transfer requirements have ensured that data transition is encrypted and allows the users to decide the networks on which the data should be sent. The details of control questions for the data transfer requirements are given in Table 4.
(d) *Requirements for access control* It is important to maintain access control in order to protect the data effectively. Access control policy guarantees the users who are who they specified they are, and they have proper access to the data. Requirements for access control ensure the creation, updating, suspension, and deletion of user accounts appropriately. The details of control questions for the requirements for access control are given in Table 5.

Table 2 Data storage requirement

Goals	Control questions
1.1. *Make sure that backup is being performed correctly.*	1.1.1. Are backups performed at fixed time intervals?
	1.1.2. Will backups be tested at fixed time intervals?
	1.1.3. Are backups stored in different locations physically?
	1.1.4. Is user data restricted to the production environment of the cloud?
1.2. *Make sure that data never gets stored in clear text*	1.2.1. Is all data stored on disk encrypted?
	1.2.2. Is it allowed to store already-encrypted data?
	1.2.3. Does each user have a unique encryption key to encrypt their data?
	1.2.4. Are the encryption keys generated by the cloud?
	1.2.5. Are the encryption keys stored by the cloud?
1.3. *Ensure that data is isolated from others using data*	1.3.1. Does the cloud ensure that all data is segregated from other data?
	1.3.2. Are all data stored on dedicated servers?
	1.3.3. Are all data stored on a segregated infrastructure?
1.4. *Ensure accuracy and context of the user's data*	1.4.1. Is the integrity of all data stored in the cloud maintained?
1.5. *Make sure secure deletion of the user data*	1.5.1. Are all duplicates of data marked for deletion, deleted within a given time frame?
	1.5.2. Are data marked for deletion, deleted by an efficient method?

Table 3 Requirements for data processing

Goals	Control questions
2.1. *Ensure that the user data is separated from other users data*	2.1.1. Are user data separated into memory (RAM)?
	2.1.2. Do the cloud has mechanisms that ensure that the virtual machines cannot interfere with each other?
	2.1.3. Are the users' applications running on a segregated infrastructure?
2.2. *Ensure that any breakage of accepted "terms of use" can be detected*	2.2.1. Are the behavior of virtual machines and applications monitored continuously?
2.3. *Ensure that the transfer of virtual machines between physical machines takes place in a secure manner*	2.3.1. Is all data encrypted while the migration of virtual machines is in progress?

Table 4 Data transfer requirements

Goals	Control questions
3.1. *Ensure that data never being transmitted/sent in clear text*	3.1.1. Will uploading and downloading of customer data be encrypted?
	3.1.2. Is all data sent between different modules in the cloud service encrypted?
3.2. *Make sure that the recipient can't refuse the data reception*	3.2.1. Does the user know for sure that data has been uploaded to the cloud?
3.3. *Ensure that users data is separated*	3.3.1. Does the cloud offer network isolation between tenants?
	3.3.2. Do users decide which data to send over defined network sections?

(e) *Requirements for security procedures* A proactive part of security is always about being one step ahead of the attackers; therefore, it is essential to have security procedures that prevent attacks. The requirements for security procedures deal with the type of security that has already been implemented. It includes vulnerability scans periodically, informing users about vulnerabilities, updating security breaches, and documentation. The details of control questions and the requirements for security procedures are given in Table 6.

(f) *Requirements for event management* If an attack occurs, it is essential to have procedures to deal with it. Event management requirements are planning responses to security attacks, logging user actions, and system recovery after an event. It is a process to identify, gather, monitor, and report security-related events in the system. The details of control questions for the requirements for event management are given in Table 7.

(g) *Privacy requirements* Privacy requirements deal with how the cloud handles its users' privacy. The details of

Table 5 Requirements for access control

Goals	Control questions
4.1. *Make sure secure access to Horizon (dashboard)*	4.1.1. Does the cloud impose on users a set of approved password creation requirements?
	4.1.2. Does the cloud support multi-factor authentication?
	4.1.3. Does the cloud offer third-party authentication?
	4.1.4. Does the cloud require the written consent of the user, who gives permission to process the user's files?
4.2. *Secure access to the cloud services for the users*	4.2.1. Is there a system that allows creation, updating, suspending and deleting user accounts?
	4.2.2. Is it possible to remove access to employees when they leave organizations or reset forgotten or stolen passwords?
	4.2.3. Do all users of the cloud have their own user account?
4.3. *Ensure that the data center is well secured*	4.3.1. Is the data center well physically secured using fences/guards/ surveillance cameras / locks?
	4.3.2. Is the data center limited to authorized personnel?
	4.3.3. Have the employees who maintain the cloud and who have access to user data undergone a background check?
	4.3.4. Is access to application, program or source code restricted to authorized personnel?

control questions for the privacy requirements are given in Table 8.

(h) *Requirements for third-party services* Third-party service requirements include analyzing and addressing the risk associated with third-party vendors or CSPs. The details of control questions for third-party services' requirements are given in Table 9.

(i) Security vulnerability Security vulnerability is a crucial factor in security assurance measurement. A vulnerability metric (VM) can be determined by assessing whether the existing vulnerability can be exploited and the severity of the vulnerability. The CSCs must consider the number of vulnerabilities while considering cloud computing services. In this paper, we have conducted a case study considering the OWASP's [56] top 10 vulnerabilities. On the other hand, CSPs should also demonstrate whether the offered services are protected against these vulnerabilities and what level of security they offer against these vulnerabilities. The severity of the detected vulnerabilities can be identified using the Common Vulnerability Scoring System (CVSS) [57], which is the industry standard for quantifying the severity of system vulnerabilities. CVSS assigned the numeric values between 0 and 10, reflecting the severity of a vulnerability. CVSS consists of three different measurement groups:

- Base score
- Temporal score, and
- Environmental score.

Each of these groups handles aspects of what needs to be weighed/quantified to obtain a complete picture of vulnerabilities. Each group's severity is measured on a scale from 0 to 10. Severity scores help to determine what needs immediate attention and what can be tolerated. In the security assurance scheme, weights for each security requirement and the risk of each vulnerability or threat are specified. Certain details about the design of the cloud and its environment can also be included in the scheme.

3.2 Assurance target

An assurance target is a system under evaluation for which the assurance level is assessed. In our case, the cloud is the assurance target. It is necessary to deploy the system in a real-world environment to measure its security level accurately.

3.3 Assurance metrics

The assurance metric (AM) is the quantitative representation that provides evidence that the cloud meets a particular level of security. AM provides a clear overview of how well the cloud fulfills the security requirements and the existence of vulnerabilities. Additionally, we can apply a statistical test and make applicable statements and decisions regarding the security needs in the cloud.

3.3.1 Quantification of the AM

The goal question metric (GQM) is a method that helps to quantify the fulfillment of security requirements and the

Table 6 Requirements for security procedures

Goals	Control questions
5.1. *Make sure that the cloud has regular audit of the system*	5.1.1. Can the user revise their own activity?
	5.1.2. Are the cloud users regularly updated on the security of the system?
5.2. *Ensure that the cloud accommodates one specific classification/standard/certification*	5.2.1. Does the cloud follow third-party certification (e.g., ISO 27001-052)?
	5.2.2. Is a risk assessment carried out on the cloud in accordance with approved standards?
5.3.*Provides the cloud for that it is implemented defense mechanisms*	5.3.1. Has a firewall been set up and configured?
	5.3.2. Have any mechanisms that protect against DoS/DDoS been set up and configured?
	5.3.3. Are there any mechanisms that prevent data loss?
	5.3.4. Are there regular updates with the latest patches?
	5.3.5. Has redundant scaling of the service been set up?
5.4. *Ensure that security to the cloud can be tested*	5.4.1. Will regular vulnerability scans be run?
5.5. Ensure that hacker attack on the cloud can be identified	5.5.1. Has an IDS been set up and configured?
	5.5.2. Are disks, memory, and networks regularly scanned for malicious software?
	5.5.3. Are procedures established for monitoring and regularly reviewing logs?
5.6. *Ensure that users receive information about security-related changes*	5.6.1. Does the cloud inform users about existing vulnerabilities?
	5.6.2. Does the cloud inform users about patches and existing security mechanisms?
5.7. *Ensure that the cloud can be recovered from an attack*	5.7.1. Does the cloud maintain periodic hotspots for virtual machines?
	5.7.2. Can the cloud guarantee that the system is up and running well within a given time frame?
5.8. *Secure and correct handling of encryption keys*	5.8.1. Are efficient methods used to generate, exchange, store, protect and replace encryption keys?
5.9. *Secure access to the cloud and its security mechanisms*	5.9.1. Are the design and security mechanisms of the cloud documented?
	5.9.2. Will users be informed in writing if the cloud is to make changes to the security architecture?

existence of vulnerabilities. In this method, we set different questions based on the goals and answers of these questions to help to represent the measurable metrics. GQM can be defined in three structured levels, which are

- Conceptual level (Goal): It defines sub-goals that help to identify the fulfillment of a security requirement or the existence of a vulnerability.
- Operational level (Question): In this level, a set of questions is used to characterize the assessment/achievement of a defined goal that is going to be performed. Questions help in the characterization of measurement objects considering the quality issues.
- Quantitative level (Metric): A set of data associated with the quantitative answer to each question based on the fulfillment/existence.

3.4 Assurance technique

The assurance technique is used to evaluate and assess the security assurance level of the assurance target. Several methods, such as review, observation, interview, independent validation, and testing, can be found in the literature [39]. In this framework, the following security assessment techniques have been used:

- Interviews and surveys with key personnel are conducted to identify relevant system components and implemented controls and determine the importance of security requirements.
- Risk calculation to discover vulnerabilities using the CVSS methodology.
- Testing to uncover potential vulnerabilities in the system.

Table 7 Requirements for event management

Goals	Control questions
6.1.*Ensure that there is a event management system*	6.1.1. Has the cloud implemented mechanisms for monitoring and quantifying the event type, volume and related cost?
	6.1.2. Is the severity of an event classified according to a well-defined scale?
	6.1.3. Has the cloud planned corrective responses, based on the severity scale, within given time frames?
	6.1.4. Does the cloud use a recognized event management method (such as NIST SP 800-61 or ISO 27035)?
6.2. *Ensure that the cloud logs security incidents*	6.2.1. Has the cloud logs off user logins, authorized and unauthorized login attempts, system and security incidents?
	6.2.2. Has the cloud made logs of relevant information available to the user?
6.3. *Make sure the security incidents are reported to the users*	6.3.1. Are security incidents reported to users within a given time frame?
	6.3.2. Are all incidents reported via a predefined communication channel?
	6.3.3. Does the cloud send data about an event that has occurred to only those concerned?
	6.3.4. Does the cloud notify the recovery process at any given time interval?
	6.3.5. Does the cloud notify when the remaining recovery time is complete, at given time intervals?
6.4. *Ensure that the cloud facilitates for data analysis*	6.4.1. Does cloud deliver the proof if there is an event that requires legal action?
	6.4.2. Does the cloud comply with legal requirements for handling data and evidence from security incidents in accordance with liability?

Table 8 Privacy requirements

Goals	Control questions
7.1. *Ensure that the user's data kept private*	7.1.1. Is there a policy that specifies the circumstances under which the cloud can access users' data?
	7.1.2. Does the cloud transfer User's data to third parties
7.2. *Ensure that users remains anonymous*	7.2.1. Does the cloud reveal details about the users of third-party companies?
	7.2.2. Does the cloud share the shared log with other users?
7.3. *Make sure unnecessary data of any users are not collected*	7.3.1. Does the cloud require minimal data to perform a service?

Table 9 Requirements for third-party services

Goals	Control questions
8.1. *Requirements for services from third parties companies*	8.1.1. Has the cloud hired services from third-party companies?
	8.1.2. Is the entire infrastructure for the service provided by the same provider?
8.2. *Ensure that the user can control how the service is built up*	8.2.1. Will the user be informed if the composition of the service changes?
8.3. *Make sure you two or more services not being delivered by same third party*	8.3.1. If services are hired, will two or more services be provided by the same third party?

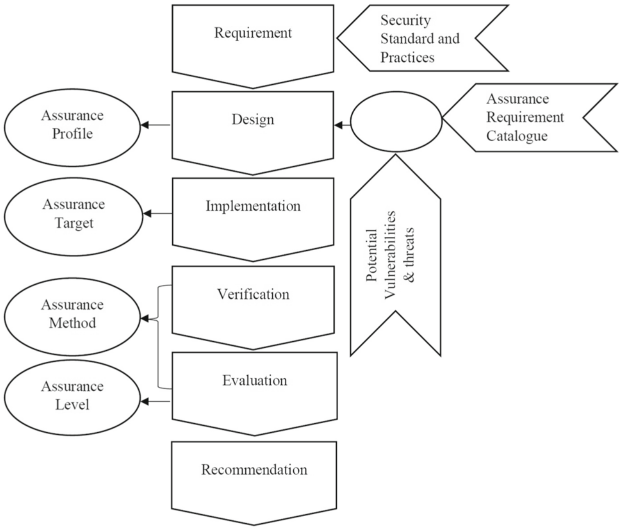

Fig. 1 Security assurance framework

The security assurance framework is given in Fig. 1.

3.5 Evidence evaluation

The evaluation of evidence is a process of measuring the level of security assurance by applying assurance techniques to the assurance target. In this paper, the security assurance metric (AM) is formulated as a mathematical equation that is a function of requirement metrics (RM) and vulnerability metrics (VM).

The AM can be formulated as follows:

$$\mathrm{AM} = \mathrm{RM} - \mathrm{VM} = \sum_{i=1}^{m} \mathrm{RM}_i - \sum_{k=1}^{n} \mathrm{VM}_k \tag{1}$$

where RM_i is the RM that represents the i^{th} security requirement considered for assurance target, for $i = 1, 2, 3, ...m$, and VM_k is the VM that represents the k^{th} vulnerability considered in security assurance measurement, for $k = 1, 2, 3, ...m$.

The RM depends on the fulfillment of control questions and test cases designed to measure the security requirements. Therefore, RM can be formulated as a function of fulfillment factor. Let f_{ij} be the fulfillment factor of j^{th} control question of i^{th} requirement, then RM can be defined as follows:

$$\mathrm{RM}_i = \left(w_i \times \frac{\sum_{j=1}^{p} f_{ij}}{p} \right), \tag{2}$$

where w_i is the weight and p is the number of control questions for the i^{th} security requirement.

VM depends on the existence of vulnerabilities and their risk factor. Therefore, VM can be formulated as a function of the existence factor and risk factor of vulnerabilities. The existence of each vulnerability is estimated by conducting some test cases. Let e_{kl} be the existence factor of the l^{th} test case defined for the k^{th} vulnerability, then VM can be defined as follows:

$$\mathrm{VM}_k = \left(r_k \times \frac{\sum_{l=1}^{q} e_{kl}}{q} \right), \tag{3}$$

where q is the number of test cases defined for the k^{th} vulnerability and r_k is the risk factor.

4 Case study

This section implements the security assurance framework on a private cloud platform. This case study includes one cloud service platform, and four CSCs. We have validated our proposed model by interviewing the system owner and IT staff operating the private cloud platform, and the result confirms their expectation. We conducted systematic penetration testing for the vulnerability part using the OWASP guide and test cases.

The proposed framework is compared theoretically with the related work, as shown in Table 1. It is difficult to compare the proposed framework with the case study because the related works are based on limited security requirements and/or threat profiles and the control questions are not detailed. Furthermore, most of these methods do not focus on quantifying the overall security assurance level and supporting CSCs and CSPs. On the other hand, the proposed framework considered the comprehensive security goals and control questions for eight categories of security requirements, and different vulnerabilities.

4.1 Architecture and structure

OpenStack is a multi-tenant virtualization platform. It provides various virtualization services to the users where they can create their networks, routers, and virtual machines; for example, a single virtual machine with an operating system of their choice. The private cloud considered in this paper is composed of several OpenStack [1] modules and support services such as databases, message queues, configuration management, and monitoring tools. The OpenStack platform comprises different modules such as Horizon, Nova, Keystone, Glance, Cinder, Neutron, Heat, and Swift. It provides

[1] https://www.openstack.org/.

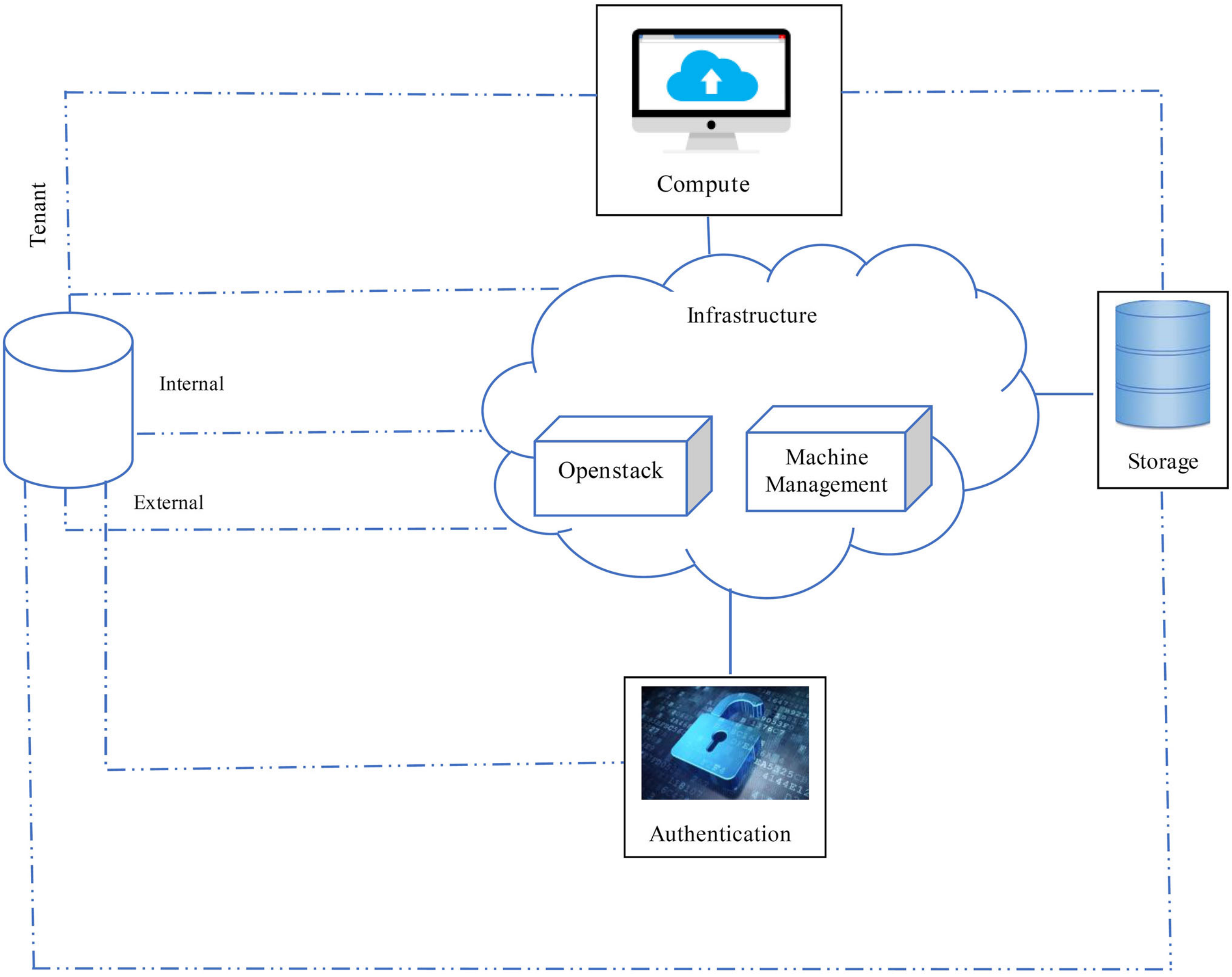

Fig. 2 The private cloud infrastructure

services that allow to plug and play components based on the requirements.

The entire architecture of the private is connected through a router. Most OpenStack modules and the underlying support services are connected to the network and infrastructure. Some components are connected to more than one network; for example, ceph-mon is connected to the infrastructure and storage. As we can see in Fig. 2, infrastructure is the primary network to which all OpenStack modules are connected and is the backbone of the entire infrastructure. Storage handles all the cloud storage. Other important components of this infrastructure are authentication, physical access, and neuron net/tenant.

Figure 2 demonstrates how the various components are connected.

4.2 Security assurance evaluation

In this section, security assurance is evaluated for the assurance target, i.e., a private cloud platform which is operational. Therefore, it is not a beneficial testing environment. Because of this, the testing has been performed on a simulated environment. This simulated environment is a test environment where administrators test the codes before scrolling out to the cloud platform.

Security assurance evaluation has been divided into two parts: the first part discusses general security assurance evaluation, and the second part discusses security assurance evaluation based on customer requirements.

4.2.1 CSP-based security assurance evaluation

The general security assurance has been evaluated considering the security requirements and vulnerabilities. It is

Table 10 Example of security requirement verification and quantification

S.No.	Control questions	Status	Score
1.1.1.	Are backups performed at fixed time intervals?	Partially fulfilled	0.5
1.1.2.	Will backups be tested at fixed time intervals?	Not fulfilled	0
1.1.3.	Are backups stored in different locations physically?	Partially fulfilled	0.5
1.1.4.	Is user data restricted to the production environment of the cloud?	Fulfilled	1

Table 11 Fulfillment of security requirements for the private cloud platform (✓: Fulfilled, ○: Partially fulfilled, ✗: Not fulfilled)

Data storage	Data processing	Data transfer	Access control	Security procedure	Event management	Privacy requirements	*Third-party Service*
1.1.1 ○	2.1.1. ✓	3.1.1. ✓	4.1.1. ✓	5.1.1. ✓	6.1.1. ✗	7.1.1. ✓	8.1.1. ✓
1.1.2. ✗	2.1.2. ✓	3.1.2. ○	4.1.2. ✗	5.1.2. ✗	6.1.2. ✗	7.1.2. ✓	8.1.2. ✓
1.1.3 ○	2.1.3. ✗	3.2.1. ✓	4.1.3. ✓	5.2.1. ✗	6.1.3. ✗	7.2.1. ○	8.2.1. ✓
1.1.4. ✓	2.2.1. ○	3.3.1. ✓	4.1.4. ✗	5.2.2. ✗	6.1.4. ✗	7.2.2. ✓	8.3.1. ✓
1.2.1. ✗	2.3.1. ✓	3.3.2. ✓	4.2.1. ✓	5.3.1. ✓	6.2.1. ✓	7.3.1. ✓	
1.2.2. ✓			4.2.2. ✓	5.3.2. ○	6.2.2. ○		
1.2.3. ✗			4.2.3. ✓	5.3.3. ✓	6.3.1. ✓		
1.2.4. ✗			4.3.1. ✓	5.3.4. ✓	6.3.2. ✓		
1.2.5. ✗			4.3.2. ✓	5.3.5 ✓	6.3.3. ✓		
1.3.1. ✓			4.3.3. ✗	5.4.1. ✗	6.3.4. ✓		
1.3.2. ✓			4.3.4. ✓	5.5.1. ✓	6.3.5. ✓		
1.3.3. ✗				5.5.2. ✗	6.4.1. ✓		
1.4.1. ✓				5.5.3. ✓	6.4.2. ✓		
1.5.1. ✓				5.6.1. ○			
1.5.2. ✗				5.6.2. ○			
				5.7.1. ✗			
				5.7.2. ✓			
				5.8.1. ○			
				5.9.1. ✓			
				5.9.2. ✓			

considered as security assurance of the cloud services offered by the CSPs. CSPs offer services based on their terms and conditions, and customers consider their priorities when choosing a cloud service and negotiate accordingly. Therefore, CSPs do not prioritize the security requirements of the various components of cloud services. However, CSPs must test the security level of their services. As we discussed in the last section, we evaluated CSP-based security assurance as follows:

(i) Security requirements verification

In this case study, we verify and quantify the security requirements for the private cloud platform based on the GQM method. Since this is the general security assurance, equal weight has been assigned to each security requirement. To quantify the security requirements, a numerical value has been assigned to each control question, which reflects how well the security requirement has been fulfilled, for example:

- 1, indicates that the requirement is fulfilled.
- 0.5, indicates that the requirement is partially fulfilled.
- 0, indicates that the requirement does not fulfill.

For example, for the "data storage" security requirements, there are five goals related to backup, encryption, isolation, location, and ownership, and there are several control questions related to each goal. We verified each security requirement and assigned different scores based on its status. An example of the security requirement verification and quantification process is given in Table 10. The details of the security requirements and their verification results for the private cloud platform are given in Table 11.

(ii) Vulnerability testing

As discussed in the previous section, the VM will be measured based on whether the existing vulnerability can be exploited and how severe it is to the system. Security vulnerabilities have been considered from the OWASP's [56] top 10 vulnerabilities list, which are

(a) *SQL injection:* SQL injection is considered as one of the most common attacks. An injection attack is where databases and other systems are vulnerable to such an extent that one attacker can inject unwanted SQL queries into the system. It has been performed as follows: open a web browser, navigate the user interface, and enter an SQL query in the login field. We entered five different queries into the login field that are given in Table 23 of Appendix A.

(b) *Poor authentication:* Poor authentication means enough controls have not been implemented for the users' authentication, allowing attackers to abuse this, bypass trust limits, and compromise passwords, keys, and sessions. This can further be used to exploit other implementation flaws and allow an attacker to take over others' accounts. A detailed description of tests for testing the poor authentication and corresponding score are given in Table 24 of Appendix A.

(c) *Exposure to sensitive data:* Applications that do not handle sensitive data appropriately, such as not encrypting it during storage and transfer, make it easier for attackers to steal or modify data. A detailed description of the number of tests considered for testing the poor authentication and the corresponding score are given in Table 25 of Appendix A.

(d) *Poor access control:* The access control defines what contents and features should be accessible to users. Due to poor access control, the user can navigate the restricted resources. A detailed description of the number of tests considered for testing the poor authentication and the corresponding score are given in Table 26 of Appendix A.

(e) *Incorrectly configured security:* Secure configuration of the application, server, and database is essential. Configuration can be done after a standardized checklist, and often the administrator needs to remember to configure all these. A detailed description of the number of tests considered for testing the poor authentication and the corresponding score are given in Table 27 of Appendix A.

(f) *Cross-site scripting (XSS):* XSS occurs when an attacker sends code to the database, which a user later retrieves. The actual attack appears when users visit the browser containing the malicious code. Therefore, it is important to use validation and sanitation of input data to avoid such attacks. A detailed description of the number of tests considered for testing the poor authentication and the corresponding score are given in Table 28 of Appendix A.

(g) *Cross-site request forgery (CSRF):* CSRF attacks exploit that the user is authenticated, and all requests from the user were requested by the user. Sending requests on behalf of the user and performing actions the user has not requested, exploit other sites. A detailed description of the number of tests considered for testing the poor authentication and the corresponding score are given in Table 29 of Appendix A.

(h) *Denial-of-Service (DoS):* DoS is an attack where the attacker aims to disrupt traffic to a specific server, service, or network by overwhelming it with so many requests that it can no longer handle the traffic and eventually crash. A detailed description of the number of tests considered for testing the poor authentication and the corresponding score are given in Table 30 of Appendix A.

Several tools such as Nessus ,[2] OpenVAS ,[3] Nmap ,[4] and GoldenEye [5] have been used to find out the vulnerabilities present in the cloud platform. Nessus and OpenVAS are used to scan vulnerabilities, and Nmap is used to map the devices in the network and find open protocols, hosts detecting, open port, servers, routers, and switches. GoldenEye is a tool for testing how the system responds to DoS attacks.

(iii) Calculation of AM

AM is calculated based on RM and VM as follows:

(a) *RM* The RM is calculated using the formula given in Eq. (2). An overview of security requirements testing results and calculated RM are given in Table 13. The RM for each security requirement is the average of points assigned based on the fulfillment of control questions of the respective security requirements. As given in this table, the calculated RM ($\mathrm{RM}_{calculated}$) is 58.5.

(b) *VM* Table 14 provides a detailed overview of the existence of the vulnerabilities and calculated values of the VM using Eq. (3). This table represents the total number of test cases used for each vulnerability, the average score per vulnerability, the corresponding CVSS score, and the result. The calculated value of the VM is 6.2.

(c) *AM*
Assurance metric can be calculated using Eq. (1) as follows: AM = RM-VM= 58.5–6.2 = 52.3. The maximum AM one can get with the same security requirements

[2] https://www.tenable.com/downloads/nessus.

[3] http://www.openvas.org/.

[4] https://nmap.org/download.html.

[5] https://sourceforge.net/projects/goldeneye/?source=typ_redirect.

Table 12 Security requirements testing results and RM for CSP

Security requirements	Control questions	Fulfilled	Partially fulfilled	Unfulfilled	Sum of points	Average	Weight	Result (RM_i)
Data storage	15	06	02	07	7	0.47	10	4.7
Processing of data	5	03	01	01	3.5	0.7	10	7.0
Data transfer	5	04	01	0	4.5	0.9	10	9.0
Access control	11	08	00	03	8	0.73	10	7.3
Security procedure	20	10	04	06	12	0.6	10	6.0
Event management	13	08	01	04	8.5	0.65	10	6.5
Privacy	5	3	02	00	4	0.8	10	8.0
Third-party services	4	4	00	00	4	1.0	10	10.00
Sum	78	46	11	21				58.5

Table 13 Vulnerability testing results and VM

Vulnerability	Total sum	Number of tests	Average	CVSS score	Result (VM_i)
SQL injection	0	5	0	8.2	0
Bad authentication	0	19	0	5.8	0
Exposure to sensitive data	0	1	0	5.5	0
Poor access control	0	10	0	8.5	0
Incorrectly configured security	0	5	0	8.8	0
Cross-site scripting (XSS)	0	1	0	4.6	0
Cross-site request forgery	0	1	0	5.0	0
DoS	1	1	1	6.2	6.2

Table 14 Security requirements weights results and RM

Security requirements	Weights			
	Customer 1	Customer 2	Customer 3	Customer 4
Data storage	8	6	10	3
Processing of data	8	3	5	8
Data transfer	7	9	5	10
Access control	8	10	10	7
Security procedure	5	10	10	4
Event management	6	8	5	4
Privacy	8	10	10	10
Third-party services	8	9	5	10

and vulnerabilities for the private cloud platform is 80. The minimum AM one can get using the same security requirements and vulnerabilities consideration is −52.6. This result is complex to interpret; therefore, the calculated value of AM is normalized for a more comprehensive and understandable value. For normalization, the min-max normalization technique has been used, which is:

$$\overline{\mathrm{AM}} = \frac{\mathrm{AM} - \mathrm{AM}_{\mathrm{Min}}}{\mathrm{AM}_{\max} - \mathrm{AM}_{\mathrm{Min}}} (\mathrm{AM}_{\mathrm{newmax}} - \mathrm{AM}_{\mathrm{newmin}}) + \mathrm{AM}_{\mathrm{newmin}} \tag{4}$$

Here, the current scale, i.e., 80 to −52.6, will be normalized to the new scale of 0 to 10. Therefore, $\mathrm{AM}_{\mathrm{newmax}}$ is 10 and $\mathrm{AM}_{\mathrm{newmin}}$ is 0. Using above equation, the normalized value of AM is 7.9111 ≈ **7.9**. An overview of security assurance evaluation process is represented in Fig. 3.

4.3 CSC-based security assurance evaluation

It is important for a CSC to evaluate the security of a cloud service using their project or business requirements to make an informed decision. A customer may request a higher level of security for some specific components of cloud services.

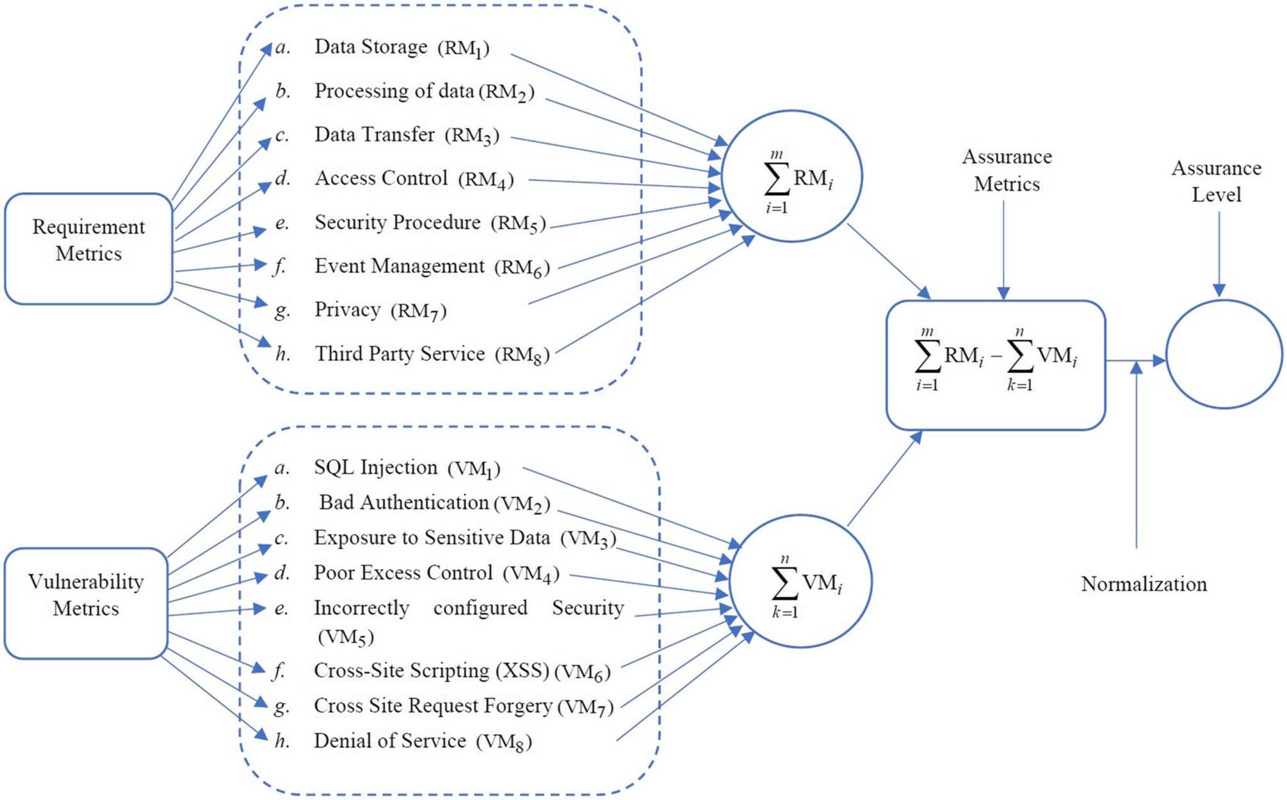
Requirement Metrics
a. Data Storage (RM1)
b. Processing of data (RM2)
c. Data Transfer (RM3)
d. Access Control (RM4)
e. Security Procedure (RM5)
f. Event Management (RM6)
g. Privacy (RM7)
h. Third Party Service (RM8)
$\sum_{i=1}^{m} RM_i$
Assurance Metrics
Assurance Level
$\sum_{i=1}^{m} RM_i - \sum_{k=1}^{n} VM_i$
Vulnerability Metrics
a. SQL Injection (VM1)
b. Bad Authentication (VM2)
c. Exposure to Sensitive Data (VM3)
d. Poor Excess Control (VM4)
e. Incorrectly configured Security (VM5)
f. Cross-Site Scripting (XSS) (VM6)
g. Cross Site Request Forgery (VM7)
h. Denial of Service (VM8)
$\sum_{k=1}^{n} VM_i$
Normalization

Fig. 3 Security assurance evaluation process

Table 15 Security requirements testing results, weights, and RM for CSC1

Security requirements	Control	Questions	Fulfillment points	Average	Weight	Result (RM_i)	$(RM_i)_{Max}$
Data storage	15		7	0.47	8	3.76	8.00
Processing of data	5		3.5	0.70	8	5.60	8.00
Data transfer	5		4.5	0.90	7	6.30	7.00
Access control	11		8	0.72	8	5.76	8.00
Security procedure	20		12	0.60	5	3.00	5.00
Event management	13		8.5	0.65	6	3.90	6.00
Privacy	5		4	0.80	8	6.40	8.00
Third-party services	4		4	1.00	8	8.00	8.00
Sum						42.72	58

The proposed framework allows customers to prioritize their requirements based on the different components. A survey was conducted with four members of the private cloud platform operation team about their security priorities for various components. We have referred to these four members as four customers. The security requirements and the respective weights for four customers are given in Table 15. Based on the weights defined in Table 8, we have calculated the AM for different customers.

4.3.1 Security assurance metrics for CSC1

For the first customer, the RM is calculated based on the customer priorities given in the form of weights for each security requirement in Table 16. The calculated RM ($RM_{calculated}$) is 42.72. The VM of the private cloud platform for this CSC is calculated considering the OWASP top 10 vulnerabilities, which is 6.2. Hence, we calculated AM using Eq. (1) as follows: AM = RM-VM= 42.72–6.2 = 36.52.

As mentioned above, the calculated value of AM is 36.52. With the same security requirements and vulnerabilities, the

Table 16 Security requirements testing results, weights, and RM for CSC2

Security requirements	Control questions	Fulfillment points	Average	Weight	Result (RM_i)	$(RM_i)_{Max}$
Data storage	15	7	0.47	6	2.82	6.00
Processing of data	5	3.5	0.70	3	2.10	3.00
Data transfer	5	4.5	0.90	9	8.10	9.00
Access control	11	8	0.72	10	7.20	10.00
Security procedure	20	12	0.60	10	6.00	10.00
Event management	13	8.5	0.65	8	5.20	8.00
Privacy	5	4	0.80	10	8.00	10.00
Third-party services	4	4	1.00	9	9.00	9.00
Sum					48.42	65

Table 17 Security requirements testing results, weights, and RM for CSC3

Security requirements	Control questions	Fulfillment points	Average	Weight	Result (RM_i)	$(RM_i)_{Max}$
Data storage	15	7	0.47	10	4.70	10.00
Processing of data	5	3.5	0.70	5	3.50	5.00
Data transfer	5	4.5	0.90	5	4.50	5.00
Access control	11	8	0.72	10	7.20	10.00
Security procedure	20	12	0.60	10	6.00	10.00
Event management	13	8.5	0.65	5	3.25	5.00
Privacy	5	4	0.80	10	8.00	10.00
Third-party services	4	4	1.00	5	5.00	5.00
Sum					42.15	60

maximum AM the first customer will be able to achieve is 58, and the minimum AM will be −52.6. After normalizing the current scale, i.e., 58 to −52.6, to the new scale of 0 to 10 using the min-max normalization technique, the value of AM is 8.057 ≈ **8.01**.

4.3.2 Security assurance metrics for CSC2

For the second customer, the RM is calculated based on the customer priorities given in the form of weights for each security requirement in Table 17. The calculated RM ($\text{RM}_{calculated}$) is 48.42. The VM for the second CSC is 6.2. The calculated AM using Eq. (1) is AM = RM-VM= 48.42–6.2 = 42.22.

With the same security requirements and vulnerabilities, the second customer can get a maximum AM of 65, and a minimum AM of -52. After normalizing the current scale, i.e., 65 to −52.6, to the new scale of 0 to 10 using the min-max normalization technique, the value of AM is 8.062 ≈ **8.1**.

4.3.3 Security assurance metric for CSC3

For the third customer, the RM is calculated based on the customer priorities given in the form of weights for each security requirement in Table 18. The calculated RM ($\text{RM}_{calculated}$) is 42.15. The calculated VM is 6.2. The calculated assurance metric (AM) using Eq. (1) is as follows: AM = RM-VM= 42.15–6.2 = 35.95.

For the private cloud platform, one can get maximum AM of 60 and minimum AM of −52.6 using the same requirements and vulnerabilities. After normalizing the current scale, i.e., 60 to −52.6 to the new scale of 0 to 10 using the min-max normalization technique, the value of AM is 7.86 ≈ **7.9**.

4.3.4 Security assurance metric for CSC4

For the fourth customer, the RM is calculated based on the customer priority given in the form of weights for each security requirement in Table 19. The calculated RM ($\text{RM}_{calculated}$) is 44.05. The calculated VM is 6.2. Based on the assurance and VM, AM can be calculated using Eq. (1) as follows: AM = RM-VM= 44.05–6.2 = 37.85.

With the same security requirements and vulnerabilities, one can get a maximum AM of 56, and a minimum AM of −52.6. After normalizing the current scale, i.e., 56 to −52.6, to the new scale of 0 to 10 using the min-max normalization technique, the value of AM is 8.33 ≈ **8.3**.

Table 18 Security requirements testing results, weights, and RM for CSC4

Security requirements	Control questions	Fulfillment points	Average	Weight	Result (RM_i)	$(RM_i)_{Max}$
Data storage	15	7	0.47	3	1.41	3.00
Processing of data	5	3.5	0.70	8	5.6	8.00
Data transfer	5	4.5	0.90	10	9.00	10.00
Access control	11	8	0.72	7	5.04	7.00
Security procedure	20	12	0.60	4	2.40	4.00
Event management	13	8.5	0.65	4	2.6	4.00
Privacy	5	4	0.80	10	8.00	10.00
Third-party services	4	4	1.00	5	5.00	5.00
Sum					44.05	56

Table 19 Security assurance metrics for CSP and four different CSCs

Metrics	CSP	CSC1	CSC2	CSC3	CSC4
RMs	58.5	42.72	48.42	42.15	44.05
Vulnerability metrics	6.2	6.2	6.2	6.2	6.2
Assurance metrics	7.91	8.06	8.06	7.86	8.33

Table 20 Results of security requirements for CSP

Security requirements	Control questions	Fulfilled	Partially fulfilled	Unfulfilled	Results (RM)$_{max}$	(RM)$_{calculated}$
Data storage	15	6 (40.0%)	2 (13.3%)	7 (46.6%)	10	4.7
Processing of data	5	3 (60.0%)	1 (20.0%)	1 (20.0%)	10	7.0
Data transfer	5	4 (80.0%)	1 (20.0%)	0 (0.0%)	10	9.0
Access control	11	8 (72.7%)	0 (0.0%)	3 (27.3%)	10	7.3
Security procedure	20	10 (50.0%)	4 (20.0%)	6 (30.0%)	10	6.0
Event management	13	8 (61.5%)	1 (7.7%)	4 (30.8%)	10	6.5
Privacy	5	3 (60.0%)	2 (40.0%)	0 (0.0%)	10	8.0
Third-party services	4	4 (100.0%)	0 (60.0%)	0 (60.0%)	10	10.0
RM	78	46	11	21	80	58.5

4.3.5 Discussion and analysis

As discussed above, we evaluated the security assurance based on the CSPs (general security assurance) and four different CSCs. An overview of calculated requirement, vulnerability, and AM is given in Table 20. The general security level of the private cloud platform is 7.91. Security assurance levels of the first and second CSC are the same; however, their priorities are different, as shown in Fig. 4 and 5. The security assurance level of the fourth customer is the maximum, while for the third customer is the least. Thus, the security level offered by CSPs may not be sufficient for some CSCs.

In some cases, the security level provided by the CSPs meets the customer's needs. Let us assume that the first customer is looking for cloud services with more focus on the privacy and security of third-party services. The customer uses our proposed framework to avoid serious security mistakes in selecting cloud services and making informed decisions. The customer prioritized the security requirements and approached the service providers to purchase its cloud services. The security assurance level of the private cloud platform is 7.96 in general; however, when the customer's priorities are considered, the revised security assurance level is 7.86. Let us assume that the expected security assurance level of the customer is 8.0. In this scenario, the customer has two options: Either they find another CSP or obtain a guarantee from the provider that their expectations will be met within a specific time frame. If the customer chooses the first option, providers can work on improving the general security assurance level to avoid losing future contracts, and if the customer chooses the second option, providers need to enhance the customer-specific security assurance level. In this section, we presented a detailed categorical analysis of how CSPs can make a decision to improve the general secu-

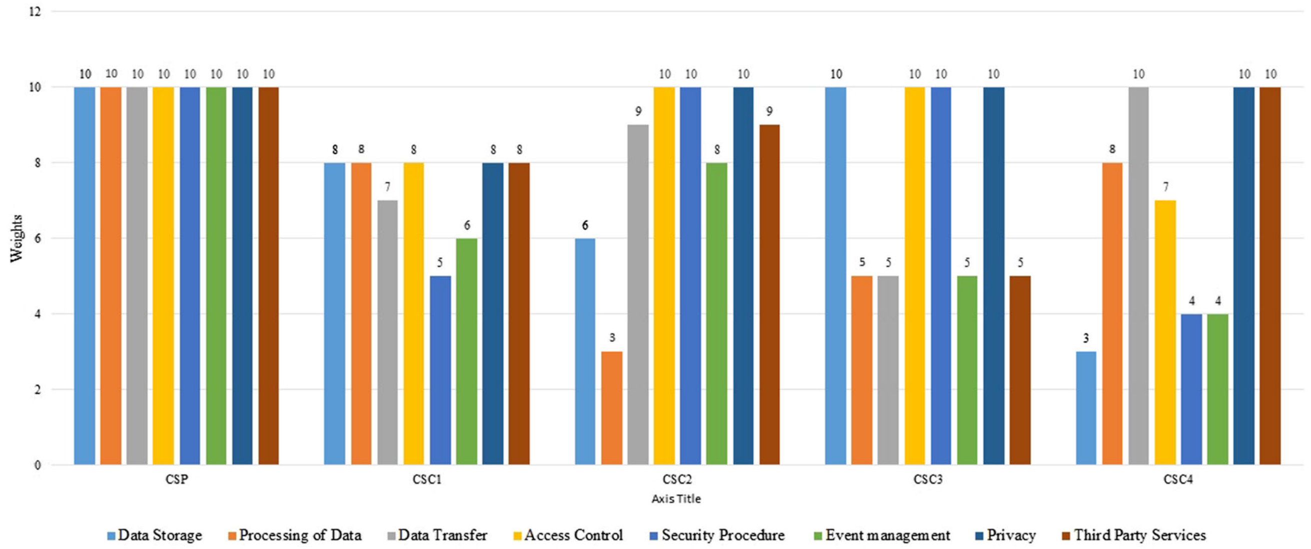

Fig. 4 Weights of the different categories of security requirements and respective weights for CSP and CSCs

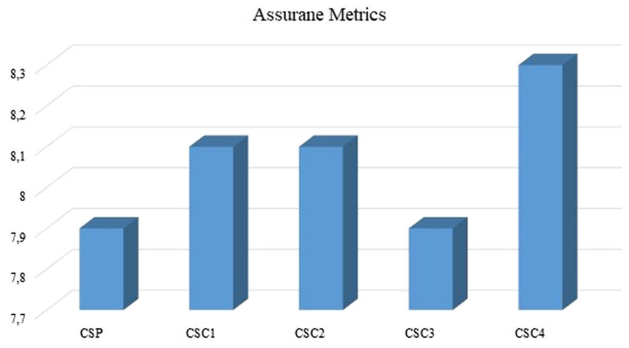

Fig. 5 Security assurance levels of CSP and CSCs

rity assurance level by targeting the least secure component of the cloud service and improving the customer requirements-based security assurance level.

5 Categorically risk assessment and analysis

As discussed in the last section, the AM has been calculated considering security requirements and vulnerability that provides the measurement of how secure the private cloud platform is. The proposed method can be helpful for CSCs as well as CSPs when evaluating the security level of the cloud, considering different priorities. However, this method does not provide recommendations about which module, function, or cloud service is not much secure and needs more attention. As discussed in the last section, in some scenarios, CSPs must improve the general security assurance level to avoid losing future contracts or improve the customer-specific security assurance level as promised. Therefore, a categorical analytical method is needed to identify the least secure parts of the cloud service and the critical vulnerabilities that support CSPs in selecting suitable measures to improve the security of the most vulnerable component to external threats. In general, a method is needed that enables CSPs to identify the significant problems in the system and assess how much gain can be achieved by solving each of them. Therefore, an analytical method is developed to identify and rank the different components of the cloud based on their current security features and vulnerabilities. In this analytical method, the impact of each security metric on security assurance is considered. Furthermore, a ranking method is developed to rank the security metric based on their security level.

The proposed method is divided into two parts: The first part discusses the development of the analytical method for the standard cloud service offered by CSPs, and the second part discusses the implementation of the analytical method based on customer requirements.

5.1 Categorical analysis of cloud services offered by CSPs

To conduct this categorical analysis, we first identified the key AM, calculated each security requirement's impact on the RM and AM, and then ranked each category of requirements.

5.1.1 Identification of key AM

As we discussed, security requirements and VM are the key metrics for security assurance measurements. Therefore, to assess the impact of each of these metrics on security assurance, we calculated their contribution to security assurance measurement and their respective performance. First, we calculated each security metric's maximum possible and actual contributions to the security assurance measurement.

The maximum contribution of the security RM (RM) to achieve 100% of the security assurance level of the private cloud platform is

$$\frac{(\mathrm{RM})_{\max}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 60.33\%, \tag{5}$$

and the actual contribution of RM in security assurance measurement is

$$\frac{\mathrm{RM}_{calculated}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 44.12\%. \tag{6}$$

The VM contributes negatively to security assurance measurement because vulnerabilities expose the system to various threats and thus decrease the security assurance level. Due to this, the positive contribution of the VM to assurance measurement is determined by the absence of vulnerabilities. The maximum possible positive contribution of the VM to achieve the 100% security assurance level is

$$\frac{(\mathrm{VM})_{\max}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 39.66\%, \tag{7}$$

and actual contribution of VM in security assurance measurement can be calculated as

$$\begin{aligned}\frac{\mathrm{VM}_{\max} - \mathrm{VM}_{calculated}}{\mathrm{AM}_{\max} - \mathrm{AM}_{\min}} \times 100 &= \frac{52.6 - 6.2}{132.6} \times 100\\ &= 34.99\%.\end{aligned} \tag{8}$$

The above results show that the RM is the most important component for security assurance because it can help achieve up to 60.33% of the assurance level, while the VM contributes 39.66%. This result indicates that the RM is more important for the cloud security assurance. According to Eqs. (6) and (8), the actual contribution of the RM and VM is 44.12% and 34.99%, respectively.

The performance of the requirements metric is

$$\frac{\mathrm{RM}_{calculated}}{\mathrm{RM}_{\max}} \times 100 = 73.12\%, \tag{9}$$

where the VM is performing very well as its performance percentage is

$$\begin{aligned}\frac{\mathrm{VM}_{\max} - \mathrm{VM}_{calculated}}{\mathrm{VM}_{\max}} \times 100 &= \frac{52.6 - 6.2}{52.6} \times 100\\ &= 88.21\%.\end{aligned} \tag{10}$$

According to the above results, the RM is the key AM for CSPs; however, its performance is inferior to the VM. Therefore, security teams should prioritize the security RM more.

Next, we will perform a categorical analysis of security requirements to identify the key components and their impact on the RM and security assurance measurement and determine how CSPs can improve performance of the RM so that the required assurance level can be achieved. In addition, the VM will be examined.

5.1.2 Analysis of RM

As discussed in the previous section, 73.12% of the security goals are achieved from the security requirements, while 26.88% are still to be achieved. It should be the primary task to fulfill the remaining security requirements, which requires identifying the categories of security requirements that are underperforming and have high priority.

In Table 21, 22 control questions are presented; six are fulfilled, two are partially fulfilled, and seven are unfulfilled. Thus, 40% of the data storage requirements are fulfilled, 46.67% are unfulfilled, and 13.33% are partially fulfilled. The security procedure has the second-lowest fulfillment of security requirements after data storage because 50% of the control questions are fulfilled, 20% are partially fulfilled, and 30% are not fulfilled. In contrast, the third-party services fulfilled all the security requirements.

It is important to determine how these requirements affect both impact assurance and requirements metrics. In this case, the impact of each requirement category is calculated based on its contribution to the calculation of the RM and AM. Using the following formula, it is possible to calculate the impact of data storage requirements on both the RM and AM:

(i) *Impact of data storage requirement on RM:* The impact of data storage requirement on RM can be calculated as follows: The maximum possible contribution of the data storage requirement in RM measurement is

$$\frac{(\mathrm{RM}_1)_{\max}}{\mathrm{RM}_{\max}} \times 100 = 12.5\%,$$

while actual contribution of this category of requirement in overall RM measurement is

$$\frac{(\mathrm{RM}_1)_{calculated}}{\mathrm{RM}_{\max}} \times 100 = 5.87\%.$$

(ii) *Impact of data storage requirement on AM:* The impact of data storage requirement on AM can be calculated as follows: The maximum possible contribution of the data storage requirement in security assurance mea-

Table 21 Requirements metric and their impact on security assurance for CSP

Security requirements	Maximum possible contribution(%)		Actual contribution (%)		Performance (%)	Priority score	Rank
	RM	AM	RM	AM			
Data storage	12.5	7.54	5.87	3.54	46.67	0.0662	1
Processing of data	12.5	7.54	8.75	5.28	70.00	0.0375	4
Data transfer	12.5	7.54	11.25	6.79	90.00	0.0125	7
Access control	12.5	7.54	9.13	5.51	72.70	0.0337	5
Security procedure	12.5	7.54	7.5	4.52	60.00	0.0500	2
Event management	12.5	7.54	8.13	4.90	65.38	0.0437	3
Privacy	12.5	7.54	10	6.03	80.00	0.0250	6
Third-party services	12.5	7.54	12.5	7.54	100	0	8
RM	100	60.32	73.12	44.12			

Table 22 Requirements metric and their impact on security assurance for CSC1

Security requirements	Maximum possible contribution(%)		Actual contribution (%)		Performance (%)	Priority score	Rank
	RM	AM	RM	AM			
Data storage	13.79	7.23	6.48	3.40	46.67	0.07310	1
Processing of data	13.79	7.23	9.66	5.06	70.00	0.04137	2
Data transfer	12.07	6.33	10.86	5.70	90.00	0.01206	7
Access control	13.79	7.23	9.93	5.21	72.70	0.03862	3
Security procedure	08.62	4.52	5.17	2.71	60.00	0.03448	5
Event management	10.34	5.42	6.72	3.51	65.38	0.03620	4
Privacy	13.79	7.23	11.03	5.79	80.00	0.02758	6
Third-party services	13.79	7.23	13.79	7.23	100	0	8
RM	100	52.44	73.65	38.62			

surement is

$$\frac{(\mathrm{RM}_1)_{\max}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 7.54\%,$$

while actual contribution of this category of requirement in security assurance measurement is

$$\frac{(\mathrm{RM}_1)_{calculated}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 3.54\%$$

Similarly, the impact of other categories of requirements on both the RM and AM has also been calculated and is tabulated in Table 22. As shown in this table, the maximum possible contribution of data storage in AM calculation is 12.5%, and its performance is 46.6% ≈ 47%, which is lower than the other categories of security requirements. Also, we can see in Table 21 that the maximum possible score for the data storage RM that can be achieved is $(\mathrm{RM}_1)_{\max} = 10$, while the actual calculated score for data storage RM $(\mathrm{RM}_1)_{calculated}$ is 4.7 that means 47.0% of security goals have been achieved for this category, and 53.0% have not been achieved. On the other hand, the performance of third-party services is 100%. Figure 6 represents the performance of each of the categories of security requirements.

In order to rank these categories of security requirements based on importance and performance to security assurance, a priority score is calculated using the following formula:

$$\text{Priority score} = \frac{(\mathrm{RM_i})_{\max} - (\mathrm{RM_i})_{\mathrm{calculated}}}{\mathrm{RM}_{\max}}, \tag{11}$$

As given in Table 22, the rank of data storage is 1. In order to achieve the maximum level of security assurance, this security requirement should be given greater priority. After data storage, the security procedure should be given priority, as it has a rank of 2. A similar decision can be made based on the ranking of other categories of security requirements.

5.1.3 Analysis of VM

From Eq. (10), 88.21 % of the VM contributes positively to security assurance measurement since only one vulnerability, i.e., DoS exists for the private cloud platform, which has a CVSS score 6.2. As a result, it is not important to analyze

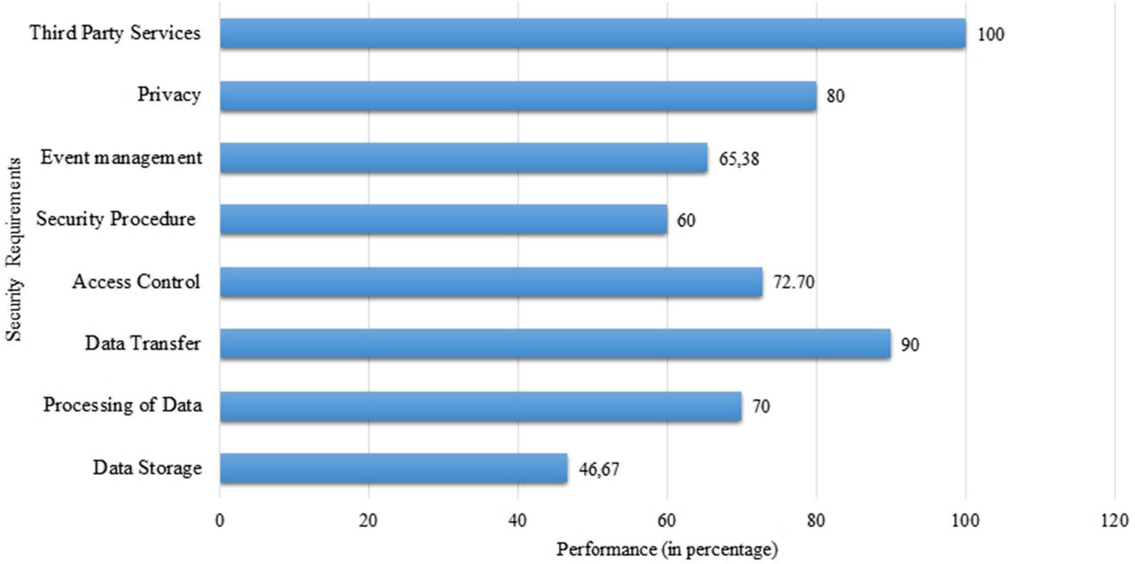

Fig. 6 Performance of security requirements

VM in detail, and it is recommended that countermeasures be taken to prevent a DoS attack.

5.2 Categorical analysis based on CSC's requirements

As part of this section, we conducted a categorical analysis of the security assurance based on customer preferences. This analysis included the first customer's requirements. Following the identification of key AM, we calculated the impact of each security requirement on the RM and AM and then ranked each requirement category.

5.2.1 Identification of key AM

Similar to the last section, we calculated each security metric's maximum possible and actual contributions to the security assurance measurement.

The maximum contribution of the security RM to achieve 100% of the security assurance level of the private cloud platform is

$$\frac{(\mathrm{RM})_{\max}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 52.44\%, \tag{12}$$

and the actual contribution of RM in security assurance measurement is

$$\frac{\mathrm{RM}_{calculated}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 38.62\%. \tag{13}$$

Similarly, the maximum possible positive contribution of VM to achieve the 100% security assurance level is

$$\frac{(\mathrm{VM})_{\max}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 47.56\%, \tag{14}$$

and actual contribution of VM in security assurance measurement can be calculated as

$$\frac{\mathrm{VM}_{\max} - \mathrm{VM}_{calculated}}{\mathrm{AM}_{\max} - \mathrm{AM}_{\min}} \times 100 = \frac{52.6 - 6.2}{110.6} \times 100 = 41.95\%. \tag{15}$$

From the above results, we can see that the RM is the most important component for the first customer because it can help to achieve up to 52.44 % of the assurance level, while VM contributes 47.56 %. These results indicate that the RM is an important factor for the first customer. As given in Eqs. (6) and (8), the actual contribution of the RM and VM is 38.62 and 41.95 %, respectively.

The performance of the RM in security assurance measurement is

$$\frac{\mathrm{RM}_{calculated}}{\mathrm{RM}_{\max}} \times 100 = 73.65\%, \tag{16}$$

where the VM is performing very well as its performance percentage is

$$\frac{\mathrm{VM}_{\max} - \mathrm{VM}_{calculated}}{\mathrm{VM}_{\max}} \times 100 = \frac{52.6 - 6.2}{52.6} \times 100 = 88.21\%. \tag{17}$$

The above results indicate that the RM is the key AM for the first customer; however, its performance is not better than the VM. Therefore, it is recommended that security teams set more priorities on the security RM.

Table 23 SQL injection

Test	Descriptions
SQL Injection to bypass authentication	1. Open a web browser and navigate to the user interface. 2. Enter standard SQL queries in the login field

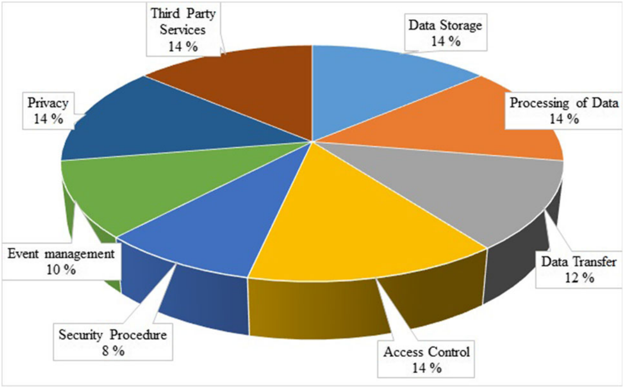

Fig. 7 Maximum possible contribution of security requirements for CSC1

5.2.2 Analysis of RM

As discussed in the previous section, 73.65% of the security goals are achieved from the security requirements, while 26.35% yet to be achieved. Now, it is the primary task of the CSPs to focus on the remaining security requirements to achieve the target security assurance level based on the CSC priorities. For this, it is important to identify the category of security requirement that is not performing well but is crucial in RM calculation.

Similar to the discussion in the last section, the maximum possible RM for data storage requirement is $(\mathrm{RM}_1)_{\max} = 8$, while the actual calculated RM for data storage requirement $(\mathrm{RM}_1)_{calculated}$ is 3.76. It means 47.0% security goals are fulfilled for this category of security requirement, and 53.0% security goals are not fulfilled for data storage.

(i) *Impact of data storage requirement on RM:* The maximum possible contribution of the data storage requirement in RM measurement is

$$\frac{(\mathrm{RM}_1)_{\max}}{\mathrm{RM}_{\max}} \times 100 = 13.79\%,$$

while actual contribution of this category of requirement in overall RM measurement is

$$\frac{(\mathrm{RM}_1)_{calculated}}{\mathrm{RM}_{\max}} \times 100 = 6.48\%.$$

(ii) *Impact of data storage requirement on AM:* The maximum possible contribution of the data storage requirement in security assurance measurement is

$$\frac{(\mathrm{RM}_1)_{\max}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 7.23\%,$$

while actual contribution of this category of requirement in security assurance measurement is

$$\frac{(\mathrm{RM}_1)_{calculated}}{(\mathrm{AM}_{\max} - \mathrm{AM}_{\min})} \times 100 = 3.40\%$$

Similarly, the impact of other categories of requirement on both RM and AM has been considered, and the calculated measurements are tabulated in Table 23. As shown in this table, the maximum possible contribution of security procedure, processing of data, access control, privacy, and third-party services in RM calculation is 13.79%. However, the performance data storage is only 46.67%, which is lower than the other categories of security requirements. On the other hand, the performance of data transfer and third-party services is 90% and 100%, respectively, and their contribution in RM calculation is 25.86% and in AM calculation is 13.56%. Therefore, these components required the least attention. The maximum possible contribution and the actual contribution of the different categories of security requirements to the security assurance measurement are given in Fig. 7 and 8.

A priority score has been calculated to rank the different categories of security assurance based on Eq. (11) and to identify the one that is most crucial for security assurance measurement. As given in Table 23, the rank of data storage is 1, i.e., this security requirement should be given more priority to achieve the required or maximum level of security assurance. The processing of data is ranked second, so it should take priority after data storage. Similarly, the decision can be made for other security requirements based on their ranking.

5.2.3 Analysis of VM

As given in Eq. (10), 88.21% of the VM contributes positively to security assurance measurement because out of eight vulnerabilities, only one vulnerability, i.e., DoS exists for the private cloud platform, which has a CVSS score of 6.2. Therefore, a detailed analysis of the VM is not required. It is recommended to take countermeasures for the DoS attack.

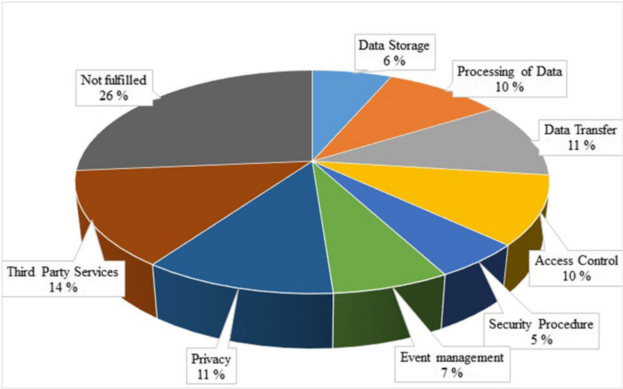

Fig. 8 Actual contribution of security requirements for CSC1

5.3 Summary of the results

As discussed above, categorical analysis of the AM is conducted for both the CSP and CSC. For the CSC, we included their security preferences. In this analysis, first, we identified the key security assurance metric based on their contribution to the security assurance level of the private cloud platform, its current performance, and its impact on the assurance level. For both the CSP and CSC, the RM is the key assurance metric. After finding the key assurance metrics, we conducted a detailed categorical analysis on it to identify the crucial components and their impact on security assurance measurement. The proposed analytical method helps to determine how CSPs can improve the performance of the key metric, i.e., the RM, to achieve the required assurance level. In Fig. 9, we have shown the performance of the different categories of security requirements based on the maximum possible contribution and actual possible contribution to the security assurance measurement for both CSP and CSC. Finally, the categories of security requirements are ranked in order of importance and performance on security assurance. As we can see in Fig. 10, the ranking of the categories of security requirements is different for both CSP and CSC because the security preference of the CSC is different from the security provided by the CSP.

As we can see in Fig. 10, there is a difference in ranking for CSPs and CSCs because of their different priorities and fulfillment of security requirements. Accordingly, they will have different priorities to further improve the security assurance levels of cloud services. The CSP must be able to meet the security requirements of the CSC and guarantee this in the service level agreement (SLA). Therefore, CSPs should match their preferences with the security preferences of the CSCs. According to Fig. 10, “data storage” and “privacy” are ranked the same for CSPs and CSCs, while other security requirements are ranked differently. “Third-party services” is an exception because all requirements related to this category are met. Our conclusion from this study is that providers do not need to change their strategy when it comes to “data storage” and “privacy” and should be given equal priority when both general security assurance levels and security assurance levels based on CSC expectations need to be increased. However, to meet the expectation of CSC, CSP should shift their priorities for the other security requirements from “security procedure” to the “processing of the data,” “event management” to “access control,” “processing of data” to “event management.” Similarly, CSP should change the order of priorities, as shown in Fig. 10.

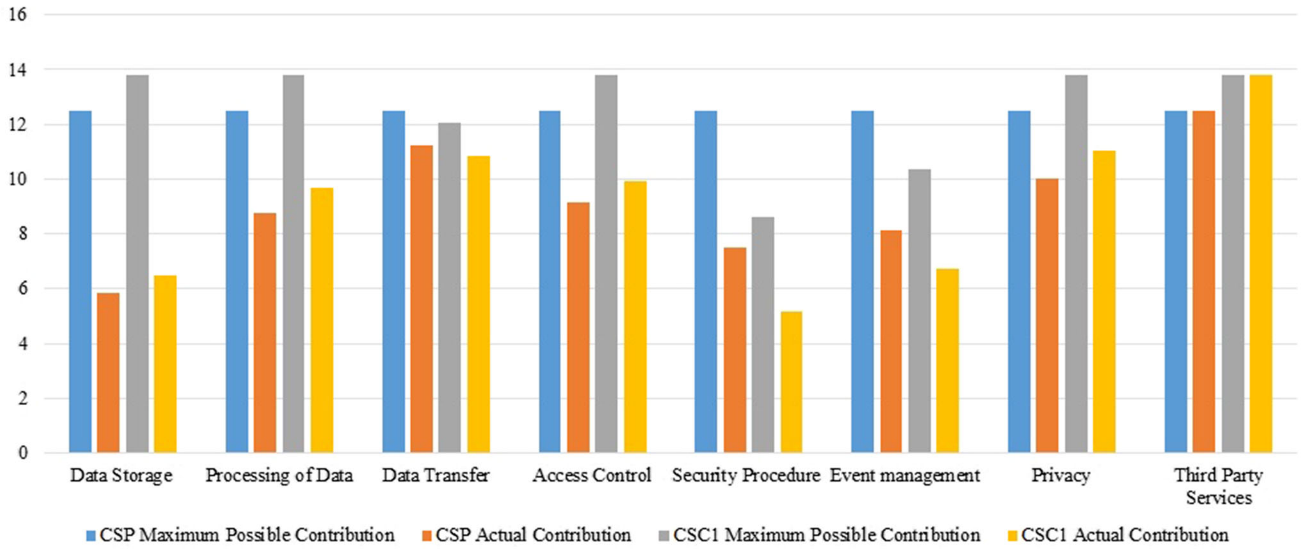

Fig. 9 Performance of security requirements for CSP and CSC1

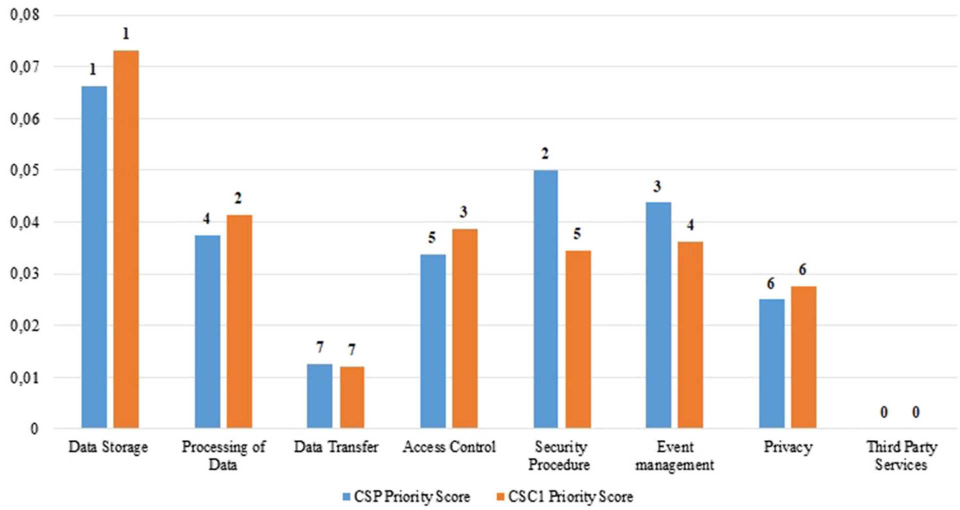

Fig. 10 Ranking of different categories of security requirements

6 Conclusion and future works

Cloud security assurance provides confidence in protecting the crucial data and information present and controlled by cloud computing services.

Estimating the security assurance level is an important measure to help CSCs to make informed decisions on which cloud platform to choose and migrate to. Other guidelines, standards, and methods for security assurance are qualitative, complex, time-consuming, and process-oriented and do not take into account the preferences and priorities of CSCs.

In this paper, we solved the aforementioned problems by proposing a security assurance methodology to measure the security level of cloud services. This approach gives a quantitative measure of the security of cloud services based on two security metrics: security requirement and vulnerability. It also incorporates the security requirement preferences of CSCs and the risk estimation based on the customer's context. Moreover, a detailed categorical risk analysis has been done to analyze the different categories of security requirements and vulnerabilities and measure their impact on security assurance. This will indicate the main security issues that a cloud service suffers from. We applied our methodology to a real case study related to a private cloud platform, and four potential customers who want to purchase services.

The results show that by considering the preferences of different customers, the security assurance score changes accordingly. To summarize, the proposed approach will be helpful for (1) CSCs to avoid severe mistakes and make informed decision while purchasing cloud computing services and (2) CSPs to measure and improve the security level of the services and find out the components of the cloud which are least secure.

In our case study, we considered one cloud platform and various customers. In the future, we will consider case studies involving multiple customers and cloud platforms. Additionally, extending the methodology with cost–benefit analysis is planned for the future.

Acknowledgements We would like to acknowledge the valuable contribution of the three Undergrad students Anders Bjørklund Jensen, Abdi Moohamued, and Yobe Najar, who took part in ongoing research activities at Norwegian Cyber range and assisted us in development of necessary artifacts for this research.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital) This work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme. This work is also partially supported by Norwegian Cyber Range, NTNU, Norway.

Availability of data and materials Authors confirm that all relevant data are included in the article.

Declarations

Conflicts of interest The authors declare that they do not have conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Appendix Assurance profile: vulnerability

SQL injection

Poor authentication

Table 24 Poor authentication

Test		Description
2.1	Is a secure cookie used for the session cookie?	Whether the variable SESSION_COOKIE_SECURE has been set to “True” in the local_setting.py file?
2.2	Is the browser allow to create a script to access cookies?	Whether the variable SESSION_COOKIE_HTTPONLY has been set to “True” in the local_setting.py file?
2.3	Is the password auto-complete turned off?	Whether the variable PASSWORD_AUTOCOMPLETE has been set to “Off” in the local_setting.py file?
2.4	Is the password reveal button disabled?	Whether the variable DISABLE_PASSWORD_REVEAL has been set to “True” in the local_setting.py file?
2.5	Is the identity of an administrative user verified when resetting passwords	Whether the variable? ENFORCE_PASSWORD_CHECK has been set to “True” in the local_setting.py file?
2.6	Is the users password complex enough?	Is there no setting other than the default in the local_setting.py for the variable PASSWORD_VALIDATOR?
2.7	Is a request secure?	whether the variable SECURE_PROXY_SSL_HEADER set to “X_Forwarded_Proto″, “http” in the local_setting.py?
2.8	Is Transport Layer Security (TLS) implemented?	TLS provides secure communication across the networks
2.9	Is a strong hashing algorithm used?	Check the hash_algorithm variable under the [token] section of the keystone.conf file is set to SHA256
2.10	Is the system use Keystone for authentication using Nova?	Check if the variable auth_strategy under the section [DEFAULT]in the nova.conf file is set to keystone.
2.11	Whether communication in Keystone performed using a secure communication protocol?	Verify if the variable www_authenticate_uri under the [keystone_authtoken] section of the nova.conf file is set to a value that begins with https: //.
2.12	Whether the communication between the components Nova and Glance takes place using a secure protocol?	Check if the variable api_insecure below the [glance] section of the nova.conf file is set to False.
2.13	Whether the system uses Keystone for authentication using Cinder?	Check if the variable auth_strategy under the section [DEFAULT] in the cinder.conf file is set to keystone.
2.14	Is TLS enabled for authentication using Cinder?	Check if the variable www_authenticate_uri under the [keystone_authtoken] section of the cinder.conf file begins with https: //.
2.15	Whether the communication between the Nova and Cinder components takes place using a secure protocol?	Checks if the variable nova_api_insecure under the [DEFAULT] section of the cinder.conf file is set to “False.”
2.16	Whether the communication between the Glance and Cinder components takes place using a secure protocol?	Check if the variable glance_api_insecure under the section [DEFAULT] in the cinder.conf file starting with https: //.
2.17	Whether the system uses Keystone for authentication using Cinder?	Check if the auth_strategy variable under the [DEFAULT] section of the file neutron.conf is set to keystone.
2.18	Is TLS enabled for authentication using Neutron?	Check if the variable www_authenticate_uri below section [keystone_authtoken] in the neutron.conf file begins with https: //.
2.19	Is TLS enabled on Neutron API server?	Check if the variable use_ssl under the [DEFAULT] section of the neutron.conf file, this file exists is set to “True.”

Exposure to sensitive data

Table 25 Exposure to sensitive data

Test		Description
3.1	Operates NAS in a secure environment (Cinder supports NFS (Network File System), which is a storage system that works a bit different from block storage. NFS does not allow an instance to access block storage, instead, it creates files that will mimic block storage. Cinder also supports secure configuration of these files by determining the rights to the files, when they are created.)	Check if the variables nas_secure_file_permissions and nas_secure_file_operations under the section [DEFAULT] is set to auto in the file cinder.conf.

Poor access control

Table 26 Poor access control

Test		Description
4.1	Are Horizon's configuration files only available for root?	This test checks for the right to open, modify, and delete configuration files for Horizon are only available for root
4.2	Is the Horizon's configuration files restricted?	This test is another form of checking to see if there are any restrictions on the configuration files to Horizon
4.3	Are keystone configuration files only available for root?	This test checks for the right to open, modify, and delete configuration files for Keystone are only available for root
4.4	Is the Keystone's configuration files restricted?	This test is another form of checking to see if there are any restrictions on the configuration files to Keystone
4.5	Are Nova configuration files only available for root?	This test checks for the right to open, modify, and delete configuration files for Nova are only available for root
4.6	Is the Nova's configuration files restricted?	This test is another form of checking to see if there are any restrictions on the configuration files to Nova
4.7	Are Cinder's configuration files only available for root?	This test checks for the right to open, modify, and delete configuration files for Cinder are only available for root
4.8	Is the Cinder configuration files restricted?	This test is another form of checking to see if there are any restrictions on the configuration files to Cinder
4.9	Are Neutron's configuration files only available for roots?	This test checks for the right to open, modify, and delete configuration files for Neutron are only available for root
4.10	Are Neutron configuration files restricted?	This test is another form of checking to see if there are any restrictions on the configuration files to Nova

Incorrectly configured security

Table 27 Incorrectly configured security

Test		Description
5.1	Is the size of the requests submitted exceed a certain value?	The variable max_request_body_size must be in the file keystone.conf and set to the default value 114688.
5.2	Is the admin token deactivated?	The variable admin_token is checked under the [DEFAULT] section of the keystone.conf file is disabled. In addition, the variable AdminTokenAuthMiddleware is checked under the [filter: admin_token_auth] section has been deleted from the keystone-paste.ini file.
5.3	Is the server return information in HTTP response?	Check if this variable insecure_debug is set to “False” under the section [DEFAULT] in the keystone.conf file.
5.4	Is the size of the requests submitted exceed a certain value?	Check the variable osapi_max_request_body_size must be under the [DEFAULT] section contained in the cinder.conf file and set to default 114688.
5.5	Whether data stored in volume is encrypted or not?	Check against the backend variable under the [key_manager] section of the cinder.conf file has been set to something. In addition, the variable backend is also checked under the section [keymanager] in the file nova.conf.

Cross-site scripting (XSS)

Table 28 Cross-site scripting

Test		Description
6.1	Is the Horizon exposed to the cross-frame scripting?	Check if the variable DISALLOW_IFRAME_EMBED has been set to “True” in the file local_settings.py

Cross-site request forgery

Table 29 Cross-site request forgery

Test		Description
7.1	Cross-site request forgery (CSRF) is an attack that forces users to execute unwanted code on a web application.	The test checks that about the variable CSRF_COOKIE_SECURE is set to True in the local_settings.py file

DoS

Table 30 DoS

Test		Description
8.1	DoS	For the implementation of DDoS, we use the software GoldenEye, which is a tool used to perform DoS attacks

References

1. KPMG, Cloud survey report: Elevating business in the cloud. (2014)http://www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/2014%20KPMG%20Cloud%20Survey%20Report%20-%20Final%2012-10-14.pdf
2. Kshetri, N.: Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommun. Policy **37**(4–5), 372–386 (2013)
3. Pearson, S.: Privacy, security and trust in cloud computing. In: Pearson, S., Yee, G. (eds.) Privacy and security for cloud computing, pp. 3–42. Springer, London (2013)
4. For Standardization IO Iso/iec 27002: Guidelines on Information Security Controls for the use of Cloud Computing Services (2014)

5. Alliance, CS.: Cloud Controls Matrix v3.0.1. https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/ (2015)
6. Of Standards NI, Technology, Security and Privacy Controls for Federal Information Systems and Organizations. NIST 800-53v4 (2014)
7. Alqatawna, J., et al.: The challenge of implementing information security standards in small and medium e-business enterprises. J. Softw. Eng. Appl. **7**(10), 883 (2014)
8. Chemerkin, Y.: Limitations of security standards against public clouds. In: International Conference on Information Society (i-Society 2013). IEEE, pp 55–60 (2013)
9. Uriarte, RB., Tiezzi, F., De Nicola, R.: Slac: A formal service-level-agreement language for cloud computing. In: 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, IEEE, pp 419–426 (2014)
10. Bousquet, A., Briffaut, J., Caron, E., Dominguez, EM., Franco, J., Lefray, A., López, O., Ros, S., Rouzaud-Cornabas, J., Toinard, C., et al.: Enforcing security and assurance properties in cloud environment. In: 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC). IEEE, pp 271–280 (2015)
11. Modic, J., Trapero, R., Taha, A., Luna, J., Stopar, M., Suri, N.: Novel efficient techniques for real-time cloud security assessment. Comput. Secur. **62**, 1–18 (2016)
12. Formoso, S., Felici, M.: Evidence-based security and privacy assurance in cloud ecosystems. In: IFIP International Summer School on Privacy and Identity Management. Springer, London, pp 205–219 (2015)
13. Trapero, R., Modic, J., Stopar, M., Taha, A., Suri, N.: A novel approach to manage cloud security sla incidents. Futur. Gener. Comput. Syst. **72**, 193–205 (2017)
14. Deshpande, P., Sharma, S., Peddoju, S.K., Abraham, A.: Security and service assurance issues in cloud environment. Int. J. Syst. Assur. Eng. Manag. **9**(1), 194–207 (2018)
15. Rizvi, S., Ryoo, J., Kissell, J., Aiken, W., Liu, Y.: A security evaluation framework for cloud security auditing. J. Supercomput. **74**(11), 5774–5796 (2018)
16. Sen, A., Madria, S.: Application design phase risk assessment framework using cloud security domains. J. Inf. Secur. Appl. **55**(102), 617 (2020)
17. Ismail, U.M., Islam, S.: A unified framework for cloud security transparency and audit. J. Inf. Secur. Appl. **54**(102), 594 (2020)
18. Pachala, S., Rupa, C., Sumalatha, L.: An improved security and privacy management system for data in multi-cloud environments using a hybrid approach. Evol. Intell. **14**(2), 1117–1133 (2021)
19. Katt, B., Prasher, N.: Quantitative security assurance metrics: Rest api case studies. In: Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings, pp 1–7 (2018)
20. Katt, B., Prasher, N.: Quantitative security assurance. In: Exploring Security in Software Architecture and Design. IGI Global, pp 15–46 (2019)
21. Weldehawaryat, GK., Katt, B.: Towards a quantitative approach for security assurance metrics. In: The 12th International Conference on Emerging Security Information (2018)
22. Beznosov, K., Kruchten, P.: Towards agile security assurance. In: Proceedings of the 2004 Workshop on New security Paradigms. ACM, pp 47–54 (2004)
23. Shukla, A., Katt, B., Nweke, LO., Yeng, PK., Weldehawaryat, GK.: System security assurance: A systematic literature review. (2021) arXiv preprint arXiv:2110.01904
24. ISO/IEC 17789:2014 (2014) Information technology - cloud computing - reference architecture. https://www.iso.org/standard/60545.html
25. ISO/IEC 19944-1:2020 (2020) Cloud computing and distributed platforms - data flow, data categories and data use - part 1: Fundamentals. https://www.iso.org/standard/79573.html
26. ISO/IEC TS 23167:2020 (2020) Information technology - cloud computing - common technologies and techniques. https://www.iso.org/standard/74805.html
27. ISO/IEC 27018:2019 (2020) Information technology - security techniques - code of practice for protection of personally identifiable information (PII) in public clouds acting as pii processors. https://www.iso.org/standard/76559.html
28. Cloud Security Alliance (CSA) (2021) The CSA cloud controls matrix (ccm). https://cloudsecurityalliance.org/research/cloud-controls-matrix/
29. Center for Internet Security (CIS) (2022) Foundational cloud security with cis benchmarks. https://www.cisecurity.org/cis-benchmarks/
30. Bernsmed, K., Meland, PH., Jaatun, MG.: Cloud Security Requirements. (2015) https://infosec.sintef.no/wp-content/uploads/2015/08/Cloud-Security-Requirements-v2.0.pdf
31. Pham, N., Riguidel, M.: Security assurance aggregation for it infrastructures. In: 2007 Second International Conference on Systems and Networks Communications (ICSNC 2007). IEEE, pp 72–72 (2007)
32. Ouedraogo, M., Khadraoui, D., De Rémont, B., Dubois, E., Mouratidis, H.: Deployment of a security assurance monitoring framework for telecommunication service infrastructures on a voip service. In: New Technol., pp. 1–5. Mobility and Security, IEEE (2008)
33. Ouedraogo, M., Mouratidis, H., Khadraoui, D., Dubois, E.: A risk based approach for security assurance evaluation of it systems. In: 2009 Seventh Annual Communication Networks and Services Research Conference. IEEE, pp 428–430 (2009)
34. Savola, RM.: Software security assurance of telecommunication systems. In: 2009 International Conference on Multimedia Computing and Systems. IEEE, pp 138–143 (2009)
35. Pavlich-Mariscal, JA., Demurjian, SA., Michel, LD.: A framework for security assurance of access control enforcement code. Comput. Secur. 29(7):770–784 (2010)
36. Savola, RM., Pentikäinen, H., Ouedraogo, M.: Towards security effectiveness measurement utilizing risk-based security assurance. In: 2010 Information Security for South Africa. IEEE, pp 1–8 (2010)
37. Vivas, J.L., Agudo, I., López, J.: A methodology for security assurance-driven system development. Requir. Eng. **16**(1), 55–73 (2011)
38. Lan, Y., Han, T.: Sadp: Security assurance development process for building reliable linux-based operating system. In: 2015 IEEE International Conference on Computer and Communications (ICCC). IEEE, pp 50–55 (2015)
39. Such, J.M., Gouglidis, A., Knowles, W., Misra, G., Rashid, A.: Information assurance techniques: perceived cost effectiveness. Comput. Secur. **60**, 117–133 (2016)
40. Ardagna, CA., Damiani, E., Schütte, J., Stephanow, P.: A case for iot security assurance. In: Internet of Everything. Springer, pp 175–192 (2018)
41. Zhi, Q., Yamamoto, S., Morisaki, S.: Quantitative evaluation in security assurance. In: 2018 IEEE 4th International Conference on Computer and Communications (ICCC). IEEE, pp 2477–2483 (2018)
42. Khan, RA., Khan, SU.: A preliminary structure of software security assurance model. In: Proceedings of the 13th International Conference on Global Software Engineering. pp 137–140 (2018)
43. Sakthivel, R.K., Nagasubramanian, G., Al-Turjman, F., Sankayya, M.: Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry. Trans. Emerg. Telecommun. Technol. **33**(4), e3947 (2020)
44. Wen, S.F., Shukla, A., Katt, B.: Developing security assurance metrics to support quantitative security assurance evaluation. J. Cybersecur. Priv. **2**(3), 587–605 (2022)

45. Rios, E., Iturbe, E., Mallouli, W., Rak, M.: Dynamic security assurance in multi-cloud devops. In: 2017 IEEE Conference on Communications and Network Security (CNS). IEEE, pp 467–475 (2017)
46. Bobelin, L., Bousquet, A., Briffaut, J.: An autonomic cloud management system for enforcing security and assurance properties. In: Proceedings of the 2015 Workshop on Changing Landscapes in HPC Security, pp 1–8 (2015)
47. Duncan, B., Pym, DJ., Whittington, M.: Developing a conceptual framework for cloud security assurance. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, IEEE, vol 2, pp 120–125 (2013)
48. Islam, S., Ouedraogo, M., Kalloniatis, C., Mouratidis, H., Gritzalis, S.: Assurance of security and privacy requirements for cloud deployment models. IEEE Trans. Cloud Comput. **6**(2), 387–400 (2015)
49. Kumar, R., Goyal, R.: Top threats to cloud: A three-dimensional model of cloud security assurance. In: Computer Networks and Inventive Communication Technologies. Springer, pp 683–705 (2021)
50. Maroc, S., Zhang, J.B.: Cloud services security-driven evaluation for multiple tenants. Cluster Comput. **24**(2), 1103–1121 (2021)
51. Rios, E., Rak, M., Iturbe, E., Mallouli, W., et al.: Sla-based continuous security assurance in multi-cloud devops. CEUR Workshop Proceedings (2017)
52. Halabi, T., Bellaiche, M.: Towards quantification and evaluation of security of cloud service providers. J. Inf. Secur. Appl. **33**, 55–65 (2017)
53. Openstack (2015) Openstack Security Guide. https://www.scribd.com/documen/330263894/OpenStack-Security-Guide
54. Amazon (2016) Aws Security Best Practice. https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf
55. Microsoft (2016) Microsoft Azure Responses to Cloud Security Alliance Consensus Assessments Initiative Questionnaire v3.0.1. https://gallery.technet.microsoft.com/Azure-Responses-to-CSA-46034a11/file/155556/1/Azure%20Responses%20to%20CSA%20CAIQ%20301.pdf
56. OWASP (2017) Owasp Top 10. https://www.owasp.org/index.php/Top_10-2017_Top_10
57. CVSS (1995-2019) Special Interest Group. https://www.first.org/cvss/specification-document

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.