Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

A SECURITY ASSESSMENT FOR CLOUD SECURITY CONTROLS

[1] Ponnam Kishore, Assistant Professor, Dept.AIDS, Sri Indu College Of Engineering And Technology.
[2] Deepika Rathod Bhukya, Associate Professor, Dept.ECE, Sri Indu College Of Engineering And Technology.
[3] Dhanavath Nagaraju, Assistant Professor, Dept.CSE, Sri Indu Institute Of Engineering And Technology.

Abstract

Cloud computing is one of the most attractive technologies today due to its scalable, flexible and Cost effective access to infrastructure and application programs. Despite these advantages, cloud service users (csus) still have serious concerns about data security and privacy. Currently, there are many Cloud service providers (csps) that offer their customers a variety of services with different levels of security. Due to the variety of cloud services available, it can be difficult for customers to decide which csp to use and which option to choose. Currently, there is no basis for csus to evaluate csps based on their ability to meet customer security requirements. we propose a framework and methodology for evaluating the security capabilities of csps based on customer security preferences. We demonstrate the feasibility of our security assessment framework through research.

Keywords Cloud computing, Cloud security, Cloud auditing, Security metrics, Security index.

1. Introduction

The National Institute of Standards and Technology (NIST), formally defines cloud computing as a service model that enables convenient, on-demand network access to a large shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Cloud computing is considered as a new computing paradigm that provides numerous advantages to ser- vice providers, developers, and customers with respect to flexibility, scalability, and availability at lower cost [2]. Cloud services are offered to consumers through three fundamental service models defined by NIST as: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS is a service model in which vendors offer computing power (e.g., virtualized computer compo- nents) and networked storage space on-demand to consumers. PaaS, on the other hand, provides a computing platform as an on-demand service, upon which applications can be deployed and executed. Finally, SaaS provides consumers with on-demand software running on a cloud infrastructure.

The cloud computing model allows customers to use relatively low-cost, scalable, location-independent platforms for outsourcing one or more types of their internal IT infrastructures to a cloud service provider (CSP). This, in turn, allows businesses to reduce their IT costs and provide services to their consumers without worrying about the essential management and maintenance of their IT infrastructure. In spite of the several advantages that cloud computing brings, there are several concerns and issues that hinder the widespread adoption of this new computing paradigm [3]. Security and data privacy rank as the top challenges facing cloud computing, as outlined by recent surveys highlighting security as the greatest deterrence for the adoption of the cloud [4,5]. Another concern for enterprises migrating into the cloud is the colocation with potentially malicious tenants that can exploit side channels in shared hardware to ex-filtrate or manipulate the victim's sensitive data [6].

In the cloud computing paradigm, once organizations join a public cloud, they have limited their control over major aspects of security, conferring a substantial level of trust onto the CSP [7]. This scenario becomes more complex when most of the security- related key factors (e.g., transparency or collocation) are not clear or fully available to cloud users or third party auditors. This is mainly due

to the fact that the current cloud computing model does not have a centralized security auditing framework that could be used as a bridge between cloud users and CSPs in deciding the security needs and data privacy preferences.

Recent research work suggests that a major obstacle in cloud adoption is the lack of cloud auditability [2]. A near-real-time auditing framework is considered as the key to assuring the cloud. A near-real-time auditing framework provides an auditing structure that can help solve and ameliorate many concerns within the cloud such as issues related to data privacy, security, transparency, and portability [2]. Currently, most CSPs offer performance metrics to measure the physical performance and system usage of a cloud such as CPU utilization, latency, and network throughput. However, there has been little effort made on information assurance and security auditing metrics. In addition, the current efforts of CSPs are not enough to establish a well-defined auditing framework. To improve the existing cloud auditing capabilities, there is a critical need of both information assurance and security metrics that can be used toward building a comprehensive cloud auditing framework. Another major obstacle to the widespread adoption of cloud computing is the lack of quantitative information about the security status of a CSP. In particular, the security- related quantitative information helps cloud stakeholders in performing the robust and accurate cloud auditing of a potential CSP. All security-related issues and challenges, therefore, need to be addressed before a ubiquitous adoption of this new computing paradigm can happen.

This work is the continuation of our earlier research on cloud security auditing [15]. At present, there is no framework that can allow CSU to evaluate service providers and rank them based on their ability to meet the customer's security requirements. In this work, we propose a framework and a mechanism that evaluate the security strength of a CSP based on the customer's specified security preferences. Specifically, we present a security evaluation framework which consists of both conceptual and quantitative models. In general, the conceptual model will advance the theoretical understanding of the security issues in cloud security auditing whereas the quantitative model will provide the scientific techniques to establish a security index score for any given CSP or compare multiple CSPs for different security preferences. In particular, the proposed security evaluation framework consists of the following three key components: (a) security evaluation rules, (b) security metrics, and (c) security index analyzer. These three subcomponents of the proposed framework will assist a cloud service user (CSU) in determining the final security index value for a given CSP as well as analyzing the security index calculations for multiple CSPs. Both security index calculations and their analysis for multiple CSPs will be performed using the proposed security evaluation rules.

The security evaluation rules are envisioned as an underlying structure or a place- holder in the proposed framework which facilitates the (a) development of new metrics for security index calculations, (b) addition of new security evaluation rules for addressing different scenarios, (c) selection of an appropriate security metric for com- puting the security index score for a given CSP. The security evaluation rules will be subsequently used to analyze the security index scores for multiple CSPs.

The rule-based analysis of security index scores for multiple CSPs helps a CSU in making rational decisions, increasing the predictability of the quality of service (QoS), and allowing the appropriate proactive planning if needed before migrating to the cloud. To compute a security index score for a CSU, many unique cloud computing security factors and subfactors will be identified. To show the practicality of the pro- posed metric, we provide two case studies based on the available security information about two well-known CSPs. The results of these case studies demonstrate how the proposed framework may assist a CSU in determining the overall security level of a CSP using one of the available security metrics with respect to the CSU's desired security preferences.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

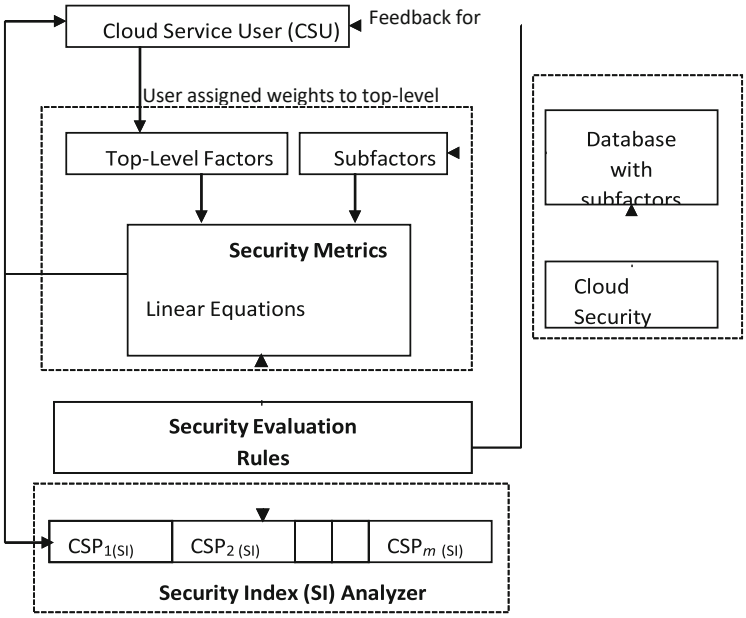

Fig. 1 A stakeholder oriented security evaluation framework

The remainder of the paper is organized as follows: In Sect. 2 of the paper, we provide the details of the proposed security evaluation framework. In Sect. 3, we dis- cuss the potential methods that can be used for computing security scores of CSPs. In Sect. 4, we derive the closed-form expressions to compute security scores using the linear equations. Section 5 presents a discussion on some of the key security factors and their relationships with cloud security auditing. In Sect. 6, we present the case studies and discuss the security index computation for multiple scenarios. Section 7 presents the related work. Finally, we conclude the paper in Sect. 8 with a brief discussion on future work.

2. Security evaluation framework

The proposed security evaluation framework consists of the following three main components: security metrics, security evaluation rules, and security index analyzer, as shown in Fig. 1. When a CSU wants to determine the security score of one or more CSPs, CSU defines its security preferences by providing weights to the top-level factors. Some of the key cloud computing top-level factors are discussed in Sect. 4 of this paper. The range of weights that a CSU can assign to a top-level factor to show its security concerns is shown in Table 1. The top-level factor may be further partitioned into one or more subfactors where each subfactor has a particular security score assigned by the database.

Table 1 System parameters and definitions

Label	Code (C_d)	Value	Definition
Critical	C_r	1.0	Represents the highest-degree of concern for a given factor
High	H_g	0.9	Represents the high-degree of concern for a given factor
Medium	M_d	0.6	Represents the mediocre concern for a given factor
Low	L_w	0.3	Represents the lowest concern for a given factor
None	N_o	0.0	Represents no concern for a given factor.
Unknown	U_k	0.5	The concern for a given factor is unknown

The cloud security auditors (CSAs) are responsible to populate, update, and main- tain the database to reflect the most appropriate security scores for the subfactors. The CSAs are assumed to be expert in the field of information security and they are able to determine appropriate scores for each subfactor based on the CSUs security require- ments and preferences. In addition, CSAs can use Consensus Assessments Initiatives Questionnaire (CAIQ) responses [30] from the Cloud Security Alliance group as a ref- erence to determine the relative importance of subfactors for a given top-level security domain. Additionally, CSAs can use their expertise to validate these responses as well as determine their appropriate security scores. Table 2 shows the top-level factors and subfactors along with their security scores.

Once the initial scores are determined, CSUs can then choose one of the available security metrics to compute security score for a CSP with respect to their security preferences. The security metrics of the proposed framework is envisioned as a com- ponent that should provide multiple scientific techniques (such as linear versus non linear methods) to CSUs for computing security scores of one or more CSPs. In this paper, we show how a security metric can be used to compute the security index scores for multiple CSPs using the linear set of equations. In general, the framework allows CSUs to use any method for computing security score of a CSP as long as it satisfies the proposed security evaluation rules.

The security evaluation rules are envisioned as an underlying structure or a place- holder in the proposed framework which facilitates the (a) development of new metrics for security index calculations, (b) addition of new security evaluation rules for addressing different scenarios, (c) selection of an appropriate security metric for com- puting the security index score for a given CSP. A CSU can use the security evaluation rules as a guideline to determine whether the final security score is in compliance with one of the specified evaluation rules. If the resultant security index score for a given CSP does not satisfy any of the evaluation rules with respect to the client's security preferences, a CSU will be notified with the recommendation of an alternative secu- rity metrics method. This instant feedback allows the CSU to choose an alternative security metrics (e.g., a security metrics based on fuzzy logic system) for computing the security index score.

Moreover, new set of evaluation rules can be created and added into the proposed framework for new security metrics (e.g., one of our future research goals is to develop a full set of evaluation rules for a security metrics using a fuzzy logic system). Finally, the security index (SI) analyzer of the proposed framework allows a CSU to examine the final security scores of one or more CSPs using the security evaluation rules. A high-level architecture of the proposed security evaluation framework is shown in Fig. 1.

3. Security metrics

In this research work, one of our goals is to develop a security evaluation framework independent to specific types of methods and consequently not to restrict a CSU to one specific method for computing security scores for one or more CSPs. In this section, we discuss some potential approaches that can be used by a CSU in computing security index score of a CSP.

4. Linear and nonlinear equations

As shown in Fig. 1, the primary objective of the Security Metrics in the proposed framework is to provide different alternative methods (such as linear and nonlinear equations) to CSUs for computing the security scores of a CSP using their defined security preferences. For a relatively simple security score calculation (e.g., one CSU needs to compute the security score of a CSP by quantitatively defining its security preferences using the weights for the top-level factors), a set of

linear equations can be used. As an example, a security metric based on the linear equations is proposed and discussed in detail in Sect. 4 of this paper.

However, when scenarios become complicated where multiple CSUs simultane- ously evaluating multiple CSPs on different security preferences for top-level factors, more generalized evaluation rules are needed to address all complexities. As a result, a simple set of equation may not be sufficient to handle the dynamics involved in complex scenarios and to provide accurate security scores.

This situation becomes worse if client's security preferences are not well defined, or the clients have partial or no knowledge about the top-level factors, making it hard to closely approximate the security scores for CSPs. To address this specific need, our proposed framework allows the development of new security metrics or equations (such as nonlinear equations and fuzzy logic) for addressing complex scenarios to provide optimal security index scores. As an example, the use of Fuzzy logic as one of the alternative methods to compute security score of service providers will be discussed briefly in the next subsection. In general, any equation can be used to compute a security index score for one or more CSPs as long as it satisfies the predefined security evaluation rules. The security evaluation rules, therefore, not only assist the development of new security metrics but also provide a systematic way to analyze multiple security indexes.

5. Use of fuzzy logic in a security metric

A Fuzzy Logic System (FLS) can be used to define nonlinear mapping on an input data set to produce scalar output data. In our proposed framework, the input data set will be populated by the CSU's input about the top-level factors as well as the evaluation performed by the CSA for the same factors. The nonlinear mapping will be done by establishing the set of rules and applying to input set of data to produce a quantitative security index. A FLS consists of four main parts as shown in Fig. 2.

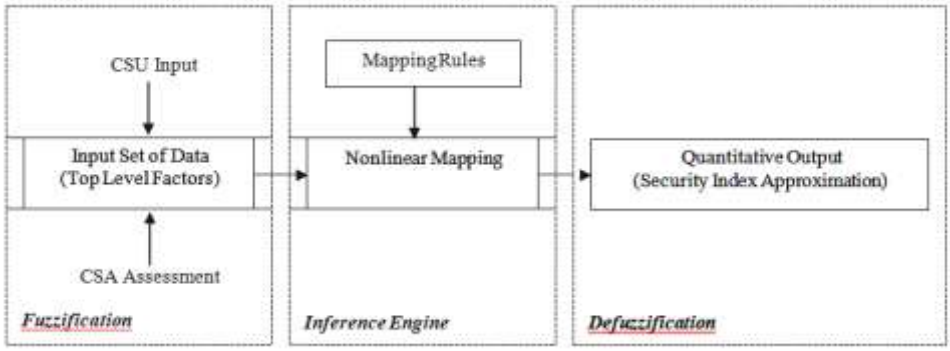

Fig. 2 Fuzzy logic system and its components

6. Security index computations using linear equations

Security metrics are used as a quantitative way to monitor and compare the level of security and data privacy attained by a CSU, as well as the current security status of a computing environment [8]. The use of security metrics promotes transparency, informed decision making, predictability and proactive planning [9].

This section presents the details of one of the alternative methods based on liner equations as a security metric. The security metric can be seen as a tool for providing information about the security status of a given cloud vendor. The security metric is developed based on the security auditing factors (some of these factors are discussed in Sect. 5). The primary objective of the security

metric is to produce a security index that describes the overall security level accomplished by an evaluated cloud computing vendor. The resultant security index will give confidence to different cloud stakeholders and is likely to help them with their decision making, increase the predictability, and allow the proactive planning if needed before migrating to the cloud.

The security metric considers a cloud user's inputs for top-level factors for quan- tifying the level of cloud computing security compliance. Some of these top-level factors will be discussed in the next section. Before the security index value is com- puted, the proposed system will inquire its users about what they care most and least about regarding various aspects of the cloud computing environment. These various aspects of a CSP will be defined by the proposed system through security-related auditing factors. For example, the data privacy and security aspects of a potential CSP might be viewed in the context of auditing factors such as portability, colocation, and transparency. This is one of the reasons that why the identification of security auditing factors is critical since it creates new security visibility in the cloud, which helps cloud auditors in performing a robust cloud audit of a potential or an existing CSP.

For instance, if transparency is considered as one of the top-level factors in secu- rity index computation, the user will be asked to provide its preferences for the given top-level factor. The security preferences of cloud user for a given factor will be spec- ified by assigning a certain weight. Although transparent from the user, the proposed security metric divides a top-level factor into multiple subfactors. The value of each subfactor is determined from system assessment of these subfactors with respect to each CSP. For example, portability can be divided in the following multiple subfactors

by the proposed system: operating system, location, storage, platform, etc. To show the implementation of the security metric, weights for the top-level factors and the security score of subfactors are shown in Tables 1 and 2, respectively.

What is most critical in computing the metric value is that each metric criterion needs to be further elaborated and mapped to subcriteria that will decide the system- generated score for the particular metric. This implies that the resultant security index will be computed by both considering the weights of the top-level factors (i.e., the user preferences) and the values of the subfactors (i.e., system assessments).

7. Related work

Research has been conducted on establishing cloud metrics and metrics-based evalua- tion algorithms that can be used to evaluate and compare the CSPs and assist the CSUs in decision making [20–23]. Zeng et al. proposed cloud service architecture to com- pare and select cloud services based on the adaptive performances and minimum cost as an evaluation metric [20]. Hussain et al. proposed a similar cloud service evaluation and selection scheme with the exception of an extended selection criterion (e.g., cost, pricing policy, and performance) [22]. Gui et al. proposed a hierarchical information model for integrating heterogeneous cloud information from different providers and a corresponding cloud information collecting mechanism [23]. Although, these research works slightly differ in their way of comparing and selecting the cloud services, they all consider performance metric (e.g., cost and performance benchmarks) as their pri- mary evaluation criterion. In this research work, our goal is to develop a framework to compare the CSPs using security as primary evaluation criterion.

There have been a few security evaluation frameworks recently proposed in the literature to evaluate and measure the security readiness of service providers [24–27]. For example, Habib et al. proposed a framework to verify and evaluate the security controls of a service provider [24]. In their work, authors introduced a decision model as an integral part of the framework to empower consumers to determine trustwor- thiness of cloud providers using both soft and hard trust properties. However, their proposed trust framework does not provide any means to take the cloud user's feed-back into account, making their security evaluation of a CSP static. Similarly, Ko et al. proposed a framework to address the issues related to cloud accountability and auditability using detective controls via technical and policy-based approaches [25]. Their proposed scheme can be considered as a conceptual framework which shows abstraction of layers needed for accountability in cloud computing. However, no quan- titative model was presented with the scientific techniques to establish a security index score for any given CSP or multiple CSPs. Tariq in [26] proposed basic building blocks needed to develop security metrics for cloud computing. Their framework assists cloud users to create information security metrics, analyze cloud threats, and perform threat assessment. However, their proposed framework does not provide specific quantita-tive ways to measure the security scores of service providers. Reixa et al. proposed a methodology to evaluate CSPs using the Multi-Criteria Decision Making (MCDM) model [27]. However, the scope of their proposed scheme is limited to small-size organizations.

Several other frameworks have also been proposed in the literature to rank the cloud services. Garg et al. proposed a framework for ranking cloud computing services using Service Measurement Index Cloud (SMICloud), which helps CSUs to find the most suitable CSP [28]. The approach proposed by them is mainly focused on the performance metric (e.g., execution time, cost, etc.) as an evaluation criterion. Our goal is to develop a framework that can evaluate the CSPs based on the customer's security requirements. Rivera et al. proposed an evaluation scheme that uses fuzzy logic to rank the CSPs based on the customer's evaluations of the Consensus Assessments Initiatives Questionnaire (CAIQ) [29]. Later, the CAIQ [30] was slightly modified to be used as a part of the proposed Fuzzy Likert Provider Security Measurement prototype [31]. Although CAIQ provides 140 security controls under eleven top-level security domains, how CSUs can objectively use them to find an appropriate CSP is still an open research problem. Lately, a framework was proposed that certify the security properties of cloud services (i.e., IaaS, PaaS, and SaaS) by using multiple types of evidence gathering with respect to security (e.g., testing services, monitoring agents or trusted computing proofs, etc.) [32].

Recently, a lot of research has been done to evaluate the CSPs and rank them based on their security readiness using the trust-based frameworks. The trust-based frameworks are critical in establishing the basic evaluation criteria for determining the trustworthiness of a CSP or comparing whether CSP A is more trustworthy than CSP B. For instance, Tian et al. proposed several factors that affect users' trust on CSP [33]. The impact of these factors was evaluated through a survey and a statistical analysis. In [34], the authors proposed a multi-faceted Trust Management (TM) system architecture which identifies trustworthy CSPs in terms of different attributes (e.g., security, performance, and compliance) using a trust metric. Since the subjectivity (i.e., customer feedback, observations, and experiences) plays a critical role in trust- based evaluation framework, it does not appropriately support the scientific ways (i.e., quantitative methods) to evaluate and compare the available CSPs.

Moreover, many schemes use the Service Level Agreement (SLA) between CSPsand CSUs as their evaluation criteria. Marudhadevi et al. proposed an SLA-based trust model to select the most suitable CSP for CSUs using performance parameters [35]. An SLA-aware trust model is proposed in [36], which uses the SLA management and trust techniques to provide a reliable model to select the best available provider among various cloud providers. In [37], a hybrid distributed trust model is proposed

to prevent SLA violations by identifying violation-prone services at the service selection stage. Recently, an SLA-based framework, SelCSP, was proposed, which combines trust- worthiness and competence to estimate the risk of interaction [38]. In their approach, the trustworthiness is computed using direct interactions or from feedbacks related to the reputations of vendors whereas the competence is assessed based on transparency in providers' SLA guarantees. We believe that SLA can be used as one of the impor- tant factors to compare the QoS of various cloud providers, but it cannot be used by itself as an evaluation framework. However, it is more like a provider-centric approach where the entire evaluation is typically done based on the SLAs of the potential CSPs without considering the user's security and QoS requirements. Since SLA varies from one provider to the other, it is difficult to build a single evaluation framework that can be generalized for all available CSPs. In addition, it puts a lot of computational burden on CSUs and requires skills/knowledge to compare and contrast the SLAs of potential CSPs.

8. Future research and conclusion

This paper presented a security evaluation framework which can be used to provide quantitative information to cloud users in the form of a security index. Moreover, we developed the security evaluation rules for a security metric that based on linear set of equations, which assist a CSU in analyzing the security index score of one or more CSPs as well as validating the final security score. We demonstrated how a security index can be calculated based on security specifications or preferences provided by a user, for different top-level factors. Since the internal details (e.g., security controls, procedures, and management policies) of cloud providers are often inaccessible to cloud users directly, the values of subfactors considered in the security index computation are assigned by a system whose input is in turn provided by either an auditor or machine. This can be considered as one of the primary advantages of the proposed security framework because the system computes the security index based on the minimum end user input. To show the practicality of the proposed framework, we provided two case studies according to publicly available security information about two well-known CSPs. The results of these case studies demonstrated the effectiveness of the security index in determining the overall security level of a CSP with respect to the security preferences of cloud users. We believe that the security index would give more confidence to different cloud stakeholders and is likely to help them with their decision making, increase the predictability of the quality of a CSP, and allow appropriate proactive planning if needed before migrating to the cloud.

One of our future research goals is to develop a full set of evaluation rules for a security metrics based on a fuzzy logic system. The ultimate goal of our cloud security auditing research is to build a system that interfaces end users on one side and auditors on the other. This system will provide a dashboard for CSUs who are interested in the up-to-date security status of their CSPs. Some of the data inputs to be processed by the semi-automated cloud security dashboard include pseudo-real-time data provided by hardware components constituting the cloud, such as the uptime of a hypervisor or the memory consumption of virtual machines leased to the CSUs. With the proposed system in place, a CSU can receive instant feedback on what the CSP is doing to keep its cloud service secure by simply taking a quick glance at the dashboard.

References

1. Peter M, Timothy G (2011) The NIST definition of cloud computing. National Institute of Standardsand Technology (NIST), version 15. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145. pdf
2. Park J, Spetka E, Rasheed H, Ratazzi P, Han K (2012) Near-real-time cloud auditing for rapid response. In: Proc. of the 26th International Conference on Advanced Information Networking and ApplicationsWorkshops, pp 1252–1257. doi:10.1109/WAINA.2012.78
3. Sen J (2013) Security and privacy issues in cloud computing. In: Antonio R (ed) Architectures and protocols for secure information technology, IGI-Global, USA, 2013. arxiv:1303.4814
4. Cloud Adoption Practices & Priorities Survey Report (2015) Cloud security alliance (CSA), https://cloudsecurityalliance.org/research/surveys/
5. Cloud Security Survey 2015: Trends in Cloud Security (2015) Alert Logic. https://www.alertlogic. com/resources/cloud-security-report-2015/

6. Juels A, Oprea A (2013) New approaches to security and availability for cloud data. Commun ACM 56(2):64–73. doi:10.1145/2408776.2408793
7. Bender D (2012) Privacy and security issues in cloud computing. Comput Internet Lawyer 29(10):1–15
8. Silva C, Ferreira A, Geus P (2012) A methodology for management of cloud computing using secu- rity criteria. In: Proceedings of the 2012 IEEE Latin America Conference on Cloud Computing and Communications, pp 49–54. doi:10.1109/LatinCloud.2012.6508157
9. Rees R (2011) PCI virtualization SIG releases guidelines. InFocus, Retrieved from: http://infocus.emc. com/richard_rees/pci-virtualization-sig-releases-guidelines
10. Litty L, Cavilla H, Lie D (2009) Computer meteorology: monitoring compute clouds. In: Proceedingsof the 12th Conference on Hot Topics in Operating Systems, USENIX Association, Berkeley, CA, USA, pp 4
11. Xen Hypervisor: the open source standard for hardware virtualization (2013) Xen.org. Retrieved from http://xen.org/products/xenhyp.html
12. Tholeti B (2011) Hypervisors, virtualization, and the cloud: learn about hypervisors, system virtu- alization, and how it works in a cloud environment. IBM Developer Works, http://www.ibm.com/ developerworks/cloud/library/cl-hypervisorcompare/
13. Sunyaev A, Schneider S (2013) Cloud services certification. Commun ACM 56(2):33–36. doi:10.1145/ 2408776.2408789
14. Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M (2013) A survey on security issues and solutions at different layers of cloud computing. J Supercomput 63(2):561–592
15. Rizvi S, Ryoo J, Kissell J, Aiken B (2015) A stakeholder-oriented assessment index for cloud security auditing. In: Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication (IMCOM '15). ACM, New York, NY, USA, Article 55, 7 pages. doi:10.1145/ 2701126.2701226
16. The notorious nine: cloud computing top threats in 2013 (2013) Cloud Security Alliance, Tech. Rep., Retrieved from: https://cloudsecurityalliance.org/group/top-threats/
17. Cappelli D, Moore A, Trzeciak R (2012) The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, aabotage, fraud). ser. SEI Series in Software Engineering. 1st edn. Addison-Wesley Professional, Boston
18. McCormac A, Parsons K, Butavicius M (2012) Preventing and profiling malicious insider attacks. Defence Science and Technology Organisation, Australian Government Department of Defense
19. Pauley W (2010) Cloud provider transparency: an empirical evaluation. IEEE Secur Priv 8(6):32–39.doi:10.1109/MSP.2010.140
20. Zeng W, Zhao Y, Zeng J (2009) Cloud service and service selection algorithm research. In: Proceedings of the first ACM/SIGEVO Summit on Genetic and Evolutionary Computation, ACM, pp 1045–1048
21. Martens B, Teuteberg F, Gräuler M (2011) Design and implementation of a community platform for the evaluation and selection of cloud computing services: a market analysis. In: Proceedings of EuropeanConference on Information Systems
22. Hussain FK, Hussain OK (2011) Towards multi-criteria cloud service selection. In: 2011 Fifth Inter- national Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp 44–48
23. Gui Z, Yang C, Xia J, Huang Q, Liu K, Li Z et al (2014) A Service brokering and recommendation mechanism for better selecting cloud services. PLoS One 9(8):e105297. doi:10.1371/journal.pone. 0105297
24. Habib SM, Varadharajan V, Muhlhauser M (2013) A trust-aware framework for evaluating security controls of service providers in cloud marketplaces. In: Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp 459–468. doi:10.1109/TrustCom.2013.58
25. Ko RKL, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, Qianhui L, Lee BS (2011) TrustCloud: a framework for accountability and trust in cloud computing. In: Proceedings of the 2011 IEEE World Congress on Services (SERVICES), pp 584–588. doi:10.1109/SERVICES.2011.91
26. Tariq M (2012) Towards information security metrics framework for cloud computing. Int J Cloud Comput Serv Sci 1(4):209–217
27. Reixa M, Costa C, Aparicio M (2012) Cloud services evaluation framework. In: Proceedings of the Workshop on Open Source and Design of Communication (OSDOC '12). ACM, New York, NY, USA, pp 61–69
28. Garg SK, Versteeg S, Buyya R (2013) A framework for ranking of cloud computing services. Futur Gener Comput Syst 29(4):1012–1023. doi:10.1016/j.future.2012.06.006
29. Rivera J, Yu H, Williams K, Zhan J, Yua X (2015) Assessing the security posture of cloud service providers. In: Proceedings of the 5th International Conference on IS Management and Evaluation— ICIME, pp 103–110
30. Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1 by Cloud Security Alliance (CSA). https://cloudsecurityalliance.org/group/consensus-assessments/
31. Yu H, Williams K, Yuan X (2015) Cloud computing threats and provider security assessment. Algo- rithms and Architectures for Parallel Processing. Vol. 9532 of the series Lecture Notes in Computer Science pp 238–250
32. Egea M, Mahbub K, Spanoudakis G, Vieira M (2015) A certification framework for cloud security properties. The Monitoring Path. Accountability and Security in the Cloud. Vol. 8937 of the series Lecture Notes in Computer Science, pp 63–77
33. Tian L, Lin C, Ni Y (2010) Evaluation of user behavior trust in cloud computing. In: Proceedings of the 2010 International Conference on Computer Application and System Modeling (ICCASM), pp.V7-567-V7-572. doi:10.1109/ICCASM.2010.5620636