Top Threats to Cloud: A Three-Dimensional Model of Cloud Security Assurance

Rakesh Kumar and Rinkaj Goyal

Abstract The incredible growth in the cloud applications and services reflects a positive swing in the thought processes of the business decision makers for cloud adoption. However, ever-evolving security and privacy issues continue to influence the decision makers to delay the cloud adoption. In this integrationist exposition, the previous publications are enriched and enhanced to holistically analyze different threats to cloud computing to conceptualize a three-dimensional model of cloud security assurance. These three dimensions, namely *Security Solution*, *Security Operation*, and *Security Compliance*, are interwoven to address the top threats to cloud computing, which are identified and reported by the cloud security alliance (CSA) research group in their latest and previous reports. The model will help practitioners to design and implement a security assurance system for a cloud ecosystem to strengthen trust in the cloud and accelerate its adoption to bring agility and velocity in cloud applications and services delivery in a cost-effective way.

Keywords Cloud security model · Cloud security requirements · Cloud security threats · Cloud security vulnerabilities · Cloud security solution

1 Introduction

In the last ten years, the observed exponential growth in cloud business model is attributed to cloud unique characteristics, extraordinary features, and evolved technologies. Figure 1 provides a snapshot of the cloud computing paradigm [29, 30]. The cloud service providers (CSPs) manage a pool of shared computing resources (storage, CPU, memory, software, hardware, network devices, etc.) to offer different services, mostly over the Internet, in the form of three service models—software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (Iaas). The cloud business model enables its consumers to allocate and deallocate the

R. Kumar · R. Goyal (✉)
University School of Information, Communication and Technology (USIC&T), Guru Gobind Singh (GGS) Indraprastha University, New Delhi 110078, India

S. Smys et al. (eds.), *Computer Networks and Inventive Communication Technologies*, Lecture Notes on Data Engineering and Communications Technologies 58,
https://doi.org/10.1007/978-981-15-9647-6_53

computing resources, as per their business requirements, using the self-service interfaces with pay-per-use model. There are five prime actors in the cloud environment as depicted in Fig. 1—*Cloud Provider*, *Cloud Consumer*, *Cloud Broker*, *Cloud Auditor*, and *Cloud Carrier*. These actors interact with each other and the deployed cloud environment as per their roles and responsibilities in the given business context.

The cloud computing environment can logically be expressed as seven layers of architectural components [29]. The user access level to these layers is determined by the service model and the deployment model used by the CSPs. *Public cloud*, *Private cloud*, *Community cloud*, and *Hybrid cloud* are the four models available for a cloud deployment (Fig. 1). These four deployment models blended with the three service models (SaaS, PaaS, and IaaS) enable the CSPs to provide a wide spectrum of service offering to fulfill the different business needs of the cloud consumers.

The distinctive characteristics of the cloud [30], like common resources pool, broad network accessibility, on request expeditious scalability, tailored self-service, service usage measurement, and others, have accelerated the growth trajectory of the cloud business models. Further, the amazing features of the cloud ecosystem, like modest initial capital investment, manageable operating cost, pay-as-you-go model, wide service accessibility, rapid deployment, provisioning, and scalability, low-cost disaster management, service continuity assurance, etc., have expedited the cloud adoption. Gartner [14] have forecasted worldwide revenue for the public cloud service will grow to 354.6 billion dollars by 2022.

However, this accelerated growth of cloud can continue to achieve the projections if the user's confidence and trust in cloud services do not lose its momentum. The lack of necessary assurance of a user's data security and privacy requirements is a significant deterrent for strengthening and maintaining the confidence and trust in cloud systems [17, 19, 37]. Table 1 highlights the fundamental security requirements—*Authentication*, *Integrity*, *Accountability*, *Confidentiality*, *Privacy*, *Availability*, and *Authorization*—of a cloud system and associated *STRIDE* threat category. The *STRIDE* security analysis technique considers—*S*poofing, *T*ampering, *R*epudiation, *I*nformation disclosure, *D*enial of service, and *E*levation of privilege—as the threat categories to analyze the impact on the security requirements of an information processing system for a given threat spectrum [26, 36]. The CSA have identified and published the top threats to cloud computing [6–9]. These threats impact fulfillment of the cloud security requirements and affecting the level of confidence and trust in cloud services [28]. The cloud service providers and consumers should analyze together the possible cause and impact of these threats and investigate its relevance for their business context. The outcome of the threat analysis will provide them an insight to identify the vulnerabilities in the cloud architectural components (Fig. 1). These identified vulnerabilities form the attack vectors and collectively the attack surface. The threat agents exploit these attack vectors to execute different attacks. Further, based on the threat analysis and identified vulnerabilities, the cloud service provider and the consumer shall design and deploy appropriate security controls as per their business context and security recommendations of the standardization organizations [4, 24, 31, 32].

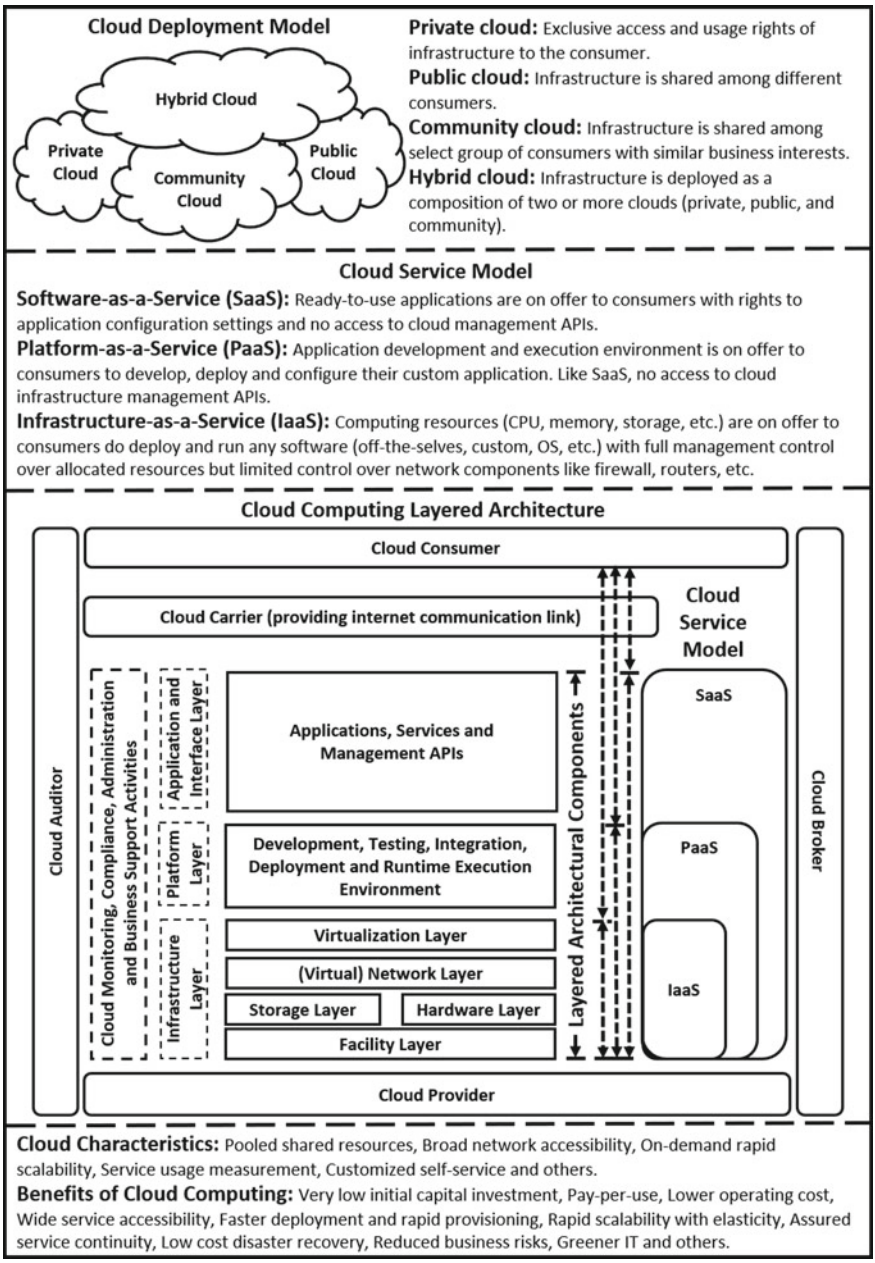

Fig. 1 A short descriptive overview of the cloud computing [29, 30]

Table 1 Security requirements and affecting *STRIDE* threat categories [26, 36]

Security requirements	Security task	*STRIDE* threat category	Threat context
Authentication	Establishing identity and right to access to cloud system and data of a requesting entity	*S*poofing identity	Using another user's credential for system access
Integrity	Ensuring and detecting user and system data are not altered accidentally or intentionally in an unauthorized manner	*T*ampering with data	Unauthorized modification of data with wrong intention
Accountability	Establishing the identify of an entity for its actions	*R*epudiation	Refutation for the actions performed by an entity
Confidentiality	Ensuring only authorized entity has access to the system information and user data	*I*nformation disclosure	Information exposure to unauthorized entities, intentionally or unintentionally
Privacy	Ensuring user data is only to be used for the agreed intended purpose		
Availability	Ensuring, when needed to use, user data is accessible and usable to authorized entities	*D*enial of service	Subscribed services are not available to the users
Authorization	Establishing access level of an authenticated entity	*E*levation of privilege	An unprivileged user gain access level of a privileged user

The proposed work is an extension of our previous publications [27, 28] to analyze the CSA's latest and previous reports, published in last ten years [6–9], on top threats to cloud computing for impact on cloud security requirements, to devise a three-dimensional model to minimize the cause and impact of these threats. The first research work [28] has analyzed the CSA's last published report [8] on twelve treacherous threats to cloud security and used *STRIDE* threat analysis for interrelated mapping of the threats, impacted security requirements, associated vulnerabilities, and suggested security solutions. The proposed research work is enhanced by including latest [9] and all previous reports [6–8] of CSA on top threats to cloud computing for a holistic impact analysis of different threats on cloud security requirements (Sect. 3 and Table 3). Our other work [27] provides a three-dimensional approach for cloud security assurance—deploying security solutions at cloud architectural layers,

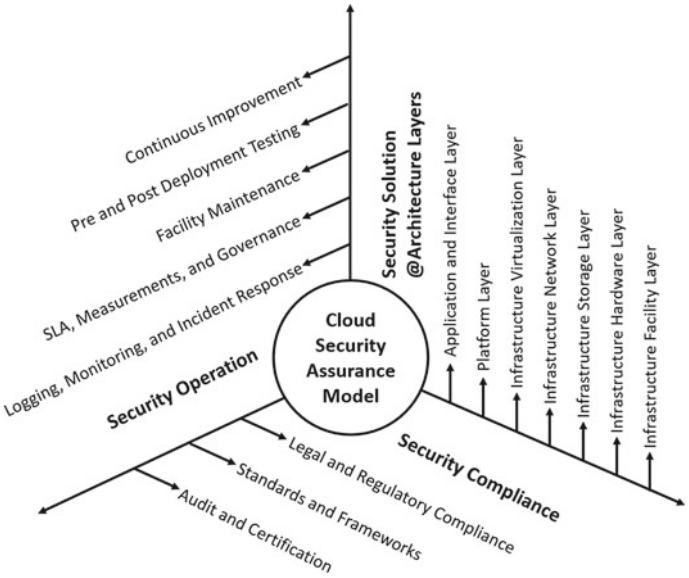

Fig. 2 Elements of the three-dimensional model for the cloud security assurance

maturing the deployed solutions with the security operation, and ensuring the required security compliance. The proposed research work enriches the three-dimensional perspective to three-dimensional model by enriching the dimensions with different security elements (Sect. 4 and Fig. 2). This work has conceptualized a three-dimensional model that comprises of adaptive, proactive, and reactive approaches. The first dimension, *security solution* focuses on eliminating or minimizing the vulnerabilities for the cloud architectural layered components by deploying the required security measures. *Security operation*, the second dimension, implements the continuous security event monitoring and security incident response system for the deployed cloud environment with continuous improvement program governed through a governing body. The third dimension, *security compliance*, focuses on providing the legal and regulatory compliance and following the recommendations of the standardization organizations. It has been believed that this three-dimensional model can be used by the practitioners as a checklist for deploying the continuous security assurance measures for the cloud business model to enhance agility and velocity of the service delivery with security.

In the rest of this paper, a comparative view of related works is provided in Sect. 2. CSA's top threats are analyzed in Sect. 3. Section 4 provides a three-dimensional model to minimize the impact of the top threats to cloud computing. Section 5 provides conclusion and future work in the related areas.

2 Related Work

Table 2 provides a comparative overview of published work in the related area of cloud computing security threats, requirements, challenges, and countermeasures. Most of the research works have discussed the cloud security challenges analysis and associated solutions [2, 3, 5, 12, 17, 28, 37, 40, 43]. However, in very few research works, the cloud security threat analysis is observed [5, 17, 19, 28, 37, 40, 41, 43] from the impact on the security requirements [2, 3, 12, 28, 41, 43] perspective and measures to address the same.

The proposed work provides an integrated three-dimensional conceptual model for addressing the impact on security requirements arising from CSA identified top threats to cloud computing [6–9]. This research work has outlined the integrated security elements for cloud security assurance along these three dimensions, namely *security solution*, *security operations*, and *security compliance* (Fig. 2). *Security solution* emphasizes on assurance of security measures implementation at all the layers of cloud architectural components during cloud adoption phase. *Security operation* enforces logging, monitoring, incident response, SLA performance, governance, continuous improvement, etc., mechanisms for security assurance. *Security compliance* practices aim to fulfill the legal and regulatory requirements for building trust and confidence in users. This three-dimensional approach is devised based on the CSA top threat analysis.

3 Analyzing CSA's Top Threats to Cloud Computing for Impact on the Security Requirements

Table 3 provides analytical mapping of CSA's top cloud threats and their impact on security requirements. This mapping is based on the *STRIDE* threat analysis model [6–9, 26, 28, 36]. A close look at Table 3 reveals five new threats *misconfiguration and inadequate change control*, *lack of cloud security architecture and strategy*, *weak control plane*, *metastructure and applistructure failures*, and *limited cloud usage visibility* are mentioned in 2019 report [9] as compared to the previous reports. In 2016 report [8], three new threats appeared, namely *weak identity, credential and access management*, *system and application vulnerabilities*, and *advanced persistent threats (APTs)*. *Denial of service* and *insufficient due diligence* were two new entrant in the 2013 report [7] as compared to the very first report of 2010 [6]. The gradual appearances of the new threats in CSA's reports on top threats to cloud computing assert the evolving spectrum of the threats.

In Table 3, the fundamental security practices mentioned along with the mapping can be used by the practitioners to minimize the impact. These fundamental practices are extended to address the vulnerabilities arising from the cloud unique characteristics, layered architecture components, enabling technologies, and evolutionary business model. The cloud security assurance is a continuous journey that

Table 2 A comparative view of the related works

Related work	Year	Major area discussed	X1	X2	X3	X4	X5	X6
Zhang et al. [42]	2010	Cloud computing design challenges and commercial solution deployed by the cloud providers	F	N	P	N	P	N
Grobauer et al. [16]	2011	Vulnerabilities and risk analysis in cloud computing inherent to its unique characteristics, architecture, and underlying technologies	F	N	F	N	P	N
Zissis and Lekkas [43]	2012	Cloud security requirements, threats, and solution recommendation using trusted third-party	P	F	F	P	F	N
Hashizume et al. [17]	2013	Threats, attacks, and vulnerabilities in the cloud from service level agreement perspective, their mapping and countermeasures	P	P	F	P	F	N
Fernandes et al. [12]	2014	Cloud security issues taxonomy, its architecture, underlying technologies, vulnerabilities, threats, and attacks	F	F	F	N	F	N
Ali et al. [2]	2015	Cloud security challenges and available solution analysis with a use case of mobile cloud computing vulnerabilities	P	F	F	N	F	N
Ardagna et al. [3]	2015	Cloud security taxonomy, design, and development recommendations for different security techniques and assurance processes	N	F	F	N	F	N
Sgandurra and Lupu [37]	2016	Attacks evolution, threat models, and solutions for virtualized systems	F	P	F	F	F	N

(continued)

Table 2 (continued)

Related work	Year	Major area discussed	X1	X2	X3	X4	X5	X6
Coppolino et al. [5]	2017	Cloud attack vectors, security challenges, existing solutions to address the attacks with example industry deployed solutions	N	N	F	F	F	N
Subramanian et al. [40]	2018	Cloud computing overview, security countermeasure for the issues at computational, SLA, and communication levels	P	N	F	F	F	N
Hong et al. [19]	2019	Cloud threats, vulnerabilities, attacks and their mappings	F	N	F	F	F	N
Kumar and Goyal [28]	2019	Cloud security threats, requirements, vulnerabilities, trust, privacy, and countermeasures with their mappings	F	F	F	F	F	N
Tabrizchi et al. [41]	2020	Cloud security threats, vulnerabilities, challenges, requirements, and solutions	F	F	F	F	P	N
This work	–	Cloud architectural overview, analysis of top threats and its impact on security requirements, security challenges, and an integrated three-dimensional model of countermeasures	F	F	F	F	F	F

X1: cloud computing overview and architecture, X2: cloud security requirements,
X3: cloud security challenges and threats, X4: cloud security threat analysis,
X5: cloud security countermeasures to the challenges and threats, X6: integrated cloud security solution model
F Fully covered; *N* Not covered; *P* Partially covered in the corresponding work

Table 3 Impact of CSA's top threats on cloud security requirements

CSA identified top threats to cloud computing	Threat order				Impacted security requirements							Fundamental security practices
	2019	2016	2013	2010	R1	R2	R3	R4	R5	R6	R7	
• Data breaches	1	1	1		×						×	Strong encryption, cryptography key size, multi-factor authentication, and a robust incident response system
• Misconfiguration and inadequate change control	2				×	×	×	×	×	×	×	Adopt agile approach to change control for cloud dynamic resource management, preferably automated
• Lack of cloud security architecture and strategy	3				×	×	×	×	×	×	×	Develop a robust security strategy and adaptive security architecture aligned with business objectives
• Insufficient identity, credential, access, and key management[a]	4	2			×	×	×	×	×	×	×	Federated identity, strong password, multi-factor authentication, cryptography key rotation policy
• Account Hijacking[b]	5	5	3	6	×	×	×	×	×	×	×	All accounts tagged to the individuals, no sharing of the accounts, two-factor authentication, and logging and monitoring of the accounts activities

(continued)

Table 3 (continued)

CSA identified top threats to cloud computing	Threat order				Impacted security requirements							Fundamental security practices
	2019	2016	2013	2010	R1	R2	R3	R4	R5	R6	R7	
• Insider Threat[c]	6	6	6	3	×	×		×			×	Segregation of duties, role-based access control, logging, monitoring and auditing of administrative activities, and encryption and key management policy
• Insecure interfaces and APIs[d]	7	3	4	2	×	×			×	×	×	Security enabling design, development and testing guidelines for APIs, like appropriate authentication and authorization, using encryption, pentesting, etc.
• Weak control plane	8				×	×		×	×	×	×	Identify and implement adaptive security controls
• Metastructure and applistructure failures	9				×	×	×	×	×	×	×	Develop cloud-native applications and security controls, regular scanning, pentesting, and patching
• Limited cloud usage visibility	10				×	×	×	×	×	×	×	Enforcement of cloud usage policies, service request authenticity and service usage monitoring, etc.

(continued)

Table 3 (continued)

CSA identified top threats to cloud computing	Threat order				Impacted security requirements							Fundamental security practices
	2019	2016	2013	2010	R1	R2	R3	R4	R5	R6	R7	
• Abuse and nefarious use of cloud services	11	10	7	1			×					Implement resource monitoring system to detect, act, and prevent the misuse of cloud service offerings and fraudulent resource consumption
• System and application vulnerabilities		4			×	×	×	×	×	×	×	Apply security by design methodology, vulnerability scanning, rectify security gaps, and apply patches
• Advanced persistent threats		7			×				×		×	Provide continuous awareness to the users on such threat techniques, like social engineering, and associated countermeasures to recognize and handle them
• Data Loss		8	2	5			×			×		The cloud provider to maintain geographic redundancy for data backup and cloud consumers can also have in-house backup for the business-critical data

(continued)

Table 3 (continued)

CSA identified top threats to cloud computing	Threat order				Impacted security requirements							Fundamental security practices
	2019	2016	2013	2010	R1	R2	R3	R4	R5	R6	R7	
• Insufficient due diligence		9	8		×	×	×	×	×	×	×	Analyze the capabilities and key performance parameters of different cloud providers against the desired business objectives for selecting a CSP
• Denial of service		11	5				×					Implement and administer an effective system for DoS attack prevention, detection, and response
• Shared technology vulnerabilities		12	9	4	×				×		×	Secured resource isolation on shared platforms and resource recycling before reallocation
• Unknown risk profile				7	×	×	×	×	×	×	×	CSPs to alert the user for deviations from the expected behavior and provide logs, data and shared infrastructure details for analysis of malicious activities

R1: confidentiality, R2: integrity, R3: availability, R4: authentication, R5: authorization, R6: accountability, R7: privacy

[a] In 2016, this threat was named as "Weak Identity, Credential and Access Management"

[b] In 2010, this threat was named as "Account, Service Traffic Hijacking"

[c] In 2010, 2013, and 2016, this threat was named as "Malicious Insiders"

[d] In 2010, 2013, and 2016, this threat was named as "Insecure APIs"

begins with the design and implementation of adaptive security solutions and continues with proactive and reactive security operations along with security compliance fulfillment. It requires an integrated three-dimensional approach, consisting of *security solution*, *security operation*, and *security compliance*, for minimizing the cause and impact of CSA's identified threats on cloud security requirements.

4 Minimizing the Cause and Impact of the Threats: A Three-Dimensional Model of Cloud Security Assurance

The objective of cloud security measures is to minimize or eliminate the vulnerabilities in the cloud computing environment to reduce the attack surface and fulfill the different security requirements (Table 1). The vulnerabilities in cloud computing environment are due to the inherent vulnerabilities in cloud computing underlying technologies (like, OS, communication protocol, APIs, etc.), vulnerabilities in its architectural components (like, virtual machine, hypervisor, virtual network, etc.), vulnerabilities arising from cloud specific characteristics (like, resource sharing, multi-tenancy, etc.), and evolving business delivery model (like, multi-cloud, inter-cloud, federated cloud, etc.) [28]. The proposed research work has conceptualized a three-dimensional model that comprises of adaptive, proactive, and reactive approaches for minimizing or eliminating the different vulnerabilities.

4.1 Security Solution: The First Dimension

The security solution dimension focuses on the design and implementation of different security measures to eliminate or reduce the vulnerabilities in the architectural components for reducing the attack surface and attack probability. Figure 1 presents the cloud computing environment as layered architectural components forming the attack vector. Table 4 outlines different security solutions to implement at corresponding architectural layered components for addressing their inherent vulnerabilities and minimizing the attack vector [4, 24, 28, 31, 32].

The implemented solutions are not static in nature. The solution shall be reviewed in regular governance for its relevance and needs to be adapted with the evolving attack surfaces and the threat spectrum. With the deployment of the security solutions, security operation takes over for continuous security assurance as second dimension.

Table 4 Recommended security solutions for cloud architectural components [4, 24, 28, 31, 32]

Cloud layered architecture components	Security vulnerabilities and issues	Recommended security solutions
Application and interface layer	SQL injection, cross-site scripting, SOAP wrapping attack, session hijacking, weak cryptography key, and credential management	• Use web services security protocols and standards, like WS-Security, WS-Trust, WS-Federation, XACML, XML-Encryption, XML-Signature, SAML, etc.
		• Limit sessions, use one-time cookies, secure protocols, and browser security patching
		• Use security enabling web application development techniques, web application scanner, and ensure security testing
Platform layer	Absence of secure software development and lifecycle processes, OS patching and monitoring, open source, and third-party software	• Access control to development, testing, and execution environment
		• Operating system (OS) level segregation to enable multi-tenancy
		• Security hardening of OS, monitoring of appropriate logs, and OS security patching
		• Follow the security development lifecycle and apply security development best practices including security testing for abuse cases and pentesting

(continued)

Table 4 (continued)

Cloud layered architecture components	Security vulnerabilities and issues	Recommended security solutions
Infrastructure virtualization layer	Cross-VM attack, VM hopping, side-channel and covert-channel attack, VM sprawl, dormant image, live VM migration attack, replay	*Measures for virtual machine (VM) life cycle security*
		• Use hardware supported trusted virtual platforms, like vTPM
		• Access control for VM image lifecycle management, VM image filtering, provenance tracking, VM images scanning, patching, and encryption
		• Secure VM migration and rollback by use of secured pre-copy and live migration techniques, trusted framework for live migration and rollback
	VM escape, VMM inspection and interposition, VMM untrusted components and single point failure	*Measures for hypervisor/virtual machine manager (VMM) security*
		• Hardware-assisted VMM chardening
		• Use VM isolation, VM introspection, and VMM level centralize monitoring
		• Use security-aware development practices for hypervisor software and function-based modular design for hypervisor to reduce attack surface
	Communication channel invisibility, cross-tenant attacks, data exfiltration	*Measures for virtual network communication security*
		• Using trusted virtual domains, secured routing and firewall protection • Use software-defined networking (SDN)-based communication

(continued)

Table 4 (continued)

Cloud layered architecture components	Security vulnerabilities and issues	Recommended security solutions
Infrastructure network layer	Sniffing and spoofing, cookie theft/poisoning, network devices inherent vulnerabilities, session hijacking/riding, weak keys in SSH and TLS, insecure protocols	• Deploy intrusion detection, prevention, mitigation, and response system
		• Use firewalls, virtual LANs, network traffic analyzers, regular scanning and pentesting for identifying vulnerabilities, their rectification and patching
		• Performance measurement and assessment of network devices, like routers and switches, to take proactive measures, like device load balancing
		• Encrypt data-in-motion and use encrypted protocols for all communication to ensure integrity, confidentiality, and privacy of user data
Infrastructure storage layer	Faulty and obsolete encryption techniques, unauthorized access, storage multi-tenancy, information disclosure, loss of control, data integrity, and availability	• Define data classification and access control level as per data criticality
		• Encrypt data-in-store, using appropriate techniques, like AES, homomorphic, etc., for data integrity and remove data before storage device recycling
		• Ensuring data availability, support for provable data possession (PDP), dynamic provable data possession (DPDP), and proof of retrievability (POR)
		• Transparency in data storage location, multi-location backup, recovery and data de-duplication methods, in-house backup of business-critical data

(continued)

Table 4 (continued)

Cloud layered architecture components	Security vulnerabilities and issues	Recommended security solutions
Infrastructure hardware layer	Hardware resource limitations, faults, data integrity, and availability	• Fault tolerant, high-performing, and scalable hardware with auto load balancing. Use secured hardware infrastructure architecture for enabling enhanced cloud security solution, like vTPM, hardware-based cryptography
Infrastructure facility layer	External and internal intruder, tampering, theft, cold boot attack, natural disaster, environmental factors, data loss	• Implement physical security controls to prevent unauthorized access to physical assets and systems, e.g., biometric, CCTV
		• Implement security controls for physical security of the facility and maintaining environmental hygiene of the facility for proper functioning of the hosted devices and equipment
		• Ensure disaster management and business continuity plans are in place

4.2 Security Operation: The Second Dimension

Security operation is backbone for data security and privacy assurance in the cloud computing environment. The security operation begins with deployment of the offered services, with required security solution measures. In cloud security operations, the implemented security solutions are continuously monitored, measured, and assessed for its effectiveness and relevance for the continuous security assurance. Based on observation and findings, necessary preventive, corrective, and improvement actions shall be initiated for continuous data security and privacy assurance.

- **Logging, Monitoring, and Incident Response**: Logging of resource usage, user activities, data processing, system changes, etc., shall be enabled and monitored. The monitoring identifies the uncontrolled and unauthorized usage of resources and system changes, deviations from the expected system and user behavior, malicious access and data traffic, etc. These deviations are captured as security events and monitored to trigger the security incident response system as per defined criteria. The objective of security incident response team is to bring the system back to normalcy and initiate the root cause analysis of the incident to take proactive

measures to avoid such incidents in the future. The resource usage monitoring provides insight into service delivery performance levels and identify any deviation from the service level agreement (SLA). For example, observed high CPU utilization may lead to slower response time to users requests causing SLA deviation. Such SLA deviations shall be captured and initiate necessary improvement actions. Monitoring also identifies fraudulent use of resources. The CSPs shall use the appropriate tools for integrated logging, monitoring, analysis, and alerting for deviations [1, 11, 39]. The effectiveness of such tools is in granularity and accuracy in capturing relevant data, evaluating the metrics, determining the performance level and deviation, analyzing them to retrieve valuable information, and presenting them from different perspectives. The cross-domain (inter-cloud, federated-cloud, multi-cloud), cross-layers, containerization and evolving cloud services put demand on state-of-the-art high-performing monitoring tools with built-in capabilities of autoscaling and autorecovery.

- **SLA, Measurements, and Governance**: SLA is a legal contract between the cloud service provider and the user with financial implications. It specifies the different terms and conditions of service delivery, including the prescribed level of service delivery performance. The unique characteristics of the cloud computing environment require a different set of SLAs as compared to traditional IT services. Time to scaling or descaling the number of VMs, auto scaling, pay-per-use (time-based or resource-based), number of concurrent user sessions, service resource availability, loss of data, data access response time, regulatory compliance, investigative support, data and service recovery, etc., are some of the parameters to consider when defining the SLA for the cloud service delivery. The SLA document contains the measurable key security control performance parameters, methods to measure them, and ranges of measured values for the expected and accepted performance level of service delivery. It is recommended to use automation tools for data collection, performance value calculation, analysis, report generation, and distribution to the stakeholders. This will facilitate the transparency, common understanding, and quick actions on deviations and improvements.
  Further, a structured governance shall be in place to regulate security policies and strategies, service offerings, and assess service delivery and security performance against the SLA along with the effectiveness of change control and patch management processes. For an effective governance, the governing body shall constitute with the representatives from all the relevant cloud actors and empowered to take decisions. The governance team plays a pivotal role in defining and improving end-to-end security of the cloud by analyzing the cloud service delivery performance, service usage experiences of end users, and initiating continuous improvement activities. The governance team shall evaluate evolving state-of-the-art cloud technologies and adopting some of them to stay relevant in the competition. This group shall, also, review and adapt the changing requirements for legal compliance, certifications, and audits.
- **Facility Maintenance**: The data centers host the cloud physical infrastructure to deliver the cloud service offerings. So, the CSPs to ensure the facility that house these data centers have appropriate levels of cooling, routine electrical mainte-

nance, and physical security controls like badges, gates, and fences in place. The regular preventive maintenance of facility can limit the damages to physical systems and network resources to improve the service availability.

- **Pre- and Post-Deployment Testing**: Most of the time, time-to-market get precedence over testing, especially the security testing. Lack of necessary testing has the cascading impacts, like disruption in offered services due to cyber-attacks caused from the untested vulnerabilities, penalty for loss of user data privacy, etc. This can be addressed through automation of testing activities aligned with change control and patch management processes. All the software applications and components in use to deliver the services must be tested for fulfillment of the security requirements. Specific security testing, including static application security testing (SAST), dynamic application security testing (DAST), and interactive application security testing (IAST), abuse cases, penetration, and injection cases, should be performed at respective phases of application development, delivery, and operation.
- **Continuous Improvement**: The outcomes of the root cause analysis of the security incidents, observed monitoring deviations, trend analysis of the performance measurements, governance reviews, etc., provide opportunities for continuous improvement in security measures implemented by the CSPs. The continuous security awareness and training sessions for stakeholders to improve effectiveness of the deployed security measures.

4.3 Security Compliance: The Third Dimension

The third dimension focuses on being transparent to legal and regulatory compliance authorities, open to audits, and following the security recommendations of the standards organizations. The CSPs must transparently share the implemented measures for data security and privacy assurance to their users and compliance authorities. The legal compliance, certification audit, and implementation of security measures, as per the recommendations of standardization organizations reflect, the level of effectiveness and sufficiency of implemented security measures.

- **Legal and Regulatory Compliance**: Cloud computing unique characteristics, like resource sharing, multi-tenancy, virtualization, multi-location outsourcing, etc., require cloud providers to ensure legal and regulatory compliance to prevailing laws of the cloud infrastructure hosting country [13]. Geographically distributed multi-location data storage, to support redundancy and business continuity, causes ambiguity in deciding the jurisdictions for data privacy compliance and data lifecycle management [18]. Digital forensic requirements may conflict with the legal and privacy requirements of the cloud infrastructure hosting country. It becomes more complex to provide compliance when user data falls under different jurisdictions. Forensic-as-a-service (FaaS), security logging-as-a-service (SLaaS), and forensic-by-design (FbD) are some of the suggested solution for providing compliance data

[25, 35]. For every individual in European Union and European Economic Area, general data protection regulation (GDPR) enforces data protection and privacy for them. Businesses and organizations, including cloud service providers, managing the personal data of users must comply to GDPR or face financial penalties [15]. The inappropriate metering and billing of resource usage arising due to on-demand and pay-per-use flexibility may lead to financial non-compliance and associated legal implications [34].

- **Standards and Frameworks**: Security standards and frameworks by the standardization organizations provide a structured approach for fulfilling the security requirements [4, 24, 31, 32]. It is not mandatory to follow the recommendations, however, being compliant to such recommendations provide a common language for understanding the best practices followed by a CSP. A CSP being compliant of such standards and frameworks raises users confidence. Using the recommended guidelines, it enhances the interoperability and portability of the service offerings and enables the CSPs to adopt inter-cloud, multi-cloud, or federated-cloud kinds of collaboration for widening their service offerings.
- **Audit and Certification**: Cloud providers shall seek for audits and certification from the third-party to assess whether required security measures are in place and are working as per expected behavior. It brings visibility and transparency on CSP's commitment for providing secured services by implementing necessary and sufficient security measures. The certification auditor performs artifact collection, verification, and validation to certify the same. The audit process shall ensure confidentiality and privacy of user data under audit. It is desirable to perform security certification and audits continuously, enabled through automation, considering dynamism in resource allocation and service requests in a cloud computing environment. Integrity check of the remotely stored data can be performed with the remote data audit (RDA) technique [38]. In RDA, a small fragment of data from the whole data is spot-checked for deterministic or probabilistic assurance of data intactness. Replication-based, erasure-coding-based, and network-coding-based are the widely used techniques of remote data auditing [38]. ISO/IEC 27001:2013 [20], ISO/IEC 27002:2013 [21], ISO/IEC 27017:2015 [23], ISO/IEC 27018:2014 [22], CSA security trust assurance and risk (STAR) [10], National Institute of Standards and Technology (NIST) 800-53 [33], are some of the recognized standards certifications for information security and data privacy assurance.

4.4 Inferences

In comparison to other works or models (Sect. 2), the proposed conceptual model provides a holistic approach for cloud security assurance against the top threats to cloud computing. In most of the works or models, the generic cloud security challenges and associated solutions are provided [2, 3, 5, 12, 17, 28, 37, 40, 43]. Some of the previous works or models have as well discussed about the cloud security threat analysis [5, 17, 19, 28, 37, 40, 41, 43] and its impact on the security requirements. However,

the proposed model provides an integrated and inter-working approach for implementation of security solution based on cloud top threats analysis, measuring the effectiveness and sufficiency of the implemented solution during security operation, and ensuring the security compliance as per the legal and regulatory requirements and standards recommendations.

The conceptual model depicted in Fig. 2 may be used as a quick reference sheet while planning and designing a security management system by cloud security practitioners. In Tables 3 and 4, the list of suggested security solutions for the different cloud architectural layers can be used as a reference checklist during due diligence for selecting a suitable cloud provider. The different aspects of cloud security operations described in the second dimension can be used for continuous security assurance and avoiding the security incidents. The fulfillment of legal compliance, certification, and audit requirements and following the security recommendations of standards organizations further strengthen the CSPs commitment to deliver security enabled services to the cloud users. Collectively, these three dimension works in tandem to boost the confidence and trust of the users for transition of their business processes to the cloud. The proposed model can measure the security assurance level that could be achieved through the proposed model by defining and measuring the applicable security metrics for a given business context. The audit and compliance reports from the third-party can also be used for determining the security assurance level provided through this model.

5 Conclusion and Future Work

In this decade, cloud business models have unleashed and capitalized the cloud potentials to a large extent and forecasted to grow further for coming years. However, the security and privacy threats remain a consistent factor to address. The adoption of the proposed integrated three-dimensional model, encompassing security solutions, security monitoring, and security compliance, will help practitioners in limiting the attack vectors. The evolution in cloud technology, business model, threat spectrum, and compliance requirements will require a regular integrated approach to review, assess, and plan continuous improvement in security control and measures to adapt. This can be done through the lens of the described three-dimensional model. With a focus on effective automation of the activities along these three dimensions, using artificial intelligence and data analytic enabled tools, is expected to address many of the CSA's identified threats to cloud computing. Further, the evolution of technologies and business delivery models will require a more comprehensive adaptive approach for managing the dynamism of cloud resources, user data, and most importantly, the user behavior. The evolving user behavior may become a dominant factor for evolved complex systems. Consequently, future research work could explore the dynamism in user behavior as the fourth dimension, focusing on analysis of user behavior using data analytic and machine learning techniques to identify and implement required level of adaptation mechanism in cloud security controls and measures, for strengthening trust in cloud solutions.

References

1. Alhamazani K, Ranjan R, Mitra K, Rabhi F, Jayaraman PP, Khan SU, Guabtni A, Bhatnagar V (2015) An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art. Computing 97(4):357–377. https://doi.org/10.1007/s00607-014-0398-5
2. Ali M, Khan SU, Vasilakos AV (2015) Security in cloud computing: opportunities and challenges. Inf Sci 305:357–383. https://doi.org/10.1016/j.ins.2015.01.025
3. Ardagna CA, Asal R, Damiani E, Vu QH (2015) From security to assurance in the cloud: a survey. ACM Comput Sur 48(1):1–50. https://doi.org/10.1145/2767005
4. CISA (2018) Cloud security guidance v0.2. Homeland Security, USA
5. Coppolino L, D'Antonio S, Mazzeo G, Romano L (2017) Cloud security: emerging threats and current solutions. Comput Electr Eng 59:126–140. https://doi.org/10.1016/j.compeleceng.2016.03.004
6. CSA (2010) Top threats to cloud computing. Tech. rep. V1.0, Cloud Security Alliance
7. CSA (2013) The notorious nine: cloud computing top threats in 2013. Tech. rep., Cloud Security Alliance
8. CSA (2016) The treacherous 12–cloud computing top threats in 2016. Tech. rep., Cloud Security Alliance
9. CSA (2019) Top threats to cloud computing: the egregious eleven. Tech. rep., Cloud Security Alliance
10. CSA (2020) Security Trust Assurance and Risk (STAR). https://cloudsecurityalliance.org/star/
11. Dobran B (2018) 23 cloud monitoring tools: the definitive guide for 2020. https://phoenixnap.com/blog/cloud-monitoring-tools
12. Fernandes DAB, Soares LFB, Gomes JV, Freire MM, Inácio PRM (2014) Security issues in cloud environments: a survey. Int J Inf Secur 13(2):113–170. https://doi.org/10.1007/s10207-013-0208-7
13. FISMA: Federal Information Security Modernization Act (2020). https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
14. Gartner (2019) Gartner forecasts worldwide public cloud revenue to grow 17. https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020
15. GDPR (2018) EU data protection rules. https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en
16. Grobauer B, Walloschek T, Stocker E (2011) Understanding cloud computing vulnerabilities. IEEE Secur Privacy 9(2):50–57. https://doi.org/10.1109/MSP.2010.115
17. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB (2013) An analysis of security issues for cloud computing. J Internet Serv Appl 4(1):1–13. https://doi.org/10.1186/1869-0238-4-5
18. HIPAA: Health Information Privacy (1996). https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
19. Hong JB, Nhlabatsi A, Kim DS, Hussein A, Fetais N, Khan KM (2019) Systematic identification of threats in the cloud: a survey. Comput Netw 150:46–69. https://doi.org/10.1016/j.comnet.2018.12.009
20. ISO: ISO/IEC 27001:2013—information security management systems requirements (2013). https://www.iso.org/standard/54534.html
21. ISO: ISO/IEC 27002:2013—code of practice for information security controls (2013). https://www.iso.org/standard/54533.html
22. ISO: ISO/IEC 27018:2014—code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (2014). https://www.iso.org/standard/61498.html
23. ISO: ISO/IEC 27017:2015—code of practice for information security controls based on ISO/IEC 27002 for cloud services (2015). https://www.iso.org/standard/43757.html

24. Jansen W, Grance T (2011) Guidelines on security and privacy in public cloud computing (SP 800-144). National Institute of Standards & Technology, Gaithersburg, MD, USA. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
25. Khan S, Gani A, Wahab AWA, Bagiwa MA, Shiraz M, Khan SU, Buyya R, Zomaya AY (2016) Cloud log forensics: foundations, state of the art, and future directions. ACM Comput Surv 49(1):1–42. https://doi.org/10.1145/2906149
26. Krishnan S (2017) A hybrid approach to threat modelling. https://blogs.sans.org/appsecstreetfighter/files/2017/03/A-Hybrid-Approach-to-Threat-Modelling.pdf
27. Kumar R, Goyal R (2019) Assurance of data security and privacy in the cloud: a three-dimensional perspective. Softw Qual Prof 21
28. Kumar R, Goyal R (2019) On cloud security requirements, threats, vulnerabilities and countermeasures: a survey. Comput Sci Rev 33:1–48. https://doi.org/10.1016/j.cosrev.2019.05.002
29. Liu F, Tong J, Mao J, Bohn R, Messina J, Badger L, Leaf D (2011) NIST cloud computing reference architecture (SP 500-292). National Institute of Standards & Technology, Gaithersburg, USA. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505
30. Mell PM, Grance T (2011) The NIST definition of cloud computing (SP 800-145). Tech. rep., National Institute of Standards & Technology, Gaithersburg, USA. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
31. Mogull R, Arlen J, Gilbert F, Lane A, Mortman D, Peterson G, Rothman M (2017) Security guidance for critical areas of focus in cloud computing v4.0. CSA
32. NCSC (2018) Cloud security guidance v1.0. https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles
33. NIST (2013) Security and privacy controls for federal information systems and organizations (SP 800-253). National Institute of Standards & Technology, Gaithersburg, USA. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
34. PCI-DSS (2018) Requirements and security assessment procedures. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
35. Rahman NHA, Glisson WB, Yang Y, Choo KKR (2016) Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Comput 3(1):50–59. https://doi.org/10.1109/MCC.2016.5
36. Scandariato R, Wuyts K, Joosen W (2015) A descriptive study of Microsoft's threat modeling technique. Requir Eng 20(2):163–180. https://doi.org/10.1007/s00766-013-0195-2
37. Sgandurra D, Lupu E (2016) Evolution of attacks, threat models, and solutions for virtualized systems. ACM Comput Surv 48(3). https://doi.org/10.1145/2856126
38. Sookhak M, Gani A, Talebian H, Akhunzada A, Khan SU, Buyya R, Zomaya AY (2015) Remote data auditing in cloud computing environments: a survey, taxonomy, and open issues. ACM Comput Surv 47(4):1–34. https://doi.org/10.1145/2764465
39. Stackify (2017) Best log management tools: 51 useful tools for log management, monitoring, analytics, and more. https://stackify.com/best-log-management-tools/
40. Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng 71:28–42. https://doi.org/10.1016/j.compeleceng.2018.06.006
41. Tabrizchi H, Kuchaki Rafsanjani M (2020) A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput. https://doi.org/10.1007/s11227-020-03213-1
42. Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1(1):7–18. https://doi.org/10.1007/s13174-010-0007-6
43. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Future Gen Comput Syst 28(3):583–592. https://doi.org/10.1016/j.future.2010.12.006