Computer Science Review 33 (2019) 1–48

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

On cloud security requirements, threats, vulnerabilities and countermeasures: A survey

Rakesh Kumar, Rinkaj Goyal *

University School of Information, Communication and Technology (USIC&T), Guru Gobind Singh (GGS) Indraprastha University, New Delhi 110078, India

ARTICLE INFO

Article history:
Received 20 July 2018
Received in revised form 15 April 2019
Accepted 2 May 2019
Available online 21 May 2019

Keywords:
Cloud computing
Security in cloud
Cloud security trust model
Cloud security challenges
Cloud security requirements threats vulnerabilities countermeasures

ABSTRACT

The world is witnessing a phenomenal growth in the cloud enabled services and is expected to grow further with the improved technological innovations. However, the associated security and privacy challenges inhibit its widespread adoption, and therefore require further exploration. Researchers from academia, industry, and standards organizations have provided potential solutions to these challenges in the previously published studies. The narrative review presented in this survey, however, provides an integrationist end-to-end mapping of cloud security requirements, identified threats, known vulnerabilities, and recommended countermeasures, which seems to be not presented before at one place. Additionally, this study contributes towards identifying a unified taxonomy for security requirements, threats, vulnerabilities and countermeasures to carry out the proposed end-to-end mapping. Further, it highlights security challenges in other related areas like trust based security models, cloud-enabled applications of Big Data, Internet of Things (IoT), Software Defined Network (SDN) and Network Function Virtualization (NFV).

Contents

* Corresponding author.
E-mail address: rinkajgoyal@gmail.com (R. Goyal).

https://doi.org/10.1016/j.cosrev.2019.05.002
1574-0137/

1. Introduction

Cloud-based business opportunities have witnessed an exponential growth in the last ten years and are expected to grow further with the emerging cloud-enabled applications of Big Data, IoT, 5G, SDN and NFV [1]. In the cloud paradigm, a pool of computing resources (hardware, CPU, storage, software, etc.) are managed by cloud service providers [2–4]. They offer their services in the form of infrastructure, platform, and software to its consumers, mostly over the Internet using multi-tenancy and resource virtualization techniques [5]. Cloud service delivery model allows consumers to lease and release computing resources through self-service interfaces with the pay-as-you-go model. The unique characteristics of cloud, like pooled sharable resources, on-demand scalability, customized self-service, services usage measurement, and broad accessibility, have propelled the growth engine for cloud-based business use cases and application [5]. Gartner, a leading research and advisory company, in its report, has forecasted worldwide public cloud services revenue to reach USD 411.4 billion in 2020 from USD 219.6 billion in 2016 [6]. The promising features of the cloud service delivery model, like no initial capital investment, pay-per-use, accessibility, lowered operating expenses, fast deployment, rapid provisioning, scalability, assured service continuity, low-cost disaster recovery, reduced business risks and like others, resulted in its rapid deployment and its adoption by enterprises [7–10].

The unprecedented growth of cloud-based applications and services have attracted research communities, both from industry and academia, to find innovative solutions for more consumer-friendly, cost-effective, technologically efficient and secured cloud systems. In previous studies, security and privacy highlighted as major challenge for accelerated growth of cloud [11–17]. Most of the security challenges are inherited from the vulnerabilities in cloud architectural components and technologies used, like, vulnerabilities in Internet communication, web services, service oriented architecture, web-browsers, virtualization, hypervisors, multi-tenancy, software, virtual machines, self-service management interfaces, etc. [18]. In cloud-based solutions, user's data is stored and managed remotely that creates fear in users for losing control of their data. So, most of the recommended solutions in literature are around ensuring confidentiality, integrity, availability, authentication, authorization, accountability and privacy of user data by enforcing the different mechanism of encryption, identity and access control, intrusion detection and prevention, software testing and quality control, secured communications, secured virtual machines and hypervisors, secured storage for user data life-cycle management, trust establishment, auditing and logging of user activities along with compliance to service level agreements (SLAs), legal and regulatory framework [19,20].

Table 1 presents a comparative study of the different works published during the year 2010 to 2019. The choice of years (2010–2019), for selection of published works, is inspired by

the phenomenal growth of cloud delivery model during these years [1]. The selected published works are referenced in different related works on security and privacy in the cloud. The choice of comparison criterion (Table 1) is based on different aspects of a cloud system that are discussed in different published works. The main contribution of this survey is to present an end-to-end mapping of cloud security requirements, identified threats, known cloud system vulnerabilities and suggested countermeasures using a unified taxonomy of cloud security. Additionally, it provides cloud architectural components view, used technologies and cloud model taxonomy. Trust-based solutions suggested by different researchers, to address cloud requirements, are also discussed. Further, this work includes an overview of the impact on the emerging cloud-enabled applications of Big Data, IoT, 5G, SDN and NFV due to cloud security and privacy issues.

In subsequent sections, Section 2 analyzes related work in cloud security and privacy. A brief understanding of the cloud computing paradigm is provided in Section 3. Section 4 presents a unified cloud security taxonomy and describes cloud security requirements, identified threats, vulnerabilities in the cloud architectural components and technologies along with suggested countermeasures in different published works. Section 5 provides inter-related analysis and mappings of countermeasures for identified security requirements, threats and vulnerabilities. It presents an approach for selection and prioritization of countermeasures. It also highlights security aspects of cloud-enabled emerging applications. Section 6 provides a conclusion and explores further research possibilities for trust-based adaptive security and privacy solution for cloud systems.

2. Related work

Researchers have touched upon different aspects of cloud security in their published works, like cloud architectural components and associated attack vectors, cloud security issues and challenges, identified threats, known vulnerabilities, observed attacks, suggested countermeasures, etc. Morsy et al. [21] explained cloud security issues from perspectives of its architecture, characteristics, service delivery models and stakeholders. They emphasized issues in virtualization and service-oriented technologies along with security dimensions related to isolation and multi-tenancy. Based on the analysis they recommended for an integrated and adaptive configuration based security model. However, their study does not have a detailed analysis of the security requirements, related threats, associated vulnerabilities, and corresponding countermeasures, and their mappings. Zhang et al. [7] mentioned about the four layers of cloud architecture to deliver the cloud services — hardware layer, infrastructure layer, platform layer, and application layer. Automated security provisioning, virtual machine migration, hardware server consolidation, energy management, software framework, data security, storage technologies, and related security aspects are highlighted as the challenges for the cloud. Takabi et al. [22] highlighted, the unique security and privacy implications in cloud arising due to the outsourcing of data and applications, virtualization and hypervisors, heterogeneity, extensibility and shared responsibility, service level agreements (SLAs), and compliance and regulation. Their proposed security solution model is around managing user authentication, identity, access control and accounting, trust management, secured service management, and security policy management along with unified organizational security management.

Vaquero et al. [23] described issues related to the three major domains of IaaS — virtualization, network, and physical domains. They reviewed threats associated with these three domains and associated solutions proposed in different literature and finds access control and encryption techniques as the major levers for ensuring the security of infrastructure components in totality. Dahbur et al. [24] emphasized, apart from inherited risks, threats and vulnerabilities of underlying cloud technologies, cloud environment itself brings in additional risks, threats, and vulnerabilities. They provided specific recommendations to address the same. However, they did not provide an insight view of these risks, threats, and vulnerabilities. Grobauer et al. [18] used risk factors to analyze the impact of cloud-specific vulnerabilities due to its characteristics and the underlying technology used. Based on risk factors, they also proposed indicators for cloud-specific vulnerabilities. Their paper does explain in detail about vulnerabilities in the cloud. However, there is no specific mention about trust mechanism. Subashini and Kavitha [8] analyzed security issues related to cloud service delivery models — SaaS, PasS, and IaaS. They identified fourteen security issues related to SaaS delivery model — data security, data integrity, data access, web application security, network security, identity management & sign-on process, authentication & authorization, data locality, data segregation, data confidentiality, data breaches, availability, backup, and virtualization vulnerability. For PaaS, they suggested to define and use security specific metrics to measure vulnerability scores of applications being developed and deployed by the PasS cloud users. They advocated for shared responsibilities of both provider and consumer to implement security measures in case of IaaS. Overall, they emphasized on issues related to data security, virtualization technologies, and storage mechanism. They suggested for further research on an integrated security model for SaaS, PaaS, and IaaS.

Zissis and Leakkas [25] have analyzed user-specific security requirements along with associated potential threats and proposed to use Trusted Third Party (TTP) security solution. Pearson [26] explained the meaning of security, trust, privacy, and their inter-relationships. Further, Pearson highlighted that traditional mechanisms are no longer flexible or dynamic enough to address the cloud-specific security, trust, and privacy issues, and also discussed challenges in addressing the same. Phaphoom et al. [9] consider cloud computing as an amalgam of existing technologies, primarily, based on the established concepts and solution for virtualization, distributed systems, and web services. They described four major focus areas — cloud architecture, virtualization, data management, and security issues and solutions. They presented a five-layer cloud architecture for service delivery. They recommended robust solutions for virtualization and data management based on the analysis of different solutions proposed in related literature. In their pertinent work, they have explained vulnerabilities associated with components of each of five layers of cloud architecture and the associated solution approach. Their work includes a mapping of the identified security issues and their suggested solution in a very precise and concise way. Hashizume et al. [27] described cloud-related threats, vulnerabilities, and countermeasures in their comprehensive work. The most important aspect of their work is about the service level security view from the end user perspective. They very well explained about different threats, vulnerabilities, and possible countermeasures along with their inter-related mapping. Xiao and Xiao [28] identified confidentiality, integrity, availability, accountability, and privacy-preservability as five most determining attributes for analyzing the vulnerabilities, attacks and associated defense strategies. Modi et al. [29] have visualized cloud environment as a layered model and discussed security issues in these layers and enabling technologies. However, issues and solutions related to privacy could have been enriched more, especially from the data storage management techniques and life cycle management point of view.

Table 1
Comparative analysis of the related works with this survey.

Survey (study)	Year	Major area discussed	C01	C02	C03	C04	C05	C06	C07	C08	C09	C10	C11
Morsy et al. [21]	2010	Security issues from the perspective of cloud architecture, characteristics, service delivery model and stakeholders, and the recommended security solution	+	+	×	×	–	+	+	×	×	–	×
Zhang et al. [7]	2010	Design challenges of cloud computing and commercial solution used with example cloud provider	+	+	×	×	×	–	+	×	×	×	×
Takabi et al. [22]	2010	Cloud computing definition and features, unique security and privacy implications, security and privacy challenges, and solution approaches	+	×	×	×	×	+	+	×	+	+	×
Vaquero et al. [23]	2011	Security risk due to multi-tenancy, security threats, solution analysis for virtual machine related vulnerabilities	+	×	×	×	+	+	+	–	–	×	×
Dahbur et al. [24]	2011	Risks, threats and vulnerabilities in cloud systems along with standard recommendations	+	×	×	×	+	–	–	×	×	×	×
Grobauer et al. [18]	2011	Risks and vulnerabilities analysis due to cloud characteristics, architectural components and underlying technologies	+	+	×	×	–	+	–	–	×	×	×
Subashini and Kavitha [8]	2011	Security issues related to cloud service delivery models: SaaS, PaaS and IaaS	+	–	×	–	–	+	+	×	×	–	×
Zissis and Lekkas [25]	2012	Cloud security requirements, associated potential threats and trusted third party based security solution recommendations	+	–	×	+	+	–	+	–	+	–	×
Pearson [26]	2013	Cloud computing concepts, cloud security, trust and privacy issues	+	×	×	×	×	+	×	×	+	+	×
Phaphoom et al. [9]	2013	Cloud computing architecture, virtualization, data management, security issues, security solution and mapping	+	+	×	–	×	+	+	–	×	×	×
Hashizume et al. [27]	2013	Vulnerabilities, threats and attacks in the cloud environment from user specific service level perspective, their mappings, and suggested countermeasures	–	–	×	–	+	+	+	–	–	×	×
Xiao and Xiao [28]	2013	Cloud architecture, characteristics, security challenges, supporting techniques, cloud security and privacy attributes, suggested security solution	+	+	×	+	+	+	+	+	–	+	×
Modi et al. [29]	2013	Cloud computing architecture, security threats, vulnerabilities, attacks, and relevant solution directives to strengthen security and privacy in cloud computing	+	+	×	×	+	+	+	×	+	–	×
Fernandes et al. [30]	2014	Cloud computing architecture, underlying technologies, threats, vulnerabilities, attacks, cloud security issues taxonomy	+	+	+	+	+	+	–	×	+	+	×
Aguiar et al. [31]	2014	Virtualization, authentication, integrity, availability, accountability and privacy of remote storage and computation	×	×	×	+	×	+	+	×	–	–	×
Khalil et al. [32]	2014	Cloud vulnerabilities, security threats, attacks, and comparative analysis of available solutions	+	×	–	×	–	+	–	–	–	–	×
Ardagna et al. [33]	2015	Taxonomy of cloud security and assurance, security techniques and assurance processes, recommendations for the design and development of cloud security and assurance techniques	×	×	+	+	+	+	+	+	+	+	×
Ali et al. [10]	2015	Cloud security issues and existing solution analysis, vulnerabilities in mobile cloud computing	+	×	+	+	–	+	+	+	+	+	×
Huang et al. [34]	2015	Cloud security mechanisms used in the IaaS industry and security problems and solution from academia	×	×	×	–	–	–	–	×	+	×	×
Singh et al. [35]	2016	Cloud security threats, issues, challenges and proposal for a three-tier security architecture	+	–	–	–	+	+	+	×	+	+	×
Khan and Al-Yasiri [36]	2016	Current and future challenges for cloud security and a cloud adoption framework	+	×	×	×	+	+	×	×	×	×	×
Singh and Chatterjee [37]	2017	Cloud underlying technologies, security issues, threats, attack and associated suggested solutions	+	+	×	+	+	+	+	+	+	+	×
Ramachandra et al. [38]	2017	Cloud components, security issues, risk and solution for mitigation of vulnerabilities in the cloud	+	+	×	×	–	+	+	×	×	×	×

(*continued on next page*)

Fernandes et al. [30] presented a comprehensive study on security issues in the cloud, using a taxonomy for vulnerabilities, threats, and attack. They reviewed different related studies published from 2008 to 2012 from the academia and industry. They classified the security issues as per defined taxonomy with real-life examples that provided a rationale for discussion and

Table 1 (*continued*).

Survey (study)	Year	Major area discussed	C01	C02	C03	C04	C05	C06	C07	C08	C09	C10	C11
Coppolino et al. [39]	2017	Cloud security issues, attack vectors, current solutions for attacks along with examples of industry used solutions	×	×	×	×	+	+	+	×	×	×	×
Subramanian et al. [40]	2018	Cloud overview, security issues at communication, computational and SLA levels and countermeasures	+	×	×	×	+	+	+	×	×	×	×
Hong et al. [41]	2019	Cloud threats, attacks and vulnerabilities in cloud components and their mappings	+	+	×	×	+	+	+	-	×	×	×
Patil and Modi [42]	2019	Security requirements, threats, vulnerabilities, attacks and solution of cloud virtualization components,	×	-	-	+	+	+	+	+	-	-	×
This paper		Cloud overview, architecture, cloud security model and taxonomy, security requirements, threats, vulnerabilities, countermeasures and their mappings, trust based solutions, privacy preservation and impact on the emerging applications and technologies	+	+	+	+	+	+	+	+	+	+	+

CC: Cloud Computing; C01: CC Overview; C02: CC Architecture; C03: CC Security Taxonomy; C04: CC Security Requirements; C05: CC Security Threats; C06: CC Security Vulnerabilities; C07: CC Security Countermeasures;
C08: CC Security analysis and mappings; C09: CC Trust mechanism; C10: CC Privacy; C11: CC Security and Emerging Applications & Technologies;
+: Specific area is covered in detail; -: Specific area is covered in less detail; ×: Specific area is not covered.

highlighted the related impact of the security issues. They provide practical recommendations for addressing these security issues. Aguilar et al. [31] in their work have discussed — virtualization security, denial of service attacks, authentication and authorization attacks and their countermeasures, remote storage verification, ensuring integrity, addressing accountability, and protecting integrity and privacy for outsourced computation. Khalil et al. [32] identified twenty-eight cloud security issues classified into five categories — data, cloud infrastructure, network, access, and security standards. They recommended best practices to control the vulnerabilities, neutralize the threats and calibrate the attacks. They also presented nine general cloud attacks and proposed countermeasures with examples from attack incidents.

In their significant work Ardagna et al. [33] have discussed cloud security assurance which is a much broader scope than cloud security. Cloud security assurance is all about identification and application of methodologies for collecting and validating evidence for supporting the implemented security requirements as per SLAs between cloud service provider along with mandatory security compliance and regulations imposed by authorities. They have provided a taxonomy for the classification of cloud security and assurance related requirements and attributes. Further, they provided an analysis of cloud security techniques and corresponding assurance processes based on the defined security taxonomy. Ali et al. [10] have discussed cloud security issues by categorizing them in three major areas — communication security, architectural security, and contractual and legal aspects. They pointed out unique security issues in virtual networks and conventional physical networks. They emphasized on specific methodologies for delineations of virtual machines for the equivalent of physical isolations. They highlighted legal compliance obligations due to the geographical distribution of cloud systems. A brief overview of security vulnerabilities in mobile cloud computing is also specified by them. Huang et al. [34] provided an analytical review of the cloud security problems that are implemented in industry and the corresponding solution provided in academic research works, primarily focused around public IaaS. They found, while the industry has implemented the best practices to deal with cloud security concerns, there is still a broader scope of innovation and experimentation in academia to find more effective, efficient and trustworthy solutions.

Singh et al. [35] outlined an extensive view of the security issues associated with the cloud environment. They discussed the existing solution and proposed for a three-tier security solution framework for the cloud — application level as the first tier, cloud-service middle layer level as the second tier, and infrastructure level as the third tier. This three-tier framework for cloud security provides an integrated security structure. A study carried by Khan and Al-Yasiri [36] on cloud security threats discussed security challenges in the cloud that have slowed down the migration of business enterprises and groups to move to the cloud-based business model. They identified eighteen threats, affecting the growth of cloud-based business model.

The survey work by Singh and Chatterjee comprehensively explained different aspects of cloud security in a very structured and detailed way [37]. They described basic features of cloud computing, its security issues, threats, attacks and countermeasures based on different studies carried out in this area. Additionally, the paper describes, cloud architecture framework, service, and deployment models enabling technologies, trust, privacy, and open issues. They, however, do not mention about how the emerging cloud technologies and applications, like IoT, SDN, NFV and Big Data, are impacted due to the increased usage of cloud and growing security concerns and incidents. Ramachandra et al. [38] highlighted that the cloud complex architecture, disruptive nature, and leveraged-resources pose unique risks to all cloud actors. They emphasized that security is the combined responsibility of all the associated actors. They pointed out existing security issues and challenges and control measures to address the same. Based on literature review, Coppolino et al. [39] identified five main security issues — shared technologies vulnerabilities, account or service traffic hijacking, data breach, malicious insiders and denial of service. These issues arise due to the three main attack vectors — computing hardware, hypervisor, and network and by three types of attackers — internal users, external users, and the cloud provider. It then further explained about current solutions against the network-based attacks, hypervisor-based attacks, and hardware-based attacks. It has given solution examples from the industry used solution. However, it did not mention privacy preservation and trust mechanism.

There are couple of interesting surveys presented in recent time [40–42]. Subramanian et al. [40] discussed different cloud security issues at communication level, computational level and SLA level with a more focused analysis of virtualization and data security issues, and suggested solutions to address the same.

However, there is no analysis of cloud security requirements, threats, vulnerabilities, and solutions inter-relationship. Hong et al. [41] have traced vulnerabilities in cloud components to threats by establishing vulnerabilities-to-attacks and attacks-to-threats relationship. They also mentioned about different countermeasure corresponding to the threats. However, there is no end-to-end mapping of cloud security requirements, threats, vulnerabilities, and countermeasures. Also, there is no analysis of trust-based security measures and the impact of cloud security issues on cloud applications based on emerging technologies. Patil and Modi [42] elaborated different vulnerabilities, threats, and attacks in virtualization components of cloud systems. They have categorized and mapped vulnerabilities recorded in the National Vulnerability Database (NVD) to respective attacks and different virtualization components — Hypervisor, Virtual machine, and Virtual network. These virtualization components form different attack surfaces. Further, they explored security requirements and challenges, and mapped them to the suggested solutions.

Here we discussed and presented a comparative view of selected relevant works of different researchers and experts related to cloud security and privacy (Table 1). Every work has touched upon different aspects of the cloud computing environment and associated security and privacy issues, challenges and solutions, however, it seems no work have put together an end-to-end inter-related mapping of cloud security requirements, identified threats, known vulnerabilities, and suggested countermeasures. Also, did not find mention of the impact of the identified cloud security challenges on emerging cloud-enabled applications of Big Data, IoT, 5G, SDN, and NFV. This narrative review provides these missing aspects and has emphasized trust-based security models, and privacy-preserving suggested solutions.

3. Cloud computing overview

3.1. Cloud computing definition

The special publication (SP) 800-145 [5] of NIST (National Institute of Standards and Technology) defines "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a 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*". The cloud consumers can use these resources on demand to develop, host and run applications and services with flexibility of any time, anywhere and on any device.

NIST definition highlights the three service models – *Software-as-a-Service* (SaaS), *Platform-as-a-Service* (PaaS), and *Infrastructure-as-a-Service* (IaaS) to offer cloud services by a Cloud Service Provider (CSP) to its consumers. It also summarizes the four deployment models – *Private cloud*, *Community cloud*, *Public cloud* and *Hybrid cloud*, highlighting computing infrastructure sharing model to deliver the cloud services. Further, it provides integrated view of five essential and unique characteristics of every cloud services – *Resource pooling*, *Rapid elasticity*, *On-demand self-service*, *Measured services* and *Broad network access*.

3.2. Cloud computing service models

Cloud computing service models describe the context in which the capabilities of a CSP is presented as services to cloud consumers. Table 2 describes the service delivery models (SaaS, PaaS, and IaaS) for offering cloud services by a cloud provider to its consumers [19].

A cloud consumer can choose one or more services for available service options from providers to fulfill its requirements. Both cloud service provider and cloud consumer signs-off SLAs that works as a contractual commitment for an agreed level of service delivery parameters, primarily containing responsibility matrix, quality, availability and financial implications on non-fulfillment of the same.

3.3. Cloud computing deployment models

Cloud computing deployment models describe the physical context of cloud delivery infrastructure, platforms, and applications. Table 3 describes the four deployment models for cloud service delivery — public cloud, private cloud, hybrid cloud, and community cloud [5].

Each of the three service models (SaaS, PaaS and IaaS) together with four deployment models (private, public, community and hybrid cloud) fulfills the relevant business needs of cloud consumers. As it looks obvious, a single large business user will benefit from the private cloud, whereas smaller business users may prefer public cloud and similar business users may go for community cloud. With the continued evolution of the cloud computing environment, as well as the business model, businesses will shift back and forth through these four deployment paradigms.

3.4. Cloud computing reference architecture and taxonomy

Fig. 1 represents brief overview of the NIST recommended cloud computing reference architecture [19]. It depicts five major actors and their functional activities within the architectural framework of the cloud. Additionally, it depicts different deployment models that a provider can use to deliver the services to its consumers.

Fig. 2 presents taxonomy for cloud computing model describing the cloud functional model based on NIST cloud computing reference architecture [19].

The taxonomy for cloud functional model depicted in Fig. 2 is explained through Table 4 specifying different roles in cloud computing environment, the activities associated with these roles, the components (specific processes, actions or tasks to perform and meet the objectives of these activities), and sub-component (a module for the associated component).

3.5. Cloud computing enabling technologies

Cloud computing is an amalgam of proven enabling technologies to provide low cost, high speed, and scalable on-demand IT infrastructure to users [9,37].

3.5.1. Virtualization technology

Virtualization technologies enable partitioning of hardware resources (like processing units, their registers, I/O devices, storages, etc.). Virtual Machines (VMs) and Hypervisors or Virtual Machine Monitors (VMMs) are the resultant components of virtualization that provides flexible and scalable on-demand computing resources. VMMs are responsible for allocating the virtual hardware resources like memory, CPUs, hard disk and virtual network interfaces to each VM. VMWare, Xen, KVM are some of the virtualization technologies solutions that enable on-demand IT infrastructure platforms. VM migration is one of the biggest advantages of using virtualization that enables to port VMs from one hardware server to another, and thus providing rapid and dynamic scaling up or down of computing resources with excellent fault tolerant capability to users [18,22].

Table 2
Cloud computing service models [5].

Service Model	Capability	Level of control	Example services
Software-as-a-Service (SaaS)	It makes a consumer to use provider's applications available on a cloud infrastructure managed by the provider. The consumer accesses services over the Internet, mostly through a thin client interface, like a web browser or through an exposed program interface.	Consumer's control is limited to possible user-specific application configuration settings. It has no access to the control and management interface for the underlying cloud infrastructure.	Email & Office Productivity, Content Management, Document Management, Collaboration, Sales, Financial, ERP, Billing, Human Resources, Social Networks
Platform-as-a-Service (PaaS)	It allows a consumer to create and deploy its applications using standard programming languages, libraries, development framework and tools supported in providers' development platform and infrastructure.	The consumer has control over the deployed application and possible limited configuration settings for environment hosting the application. It has no access to the control and management interface for the underlying cloud infrastructure.	Application Deployment, Database, Development & Testing, Integration, Business Intelligence.
Infrastructure-as-a-Service (IaaS)	It allows a consumer to provision minimal computing resources like processors, storage, networks, and others where the consumer can deploy and run arbitrary software including operating systems and applications.	The consumer has control over deployed applications, storage and operating systems with possible limited control of selecting network components (e.g., firewalls).	Backup & Recovery, Compute, Storage, Platform Hosting, Services Management, CDN.

Table 3
Cloud computing deployment models [5].

Deployment model	Description
Private cloud	The provider provides exclusive access and usage rights on the infrastructure and computational resources to its consumers. The cloud infrastructure and resources may be hosted in consumer premises or outsourced to a third-party hosting organization and so can be managed by the consumer or by the third party.
Public cloud	In this deployment model the provider provides cloud services to a diverse pool of cloud consumers and so is named as public. The services are provided over a public network (wireless or wireline).
Community cloud	It provides cloud services to a group of consumers with a common interest like shared objectives and goals, security, privacy, and compliance policy. A community cloud may be implemented as, similar to private clouds, an on-site community cloud in consumer premises or as off-site outsourced to a hosting organization.
Hybrid cloud	It is a composition of two or more clouds (public, on-site private, on-site community, off-site private and off-site community). The individual clouds in composition remains a distinct entity but provide standard or proprietary interfaces for application and data portability between them.

Table 4
Cloud computing active roles and their activities [5].

Roles	Description	Activities
Cloud consumer	A person or an organization that uses and pays for services provided by a cloud provider as per business relationships maintained through a service contract between them.	Service consumption as per requested service model — SaaS, PaaS and IaaS.
Cloud provider	A cloud provider, a person or an organization, is responsible for providing services to its cloud consumer. It owns the computing infrastructure, runs software and establishes the framework to deliver the cloud services to its consumers, primarily through the Internet.	To provide and manage cloud infrastructure and services — service deployment, service orchestration, cloud service management, and security and privacy.
Cloud carrier	A cloud carrier acts as a connecting link that provides access to cloud consumers for connectivity and transport of services from cloud providers. Depending on the level of SLAs provider has offered to its cloud consumer, it will set up corresponding SLAs with a cloud carrier.	To provide connectivity and transport services — cloud distribution and cloud access.
Cloud broker	A cloud broker negotiates business relationships between cloud providers and their cloud consumers. It offers tailored service packages, maybe from different providers, to make things simple and easy to use and bill the services. It manages the usage delivery and performance, as per agreed SLAs, of cloud services.	To add value between provider and consumer — service consumption and service provision.
Cloud auditor	A cloud auditor is an independent party that conducts a neutral assessment of cloud implementation concerning cloud services, performance, information system operations, security, and privacy control measures. A cloud auditor performs audit through review of objective evidence to verify conformance to agreed standards and compliance to regulatory obligations.	To assess compliances against standards and regulations and provide suggestions for improvement — security audit, privacy impact audit, and performance audit.

3.5.2. Multi-tenant technology

It enables multiple users to access the single instance of application logic and at the same time allowing users to have a separate view of the application to manage the application's features and data individually. Multi-tenant technology allows having the user isolation at the application and hardware resource level to ensure data privacy and security along with user-level application upgrades, system scalability, and metered usage [37].

3.5.3. Web services and service oriented architecture (SOA)

Cloud system provides its services mostly through Web Services using SOA. SOA provides an architectural framework that enables communication between systems through interacting services implemented by the systems. Hypertext Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP), Representational State Transfer (REST), eXtensible Markup Language (XML),

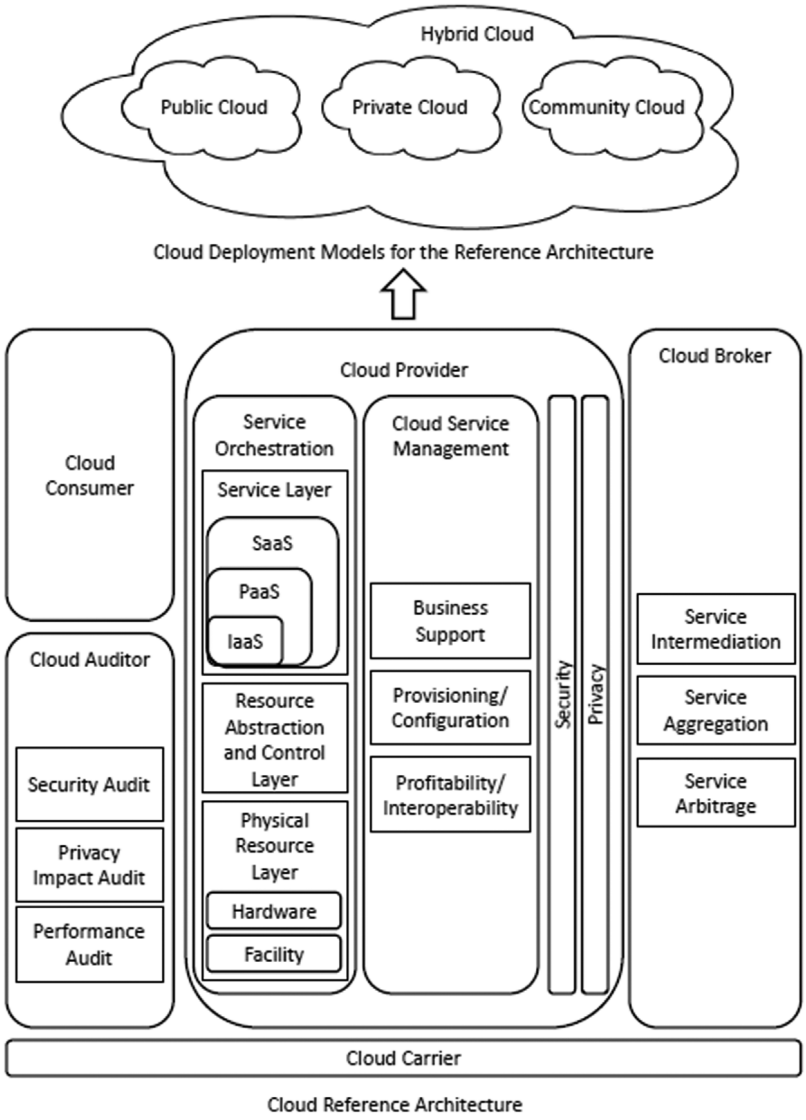

Fig. 1. Cloud computing reference architecture with different deployment models.
Source: adapted from NIST SP 500-292 [19] and NIST SP 800-145 [5].

Web Services Description Language (WSDL) and Universal Description, Discovery and Integration (UDDI) are some of the most widely used technologies for implementing the web services [43].

3.5.4. Internet technology and broadband networks

Internet technologies and broadband networks provide easy access to services offered by a cloud service provider. Internet-based technologies, like the World Wide Web (WWW), allow connecting IT resources which enables load balancing, fault tolerance, and scalable solutions and services for cloud users [30].

3.5.5. Data-center technology

In the context of cloud, a data-center hosts a large number of application and storage servers connected through Gigabit Ethernet. These servers are virtualized to provide an illusion of infinite resource availability. Inexpensive multi-core hardware, easy broadband access along with state-of-art secured data-center facility is enabling remote service delivery for a cloud service provider at low cost and agreed with SLAs to its consumers [44].

4. Modeling security in cloud computing

Modeling security in cloud computing involves, identifying cloud security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements. Further, it involves determining countermeasures to address these known vulnerabilities to reduce or eliminate attack vectors to fulfill cloud security and privacy requirements.

4.1. Cloud computing layered model

To understand the security aspects of cloud computing, it is required to know the architectural component associated with the cloud computing system. One of the widely used representations of the cloud architecture components is the multi-layered stack model that allows depicting technology associated with each layer representing *as-a-service* delivery model [9]. Table 5 provides some of the layered model proposed in previous works from Foster et al. [45], Youseff et al. [46] and Cloud Security Alliance (CSA) publication Security Guidance v4.0 [20].

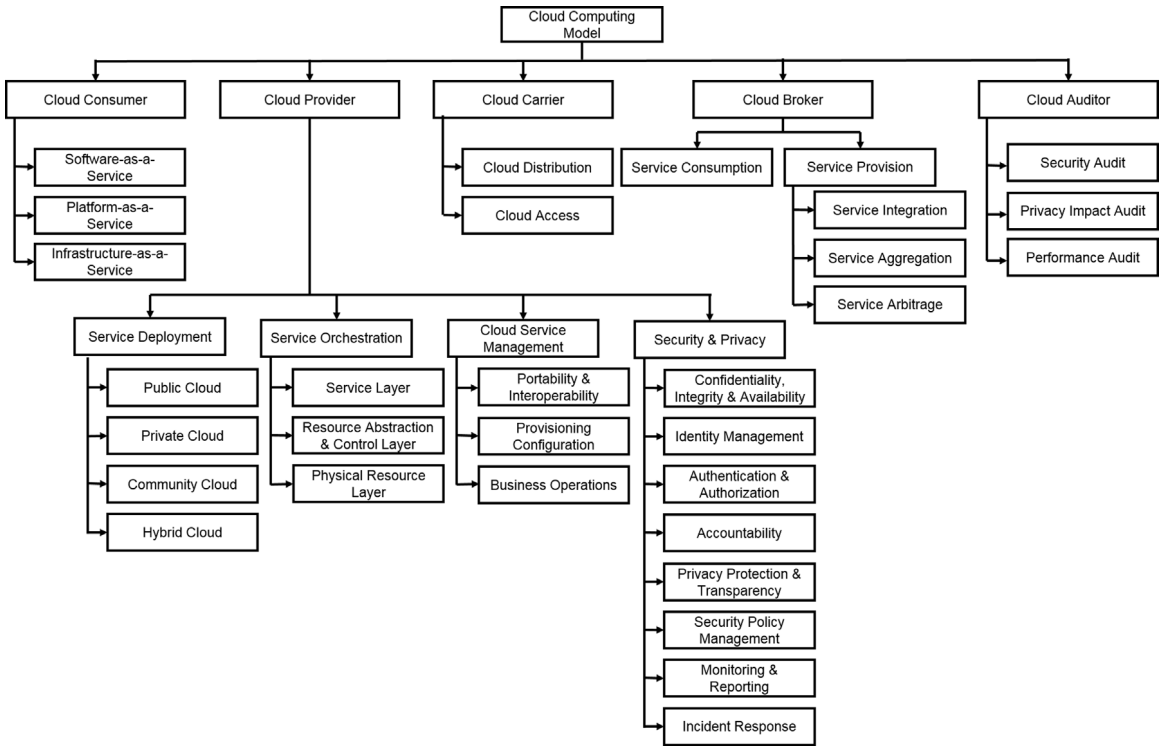

Fig. 2. Cloud computing taxonomy.
Source: adapted from NIST SP 500-292 [19].

Table 5
Layered models for cloud computing architectural components [9].

4-Layer model by Foster et al. [45]	5-Layer model by Youseff et al. [46]	7-Layer model by Mogull et al. [20]
Application Layer: which contains applications that runs on cloud *Platform Layer:* provides middle-ware, added specialized tools and services on top of unified resources *Unified Resource Layer:* which contains encapsulated/abstracted (mostly virtualized) resources exposed to upper layer or end users *Fabric Layer:* which contains the raw hardware resources	*Application Layer:* provider hosts applications for the users that run in cloud environment and accessed by users using web portals *Software Environment Layer:* provides user-specific application development and execution environment *Software Infrastructure Layer:* provides fundamental resources like computational resources (VMs), data storage, communication, etc. *Software Kernel Layer:* provides basic software management for the physical hardware that composes the cloud, like hypervisor, VMM, clustering middle-ware, etc. *Hardware and Firmware Layer:* consist of actual physical hardware and network components forming the cloud	*Application and Interface Layer:* which provides applications and services hosted on cloud infrastructure through standard interfaces to software-as-as-service consumers *Integration & Middleware Layer:* which provides customized development and execution environment for the platform-as-a-service consumers *APIs Layer:* which provides interface services to access and provision cloud resources to avail the legitimate services offered *Core Connectivity & Delivery Layer:* which works as backbone for cloud functioning and operation as it provides tools and framework for multi-tenancy, orchestration, load balancing, monitoring, backup, and other related support services *Abstraction Layer:* which provides unified and integrated view of distributed and heterogeneous physical resources *Hardware Layer:* which consists of physical resources located in data center, like computing resources, storage resources, network devices and connecting access devices and network cables *Facility Layer:* which comprises of data center space and its physical environment

Fig. 3 depicts a layered stack model containing cloud architectural components. Each layer's component forms an attack surface. This layered stack model has been used for analysis of vulnerabilities in cloud architectural components and suggested countermeasures around it. The layers and their associated components surrounded in dotted boxes are of interest for the analysis in this survey.

4.1.1. Application and interface layer

This layer primarily enables SaaS offerings through web services and technologies like REST, SOAP, WSDL, HTML, JavaScript, AJAX, CSS, etc. A cloud consumer accesses the services using web clients (web browsers), installed on their access devices, mostly through the Internet. Access to services is secured through user identification, authentication, and authorization, using standard mechanism and protocol like public-key cryptography, OAuth,

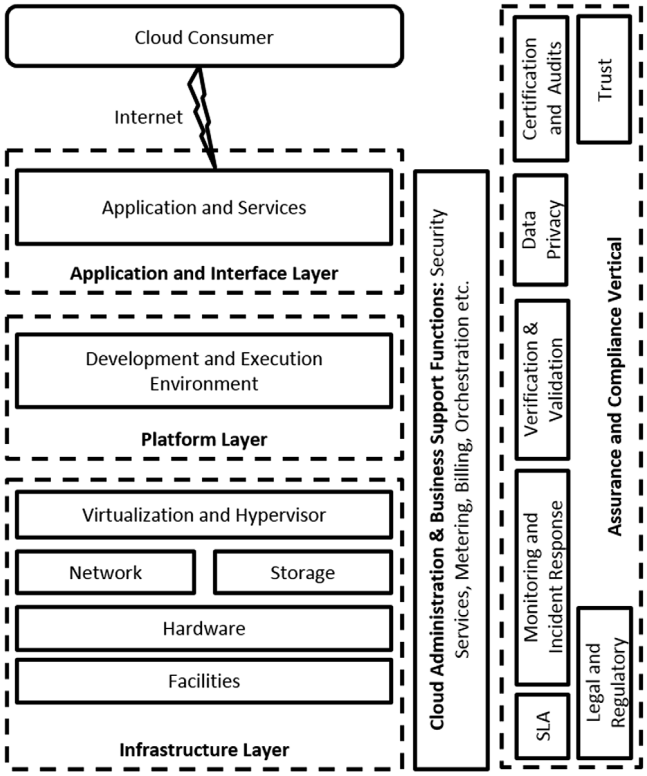

Fig. 3. Cloud computing layered model. *Source:* adapted from CSA Security Guidance v4.0 [20].

OpenID, etc. It ensures secure data communication between the service provider and the consumer using appropriate encryption techniques.

4.1.2. Platform layer

This layer provides software development, testing, deployment, and run-time execution environment to the cloud consumer wherein an end user can develop and deploy its customized application or can install off the shelves software applications, customized to suit the end user's requirements. This layer equips the end user with the required operating system and integrated development environment. Technologies and frameworks, like Java SDK, IDE, .NET, Google App Engine etc., enable this layer to provide PaaS over the underlying cloud infrastructure.

4.1.3. Infrastructure layer — virtualization and hypervisor

Virtualization and multi-tenancy are the key technologies used in cloud computing that enable optimal utilization of pooled physical computing resources. Virtual machine monitor (VMM) or hypervisor is a software that works as an abstraction layer to provide a unified and transparent view of underlying physical pooled resources to hosted virtual machines utilizing multiplexing. VMM or Hypervisor manages virtualized resources like processors, memory, I/O devices, etc.

4.1.4. Infrastructure layer — network

This layer provides services for internal communication among virtualized components. It is very likely that the network infrastructure elements like DNS servers, DHCP servers are shared by virtual machines instances, and so this layer provides secure communication mechanism among them. Technologies like OpenFlow, Open vSwtich are used for this purpose.

4.1.5. Infrastructure layer — storage

Data availability and protection is vital and critical for any business and so, for the cloud consumer who decides to outsource storage of its business data to a third-party (cloud provider) on the cloud. So, storage becomes one of the most cared about component of the cloud computing environment. This layer provides services for data storage for user data life cycle management.

4.1.6. Infrastructure layer — hardware

This layer consists of all the raw computing hardware. Generally, a cloud provider has distributed and heterogeneous set of hardware resources. The hardware comes with processors, memory, I/O devices, and other supporting peripheral devices and these are allocated and managed mostly using virtualization technology.

4.1.7. Infrastructure layer — facilities

This layer is all about the data center and its physical environment management. The physical environment of the data center where the cloud infrastructure of the cloud provider is installed and running do have an impact on data availability and service continuity. It includes heating, air-conditioning, ventilation, and power supply management. At this layer, network access of the installed hardware is controlled by defining appropriate network firewall access control policies.

4.1.8. Assurance and compliance vertical

It cut across all the layers of the cloud computing environment managed by a cloud provider, and it as well gets into some of the functional areas of cloud consumer and so is named as *Vertical*. It provides critical functionalities to ensure and support the well-functioning of the offered cloud services and cloud environment in totality. Assurance function includes ensuring the SLAs, monitoring, and logging of users and systems activities. It enables to initiate appropriate corrective actions for deviation from expected behavior. Any new or updated application or service must be verified and validated for its intended function before making it live for the intended use. Compliance to legal and regulatory clauses need to be provided as and when required as per the law of the land and it might involve both cloud provider and consumer as per applicability. Data privacy compliance requirements must be furnished to ensure user data stored and managed by a cloud provider is not being used other than agreed intended purpose.

4.1.9. Cloud administration & business support functions

This provides shared services to perform cloud administration and business support activities. One of the most critical functions is, to provide security services related to user identification, authentication, and authorization. It provides services for cloud orchestration which is primarily a composition of cloud resources in an optimal way to provide best value propositions of services offered to the cloud consumers. It as well includes measuring the service usages (like volume and duration of service usage) and performing the charging and billing for consumed services. It performs administrative functions like cloud service deployments, configuration and provisioning apart from needed support for load balancing of the offered services.

4.2. Cloud computing security taxonomy

A cloud security taxonomy is defined here (Fig. 4) to identify and describe, different cloud security requirements, threats affecting these requirements, vulnerabilities in cloud computing reference architecture components and underlying technologies

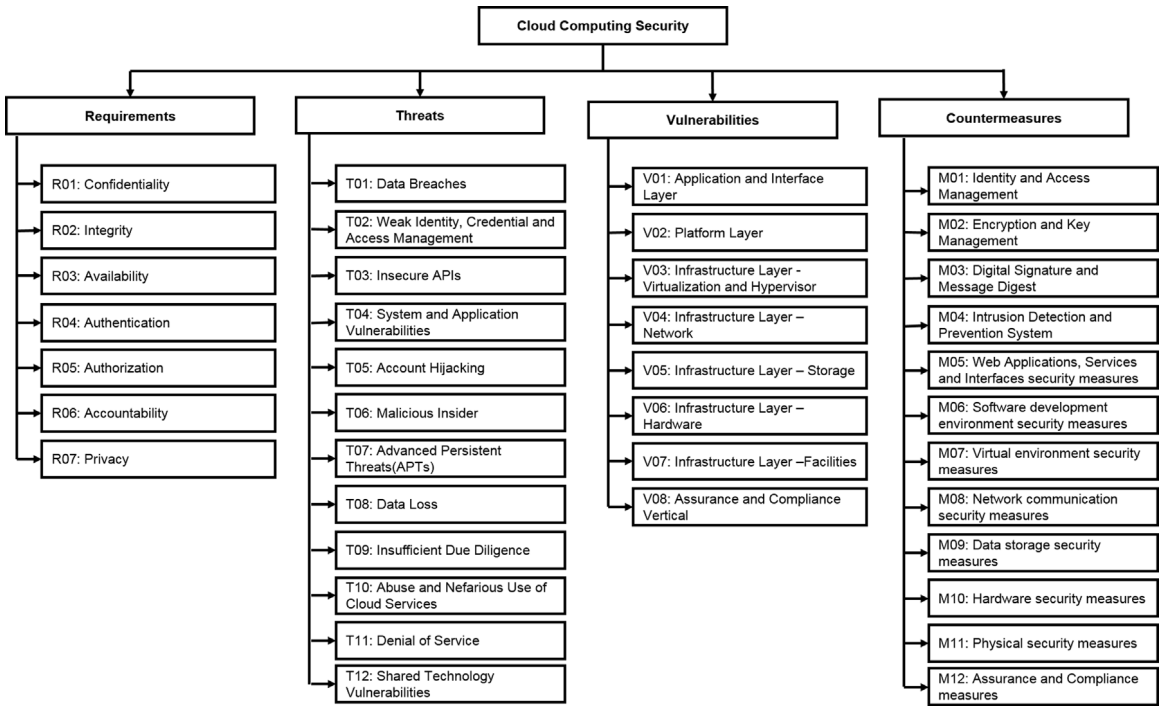

Fig. 4. Cloud computing security taxonomy.

that makes up these threats, and countermeasures to address these vulnerabilities.

This taxonomy has been defined based on studies of published guidelines and standards by the organizations working in cloud security and published work of researchers in the area of cloud [10,13,19,20,27,30,33]. Subsequent subsections describe different aspects of this cloud security taxonomy, which are security requirements, threats, vulnerabilities, and countermeasures. This taxonomy formed the basis of subsequent analysis of previously published works to create an end-to-end mapping of cloud security requirements, CSA's treacherous twelve identified threats [47], known vulnerabilities in cloud architectural components and suggested countermeasures to address these vulnerabilities, which is one of the main contributions of this work.

4.3. Cloud security requirements

NIST has mentioned *confidentiality*, *integrity* and *availability* as basic cloud security requirement like for any other information security management system [19]. It adds up further *authentication*, *authorization*, *accountability* and *privacy* as cloud security requirements. Same has been emphasized by CSA in their publication on guidelines for cloud security requirements [20]. In fact, these security requirements are not new or specific for the cloud computing system, but for any information processing system. From the cloud perspective, these requirements are summarized in Table 6 [48].

4.4. Cloud security threats

NIST Security Glossary defines threat as, "*Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service*" [48]. The researchers of CSA, which is a frontier organization that provides guidance for cloud security for the cloud community, have been doing the threat identification and analysis related to the cloud ecosystem and have released a series of publication on top threats to cloud [47,49,50]. Table 7 presents the changing spectrum and order position for the top threats to the cloud.

For this survey CSA's *The Treacherous Twelve* (Table 7), top threats in cloud security has been used as a baseline to identify what are those vulnerabilities in the cloud architectural framework which causes these threats and what is suggested countermeasures in the literature. Table 8 provides a short description of these threats.

4.5. Cloud security vulnerabilities

NIST Security Glossary defines vulnerabilities as, "*Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source*" [48]. Grobauer et al. [18] highlighted the weaknesses in enabling technologies result in vulnerabilities in cloud computing architectural components. Study about vulnerabilities in cloud computing architecture component has been done by different researchers [29,30,51–54]. Gruschka et al. [52] modeled cloud in three entities as provider, services, and users, and explained about six attack surfaces resulting as the combination of these. Fernandes et al. [30] in their work provided a comprehensive detail of threats, vulnerabilities, and attacks to the cloud infrastructure. Hashizume et al. [27] described different vulnerabilities in the cloud systems and proposed for associated countermeasures. Here we discuss vulnerabilities in architectural components of the layered stacked model (Fig. 3) as per our defined cloud security taxonomy (Fig. 4).

4.5.1. Vulnerabilities in application and interface layer (V01)

This layer works as the entry point to access the services of a cloud provider, mostly through the Internet. The cloud consumer accesses the services generally using a web browser. So, this layer is as vulnerable as the flaw and weaknesses in web technologies

Table 6
Cloud security requirements [19,20,33,48].

Requirement	Requirement Id	Requirement description
Confidentiality	R01	Cloud user's sensitive data (information) is not disclosed to unauthorized individuals, entities or processes.
Integrity	R02	Cloud user sensitive data is not modified or deleted in an unauthorized and undetected manner.
Availability	R03	Cloud user data, when it is needed, should be accessible and usable for the authorized entities (user, process or device)
Authentication	R04	It means user identity verification of the cloud user, user data origin and content authentication. In fact, it is the process of establishing confidence of authenticity.
Authorization	R05	Providing right access level to the authenticated cloud user for the subscribed cloud services.
Accountability	R06	Cloud provider must be able to legitimately establish every action performed or executed in its cloud environment to unique entity either to the cloud user, the process, or the device.
Privacy	R07	Cloud user data must not be used for any other purpose than it is intended to be used for.

Table 7
CSA top threats to cloud computing [47,49,50].

Top threats	2010	2013	2016
1	Abuse and nefarious use of cloud computing	Data breaches	Data breaches
2	Insecure application programming interfaces	Data loss	Weak identity, credential and Access management
3	Malicious insiders	Account hijacking	Insecure APIs
4	Shared technology vulnerabilities	Insecure APIs	System and Application Vulnerabilities
5	Data loss/Leakage	Denial of Service	Account hijacking
6	Account, Service & Traffic hijacking	Malicious Insiders	Malicious Insiders
7	Unknown Risk Profile	Abuse of Cloud Services	Advanced Persistent Threats (APTs)
8	–	Insufficient Due Diligence	Data loss
9	–	Shared Technology Issues	Insufficient Due Diligence
10	–	–	Abuse and Nefarious Use of Cloud Services
11	–	–	Denial of service
12	–	–	Shared technology vulnerabilities

used, including the Internet [55,56]. The cloud user authentication and authorization are one of the basic security requirements to be fulfilled by this layer apart from confidentiality and privacy. Ten most critical web application security threats identified by the Open Web Application Security Project (OWASP) is as well applicable to the cloud computing environment, [57]. These are — Injection, Broken authentication, Sensitive data exposure, XML External Entities (XXE), Broken access control, Security misconfiguration, Cross-Site Scripting (XSS), Insecure de-serialization, Using components with known vulnerabilities and Insufficient logging & monitoring. Due to the own characteristics of cloud, the conventional way of handling these vulnerabilities will not be enough and a new approach to handle vulnerabilities related to web technologies needs to be adopted. Services provided through PaaS and IaaS as well needs management interfaces and application for users, which is accessed through web services and interfaces, so, these management interfaces as well possess the same level of vulnerabilities as for any SaaS applications [9,18].

Web Services and Interfaces vulnerabilities (V01.1): The vulnerabilities in web services and interfaces can lead to data leakage and unauthorized access to resources. Grobauer et al. [18] in their work have highlighted cross-site scripting, command injection, and SQL injection, as service request manipulating mechanisms to exploit the vulnerability in web services interfaces. They further mentioned the credential of a requester of web services are likely to be stolen by a malicious agent as the faulty implementation of session handler leads to session hijacking and session riding. WSDL is used for describing web services related parameter types. The created meta-data is vulnerable to spoofing attack, and a possible forged WSDL document may allow invoking non-published operations through web interfaces [56]. SOAP envelops stores and maintains valid signatures of the documents requested by a web client. So, a rewritten modified SOAP message, known as wrapping attack, by a malicious user can get executed using SOAP envelops which had stored a valid signature of the original document [56]. Other attacks, exploiting the vulnerabilities in web services and interfaces, like SOAPAction spoofing (which manipulates HTTP Headers), XML injection (forged XML fields) WSDL scanning (discovering and fingerprinting Web services) are highlighted in different studies [58–60]. The SOAP-based approach of providing web services in the cloud leads to data manipulation related attacks at the server side as the HTTP does not provide the data integrity in its transactions [8]. Web Services are vulnerable to advanced persistent threats as well [61,62].

Web client data manipulation vulnerabilities (V01.2): Allowing read and modify data permission to the web browser components (like, mash-ups and plug-ins) while making transactions between client applications, of a cloud consumer, and web application server of the cloud provider, causes client-side data manipulation vulnerabilities [18,63]. Information confidentiality and integrity are impacted when attacks are made targeting this class of vulnerabilities [9]. *Injection* as the security risk stands at the top in *OWASP Top 10 Application Security Risks - 2017* [57], that reflects data manipulation vulnerabilities at web client is the major loophole in providing a secured cloud computing environment. In fact, *Injection* as a security risk is at the top also in previous lists of *OWASP Top 10 Application Security Risks* in 2013 and 2010 [64,65]. The most common form of exploiting the injection weakness is SQL injection, by injecting a valid parsing string with malicious intention, which modifies the original legitimate SQL query request from web client towards web application server through the provided application interface. HTTP hidden fields, generally used for storing login information of the web user through web forms is, yet another source of data manipulation vulnerabilities as the duplicate fraudulent web site of the original looking web site makes possible for attackers to steal user credentials, better known as watering hole attack (falling in the trap of duplicate or fake, fraudulent web sites) [66]. The growing trend of using social networking sites exposes the user's browser to self-installing malware and a major source of data manipulation vulnerabilities for web browsers as it can exploit user credentials entered by users [67]. Different studies carried out by researchers discussed the vulnerabilities in plug-ins, and web browsers are allowing *man-in-the browser* (MitB) attacks using the data manipulation [68,69].

Table 8
Cloud computing treacherous 12 top threats [47].

Rank	Threat	Threat description
1	Data breaches (T01)	It means releasing, viewing, stealing or using of sensitive, protected or confidential information by any party for any purpose which was not authorized to do so. Any information leaked that was not intended for public release may come under the purview of data breaches like personal health information, personally identifiable information (PII), etc. The extent of damage due to data breaches could be determined based on the sensitivity of the breached information.
2	Weak identity, Credential and Access Management (T02)	It results in attackers masquerading as legitimate users and getting unauthorized access to data resulting into data breaches which potentially damaging to the owner of data and associated stakeholders.
3	Insecure APIs (T03)	For monitoring, provisioning, orchestration, and managing the allocated resources, cloud consumers are provided with application programming interfaces (APIs) and/or user interfaces (UIs) which exposes the cloud computing environment to the external world and potentially to attackers. These UIs and APIs are generally designed and implemented using web services which have inherent vulnerabilities. These APIs can be further used to build value-added services which might further dilute the user's credentials to the third party.
4	System and Application Vulnerabilities (T04)	This threat appears due to bugs in the system and application software which could be exploited by the attackers to steal data and take control of the systems' operation. Vulnerabilities in libraries, kernel and application tools of an operating system put all services and data at the security risk. The feature like multi-tenancy creates yet another attack surface as it needs usage of shared memory and resources among different systems of organizations, hosted in the same cloud environment.
5	Account Hijacking (T05)	This is the traditional threat of any computer system and so is in the cloud computing environment which means gaining access to a system by hacking credentials and password of a legitimate user. From the cloud perspective, if attackers hijacked a user's account, they can redirect clients to illegitimate sites, manipulate data, return falsified information, and eavesdrop on activities and transactions.
6	Malicious Insiders (T06)	A malicious insider is a current or former employee or any business partner that has or had authorized access to information system creates threat if he or she intentionally misused that access to negatively impact the security and privacy aspects of the information system.
7	Advanced Persistent Threats (APTs) (T07)	APTs refer to a higher degree of sophisticated attack which is of very much of specific purpose and aimed to specific target. These attacks are difficult to eliminate as they adapt to deployed security measures while pursuing their goals over an extended period.
8	Data loss (T08)	Data can be lost other than malicious attacks as well, like accidental deletion or unfortunate damage or physical catastrophe like fire, earthquake, flood, etc., which may lead to permanent loss of stored outsourced data unless it is backed up to some alternate safe location which can be made accessible to the legitimate consumer.
9	Insufficient Due Diligence (T09)	While making a choice and decision for selection for cloud technology to use and cloud provider to provide services to host business functions the selection committee must consider many factors. Lack of proper approach and plan for conducting due diligence leads to security risks.
10	Abuse and Nefarious Use of Cloud Services (T10)	It is potentially caused due to unaccounted, mismanaged, fraudulent, free trails user accounts and poorly secured cloud deployments that allows attackers to access the computing resources and misuses it to target victims. Launching distributed email spam, denial-of-service attacks, and phishing campaigns are some of the examples of misuse of cloud-based resources.
11	Denial of Service (T11)	It simply means legitimate users are prevented from accessing their data and application due to slow response or simply no availability of the cloud resources. An attacker causes system slowdown by forcing the target cloud service to consume more than allocated finite system resources and virtually resulting in no access to legitimate users.
12	Shared Technology Vulnerabilities (T12)	Sharing technology, either for infrastructure, platforms or applications, is the basic characteristics of the cloud computing system. The components which facilitate sharing of technology are, generally, not designed to offer an effective isolation property for a multi-tenant environment where applications of multiple customers are hosted together. This potentially can lead to shared technology vulnerabilities like flaws in hypervisors.

User Identity and Access vulnerabilities (V01.3): On-demand service and multi-tenancy characteristics of cloud make identity management, authentication and authorization processes vulnerable [8,70,71]. Identity Management (IdM) broadly deals with identifying entities, including cloud objects, and controlling access to resources as per enforced policies [72]. Authentication vulnerabilities arise due to insecure user practices like weak passwords, reused credentials, usage of one-factor authentication and a weak credential life cycle management process [18]. Insufficient authorization checks and weak user privilege management process results into authorization vulnerabilities [73]. Fernandes et al. [30] in their survey have highlighted even the graphical, biometric and 3D passwords have limitations. Weaknesses in authentication and authorization protocols have been highlighted in different studies. OpenID Connect, along with OAuth2.0, widely being used as single sign-on (SISO) mechanism for end-user authentication by web applications, has the security issues [74–76]. Li et al. [77] in their study have exposed the vulnerabilities in OpenID Connect implementation by Google which is caused mainly due to Relying Party (RP) making a design decision for easy implementation, and so compromising the security that allows an attacker to get into an RP website with credentials of a user. Naik et al. [78] mention about the security vulnerabilities in Federated Identity Management (FIdM) using SAML, OAuth and OIDC because of their improper or erroneous deployment opening the doors for the attackers. Using a comprehensive and expressive web model with malicious RPs, OPs and corrupted browsers, Fett et al. have established both OAuth and OpenID Connect are vulnerable to attacks, categorically for redirect attacks and IDP mix-up attacks [79]. Li et al. [80] also established OpenID Connect vulnerability to web-spoofing and phishing attacks. In their study they showed, an attacker could successfully login the client as a protected user. Both OAuth and OpenID Connect are vulnerable for cross-site request forgery (CSRF) and XSS attacks. Mainka et al. [81] revealed second-order vulnerabilities in OpenID Connect with the potential for breaking user authentication, client-side code injection, DoS and SSRF. Fett et al. [82] proposed security guidelines for the implementer of OpenID Connect to avoid attacks. Issues related to federated identity management, like logistics and transport of user data and token information and interoperability, has been highlighted by other researchers in their work [22,83]. Xiao and Xiao [28] highlighted the privacy challenges in using the identity of the cloud users by

the providers. Ding et al. [84] described the de-anonymization attacks on dynamic social networks. Narayanan et al. [85] proposed an algorithm for anonymization of user identity to preserve privacy. Stealing of user credentials by attacks like phishing, keyloggers, MitM, session hijacking has been highlighted in different studies [29,86].

Encryption and Keys vulnerabilities (V01.4): Encryption algorithms and encryption keys are the widely used mechanism to ensure confidentiality and integrity of data for an information system, which is applicable for the cloud computing environment as well. Lack of sufficiently strong encryption algorithm and a weak key management process leads to encryption and key related vulnerability that compromises the confidentiality and integrity of data [9]. Sound key management focuses on strong policies around encryption key creation, key storage (including backup and restoration mechanism) and secure key transfer across the network [70,87]. The use of insecure and obsolete cryptographic algorithm makes systems vulnerable to different attacks [18,29,88].

4.5.2. Vulnerabilities in platform layer (V02)

Platform layer provides development and deployment tools, middleware and operating system to enable platform-as-a-service offerings to cloud consumers for development and deployment of their custom applications [9]. The vulnerabilities decide the security level of this layer in developed custom software and the underlying operating system. Business critical and real-time software applications must pass through functional and non-functional (like system performance and security) testing before using them [30].

Software development framework and practices vulnerabilities (V02.1): The quality of software is very much dependent on the software development framework used in software development life-cycle by the programmers. Most of the time basic design and development practices are undermined citing project time constraint. Insufficient and incomplete verification and validation of the software deployed at the platform layer leads to vulnerabilities. Most of the time security aspects are underestimated or ignored in the software development life cycle [55,89].

Software code vulnerabilities (V02.2): Security issues in a software application are, generally, due to vulnerable programming codes [90] and is the reason for increased exploitation [91]. Non-compliance to best coding practices and guidelines by the programmers introduces vulnerabilities in code [25,27,55]. Rodero-Merino et al. [92] highlighted security issues in Java and .NET platform development environment in cases of unsafe thread termination and memory zone isolation violation. Deployment of untrusted third-party software, mostly open source code, on a cloud platform, makes it vulnerable to different security attacks [30]. The back-end server code for cloud application is vulnerable to malicious masked code injection (like SQL injection) into a request from front-end, like web browser [8].

Operating system traditional vulnerabilities (V02.3): Operating systems installed on a virtual machine facilitates communication between applications and hardware through system calls. Hence it has access to all the data in a virtual machine. So, any malicious services running in the background may lead to data leakage [9]. Malicious system admin can bring down whole OS software [25,93,94]. Inappropriate system resource allocation and monitoring adversely impact system performance and availability [95]. Inappropriate memory isolation may lead to data leakage [21,92]. Incomplete and insufficient OS monitoring leads to malicious actions to go un-noticed [95]. As per the year, 2015 data from the National Vulnerability Database (NVD) 38% of reported vulnerabilities are for OS from different vendors [96].

4.5.3. Vulnerabilities in infrastructure layer — virtualization and hypervisor (V03)

Virtualization and hypervisor technologies are critical enabling technologies for cloud systems. However, in different surveys and studies conducted by researchers have highlighted the vulnerabilities with virtualization and hypervisor [30,33,37,97]. Apart from traditional vulnerabilities, cloud-specific characteristics and processes, like VM image, VM migration, VM rollback, and multi-tenancy as well have witnessed vulnerabilities.

Virtual Machine traditional vulnerabilities (V03.1): Trend Micro, a cybersecurity and defense company, in its publication has highlighted traditional data center perimeter-security measures like firewalls, network segmentation, Demilitarized Zones (DMZ), network monitoring tools and Intrusion Detection and Prevention Systems (IDS/IPS) are not enough to secure the virtual machines as each virtual machine has its OS and application hosted on a shared hardware with other co-located virtual machines [98]. It is highlighted — the ease of dynamic reconfiguration might lead to the propagation of unknown errors; remote access to administrative tasks might cause for authentication and authorization vulnerabilities; and keeping VMs updated with regular patch management is difficult task [9,99]. There are other VM specific attacks mentioned in different studies, like covert-channel attack [100], side-channel attacks [101,102], cross-VM attacks and VM-hopping [28,103], etc.

VM Image vulnerabilities (V03.2): Wei et al. [104] pointed out, a publisher of VM image has a risk of releasing sensitive information and a retriever has a risk of running a vulnerable or malicious VM image as it might have contaminated while at rest. They further highlighted the risk of a potential security risk due to inactive and dormant images not used for a longer period and administrator might not have taken care of its security patches and software licenses due to high maintenance cost. Vaquero et al. [23] highlighted the problem of encrypting the large size images. Morsy et al. [21] highlighted the issue of VM image theft and malicious code injection. Luo et al. [105] highlighted the issue of VM sprawl related to VM management when the number of VMs is growing, and most of them are idle that complicates VM management due to resource wastage. Infected VM images might lead to sporadical dissemination of malware, a phenomenon of transience, and it becomes unmanageable as the VM images grow [106].

VM Migration and Rollback vulnerabilities (V03.3): Zhang et al. [107] defines VM migration as the process of relocating a VM from one physical server to another without shutting down the VM. This important feature as well suffers from security issues as generally it is performed by copying the VM image across the network from one source VMM to destination VMM [103,108]. Live migration might result into man-in-the-middle (MitM) and insider attack [69,109,110] and other related security vulnerabilities like information disclosure [111]. Ali et al. [10] mentioned that VMs could be rolled back to its previous state if needed so. However, this re-surface the previous security vulnerabilities patched out or restores disabled security credentials [97,112]. A rollback can also revert to previous configuration error and outdated security policy [27]. Also, to enable the rollback a copy of the VM image is maintained which can result in propagation of configuration errors and other vulnerabilities [113].

Multi-tenancy environment vulnerabilities (V03.4): Multi-tenancy architecture allows a software application to partition its data and configuration in the virtual environment. Individual cloud user works with a customized virtual application instance,

but sharing the same hardware platform so poses the security and privacy challenges [25]. Sood and Enbody [61] highlighted co-located services and hosts may result in targeted cyber-attacks which is a superset of advanced persistent threat (APT). Also, multi-tenancy may result in violation of integrity [10]. Sharing computing resources to multiple tenants may allow malicious users to launch attacks on data under processing by another tenant [27,114]. Multi-tenancy might result in challenges in device sanitization as the devices might be in use by other tenants [30].

Hypervisor vulnerabilities (V03.5): A hypervisor or VM Monitor (VMM) is a software that manages the VMs and enables multiple operating systems to run concurrently on the same hardware. A hypervisor, like any other cloud components, suffers through security and privacy challenges [115]. A threat of VM escape, (a situation in which a VM escapes, possibly by the act of a malicious user, from the control of hypervisor) can lead to bringing down the hypervisor itself and illegitimate access to other VMs [70]. Further, a compromised VMM can bring all the associated VMs to a halt or non-functioning as it exposes the larger attack surface [107,116,117]. After a thorough code review of open-source hypervisors Xen and KVM, Perez-Botero et al. characterized hypervisor vulnerabilities with three dimensions: the trigger source (attacker's location), the attack vector (vulnerable hypervisor functionality), and the attack target (compromised domain/component) [118]. Wang et al. [119] mentioned the large code base of VMM exposes it for the software related vulnerabilities [35]. Subashini and Kavitha [8] highlighted isolation, inspection and interposition properties yet to be achieved in VMMs. Pearce et al. [97] in their work on virtualization described issues like single point failure, maliciousness and untrusted components of VMM.

4.5.4. Vulnerabilities in infrastructure layer — network (V04)

Cloud network communication can be put under two classes: External and Internal [10]. External communication involves communication external to the cloud, i.e. between cloud components and consumers, which happens over the Internet. Internal communication involves communication within cloud components and VMs over virtual network communication channels. So, vulnerabilities of protocols and technologies associated with the Internet and virtual network is inherent to the cloud network infrastructure [9,27,30].

Network communication protocol and technology vulnerabilities (V04.1): These are inherent vulnerabilities associated with network communication protocol and technology used for accessing the cloud services. The TCP/IP stack based protocols like DHCP, IP, and DNS, have inherent vulnerabilities and are susceptible to IP spoofing, DNS cache poisoning or DNS spoofing [66] and might cause cross-tenant attacks [21]. When a malicious website is visited the DNS settings of the user's broadband network router might be changed by an attacker [120]. Inappropriate implementation of session handling techniques, to handle HTTP statelessness, might lead to session riding or session hijacking [18]. Mixing of HTTPS with HTTP in web client communication with cloud services results in unsecured communication [121,122]. Jensen et al. [60] describe flooding attacks as a real threat to the cloud, leading direct DoS, indirect DoS, and accountability issue. Panah et al. [66] mentioned about cookie theft, cookie poisoning, and impersonation attacks in the web-based communication. Heninger et al. [87] have demonstrated TLS and SSH vulnerabilities due to weak cryptographic key usage. MitM attack demonstrated by using forged certificates for HTTPS [123]. The cloud users get superuser access for managing their VMs, and that enables a malicious user to acquire IP and MAC addresses of VM machines to make malicious use for attacks, like sniffing and spoofing attacks on network [10].

Network shared component vulnerabilities (V04.2): It is very likely that VM instances share network infrastructure components like DHCP servers, DNS servers, routers, etc., and these shared network components have inherent vulnerabilities [9]. Sharing resources may lead to cross-tenant attacks [10,18,27]. The shared component in the network, like routers, if not dimensioned correctly might lead to traffic bottlenecks on a cloud network, like routers [31].

Virtual network vulnerabilities (V04.3): Virtualization of servers is leading to evolving a new type of access layer (Virtual Network Layer) to provide inter- and intra-VM connectivity [124]. Generally, users get the capability to configure, through management interfaces, communication channels to connect from one VM to other running on the same physical platforms. The communication through these virtual channels is hidden from any monitoring and so untraceable and are vulnerable to attacks [9,70,125,126]. Reuben [127] highlighted ex-filtration of data from/to the host OS of VMs through virtual network channels by malicious code running as VMs. Hypervisor uses virtual networks to connect the VMs that might lead to sniffing and spoofing attack for malicious VMs [27,97]. A malicious VM may use ARP spoofing to redirect packets to other VMs [112]. Morsy et al. [128] highlighted that the software in vSwitch might result in network-based VM attacks.

4.5.5. Vulnerabilities in infrastructure layer — storage (V05)

Huge storage capacity, high availability and stable performance make online storage services very exciting. At the same time, it poses security challenges due to lack of transparency and direct control over the data stored in the cloud environment [31]. Also, the cloud-specific characteristics like virtualization and multi-tenancy bring inherent security challenges for data storage in the cloud [10]. Chen and Zhao [129] discussed different vulnerabilities associated with the life-cycle of data in the cloud environment. Singh et al. [35] mentioned storage security concerns related to cryptography, data-remanence, data-sanitization, data-leakage, snooping of data malware and availability.

Data storage cryptography vulnerabilities (V05.1): Poor key management, faulty, insecure and obsolete encryption algorithm [18] makes data storage vulnerable to security attacks [18,30,70,88]. The poor encryption technique is highlighted as the biggest risk by Modi et al. in their detailed survey [29].

Data access vulnerabilities (V05.2): Data stored within a cloud environment is always under threat of being tampered by outsiders and insiders [130]. Data in cloud storage (data-in-rest) is vulnerable to unauthorized access due to a shared environment, compromised keys and application vulnerabilities [29].

Data storage location, backup and recovery vulnerabilities (V05.3): Cloud computing environment, generally, is distributed over multiple geographical locations to meet the cost -effectiveness, scalability, redundancy, disaster recovery, and other requirements. Local legal and regulatory policies affect the security and privacy of user data. The physical location vulnerability of data center hosting the storage and its backup is a concern for cloud users. The backup storage is vulnerable for unauthorized access and tampering [8]. Resource pooling and elasticity characteristics of cloud have enabled dynamic allocation and sharing of the resources, but invite unique security challenge in terms of data recovery vulnerabilities, of the previous user by

the newly allocated user [131]. Cloud storage is vulnerable to recovery from back up data [29].

Data sanitization vulnerabilities (V05.4),: Data sanitization is about the destruction of media containing cloud user data, especially user sensitive data, and it might arise either due to a need of changing the data media, or the data in the media is no longer needed, or termination of the user service contract [70]. Improper sanitization leads to security risks [132]. Grobauer et al. [18] mentioned, it might not be feasible to destroy the storage media as the associated hardware might still be in use by other tenants, and so there are associated risk of information disclosure [129].

4.5.6. Vulnerabilities in infrastructure layer — hardware (V06)

Virtualized hardware is one of the basic components for the cloud, and any small issue in it can lead to a partial or complete outage of the cloud system. Hardware availability is paralyzed due to faults in its component or its limited capacity [25,133,134]. Scalability and fault tolerance for the hardware must be taken care while designing and building the cloud solution. Ahuja et al. [135] pointed out a weak implementation of hardware-level encryption can lead to data integrity issues. Pearson [26] mentioned that there are more security risks in using the shared hardware than the dedicated hardware.

4.5.7. Vulnerabilities in infrastructure layer — facilities (V07)

Cloud computing resources are placed physically in facilities, known as data centers. These facilities are vulnerable to malicious insiders, natural disasters, poor infrastructure support (like bad cooling, power management, etc.) and inappropriate design.

Physical access vulnerabilities (V07.1): Malicious insiders can get physical security controls to penetrate the facilities [66]. Rocha and Correia [136] presents a threat to confidentiality due to a malicious insider. Santos et al. [137] talked about hardware tampering and cold boot attacks if some distrusted personnel get physical access to the data center. The BYOD (Bring-Your-Own-Device) paradigm is changing the DMZ static definition and access strategy for physical resources [30].

Natural disasters (V07.2): Natural disasters, like flood, earthquake, fire, etc., can lead to the destruction of a data center which may result in loss of data and service discontinuity [9,25].

4.5.8. Vulnerabilities in assurance and compliance vertical (V08)

Assurance and compliance provide a framework for the cloud user to evaluate the level of security a provider provides while delivering the cloud services. In a cloud environment assurance refers to ensuring SLAs, monitoring, incident response, and verification and validation of the deployed applications [33]. Compliance refers to providing services as per the laid down standards, legal and regulatory obligations, enforced privacy laws, openness to audit and forensic investigations [30,33,37]. More the assurance level of security a user finds in its provider, more the trust relationship strengthens between them.

Assurance vulnerabilities (V08.1): A weak SLA may result in SLA violations which in turn negatively affects the trust in cloud services and its provider [28,138]. Cloud monitoring is required to ensure efficient utilization of cloud computing resources and to ensure uninterrupted service continuity to its users [139]. Grobauer et al. [18] have highlighted the issue of insufficient monitoring and logging. From a security perspective, weakness in monitoring and audit of user activity logs might result in security incidents, and then prompt actions on those security incidents become inevitable [140]. To ensure system perform at a desirable level, conventional testing methodology is not sufficient for cloud-based applications and services [141]. A strong verification and validation methodologies and tools to be used for testing the software and applications performance [142]. Endo et al. [143] highlighted the challenges for providers for ensuring high availability of services as per SLA. Jensen and Schwenk [144] mentioned about flooding attacks in SOA which results in uncontrolled and unauthorized cloud resource usage. Idziorek and Tannian [145] described fraudulent resource consumption (FRC) using HTTP flooding attack to attack application layer resources in the cloud. Trust plays an important role in assuring cloud services. Social engineering and phishing negatively affect the trust in cloud services [146]. Thompson [147] pointed out ignorance of human factor in the past for implementation of information security.

Compliance vulnerabilities (V08.2): Spanoudakis et al. [148] highlighted security issues in the cloud environment and need for certifications of the cloud providers by a third party. Almost all the key characteristics of cloud, like outsourcing, virtualization, offshoring, and autonomic technologies poses problems for compliance with legal and regulatory obligations mainly due to the signed-off licensing and SLAs [26]. Such compliances are mainly related to determining which jurisdiction's law applies to hosted data lifecycle and data privacy law [149,150]. Yimam and Fernandez [151] highlighted six major compliance issues — security threats, overlap with security, lack of full control and transparency, lack of standard reference architectures, the complexity of regulations, and regulation overlaps. Subashini and Kavitha [8] highlighted the concerns about data breaches, availability and application vulnerabilities might lead to financial and legal implications. Zissis and Lekkas [25] highlighted about organizations dealing with personal data must align with the country's legal framework to protect the confidentiality and privacy of its clients. Cloud poses several legal challenges towards privacy issues as the data is stored in multiple locations. Other issues related to the law of the land has been highlighted are — laws of the countries, regulatory e-discovery compliance (including privacy), auditing and monitoring activities, and privacy [152–155].

Most of the cloud solutions lack support for forensic investigations [30]. Digital forensic involves data seizing, data disclosure, data analysis, data recovery and producing data as evidence, and that compromises the confidentiality and privacy of the user data [35,88,156,157]. Taylor [158] described the legal implications for computer forensic analyst in acquiring and analyzing digital evidence to establish — which data and how much was stored where; what data was processed by which software at which computing device; and investigations becomes even more complicated when the data under investigation falls under different jurisdiction. Katilu et al. [159] highlighted the challenges related to data provenance in the cloud to support forensic investigations.

The availability of log files generated in the cloud system is essential for any audit compliance and forensic investigation to establish the accountability of any event that occurred within the identified scope of cloud computing environment [160].

Compliance issues related to incorrect resources usage and billing in cloud services are highlighted in works of Xiao and Xiao [28], Sekar and Maniatis [161].

4.6. Cloud security countermeasures

Researchers from academia, industry experts and standards organizations have provided recommendations and best practices to use for securing the cloud computing environment. Amazon, one of the well known commercial cloud service provider, in

its whitepaper highlights best practices to use for cloud security [162]. The whitepaper suggests an approach for — identifying, categorizing and protecting one's assets on AWS, managing access to AWS resources and securing data, operating systems, applications, and overall infrastructure. Further, twelve steps best practices to follow for Amazon Web Services (AWS) has been explained by Trend Micro, a cybersecurity and defense company, which is in general applicable for any cloud computing environment [163]. CSA [20] in its security guidelines provides recommendations for twelve different domains related to the cloud.

4.6.1. Identity and access management (M01)

Gartner IT Glossary [164] defines Identity and Access Management (IAM) as "*The security discipline that enables the right individuals to access the right resources at the right times for the right reasons*". IAM involves management of user identity, user authentication and user authorization at all levels of cloud environment — from application level to platform level to virtual infrastructure machine, hypervisor, network, storage, and hardware level [9]. CSA in its Security Guidance details out for Identity and Access Management in Domain 12 section [20].

User identity management is all about life cycle management of digital identity of end-user which can be a human or machine involving registration, provisioning, propagating, managing, deprovisioning and deregistration. User identity management mostly involves password management which involves enforcing a strong password with strict life-cycle management procedures, covering change, resetting and expiration policy for passwords. IBM Cloud Security Guidance [165] provides recommendations for password policy management. Authentication is a process of confirming the identity of an end-user when the end user is logging in. CSA [20] recommends using federated identity (FDI) and multi-factor authentication (MFA) by using hard tokens, soft tokens, out-of-band passwords, and biometrics. Authorization is granting an end-user to use or to act upon permitted resources of interest. Access control is a condition to execute to true for authorization to succeed like an end-user must be authenticated before allowed to use the permitted resource. Attribute-Based Access Control (ABAC) is preferred over Role Based Access Control (RBAC).

There are quite a few available IAM standards which are being used in the cloud environment. Security Assertion Markup Language (SAML) 2.0, from OASIS, defines a framework for exchanging security information between entities that supports both authentication and authorization along with federated identity [166]. SAML uses XML based assertions between two communicating parties, the identity provider party, and the identity relying party, containing statements for authentication, attributes and authorization decision. Open Authentication (OAuth) 2.0 [167] is an Internet Engineering Task Force (IETF) standard for authorization wherein a third-party application is provided limited and restricted access to the HTTP Services. Web services mostly use it for delegating access control authorization. An updated version of the same suggests using external user-agents, rather than embedded user-agents by native apps while interactive with authorization end-point [168]. It details out authorization flows for a browser as the external user-agent and poses the requirements for authorization servers to implement the flow. OpenID Connect 1.0 [169] is an identity layer over OAuth 2.0 protocol that verifies the identity of an End-User for a Client, (Relying Party (RP)), using the authentication services of an Authorization Server (OpenID Provider (OP)). It also enables RP to get basic End-User's profile information in interoperable REST-like format. It uses JSON [170,171] data format to specify HTTP based REST [172, 173] Web Services. The SAML, OAuth 2.0 and OpenID Connect 1.0 together provide Federated Identity Management (FIdM) to authenticate and authorize users across multiple service providers to get access to their resources without sharing and transmitting sensitive user information to each other. Naik et al. [78] in their study have highlighted how these three, SAML, OAuth and OIDC, together provides secured digital identity. Lu et al. [174] provides a mechanism for automatic verification, ProVerify, of security of OpenID Connect protocol using Prolog rules [175]. In his book Prabath Siriwardena [176] advocates for the usage of OAuth 2.0, OpenID Connect with JSON Web Encryption (JWE) [177] and JSON Web Signature (JWS) [178]. Manika et al. [179] evaluated OpenID Connect libraries and found that all libraries are susceptible to Single-Phase and Cross-Phase Attacks due to a logical flaw in the protocol. They proposed for Practical Offensive Evaluation of Single Sign-On Services (PrOfESSOS) to address the existing problems. The eXtensible Access Control Markup Language (XACML) defines attribute-based access controls and can be used with both SAML and OAuth as a policy language for defining access controls. Another standard, System for Cross-domain Identity Management (SCIM) [180] used between the domains for exchanging identity information. It enables for provisioning and de-provisioning of user accounts in external systems and used for exchanging attribute information.

Industry leaders for the cloud, IBM [165], Google [181,182] and [183] in their cloud security guidelines have emphasized on strong multi-factor authentication with the capability of delegated authentication including federated identity management and secured communication tunnel for any end-user sensitive data propagation. They also emphasize to implement a notification mechanism to inform end-user for a security breach. Further, for a strong authorization, CSA [20] recommends for the least privileged scheme and asset classification to map the level of authentication needed to grant the access. Abdellaoui et al. [184] proposed a password generator for cloud user with a combination of multi-factor authentication, one-time password, and SHA1. Habiba et al. [185] in their work reviewed identity management systems for clouds and suggested to choose for the one which suits to your requirement as no one is fit for all cases.

Xie et al. [186] proposed a model of access control for the cloud users that combines role-based and trust-based access control. The user's role classes define the role assessment weights. A comprehensive trust-degrees (direct, recommendation and feedback) are calculated as per role assessment weights and behavior of the role. Tang et al. [187] proposed a Multi-Tenant Role Based Access Control (MT-RBAC) wherein the trustee authorizes cross-tenant access to the trustor's resources in line with the trust relation and access granting criterions. Beaty et al. [188] proposed Cloud Access Manager (CAM) for providing network-level access control management for the cloud. It uses Session Traversal Utilities for NATs (STUN) [189] to identify the publicly known IP of the client (that might be in a private network with its private IP) which gets registered in CAM with a permitted level of access control for hosted cloud services. This way CAM ensures only authorized IP addresses to get access to the IP address and port of a VM instance on the cloud. Gonzalez et al. [190] proposed the concept of credential classification integrated with a unified framework in the cloud context comprising entities, service types, deployment model and lifecycle control.

Zhang et al. [191] proposed Flexible and Efficient Access Control Scheme (FEACS) that uses Attribute-Based Encryption (ABE) mechanism which facilitates dynamic membership, accurate and efficient access policy definition and evaluation. Liu et al. [192] extend Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme to provide hierarchical attribute based scheme that uses the attribute-based signature (ABS) to provide a hierarchical structure of multi-authorities. It uses XACML for policy management. Habiba et al. [193] proposed a user-centric, instead

of application-centric, identification, authentication, and authorization Access Control Management (ACM) framework for the cloud system. The framework has different modules to ensure dynamic security, policy conflict resolution, authorization confidentiality, potential threat detection, cost reduction, and single point identification.

4.6.2. Encryption and key management (M02)

Encryption mechanisms are used to cater to data security and privacy requirements of confidentiality, integrity in combination with message digest, and both authentication and accountability in combination with a digital signature. There might be different encryption mechanisms for data in-store, data in-process and data-in-transit. Phaphoom et al. [9] suggest, for symmetric encryption a minimum 128-bit key and for asymmetric encryption 2048-bit key to use. They insist for a strong key management process for key storage, key access control, and its backup and recoverability. They recommend for users to know the encryption mechanism used by cloud providers so that they could apply additional mechanisms when they find insufficient security level.

For data in-store, Martin [194] suggest using AES for encrypting hard disks storage in XEX-based tweaked-codebook mode with ciphertext stealing (XTS). Lin and Tzeng [195] used proxy re-encryption in combination with decentralized erasure code for secured storage to provide confidentiality, privacy, and availability. Ahmed et al. [196] introduced SECRESO, a SEcure storage model for Cloud data based on REed-SOlomon. In this model, an enhanced Reed-Solomon code-based encryption, along with log-based recovery, is used for secured storage, that supports confidentiality, integrity, availability and fault tolerance for data in-store. Dick et al. [197] came up with hourglass protocol to encrypt data files, and at the same time allows users to verify the correctness of file encryption.

To process the encrypted data, a cloud provider needs to decrypt the ciphered data that raises privacy concerns. To address this fully homomorphic encryption is used that allows us to perform arbitrary operations on encrypted data without decrypting it. There are different flavors of fully homomorphic encryption techniques proposed by researchers, based on the applications usage scenarios [198–205]. Pearson et al. [26] proposed a privacy manager component using encryption-based obfuscation to for privacy protection. Zissis and Lekkas [25] advocates trusted third party based mechanism for secured encryption to achieve confidentiality and integrity of shared information and messages. Diallo et al. [206] proposed CloudProtect, a middleware system to protect data privacy by providing encryption functionality.

Secured search on stored encrypted data is required to ensure confidentiality and privacy of it. Wang et al. [207] and Yu et al. [208] provides the solution for secure search, including ranked keyword search and multi-keyword top-k search, over encrypted stored data. Wei and Reiter [209] proposed a mechanism that facilitates access to encrypted data for pattern-matching applications. Pattuk et al. [210] proposed a framework BigSecret that provides three encryption models for secure outsourcing of data as key–value encrypted storage on the cloud. It provides secured data management as well secured queries on encrypted data. The models allow get, scan and delete operation over encrypted data while using crypto indices based on pseudo-random numbers or packetization.

Tysowski and Hasan [211] proposed a key management system for secured data outsourcing applications that use a group keying mechanism in combination with attribute-based encryption and re-encryption to allow access of data to authorized users only. Chu et al. [212] used a key-aggregate cryptosystem to aggregate secret keys into a single key and used this single key for encrypting information and messages. Jajodia et al. [213] proposed recoverable encryption using a noised secret for key backup storage to limit the risk of key disclosure, and breach of confidentiality and so increasing data safety and availability.

Wang et al. [214] proposed a scheme that combines the hierarchical identity-based encryption (HIBE) system with the ciphertext-policy attribute-based encryption (CP-ABE) system and then applying proxy re-encryption and lazy re-encryption to provide confidentiality and secured access control to enterprise cloud users. Kumar et al. [215] proposed Attribute-Based Encryption (ABE) scheme using hash functions, digital signature, and asymmetric encryptions. The scheme implements, dual authentication scheme with a digital signature and public key. To address the problem of untrusted attribute authority in the cloud system, Hong et al. [216] propose a signature scheme based on a key-policy attribute with untrusted authority and traceability (KP-ABS-UT). In this scheme, the signer's private key has two parts, the first part is received from attribute authority and the second part is the signer's private keys and so making it challenging to forge any signatures by attribute authority. The scheme also has a *tracer* module to trace the identity of a signer.

Gan et al. [217] propose a revocable key-aggregate encryption scheme that realizes key aggregation and access control with revocation capabilities. When user revocation occurs, cloud server updates the ciphertext so that revoked user does not have access to the new ciphertext and non-revoked users do not need to update their private keys. Also, it has a verification mechanism to verify the updated ciphertext and successful revocation of the user. Wang et al. [218] combine mechanisms of Proxy Re-Encryption (PRE) and Key-Insulated Cryptosystems (KIE) to propose a key-insulated proxy re-encryption (KIPRE) scheme. This scheme provides resilience to the key-exposure problem. Yang et al. [219] propose to use Batch Attribute-Based Encryption (BABE) to address the limitation of ABE being designed for users belonging to one group or organization. If the same data is to be shared with multiple requestors of the different organization, then the provider must send to one organization at one time. The proposed scheme enables to send the same data in parallel to the users of different groups or organizations.

4.6.3. Digital signature and message digest (M03)

Message Digest [220], Digital Signature [221] and Message Authentication Code (MAC) [222] are the mechanisms to ensure authenticity, integrity, and non-repudiation of data/messages exchanged between any communicating parties and so is recommended to be used in the cloud system [9,33,223]. In Message Digest, the message is hashed using a standard hash function like MD5 [224], SHA [225], etc., and in Digital Signature, Message Digest signed by asymmetric key-pair while in Message Authentication Code (MAC) Message Digest signed by the symmetric key. In distributed environments, like a cloud, a digital signature with SSO and Lightweight Directory Access Protocol (LDAP) provides a stronger authentication process while providing user mobility and flexibility at the same time. The signing private key authenticates the user automatically and transparently around the network wherever and whenever the user wants to establish a connection with communicating servers and devices [25]. Santos et al. [137] proposed to use the digital signature with the RSA algorithm for secure data communication over the Internet for cloud environments.

Apart from providing authentication, non-repudiation (accountability) and integrity, digital signatures have been used with the combination of other approaches to provide availability, confidentiality, privacy, anonymity and traceability services also. Encryption-based digital signatures may support both integrity and privacy. Shraer et al. [226] present Venus that uses a key-based object store service to ensure integrity and consistency for

applications. These applications do not require trusted components. Chow et al. [227] designed a group signature, and along with identity-based broadcast, encryption used it to provide anonymity, confidentiality, and traceability. Xu et al. [228] used the digital signature in Software Service Signature (S3) solution to arrest free-riding cases of SaaS. In free-riding, malicious users try to maximize their benefits in using the service(s). S3 uses ID-based proxy signatures from pairings for authentication of users so that service requests are verifiable. Wang et al. [229] proposed a security mediator that uses verification metadata based on digital signatures for providing anonymous proofs of data possession and to do so it does not need to know about outsourced data. Attasena et al. [230,231] proposed to use two types of signatures to support data availability and integrity for a multi-secret sharing scheme that uses block cryptography, hash functions, and secret sharing. First, the inner signature is generated from all data in each shared data block that ensure data integrity. Second, the outer signature is generated from each encrypted data block that preserves data availability by quickly identifying and correcting erroneous data blocks.

Shiny et al. [232] proposed a framework to use a digital signature for data auditing to ensure the authenticity and integrity of the data. Dey et al. [233] use message digest based authentication to establish authenticated communication sessions between cloud servers and mobile devices.

4.6.4. Intrusion detection and prevention system (M04)

IDPSs are generally dependent on identifying anomalies based on the analysis of the traffic patterns and activities to detect the possibilities of different attacks [10]. However, virtualized network challenges the goal of such preventive mechanism [70]. For cloud systems, intrusion detection and prevention system is required both at the network level and at VM instance level. The network-based intrusion detection system is recommended to address the vulnerabilities due to Internet protocols, session hijacking, authentication and authorization intrusions, and backdoor attacks [234].

Intrusion detection system (IDS) for cloud could be classified as Network based IDS (NIDS), Host-based IDS (HIDS), Distributed IDS (DIDS) and Hypervisor based IDS [234–237]. In network-based IDS [238–245] for the cloud environment, all the network packets are captured and analyzed using signature and/or anomaly based detection approach for identifying malicious activities or events such as DoS attacks, port scanning, user to root attacks, etc. In a signature-based approach, information captured in packets is matched with the known attack signature pattern. In the anomaly-based approach, it compares the current and the previous behavior of the user. In host-based IDS [246–248] information is collected, monitored, and analyzed at the host level. It observes and detects change in the host kernel, host file system and behavior of the program. The HIDS can be deployed on a host or VM or hypervisor (VMM) to analyze the system logs against user credential and access control policies to detect intrusion events. Distributed IDS [249,250] contains multiple IDSs (like NIDS, HIDS) deployed over a large network to monitor and analyze the traffic pattern for detection of any intrusion and can work independently and/or collaboratively. Hypervisor-based IDS [251,252] are deployed at the hypervisor layer and detects anomalous activities and events by monitoring and analyzing the information exchanged in communications between VMs, VM and hypervisor, and communication within the virtual network of a hypervisor.

A. Bakshi and Yogesh [238] proposed A SNORT based system that monitors for any suspicious activities [253]. If detected, it blocks packets coming from the source IP and notifies back to the source IP about the same. In the case of observed DDoS, it blocks all the packets and transfers the service from the affected VM to another VM. Lo et al. [249] proposed for a Cooperative IDS (CIDS) wherein IDSs in cloud region exchanges the alerts and cooperative agents at each of these IDSs evaluate whether to accepts these alerts, or not, and so to avoid the same type of attacks happening. Teng et al. [254] proposed for a Cooperative IDS (CIDS) model which is based on Common Intrusion Detection Framework that has event generator, statistical detector, feature detector, fusion center and response unit [255]. Ficco et al. [256] proposed a scalable multi-layer architecture for monitoring and detection of the distributed DoS attack in federated cloud systems. It uses publish/subscribe middleware to collect and share security information as well present an open source framework for defining customized event correlation rules and to develop and deploy security components. Somani et al. [257] performed a comprehensive analysis of cloud DDoS and provided schemes for combatting cloud DDoS through structured prevention, detection, and mitigation methods. They suggest challenge response, hidden servers/ports, selective access, resource limits, crypto puzzles and reputation based access as prevention methods; botcloud detection, anomaly detection, source/spoof trace, session duration, web behavior, usage-based filtering, count-based filtering and hop count based filtering as detection methods; and backup resources, resource scaling, migration, shutdown, SDN based and third-party mitigation as the mitigation methods. Yu et al. [258] suggest, in the event of DDoS detection, to dynamically allocate idle resources to the cloud customers affected due to the DDoS for guaranteeing the QoS to benign users. They used queuing theory model to implement this mitigation strategy. Xing et al. [259] proposed SDN based IPS, SDNIPS, in the cloud virtual networking. It leverages the capabilities of snort and flexible network reconfiguration from SDN (Open vSwitch). It uses variable attack surfaces as an attack mitigation strategy. In yet another study by Xing et al. [260] have proposed SnortFlow an OpenFlow and Snort-based IPS, that enables the cloud system for intrusions detection and activate reconfiguring the cloud networking system on-the-fly as a countermeasure. Machine learning algorithm based intrusion detection and prevention system have been proposed by different researchers [261–265].

4.6.5. Web applications, services and interfaces security measures (M05)

As described in work of Phaphoom et al. [9] cloud applications and operations (like service provisioning, administration, and orchestration) heavily rely on web services as a core enabling technologies and WS-Security [266] is a standard to countermeasure the vulnerabilities in web services communication. WS-Security combines: *security tokens* — used for authentication and authorization; *encryption* — to provide confidentiality and integrity; *digital signatures* — for integrity and accountability (non-repudiation). WS-security [267] provides end-end-end security using XML-Encryption and XML-Signature. Apart from web services, the user's frontend environment, primarily web browsers, to access cloud services and operations through web services, also needs countermeasures to address vulnerabilities in web browsers. Vulnerabilities in web browsers are very much attributed to permission levels given to the plug-ins. It is suggested to use only trusted plug-ins along with anti-virus and anti-spyware with updated profiles [9].

Fernandez et al. [268] explained different web services security standards that are used for ensuring integrity, confidentiality, authentication and authorization for the communication between the web applications and web clients, like SAML, [166], XACML [269], XML Key Management Specification (XKMS) [270], WS-Security [266], WS-Federation [271], WS-Secure Conversation [272], XML Digital Signature [273], XML Encryption [274], WS-Security Policy [275] and WS-Trust [276].

Web application programming interfaces (APIs) are used by cloud service providers to make the service features available to their users which can be extended by the users to customize the feature, and that leads to security vulnerabilities. The secured APIs provide confidence in protected and non-malicious use of cloud services. Some of the common vulnerabilities in APIs are incorrect and/or insufficient input validation, weak credentials and inappropriate authorization [10]. Wu et al. [277] proposed an API management platform based on OAuth which is a token-based access control (TBAC). In this scheme, APIs from API provider is registered with the API management platform and receives a private key for validating the tokens. On API consumer's requests for access token, the API management platform validates the request and once validated, API consumer receives the token along with another private key. The API consumer calls provider's registered API using the received token and signed by its private key. The provider gets token validated from the API management platform, and on success, access is granted to the consumer.

Web application scanner [278] is used to identify security vulnerabilities in a web application while communicating to the web application through the frontend. It performs black-box testing to detect vulnerabilities in web application and architectural weaknesses by performing attacks [279]. Web Application Firewall [280] is recommended to use to filter, block and monitor HTTP traffic between web applications and web clients, like browsers, to prevent web attacks due to web application security flaws [281].

The best way to counter web services and web client vulnerabilities is to develop a more security robust web applications and for that the software development teams must have adequate security training [89]. Insufficient input validation might lead to SQL injection attacks. Fragile GET method can lead to XSS and URL-guessing attack. POST method can get impacted due to hidden field manipulation or stealing cookies. It is recommended to use HTTP over TLS. Standards Organization OASIS recommends using SAML assertions [166] for web services confidentiality and authentication/integrity on an end-to-end basis. CSA security guideline recommends, to use the secure Software Development Life Cycle (SDLC) and software architecture, to reuse the security validated software components, to perform periodic penetration testing for web applications, and manual periodic testing for secure session management of web application. One-time cookie stateless method [282] can be used to prevent session hijacking attacks. To provide data confidentiality and integrity, the one-time cookie method is complemented with HTTPS. In a one-time cookie mechanism, a unique token is generated per request using the session key, that is combined with Message Authentication Codes (HMACs).

Gupta and Gupta [283] describe a defensive XSS framework to detect and mitigate the XSS vulnerabilities in the cloud-hosted web applications. The framework does so by discovering vulnerable malicious user injection point in web applications through execution of crawling sessions in all the extracted web pages. The framework automatically places sanitizers on the untrusted variables of XSS attack payloads in a context-sensitive manner. Akrout et al. [284] use web page clustering technique, a black box approach, to identify vulnerabilities in web applications corresponding to SQL injection attacks, OsCommanding, File Include, and XPath. Mitropoulos and Spinellis [285] surveyed countermeasures for the code injection attacks for web applications and web services. They categorized countermeasures based on whether the solution suggested identifies the vulnerability in sources code, or binary executable (static analysis) for a possible software bug that could lead to the code injection attack, or suggested solution detects and prevents the code injections attack in a running application (dynamic analysis). Mao et al. [286] proposed a tool to detect timing-based probing attacks in web applications [287]. Timing-based probing attacks study variations in the time taken by the system to process different inputs like loading the page resources by a web browser that depends on the system's cache. Through variation in time attackers gets the browsing history information that leads to privacy leakage.

4.6.6. Software development environment security measures (M06)

To develop a consistent and high-quality software system, certain characteristics needs to be taken into consideration, right from concept formation to software delivery [288]. SDLC must be religiously followed to achieve the functional and non-functional requirements. Martin [89] suggested to define solid software quality metrics and SDLC to measure them for ensuring controls are effective and correctly implemented along with quality assurance. Microsoft defines a Security Development Lifecycle (SDL) [289] which is a software development process to help developers to build more secure software and meet security compliance requirements at a reduced cost. Rittinghouse and Ransome [55] proposed for a six-phase Secure Software Development Lifecycle (SecSDLC) to identify software application specific threats and associated risk that, enables to design and implement specific controls to counter the threats and manage the associated risks. The six steps are — investigation, analysis, logical design, physical design, implementation, and maintenance. Also, at the broader level, the user experience of a software system takes higher precedence over quality and usability of the software and ensuring security and privacy of user data enhances user experiences [290].

Rodero-Merino et al. [92] mentioned about five security areas that an OS must support for the cloud virtual environment for safe multi-tenancy, as it is the OS that controls the resources such as processes, memories, network, devices, and data. These five areas are — access control, integrated firewall, data encryption, prevention of execution of memory zones and isolation. Further, it explained how .NET and Java development framework provides the isolation at OS level for access to system resources, like memory.

To secure cloud OS, Spring [95] advocated for, cloud providers to deploy single, hardened, paired-down OS and monitor binary changes on the OS image. Malicious system admin is seen as insider threat and researchers have provided different approaches to address the same which primarily focused around monitoring such behavior through activity logs analysis followed by security breach notification to take appropriate corrective and preventive actions [54,93,94].

Apart from cost and schedule, the development team must set quality as priority [9]. Martin [89] advocates for the training of the development team on security and threats so that they integrate required checks and controls in the application stack while following the SDLC. Park et al. [291] proposed four best practices to evolve SaaS Cloud Oriented Development Process (SCoDP) — the incremental transformation of cloud applications, respond resiliently to extended changes, multi-tenancy considerations in applications and software vulnerability management. In his book, McGraw [91] describes some of the best practices to build security in code as — security requirement analysis, architectural risk analysis, static code review analysis, security testing, abuse case development, and penetration testing. Bachmann et al. [292] recommends a holistic security testing approach all through the software development lifecycle across to address security threats.

4.6.7. Virtual environment security measures (M07)

In the cloud computing environment, virtual machines and their images, shared hardware and other resources (to support multi-tenancy), hypervisors and virtual network for internal communications together form the virtual environment. All these

components have the associated vulnerabilities, and cloud service provider needs to implement countermeasures to secure them.

Trusted computing (M07.1): Trusted computing is based on Trusted Platform Module (TPM) which is a hardware device that works as a cryptographic co-processor to support for cryptographic algorithm acceleration, sealing data, secure boot and attestation [293]. From the cloud perspective, virtual Trusted Platform Module (vTPM) introduced by Berger et al. [294], that provides cryptographic and secure storage functions of TPM to operating systems and applications running on virtual machines. In vTPM, there are vTPM instances that are associated with individual virtual machines and a vTPM manager that instantiates vTPMs and multiplexes incoming requests from virtual machines. The Trusted Cloud Computing Platform (TCCP), proposed by Santos et al. [137], provides a closed, confidential execution environment and allows users to attest the cloud provider before launching the service execution. Boampong and Wahsheh [295] while discussing different aspects of cloud security, have mentioned trusted computing platform can help to achieve confidentiality, authentication and integrity requirements. Santos et al. [296] proposed Excalibur system which used attribute based encryption mechanism to encrypt and decrypt data, based on the customer-defined policies. Ma et al. [297] described the usage of trusted computing to address security issues related to virtual machine replication to increase availability. Li et al. [298] proposed a non-cryptographic solution for privacy protection by introducing MyCloud which is based on trust computing. MyCloud removes control VM from the root mode and only keeps security and performance crucial data in trusted computing base (TCB), and so facilitates for user privacy protection as cloud provider cannot inspect user memory anymore due to the removal of control VM. Lee [299] proposed a hardware architecture for supporting access control for cloud computing as software-based access control is more prone to attacks. Szefer et al. [300] proposed for a secure hardware infrastructure to increase the protection of user's data and application against attacks from malicious software and other tenants in the cloud.

Intel's Software Guard eXtensions (SGX) offers hardware -based memory encryption, enabling isolation of specific application code and data in memory, termed as *enclave*, to provide confidentiality and integrity of cloud applications [301]. Arnautov et al. [302] proposed a secure container mechanism for Docker, SCONE, having a small TCB with low-performance overheads for I/O data encryption/decryption based on SGX. Brenner et al. [303] presented *Vert.x Vault*, based on SGX for secure cloud microservices implementation. Tsai et al. [304] proposed Graphene-SGX, a Library OS, to explain SGX usability without modifying an existing application. Campanile etc al. [305] presented an application PoGriMon for real-time monitoring of Power Grid over *SecureCloud* IaaS that supports SGX enable containers for cloud applications [306]. Sun et al. [307] proposed *enclave TPM* (eTPM), a trusted cloud platform security component emulating TPM functionalities, to protect cloud applications and employed Intel SGX for enhanced security of eTPM. There are other hardware-based security solutions, like IBM's SecureBlue++ and AMD SEV, emulating TPM functions for providing secured virtual cloud environment [308–310].

Virtual Machine and Hypervisor security (M07.2): The easiest approach to safeguard a guest VM is to allow VMM to know guest VMs's operating system so that it can monitor and analyze the activities at the guest VM [31]. However, this may not be feasible always as provider might not get the guest VM details from the user. Christodorescu et al. [311] proposed an architecture based on VM introspection [251,312]. In this approach guest VM sits on reliable VMM which collects data for the interaction between the VM and VMM. VMM send the collected data to other specially designed safe VM for monitoring and analysis.

Zhang et al. [313] presented a hardware-assisted framework, HyperCheck, to protect the integrity of operating systems and hypervisors. The framework leverages System Management Mode (SMM) of x86 architecture to transparently and securely transmit the full state of the VMM to a remote server at a regular interval. The current state is compared with the initial state for any malicious modification. The framework provides detection and defense against DoS, rootkits and code and data integrity. Pan et al. [314] divide the functionality of hypervisor into two components to reduce the TCB. The first component GuestVisor is excluded from the TCB and runs in user mode and the second component SplitVisor resides in TCB, executes in root mode and responsible for providing isolating multiple GuestVisors. GuestVisors emulate the hardware for the VMs.

Wang et al. [315] presented HyperLock that provides a separate address space and restricted instruction set to execute. This way it provides secure hypervisor isolation at runtime. In this scheme, hypervisor cannot interact with guest VM directly and all interaction to happen through HyperLock. They also suggest hypervisor shadowing wherein each guest VM is paired with a separate shadow hypervisor so that a compromised hypervisor can affect only the paired guest VM. Wu et al. [277] presented a scheme wherein the VMM code is divided into smaller modules to grouped into two components. The first component, DeHype, has all the de-privileged code that can be executed in user mode and the second component, HypeLet, has all the code modules that could not be reduced to get executed in user mode and needs privileged access. This way the attack surface of hypervisor has been reduced.

The CloudVisor system [316], a lightweight security module that segregates security and VM management, ensures the privacy and integrity of VM resources during execution using nested virtualization by working beneath VMM. It intercepts control transitions between VMM and VMs for security operations. It does, hiding of general purpose registers, monitoring address translation to ensure memory isolation, and encryption of page table for a VM to prohibit VMM to overwrite, in case of mismatch in page ownership and the page table.

Szefer et al. [116] proposed a system, NoHype, without hypervisor to eliminate the hypervisor attack surface. This system makes use of four ideas — during bootup the guest OS, with minor modification in it, to perform all system discovery, pre-allocation of processors and memory, use of virtualized I/O devices and bringing the guest VM in more direct contact with the underlying hardware to avoid indirection.

Zhu et al. [317] introduce a hardware-assisted VM isolation, HA-VMSI, for ARM processors based hypervisors to provide runtime protection for guest VMs. HA-VMSI works as a thin security monitor that resides in ARM TrustZone with its entire TCB residing in ARM TrustZone. HA-VMSI provides an isolated address space to each VM and non-bypassable event-driven monitoring on the hypervisor.

NIST [318] recently has released security recommendations for a hypervisor that focus on secure execution of baseline functions of the hypervisor that is independent of the hypervisor architecture. The recommendations cover five basic functions for any hypervisor — VM process isolation, execution of privileged operations by the hypervisor for guest VMs, devices emulation and access Control, VM life-cycle management, and management of hypervisor.

Virtual Image security (M07.3): Wei et al. [104] proposed Mirage, a VM image management system, that has four measures

for protection of VM Images – a framework for access control to regulate sharing of VM images, remove unwanted information in the image by applying appropriate image filters before putting it in use, a provenance tracking mechanism to track performed operations on an image and a set of repository maintenance services, like virus scanning and security patching, to ensure secured usability of the VM images. Kazim et al. [319] proposed an image encryption module in their solution Encrypted Virtual Disk Images in Cloud (EVDIC) that encrypts an image, with AES-256 key, whenever a VM is terminated. Fan et al. [320] proposed Offline Patching Scheme (OPS) with two modules, a collector and a patcher, to identify the images from repositories that have outdated software and presence of any malware and rectify the vulnerabilities. Jeswani et al. [321] proposed a patch update for both running and dormant VM image. It groups similar VMs in classes and applies the patch in one, and if it is successful on one then it applies to all the VMs in that group in parallel and so save the time in patch updates. Schwarzkopf et al. [113] proposed two components to secure the cloud, first, Update Checker that identifies outdated software packages in virtual machines, for both running or dormant, and second, Online Penetration Suite performs pre-rollout penetration testing of virtual machines for security vulnerabilities. The outcome of these two components is sent a report to the stakeholder to take appropriate actions.

VM Migration and Rollback security (M07.4): Choudhary et al. [322] and Medina et al. [323] have provided a detailed survey on different VM migration techniques. Danev et al. [324] proposed for VM-vTPM migration that used vTPM key hierarchy for the secured migration. Kazim et al. [325] recommended for deletion of VM images, after VM migration, from old disks as attackers can recover data from old disks. Tavakoli et al. [326] proposed a framework for migrating VMs along with their security context that is secured by a stateful firewall at the hypervisor level. Wan et al. [327] used Virtual TPM and migrated this vTPM with VM to ensure the integrity of VM. They also used property based remote attestation to verify the security requirements at destination host for migration and a trusted communication channel between the source and destination by mutual authentication and a session key. Aslam et al. [328] introduced Trust Assurance Level (TAL) and Trust Tokens. TAL is computed using the credentials of a TPM to get the trust level of the cloud platform hardware, and Trust Tokens specify the trust level of a software stack. VM migration takes place only when the destination host is evaluated the specified TAL and Trust Tokens. Fan et al. [329] proposed to use TPM-based TLS protocol for both source and destination platform secured VM migration. Hong et al. [330] proposed for a three-phase protocol (authentication, remote attestation, and secure data transfer) for VM-vTPM live migration. Sharma et al. [331] presented a three-phase optimization (TPO) method for pre-copy VM migration — the first phase is to reduce the transfer of memory pages; the second phase is to reduce transfer of duplicate pages and third phase to reduce the data transfer for migration by applying the Run Length Encoding (RLE) compression technique. Song et al. [332] proposed Three-Stage Memory Copy (TSMC) based live VM migration mechanism — the first stage does full memory copy from source to destination; second stage copy the dirty bitmap of the source VM to destination VM and third stage copy dirty pages on demand from source to destination VM. Zhang et al. [107] proposed a secure live migration framework, PALM, ensuring the integrity and privacy protection for VM migration. Anala et al. [333] proposed a framework for live migration for a comprehensive security solution that includes role-based access policy, firewall protection, network intrusion, and encryption. HyperCoffer a, secure runtime environment for VM proposed by Xia et al. [334], uses logging and auditing mechanism for the protection against VM rollback issues. Gofman et al. [335] proposed a system SPARC to protect the privacy leakage due to rollback that uses secure check-pointing mechanism.

Virtual network communication security (M07.5): The shared use of routers and other network devices along with shared communication channels led to security-related concerns and research communities have proposed countermeasures to address the same [336]. Wu et al. [112] proposed a virtual network framework composed of three layers — routing layer, firewall and shared networks to prevent VMs from sniffing and spoofing. They tested this framework for Xen in two configuration modes of *bridged* and *routed*. They employed subnetting to provide security against unauthorized information disclosure. Fernandes et al. [337] proposed an architecture to provide isolation of resources, routing efficiently, and a secured channel for communication between routers and the VMM. Virtual routers copy routing-related information to the VMM for efficient routing, and virtual routers use symmetrical cryptography for secured communication with VMM. They put timestamps inside encrypted messages to ensure non-reproducibility and uniqueness of the messages.

Cabuk et al. [338] proposed security-enhanced network virtualization based on the Trusted Virtual Domains (TVDs) concept. It enables groups of related VMs on separate servers to get connected as if they are on the same network fabric and ensure cross-group security requirements such as confidentiality, integrity, isolation and controlling information flow. They implemented TVDs by combining the existing technologies such as VLAN tagging, Ethernet encapsulation and virtual private networks (VPNs). Wolinsky et al. [339] use virtual machine sandboxes to limit the VM access to physical resources, and each VM supports IPSec enabling the creation of secure channels and X.509 to provide VM authentication. They make use of tunneling to isolate network traffic between VMs and used firewalls to prevent communication between two different virtual networks.

Huang et al. [340] present a framework for secured routing. The routing information propagated through a virtual network is protected through group-keys assigned to virtual routers, and the group having the group-key can decrypt the encrypted routing information. This way, group routing information is not accessible to unauthorized groups, i.e. from other virtual and physical network. They used variable paths to propagate data flows in virtual networks. Yeow et al. [341] proposed for dynamic backup link creation with virtual routers to support virtual network resilience. To ensure reliability, each physical router is configured to hosting up to allowed maximum number of backup instances. Luo et al. [105] proposed to use virtual firewall entirely within a virtual environment to provide packet filtering and monitoring to protect VMs from outside threats. This virtual firewall can be realized in a traditional software running at one of the VMs or as extended functionality of a virtual switch or can be purpose-built device keeping the virtual network in mind.

Moraes et al. [342] proposed DCPortalsNG, a Software-Defined Network (SDN) methodology to isolate the tenant's VMs to provide virtual network security. It uses a per-tenant virtual network description by providing a unique identifier to each tenant. The SDN controller then rewrites packets using MAC addresses of these uniquely identified tenant's VMs and directs to the virtual switches to route the packet to the corresponding tenant virtual network only that flow through the physical network.

4.6.8. Network communication security measures (M08)

CSA guideline [20] recommends cloud provider should take appropriate security measures to protect data in transit by using a combination of firewalls, IDS, IPS, and virtual LANs. It should deploy firewalls to protect each external interface with only necessary ports opened and default settings as denial. An updated intrusion detection and prevention mechanism should be in place. The virtual and conventional devices should be closely connected with a hypervisor for monitoring of traffic over the virtual network. It recommends strict access management policies in place. Advanced Cloud Protection System (ACPS) [343] uses logging and periodic checksum verification of the binaries components as network intrusion detection system. ACPS remains transparent yet undetectable by the VMs. He et al. [344] proposed for tree-rule firewall to address security issues of swapping positions, shadowed rule and redundant traditionally listed firewall rule, especially for a large system like a cloud. This scheme as well improves the performance as it does tree-based searching wherein rules attribute from the received network packet is searched at the root node and then branched out to next sub-tree based on next expected rule-attribute. Subashini and Kavitha [8] proposed to test and validate provider's network security by performing network penetration and packet analysis, session management weaknesses assessment, insecure SSL trust configuration, and take appropriate security measures for observed deviations. See Section 4.6.7 for network security measures related to the virtual network, Section 4.6.4 for the intrusion detection and prevention measures, and Section 4.6.5 for the web interfaces security measures.

4.6.9. Data storage security measures (M09)

A survey on security issues in cloud service delivery models, by Ali et al. [10] identified, lack of control, multi-tenancy, virtualization and shared resources cause to data storage security issues in cloud computing model as compared to conventional computing model. CSA [20] has recommended to use the best practices to provide data storage security solutions.

Data Classification and Access Control (M09.1): The user data outsourced to cloud storage, generally, have different degrees of confidentiality and sensitivity. So, the encryption mechanism and access control to the user data can be defined accordingly. Tawalbeh et al. [345] suggested data stored in the cloud can be classified into three categories — Basic Level, Confidential Level, and Highly Confidential Level. The basic level contains data like videos and photos that are not very confidential, and it can use TLS and AES-256 for transport and storage data. The confidential level contains personal data and can use AES-128 with 128 bits block size with 128-bit keys and ten rounds of iterations. Highly confidential level data contains financial and military data and can use AES-256 and SHA-2 to prevent from unauthorized access. Shaikh et al. [346] suggested for a set of parameters for the classification of data based on three characteristics (access control, content, storage) of data classification in cloud storage. These parameters value together defines the security level of stored data. Access control mechanism mentioned in Section 4.6.1 is as well applicable for data storage access control.

Data integrity and availability (M09.2): Data confidentiality in cloud can be ensured through traditional encryption or secret sharing mechanism, and data authentication can ensure the integrity of data transmission. However, the integrity of stored data in the cloud is challenging [31]. Bowers et al. [347] introduced a distributed cryptographic system HAIL (High-Availability and Integrity Layer) that relies on a set of servers to prove a stored file is intact and retrievable for a client. Barsoum et al. [348] address the challenge of confirmation of storing multiple copies of data at multiple location and integrity of stored data by introducing Efficient Multi-Copy Provable Data Possession (EMC-PDP) protocols. Juels et al. [349] implemented a proof of retrievability (POR) mechanism by inserting encrypted disguised blocks in data files to detect any data modification by the server. Shacham et al. [350] proposed a small proof of retrievability model based on BLS signatures and Pseudo-Random Function(PRF). Curtmola et al. [351] suggested using remote data check protocol like PDP with the forward error-correcting code for ensuring the integrity of stored data. The PDP and POR mechanism focus on static data. Dynamic Provable Data Possession (DPDP) mechanism puts a check for dynamic file operations such as insert, append, update and delete operations. Ateniese et al. [352] introduced a DPDP model using a cryptographic hash function and symmetric key encryption. However, their work has a limitation of a fixed number of updates and does not support block insertion operation. This was rectified in the work of Erway et al. that uses authenticated skip list to support data dynamics [353]. Zhu et al. [354] proposed Cooperative Provable Data Possession (CPDP) mechanism that uses homomorphic verifiable response and hash index hierarchy. Ali et al. [355] proposed Secure Provable Data Possession (SPDP) scheme with replication support in the cloud using Tweaks protocol that ensures the number of available replica maintained by cloud provider as per the SLA and allows for dynamic operations.

Location, backup and recovery transparency (M09.3): The provider must be transparent to its user for backup related information like storage location, the frequency of backup, encryption mechanism used, access control used, and its availability during the recovery [356]. Armknecht et al. [357] proposed a storage solution ClearBox enabling a storage service provider to transparently attest the de-duplication patterns of the (encrypted) data being stored, to its customers. This way user will know the related information about the data storage. Wang [358] proposed a data secure storage scheme based on Tornado codes that combine symmetric encryption and erasure codes techniques that helps in error correction of recovery of lost data.

Data sanitization (M09.4): Reardon et al. [359] has detailed about secure data deletion by defining a taxonomy of adversaries having different capabilities and having different manners of access to the storage medium. They mentioned about different layers used to access the physical media and use of interfaces between these layers for secure deletion. NIST [360] provides a stepwise guideline for secured physical deletion of data for complete sanitization. Diesberg et al. [361] surveyed data deletion and sanitization processes and methods, and described a complete sanitization approach.

4.6.10. Hardware security measures (M10)

Hardware availability, as per agreed SLA, is a key ingredient to build trust in a cloud computing environment. Hardware can be unavailable partially or fully. Partial unavailability happens due to limited resource allocation, and in that case, a load balancing mechanism is used to ensure hardware availability as per current need and SLA [133]. Patra et al. [362] highlighted different fault tolerance mechanisms used in the cloud. Szefer et al. [300] proposed for hardware enhancement to make the cloud more secure. Hacigumus et al. [363] emphasized to use hardware-based encryption than software encryption for data integrity. Dharsee et al. [364] proposed Secured Virtual Architecture(SVA) as a software solution for processor bugs. SVA does it by three methods — first, use a code generator to generate instruction sequences that never trigger any processor bug, second, verify the generated native code for a program that does not trigger any processor bug, and third, inserts run-time checks into the generated native code to check for any processor bug is going to be triggered.

4.6.11. Physical security measures (M11)

Physical security measures include preventing malicious insiders and outsiders from getting physical access to cloud physical resources. In the case of natural disasters measures should include minimal or no loss of data for the cloud user and business continuity is assured.

Physical access control (M11.1): A strong physical identity, authentication and authorization must be in place for secure access to the data center. Bio-metric authentication and authorization mechanism for cloud environment access management could be more effective than the conventional mechanism [365–367].

Business continuity and disaster recovery planning (M11.2): Phaphoom et al. [9] recommended for implementation of standard Business Continuity Plan (for example BS25999, ISO22301) for the cloud providers. For disaster recovery, Nakajima et al. [368] proposed for a Management Engine (ME) that prioritizes resource allocation to the high priority services over low priority services. Bernstein et al. [369] and Rong et al. [370] proposed for to opt for Inter-Cloud provider to address data lock-in challenge in case of natural disaster as one cloud provider environment will be available if other is not available due to a natural disaster.

4.6.12. Assurance and compliance measures (M12)

Assurance and compliance measures are a set of proactive actions that a provider executes to ensure necessary countermeasures are implemented to address known vulnerabilities in the cloud computing architectural components and used technologies and are sufficient to detect any malicious use of the cloud resources. Assurance and compliance measures are about monitoring and assessing implemented security solutions sufficiency for secured cloud operation. A recent work presents a three-dimensional perspective of cloud security assurance describing the relationship among security solutions, security operations, and security compliance [371].

Service Level Agreement (M12.1): SLA document defines the contractual agreement between the cloud user and the cloud provider. It contains — minimum performance level of the cloud provider, counteractive actions, and consequences on SLA breach. The security requirement must be explicitly mentioned into the SLA along with monitoring and measurement mechanism [10]. Kandukuri et al. [372] advocated seven major areas related to security that needs to be discussed in detail in SLA documents — privileged user access, data segregation, data location, recovery, regulatory compliance, investigative support, and long-term viability. Each service has its security issues, so SLA should be defined at the service level. Li and Du [373] describe security attribute based adaptive trust management scheme for SLA guarantee of cloud services.

Monitoring and Incident Response (M12.2): Monitoring helps to increase transparency and trust in the cloud environment [33]. Ward and Baker [140] described about the need of cloud monitoring and general purpose distributed systems monitoring tools like Gangila [374,375], Nagios [376], Astrolabe [377], collectd [378], Riemann [379], Zabbix [380] and others which can be used for cloud monitoring for specific areas. They also mentioned about cloud-specific monitoring tools cloudinit. [381]; Sensu [382] — event-based model for monitoring; SQRT-C [383] — real-time monitoring of cloud resources. Konig et al. [384] proposed an elastic monitoring framework consisting of three layers. Povedano et al. [385] proposed DARGOS — centralized resource monitoring. The study conducted by Ward and Baker [140] also includes tools like, GMonE [386] — attempts to provide a comprehensive monitoring for physical, infrastructure, platform layers; OpenNebulasin [387] — manages VM lifecycle; CloudSense [388] – a data center monitoring tool that works at switch level. Ward et al. [389] proposed the Varanus tool that provides fault-tolerant robust monitoring for large scale clouds. Amazon CloudWatch [390] and Google Stackdriver [391] are some of the industry used cloud monitoring tools. Monfared and Jaatun [154] proposed a cross-layer security monitoring solution to deal with cloud-specific challenges with the special focus on incident handling. They emphasized policies and procedures for handling incidents must be included in the security monitoring system so that incidents could be mitigated. Shin and Gu [392] proposed CloudWatcher as a monitoring solution for a large and dynamic cloud environment. Cai et al. [393] proposed design of cloud monitoring system for enhanced auto-scaling functionality in a video streaming system, based on Ericsson case study, using Data AGGregation TAXOnomy (DAGGTAX) [394].

Activity, event and traffic logs allow to establish accountability in the cloud and helps us to establish proactive and reactive measures to secure the cloud environment. Shetty [395] considers online mining of the cloud auditing logs generated by cloud network traffic as the key method to monitor the cloud security along with IP geolocation of network devices and monitoring of the cloud network path. Size of the cloud logs always poses challenges in log analysis. Lemoudden et al. [396] proposed a binary-based approach for frequency mining of correlated attack from log data which uses the MapReduce programming model. It is critical to ensure the confidentiality and integrity of the log file itself. Muthurajkumar et al. [397] proposed for temporal secured cloud log management algorithm which encrypts the data log before storing in the cloud storage and for easy retrieval they are stored in batches. Chen et al. [398] considers audit log as provenance data and compares different provenance security audit schemes based on audit logs. Suen et al. [399] raised the need for data-centric logging mechanism to establish full transparency and accountability of data movement in the cloud. They proposed S2Logger for capturing, analyzing and visualizing the data through its complete lifecycle within the cloud, both at a file level and block level. It helps to detect any data related security problems like malicious action on data, data leakage, and privacy violations. Sundereswaran et al. [160] in their cloud accountability framework keep track of usage of the user data stored in the cloud using automatic data access logging and auditing mechanism.

Verification and Validation (M12.3): Verification and validation are the static and dynamic testing approach in a system or application software development life-cycle process. Security testing of the application software is generally focused around user authentication, system database, and network testing. Well tested software in use increases trust in a cloud-based solution. There are two aspects of verification and validation, first is the use of verified and validated cloud infrastructure to gain the trust of the cloud user, and second is to use the cloud infrastructure to test any of the cloud system and application software and services [33].

For the first aspect, there are different solutions proposed wherein cloud infrastructure can be tested before putting in use. Zech [400] proposed a risk analysis based model for security testing of cloud infrastructure. Tsai et al. [401] proposed a mechanism to identify and establish a test group, called oracle, for service composition and then reuse this oracle for testing a new service or composition continuously. Moreno [402] in his master thesis presented a distributed framework for cloud storage testing based on simple put/get of stored data items with a statistical presentation of system behavior on test execution. Pham et al. [403] presented a framework for validating

the reliability of virtualization in cloud infrastructure by injecting faults. The framework was tested with KVM hypervisor as well Xen hypervisor which can be used as a benchmark for subsequent studies. Siddiqui et al. [404] described four software testing approaches for cloud application — clustering techniques, prioritization techniques, load distribution scenarios, and security mechanism. Bertoglio et al. [405] mentioned about different works carried over penetration testing to know the state of security for any IT system which can be applicable to the cloud environment as well. Ping et al. [406] proposed to use Stochastic Petri Nets (SPN) theory to analyze the security of the software which can as well be applicable for cloud-based software applications and services. The mechanism finds out vulnerabilities in the module which might lead to software failure. Once identified developers can do the needful to rectify those vulnerabilities. Jayasinghe et al. [407] proposed a code generation framework, Expertus, for automating performance testing of distributed applications in the IaaS cloud environment. It uses a template-driven code generation mechanism through a multi-pass compiler approach.

For the second aspect wherein, cloud infrastructure can be used to provide Testing-as-a-Service (TaaS) to verify and validate any cloud-based application services before putting in use. Candea et al. [408] proposed for automated testing as a cloud-based service. They described three kinds of TaaS: *programmer's sidekick* — for developers to test their code; *home-edition* — providing on-demand testing services for its consumer; *certification service* — enabling independent assessment for reliability, safety and security of software. Yu et al. [409] proposed a mechanism for how to use the cloud resources in an optimal way for the scheduled testing tasks.

Trust Establishment (M12.4): Cloud system faces trust issue mostly because cloud heterogeneous infrastructure is located off-site, mostly multi-location, and is managed by another party and establishing trust is a multi-dimensional and multi-phased phenomenon [30]. Establishing trust involves both infrastructure stability and human behavior responsible for managing the infrastructure [147]. Infrastructure includes virtualization techniques, storage hardware, computational algorithms, and web-based access mechanism [410]. Auditability (open to audit) and anonymization (privacy of user data) are other aspects of trust establishment. Audit of cloud environment enables to assess service conditions, monitoring capabilities for access, intrusions and other events, and the effectiveness of recording of detailed event logs [411]. Infrastructure trust established through Trusted Platform Modules (TPMs) [293] and associated hardware to ensure the integrity of software, processes, and data. See Section 4.6.7 on Trusted Computing for more on infrastructure based trusted computing. Banirostam et al. [412] proposed User Trusted Entity (UTE) which contains the Trusted Coordinator (TC) functionality keeping it separate from Cloud Manager (CM) and so preventing IaaS administrator from accessing user information. Rizvi et al. [413] proposed for a trusted third party (TTP) based encryption mechanism for data confidentiality. They proposed to use the combination of a symmetric and asymmetric cryptographic algorithm. Contractor et al. [414] proposed to use the chain of trust to establish accountability in the cloud.

Certification and Audits (M12.5): Certification process involves assessment, by accredited authorities, of security properties of cloud services and the underlying security mechanism to ensure the same. Certified services provide trust in the service and service provider. Spanoudakis et al. [148] proposed for Certification InfrastrUcture for MUlti-Layer cloUd Services (or shortly CUMULUS). It provides models, processes and tools to enable certification of compliance and security properties for all types of cloud service models — IaaS, PaaS, SaaS, by using the evidence from monitoring, testing and trusted computing. If needed, it allows for incremental certification as well. Further, based on CUMULUS, Cimato et al. [415] defines a unifying meta-model to provide a guideline for the definition of security properties for the cloud service to be certified, types of corresponding acceptable evidence and generation mechanism of the evidence agreed, and the phases of certificate's life-cycle. Katopodis et al. [416] suggested for a hybrid approach that combines monitoring and testing data to validate their security properties for certifying cloud services. Stephanow and Khajehmoogahi [417] suggested making use of web application testing techniques for a continuous security certification of SaaS applications. Anisetti et al. [418] have presented a semi-automatic and trustworthy scheme for continuous cloud service certification which is based on testing the security requirement of the cloud service defined by the certification authority and by a model of the service under certification. Anisetti et al. [419] further explain about the evidence collection model and service under verification interactions through a third-party regulator using CUMULUS framework. Foster et al. [420] presented an integrated approach to certification and compliance using analysis and monitoring technique that provides both design-time and run-time behavioral compliance checking for a cloud services architecture. Anisetti et al. [421] suggested a low-cost security certification management scheme for service changes which need a reissue of the certificate. The proposed scheme is based on testing evidence wherein aim happens to minimize test generation and execution activities for the service under certification. Anisetti et al. [422] suggested a test-based security certification scheme for web services. Supporting evidence is tested using a model-based testing approach that automatically generates the test cases starting from the service model. Anisetti et al. [423] provides a test-based incremental security certification scheme by reusing the pieces of evidence in the previous certification and adapt to the relevant changes which ultimately reduces the re-certification activities.

Data audit is required to ensure the integrity of user data stored at a remote location which is being managed by a third party. The conventional integrity check methods, like hash functions, message digest, are not sufficient for the cloud environment as there is no local data available and downloading the entire data is a challenge [424]. The design of remote data audit (RDA) technique must take care of the following aspects: *efficiency* – use of least computational complexity; *public verifiability* – permissible to delegate audit responsibility to a trustworthy Third Party Auditor (TPA); *frequency* – permissible to repeat the audit any number of time with different input sets; *detection probability* – probability of detection of potential corruption of stored data; *recovery* – probability of restoration of any corrupted data; dynamic update — permissibility of updates in stored data while audit continues [425,426]. To optimize the audit process, only a fraction of stored data is taken for remote auditing purpose [427]. In *replication-based remote data auditing*, same copy of the data is replicated over multiple distributed storage [348,351,354,428,429]. In *erasure-coding-based remote data auditing,* Maximum Distance Separable (MDS) technique is used to achieve reliability for the same level of replication [315,347]. In *network-coding-based remote data auditing* a new data block is created, at the time of repair, based on linear combination of the stored data blocks of the intact servers [264,430–432]. Saxena et al. [433] proposed data integrity verification approach for multiple third-party auditors which uses Combinatorial Batch Codes (CBC), Paillier Homomorphic Cryptography (PHC) and homomorphic tag for verification of data integrity. Kwon et al. [434] proposed a new index table management scheme that uses less complex operations and reduces the auditing cost. [435] proposed certificateless public

auditing scheme for shared data in constant verification time. Tian et al. [436] proposed a two-dimensional hash-table structure for Dynamic Hash Table (DHT) located in TPA which significantly reduces the computational cost and communication overhead.

Legal and regulatory compliance (M12.6): Zhou et al. [437] have highlighted different legal acts that a cloud provider must comply with providing services to users of the land of enforcement. Cloud provider must comply to the legal and regulatory obligation of the data transfer and storage across boundaries of nations as data centers of the cloud provider are geographically distributed across the globe to address the business continuity for the users and cost-effectiveness [437].

Most of the cloud computing architecture solution lack support for forensic investigations [30]. Zawoad et al. [438] presented a scheme Security Logging-as-a-Service (SecLaaS) which stores VMs logs and facilitates access to forensic investigators while preserving the confidentiality and privacy of the cloud users. SecLaaS as well preserves proofs of past logs to ensure the integrity of logs under investigation for any accidental or intentional damage of the logs. Martini and Choo [439] suggested a six steps process for the remote programmatic collection of data evidence. They also described artifacts that are available in VMware vCloud cloud computing environment. Roussev and McCulley [440] proposed for collection and analysis of cloud-native digital artifacts for forensic investigation in place of a snapshot in time artifacts of client-based data. The web-based client does not hold any significant data as the persistent data lies at the cloud server side and so termed as cloud-native data which can be described as internal data structures used by SaaS application. So, to support forensic investigation tools to extract such cloud-native digital artifacts shall be provided. Khan et al. [441] discussed about different mechanisms in cloud log forensics. They pointed out that the lack of standardization in cloud logging makes forensic investigation difficult as the correlation of different cloud logs becomes challenging in lack of standardization. They provided a set of recommendation for cloud log-as-a-service. Dykstra and Sherman [442] in their work divided the IaaS service model into six cloud layers and highlighted the data acquisition method along with the cumulative trust required at each layer. They also tested different prominent forensic tools available and found them working for the cloud environment as well. Choo et al. [443] mentioned about cloud *forensic-as-a-service* and cloud *forensic-by-design* as the evolving solution for supporting forensic investigation. Conceptually, *forensic-as-a-service* provides cloud-based methodologies to acquire forensic pieces of evidence like webpages, chats, documents, photos, and videos. Rahman et al. [444] describes *forensic-by-design* where forensic requirements are integrated into multiple phases during the system life cycle development. Nanda et al. [445] suggest a three-tier architecture for implementation of *forensic-as-a- service* that addresses the challenges highlighted in cloud forensics and works as a bridge between investigating agencies and cloud provider.

Park et al. [446] proposed THEMIS system that uses the concept of the cloud notary authority for the supervision of billing by generating mutually verifiable binding information. This binding information, then, used to resolve future disputes, in a computationally effective and efficient way, between the user and the cloud service provider. Armknecht et al. [357] provides a storage solution ClearBox, to verify the effective storage space used in the cloud, and so avail the pricing and other benefits accordingly.

Data privacy (M12.7): Mather et al. [447] explains privacy as obligations related to the collection, use, storage, disclosure and destruction of Personally Identifiable Information (PII) or personal data. Further, it explains, type, nature, and constitution of personal data depends on public expectations and legal interpretations of that culture, country and jurisdictions that go through generation, use, transfer, transformation, storage, archival, and destruction phases of data life-cycle. The responsibility of data privacy and security lie with the organization which has generated or collected the user data in the first place [447]. Encryption, storage, retrieval and logging techniques used during the data life cycle is the key in preserving the data privacy. Malina et al. [448] provide a non-bilinear group signature for anonymous authentication of cloud service registered users. Registered user's attributes can be validated without disclosing the person's identity, and they can use the cloud service without fear of profiling of their behavior. Salam et al. [449] provides a mechanism for privacy-preserving search algorithm over encrypted stored user data without downloading and decrypting it. Tu et al. [450] provides a method for privacy-preserving public auditing of storage data wherein it uses Blockless verification, Homomorphic tags, and Merkle Hash Tree (MHT) techniques to maintain the integrity of shared data with TPAs. Ranchal et al. [451] explains in SOA, in a chain of service invocation there is a fair chance of sharing of data with unauthorized services violating the client's privacy, as the client has no control beyond its trust domain. They proposed privacy-preserving access control in SOA wherein a client dynamically defines the access policies and controls the data access for each of service interaction. Horandner et al. [452] through the CREDENTIAL consortium proposed a novel cryptographic mechanism to store and share identity data of the cloud user. The two basic technologies used within CREDENTIAL are Proxy Re-Encryption (PRE) and Redactable Signatures (RS). Razaque et al. [453] proposed a mathematical model for privacy-preserving auditing of cloud stakeholders, cloud user, cloud service provider, and malicious third-party auditor. Hong et al. [454] highlighted reduced computation and communication cost by using Elliptic Curve Cryptography (ECC) based homomorphic encryption scheme for solving Secured Multiparty Computation (SMC) to protect the user's data privacy. Privacy-preserving encryption techniques ensure user data is exposed only for the purpose it is meant and used by authorized entities [206,455]. Benali et al. [456] proposed for a privacy-preserving intrusion detection system which is based on collaborative intrusion detection and use of secured privacy-preserved multiparty computation to evaluate the global state of the network. Li et al. [298] proposed for MyCloud trust based privacy-preserving computation where the end users themselves do privacy settings and taking control out of the cloud administrator for privacy settings. Khalid et al. [457] introduced an authentication and authorization protocol which integrates with an IDentity Management System (IDMS) to provide privacy-preservation of users. They replaced the real identities of users with anonymous identities with keys generated and managed within IDMS. Jung et al. [458] suggested for AnonyControl, that exploits multiple authorities for privacy-preserving attribute-based access control in a cloud storage server. Chow et al. [227] proposed for a revocable group signature along with identity-based encryption to provide confidentiality, anonymity, and tractability of the user data.

5. Cloud security requirements, threats, vulnerabilities and countermeasures inter-related analysis and mappings

The unprecedented growth of cloud-based applications and services delivery model is bound to grow further with the emerging cloud-based applications in Big Data, IoT, 5G, SDN and NFV, provided suggested countermeasures are implemented effectively to address the vulnerabilities in cloud computing architectural components to limit the attack vectors for identified threats and fulfilling the desired level of security and privacy requirements. Based on the discussion in previous sections on cloud

service models, deployment models, characteristics, architectural components, security taxonomy, security requirements, identified threats, known vulnerabilities, and suggested countermeasures, this section analyzes them together and provides their interrelated mappings along with analysis on trust-based countermeasures. Additionally, effects of cloud security aspects for Big Data, IoT, 5G, SDN and NFV applications have been summarized.

5.1. Threat ranking trend analysis

Fig. 5 presents relative ordering or ranking of different threats prominent in the years 2010, 2013 and 2016 as per the CSA' reports [47,49,50]. As it is evident, in 2013 three new threats, *Data Breaches*, *Denial of Service* and *Insufficient Due Diligence* were identified while *Unknown Risk Profile* is removed w.r.t 2010 identified threats. In 2016, which is the latest released report, three new threats *Weak Identity, Credential and Access Management, System and Application Vulnerabilities* and *Advanced Persistent Threats* (APTs) have been added. The identification of these new threats witnesses the evolving spectrum of threats to the cloud.

Abuse and Nefarious Use of Cloud Computing, which was at the top of the list of identified threats in 2010 have been placed at the tenth position in 2016 which reflects the swing in the mood of the cloud community. It witnesses that the cloud computing model has got wider acceptance over the last couple of years. *Shared Technology Vulnerabilities* is shown at the bottom of the list in 2016 which reflects shared technologies which are being used in providing cloud solution has also been evolved to find solutions for the associated vulnerabilities in them.

The threat *Data Breaches* appear at the top consecutively both in 2013 and 2016, which puts a question mark on credibility and trust in a cloud-based solution. The threat *Advanced Persistent Threats* (APTs) appearing first time in 2016 report reveals how social engineering techniques, like spearphishing, is now being used to smuggle the data and intellectual property rights.

The threat *System and Application Vulnerabilities* which appears first time in 2016 report reflects the weakness in software development processes and methodologies being followed by the system designer and developers during system and application design, development, testing, integration, deployment and life cycle management. The technologies being used for building system and application have inherent vulnerabilities. So, while making a choice for technology and software engineering methodology for building a trustworthy system and application for a cloud-based solution, it is recommended to use the CSA Security Guidance [20].

5.2. Mapping affected requirements to identified threats

STRIDE [459–461], developed by Microsoft, is a threat classification model that uses six categories to classify the threats associated with a computing system. Further, the STRIDE threat modeling technique helps to perform threat analysis based on attack properties, and each of these attack properties affects the security requirement [462–464]. Table 9 explains the mapping of STRIDE threat categories and affected security requirement.

The CSA Cloud Security Working Group surveyed to analyze the security concerns using the STRIDE threat model and published in the report *The Treacherous 12 - Cloud Computing Top Threats in 2016* [47]. CSA carried out this analysis based on the survey data collected from the respondents from the technology industry, professional services, and public sectors. The respondents were primarily specialist from security, software development, and networking. CSA further published a report on industry reported incidents which confirm the relevance of these threats [465].

Using the CSA's [47] STRIDE threat analysis and STRIDE mapping to security requirements (Table 9), a mapping of the effect of CSA's *Treacherous Twelve Threats* on cloud security requirement is depicted in Table 10.

The mapping shown in Table 10 is applicable for all the three cloud service models: SaaS, PaaS, IaaS. In a recent CSA's report published on industry reported incidents confirms the existence of these threats and affected security requirements [465]

5.3. Mapping known vulnerabilities to identified threats and affected requirements

Table 11 summarizes the analysis provided in Sections 4.1, 4.3, 4.4 and 4.5 by providing a mapping for known vulnerabilities in cloud architecture layered components to identified threats and affected security requirements.

5.4. Mapping suggested countermeasures to known vulnerabilities and fulfilled requirements

Table 12 summarizes the analysis provided in Sections 4.1, 4.3, 4.5 and 4.6 by providing a mapping for suggested countermeasures to address the vulnerabilities in cloud architectural components to meet the desired level of security and privacy.

5.5. Trust based countermeasures

Vendor lock-in and lack of user control are major factors to have low trust in cloud computing system [26]. In the cloud, trust is very much dependent on the chosen deployment model. Trust is very low for public or community clouds whereas it is high for private clouds for the very reason of level of control that the user perceives. In the case of public or community clouds the control is delegated to the infrastructure owner whereas in the case of private cloud infrastructure is managed within the users' premise [25]. Hard Trust involves verifiable security measures through hardware enabled Trusted Platform Module (TPM), Trusted Third Party (TTP) certificates taking care of authenticity, encryption, secure communication and like that whereas Soft Trust involves brand loyalty, human psychology, and user-friendliness which typically, is evaluated dynamically that can be, for example, reputation-based, content-based, context-based or evidence-based [25,26,469,470].

The literature review on vulnerabilities in cloud architectural components and suggested countermeasures provides useful insight into the role of trust-based solutions to meet the security requirements. Trust-based approach for strengthening the security and privacy in cloud computing is found mostly centered around TPM and TTP. Table 13 summarizes the trust based countermeasures to address known vulnerabilities for fulfilling the cloud security and privacy requirements.

Establishing trust is a multi-faceted and multi-phased phenomenon, and it involves both infrastructure stability and human behavior responsible for accessing, using and managing the infrastructure [30,147]. There are different models proposed for trust evaluation [223,471–478]. Habib et al. [479] provide a survey of trust and reputation (TR) models and systems where it highlights different mechanism used for trust computations. In the changing landscape of security threats for cloud system, adaptive security is key in building the trust of cloud consumers. Since trust can be dynamically evaluated based on the previous history of user interactions and current recommendations, so trust based adaptive security model can be evolved for ensuring security and privacy in a cloud computing system. Huang et al. [480] explain how the trust mechanism can be built for cloud systems. They have proposed five categories in which trust

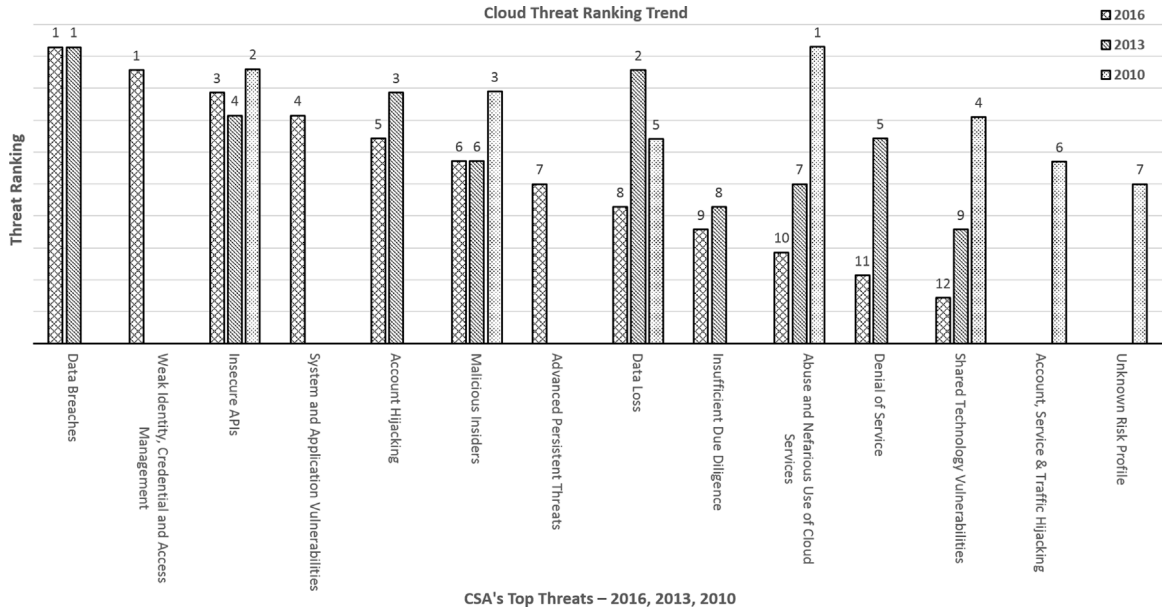

Fig. 5. Cloud threat ranking trend analysis [47,49,50].

Table 9
STRIDE threat classes and affected security requirement [462–464].

Threat category	Threat context	Affected security requirement
Spoofing identity	Using another user's authentication data	Authentication (R04)
Tampering with data	Malicious modification of data	Integrity (R02)
Repudiation	Denial for the performed action by the user	Accountability (R06)
Information disclosure	Intentional or un-intentional exposure of information in the public domain which is not supposed to be exposed	Confidentiality (RO1) and Privacy (R07)
Denial of service	Denial or unavailability of services to legitimate users	Availability (R03)
Elevation of privilege	Privileged access gained by an unprivileged user	Authorization (R05)

Table 10
Effect of the Treacherous 12 threats to cloud computing on cloud security requirements [47,460,462].

Top threats	Treacherous 12 — Top threats to cloud computing	R01	R02	R03	R04	R05	R06	R07
1	Data breaches (T01)	×						×
2	Weak identity, Credential and Access Management (T02)	×	×	×	×	×	×	×
3	Insecure APIs (T03)	×	×			×	×	×
4	System and Application Vulnerabilities (T04)	×	×	×	×	×	×	×
5	Account Hijacking (T05)	×	×	×	×	×	×	×
6	Malicious Insiders (T06)	×	×		×			×
7	Advanced Persistent Threats (APTs) (T07)	×				×		×
8	Data loss (T08)			×			×	
9	Insufficient Due Diligence (T09)	×	×	×	×	×	×	×
10	Abuse and Nefarious Use of Cloud Services (T10)			×				
11	Denial of Service (T11)			×				
12	Shared Technology Vulnerabilities (T12)	×				×		×

Requirement legends — R01: Confidentiality; R02: Integrity; R03: Availability;
R04: Authentication; R05: Authorization R06: Accountability; R07: Privacy

mechanisms can be practiced — reputation based, SLA verification based, transparency mechanism, trust as a service, and formal accreditation, audit, and standards. Trust-based adaptive security for cloud computing is of interest as a further research area.

5.6. Prioritizing countermeasures based on expected impact analysis

The countermeasures listed above are intended to address the respective vulnerabilities and fulfill the related security and privacy requirements. These countermeasures can be broadly classified as proactive measures and reactive measures. All the countermeasures discussed comes under proactive measures except the two, Intrusion Detection and Prevention System (M04) and Monitoring and Incident Response (M12.2), which are reactive measures. It is recommended to implement all the mentioned countermeasures for creating confidence and trust in the cloud-based service delivery model. However, depending on business needs and constraints both service provider and the consumer can agree to prioritize countermeasure implementation based on the expected impact of these countermeasures. One approach for selection of the countermeasures could be to identify those measures catering the top threats or threats impacting the maximum number of security requirements (Table 10). In the second approach select the countermeasures that can address maximum security requirements (Table 12).

For the first approach, Table 10 suggests the threats *Weak identity, credential, and access management* (T02), *System and application vulnerabilities* (T04), *Account hijacking* (T05) and Insufficient due diligence (T09) are impacting all the seven security requirements. So, associated countermeasures (Table 12) can be

Table 11
Vulnerabilities mapping for associated threats and affected security requirements.

Cloud computing model layer and associated vulnerabilities	Associated security issues and challenges	Related survey and study	Associated threat(s)	Affected security requirement(s)
Application and interface layer (V01)				
Web services and interfaces vulnerabilities (V01.1)	SQL injection, command injection, cross-site scripting	[18], [9], [57]	T01, T02, T03, T05, T07	R01, R02, R04, R05, R06, R07
	Session riding, session hijacking, MitB attack, Service unavailability	[18], [8]		
	XML injection, metadata spoofing, WSDL content misuse, SOAP wrapping attack	[56], [58], [59], [60], [27]		
	Advanced persistent threats and malicious outsiders	[61], [62]		
Web client data manipulation vulnerabilities (V01.2)	Malicious web sites, watering hole attacks	[63], [18], [66]	T01, T02, T03, T05, T07	R01, R02, R04, R05, R06, R07
	HTML hidden field manipulation, Code injection, XSS attack, MitB attack	[9], [68], [69], [67], [57]		
User Identity and Access vulnerabilities (V01.3)	Weak password/credentials and their lifecycle management	[18], [30], [72], [9]	T01, T02, T05, T10, T11	R04, R05, R06, R07
	Phishing, key-logger attack, MitM attack, session hijacking	[86], [29], [8]		
	De-anonymization and hidden identity	[84], [85], [28]		
	Weakness in authentication and authorization protocols (OpenID Connect, OAuth2.0, Token management)	[77], [78], [79], [82], [80], [81], [83], [22], [9]		
	Inappropriate authorization scheme and policies, URL guessing attack	[73], [18], [57]		
Encryption and Keys vulnerabilities (V01.4)	Weak keys for cryptography, Weak management of cryptography keys	[87], [9], [70]	T01, T12	R01, R02, R07
	Weak and/or obsolete encryption algorithms	[18], [88], [29]		
Platform layer (V02)				
Software development framework and practices vulnerabilities (V02.1)	Non-compliance to software development life cycle process	[89], [55]	T03, T04	R01, R02, R03, R04, R05, R06, R07
Software code vulnerabilities (V02.2)	Non-compliance to best coding practices and guidelines	[90], [27], [55], [25]	T03, T04	R01, R02, R03, R04, R05, R06, R07
	Unsafe thread termination, memory zone isolation violation	[92]		
	Untrusted third party and open source code, masked code injection	[30], [8]		
Operating system traditional vulnerabilities (V02.3)	Malicious insider system admin, advance persistent threats	[93], [94], [25], [61], [62]	T03, T04, T06, T07	R01, R02, R03, R04, R05, R06, R07
	Insecure system calls, inappropriate resource allocation and memory isolation	[21], [92]		
	Incomplete and insufficient OS monitoring, malicious backend process	[95], [9]		
Infrastructure layer — Virtualization and hypervisor (V03)				
Virtual machine traditional vulnerabilities (V03.1)	Traditional datacenter perimeter-security measures	[9], [99], [98]	T01, T07, T10, T11, T12	R01, R03, R05, R07
	Lack of physical segregation of among the VMs	[99], [98]		
	Remote access for administrative activities	[9], [99], [98]		
	Dynamic reconfiguration, VM at rest, co-located VM, patch management	[9], [99], [98]		
	VM hopping, Cross-VM attack, side-channel attack, covert-channel attack etc.	[103], [28], [101], [102], [100]		
VM Image vulnerabilities (V03.2)	Release of sensitive information to next allocated user	[104], [37]	T01, T12	R01, R07
	Getting contaminated with malware while at rest	[104], [23]		
	Latent security risks of inactive and dormant images (no security patch)	[104], [320]		
	VM sprawl and transience	[105], [106]		
VM Migration and Rollback vulnerabilities (V03.3)	Live VM Migration attack (MitM, Replay, Insider) and information disclosure	[109], [111], [69], [110]	T01, T02, T06, T12	R01, R03, R04, R05, R07
	Rollback restores to previous outdated patch and credentials	[10], [112], [97]		
	Rollback reverts to previous configuration errors and security policy	[27]		
	Dormant rollback image might propagate security vulnerabilities	[113]		

(*continued on next page*)

Table 11 (*continued*).

Cloud computing model layer and associated vulnerabilities	Associated security issues and challenges	Related survey and study	Associated threat(s)	Affected security requirement(s)
Multi-tenancy environment vulnerabilities (V03.4)	Attacks on data under processing — data leakage, integrity violation	[27], [114], [10], [25]	T01, T02, T05, T07, T10, T12	R01, R02, R03, R04, R05, R06, R07
	Advance persistent threat (targeted attack)	[61]		
	Data sanitization challenges	[30]		
Hypervisor vulnerabilities (V03.5)	Larger attack surface — VM escape, compromised VMM	[70], [115], [116], [117], [107], [18]	T01, T04, T07, T10, T11, T12	R01, R02, R03, R04, R05, R06, R07
	VMM software code vulnerability — unreliable and untrusted components	[118], [119], [8], [35]		
	Incompleteness of isolation, inspection and interposition properties in VMMs	[8]		
	Single point failure, maliciousness and untrusted components of VMM	[97]		
Infrastructure layer — Network (V04)				
Network communication protocol and technology vulnerabilities (V04.1)	DNS spoofing, DNS cache poisoning, malicious change in DNS settings	[66], [120]	T01, T05, T07, T10, T11, T12	R01, R03, R04, R05, R06, R07
	HTTP statelessness, inappropriate session handling, session hijacking/riding	[18], [8]		
	Mixing HTTP and HTTPS, MitM attack, weak keys in SSH and TLS	[121], [122], [123], [87]		
	Flooding attack, cookie theft/poisoning, network sniffing and spoofing	[60], [66], [10]		
Shared network vulnerabilities (V04.2)	Cross-tenant attack, traffic bottlenecks, network devices inherent vulnerabilities	[10], [18], [9], [27], [31]	T01, T07, T10, T11, T12	R01, R03, R07
Virtual network vulnerabilities (V04.3)	Loss of visibility of communication channels	[9], [70], [126], [125]	T01, T04, T11, T12	R01, R03, R06, R07
	Data exfiltration to/from the host operating system	[127]		
	Sniffing/Spoofing virtual networks	[27], [112], [97]		
	Virtual devices software vulnerabilities	[21]		
Infrastructure layer — Storage (V05)				
Data storage cryptography vulnerabilities (V05.1)	Poor key management	[70]	T01, T12	R01, R07
	Faulty, insecure and obsolete encryption technique	[88], [18], [29]		
Data access vulnerabilities (V05.2)	Unauthorized access to insiders and outsiders	[130], [29]	T01, T02	R01, R07
Data storage location, backup and recovery vulnerabilities (V05.3)	Data integrity and availability	[8], [131], [29]	T01, T02, T08	R01, R02, R03, R07
	Information disclosure and data loss	[129], [132]		
	Loss of control, data locality and multi-location	[28], [437]		
Data sanitization vulnerabilities (V05.4)	Information disclosure	[70], [129]	T01, T12	R01, R07
	Disk multi-tenant use, improper disk recycling	[18], [26], [132]		
Infrastructure layer — Hardware (V06)				
Hardware vulnerabilities (V06.1)	Hardware limited resources and availability	[134]	T01, T08	R01, R03, R07
	Hardware fault and availability	[133], [25]		
	Hardware level encryption	[466]		
Infrastructure layer — Facilities (V07)				
Physical access vulnerabilities (V07.1)	Infrastructure and DMZ limitation	[30]	T01, T02, T06, T08	R01, R03, R05, R07
	Malicious insiders, infrastructure misuses and theft	[136], [66]		
	Hardware tampering and cold boot attacks	[137]		
Natural disasters (V07.2)	Business continuity, loss of data	[25], [9]	T08	R03
Assurance and compliance vertical (V08)				
Assurance vulnerabilities (V08.1)	SLA violations	[28], [138]	T01, T02, T06, T10, T11	R01, R02, R03, R04, R05, R06, R07
	Insufficient monitoring, logging and incident response	[139], [140], [18]		
	Uncontrolled and unauthorized resource usage	[144], [145]		
	Inappropriate resource configuration and provisioning	[103], [134]		
	Undesired service interruption and system performance	[143], [141], [142]		
	Distrust, social engineering and phishing	[146], [147]		

(*continued on next page*)

Table 11 (*continued*).

Cloud computing model layer and associated vulnerabilities	Associated security issues and challenges	Related survey and study	Associated threat(s)	Affected security requirement(s)
Compliance vulnerabilities (V08.2)	Non-compliance to standards, certifications, audits and log record	[447], [437], [151], [148], [160]	T01, T02, T06, T10, T11	R01, R02, R03, R04, R05, R06, R07
	Non-Compliance to cross boundaries government policies and laws	[153], [154], [152]		
	Conflicting legal jurisdictions	[437], [158], [149], [150]		
	Forensic data seizing, confiscation, collection, verification	[158], [35], [88], [156], [157], [159]		
	Data privacy compliance and breaches	[25], [8], [26], [411], [447]		
	Incorrect resource usages and metering – FRC, EDoS etc.	[145], [28], [161]		
R01: Confidentiality R02: Integrity R03: Availability R04: Authentication R05: Authorization R06: Accountability R07: Privacy	T01: Data breaches; T02: Weak identity, Credential and Access Management; T03: Insecure APIs; T04: System and Application Vulnerabilities; T05: Account Hijacking; T06: Malicious Insiders; T07: Advanced Persistent Threats (APTs); T08: Data loss; T09: Insufficient Due Diligence; T10: Abuse and Nefarious Use of Cloud Services; T11: Denial of Service; T12: Shared Technology			

prioritized for implementation. Similarly, other countermeasures can be selected for implementation based on the priority of addressing a specific threat.

For the second approach, Table 12 depicts, proactive measures for virtual environment security (M07) and software development environment security (M06) can be prioritized first as all the seven security, and privacy requirements are expected to be fulfilled through these measures. Next, in proactive measures to prioritize can be Digital Signature and Message Digest (M03) and Encryption and key Management (M02) with Identity and Access Management (M01). Further, Web Applications, Services, and Interfaces measures (M05) and Data storage measures (M09) can be prioritized next. Rest other proactive countermeasures can be implemented in any order with particular focus on Assurance and Compliance measures (M12). The reactive countermeasures Monitoring and Incident Response (M12.2) and Intrusion Detection and Prevention System (M04) should be prioritized to implement in parallel to proactive measures.

5.7. Cloud computing security for big data, IoT, 5G, SDN, NFV applications

Cloud computing, IoT, SDN, NFV, Big Data, and upcoming 5G technologies are enabling the proliferation of applications for connected devices forming the networked society. With the evolution of ubiquitous computing and these enabling technologies, the world is embracing everything getting connected everywhere, and that inherently brings security and privacy challenges.

5.7.1. Big data and cloud computing security

Information systems are producing large data from heterogeneous sources which demand efficient architecture and technologies for handling and managing the new data sets [481]. Apache Hadoop, Hadoop Distributed File System (HDFS), Google File System (GFS) and Map/Reduce (MR) are some of the suggested Big Data solutions to handle this huge amount of information [482–485]. These solutions can capitalize the benefits of cloud, such as availability of virtualized resources on demand, availability of automated tools for data collection and analysis, in a cost-effective way. While it is cost effective and practical to use cloud computing for Big Data, however, there are concerns raised over security and privacy of hosting Big Data on cloud due to loss of control, multi-tenancy, trust, and accountability. Gholami et al. [486] in their paper have reviewed security and privacy challenges on Big Data in the cloud, especially providing compliance to privacy legislation such as EU DPD (Data Protection Directive) and USA HIPAA (Health Insurance Portability and Accountability Act). They have mentioned about state-of-art technologies for Big Data infrastructures and programming models along with privacy-preserving Big Data solutions in the cloud. Salleh et al. [487] highlighted issues and challenges for Big Data applications are not only because of technological deficiencies but also from organizational culture and environmental influences. Nuaimi et al. [488] have highlighted the weakness of technologies used in Big Data for assuring appropriate security and privacy in its application for Smart City. Li et al. [489] have proposed a unique architecture for enabling security of Big Data applications based on EnCoRe [490] that implements sticky policies. Gai et al. [491] proposed to split the user data file and store in distributed cloud servers to prevent cloud providers from accessing the user data. This scheme uses Security-Aware Efficient Distributed Storage (SAEDS) model, with Secure Efficient Data Distributions (SED2) and Efficient Data Conflation (EDCon) algorithms. Big Data based security analytics as well can help for protecting virtualized infrastructures in cloud computing [492]. Abouelmehdi et al. [493] reviewed state-of-art security and privacy challenges and available solutions, focused on anonymization and encryption, related to Big Data usage in healthcare data management system. Manogaran et al. [494] have proposed MetaCloudDataStorage Architecture using Map/Reduce framework for securing Big Data in the cloud.

5.7.2. IoT and cloud computing security

Shahmim et al. [495] pointed out security and privacy concerns for Internet-based computing like cloud computing, Internet of Things and Cloud of Things. There exist IoT cloud platforms to meet the requirements of different user and application groups, like healthcare, communication, transportation, manufacturing, enterprises, government, and others. In the survey paper of Partha Pratima Ray [496] cloud-based IoT platforms have been discussed which are providing the services in multiple domains, like data management, system management, device management, application development, different utility tools, etc. With the rise of 5G, SDN and Mobile Edge Computing (MEC) the proliferation of several connected devices is expected to be 20+ billion devices by 2020 [497], a correction from the previous prediction of 50 billion connected devices by 2020 [498]. Heterogeneity of connected *Things* with limited power consumption and computing processing capability puts a constraint on implementing security and privacy mechanism for IoT. To address this, Salman et al. [499] proposed a security framework, based on SDN and Cloud/Edge computing, for authentication and authorization security functions embedded in a global IoT network

Table 12
Countermeasures mapping to vulnerabilities and requirements.

Countermeasure	Security solution approach	Related survey and study	Addressed vulnerabilities(s)	Addressed requirements(s)
Identity and Access Management (M01)	Strong and strict password lifecycle management	[165], [184], [185],	V01.3, V05.2	R04, R05
	Federated identity and multifactor authentication	[20], [165], [181], [182], [183]		
	Strong access control and authorization — attribute, trust and role based	[20], [186], [187], [188], [191], [192]		
	Use of standard protocols for authentication and authorization — SAML, OAuth, OIDC, JSON, REST, JWE, JWS, XACML, SCIM	[166], [167], [168], [169], [170], [171], [172], [173], [78], [174], [176], [177], [178], [179], [269], [271], [180]		
	Unified framework for identification, authentication and authorization	[20], [185], [190]		
Encryption and Key Management (M02)	Strong encryption schemes — AES, proxy re-encryption, SECRESO, hourglass protocol, trusted third party, attribute-based, HIBE, CP-ABE, KIPRE, BABE	[194], [195], [196], [197], [25], [214], [215], [216], [218], [219]	V01.4, V05.1	R01, R02, R07
	Strong key management — storage, access control, backup and recoverability	[9], [211], [212], [213], [217]		
	Encrypted data processing (homomorphic encryption) and search schemes with privacy protection	[198], [199], [200], [201], [202], [203], [204], [205], [207], [208], [209], [210], [26], [206]		
Digital Signature and Message Digest (M03)	Hash functions and private key encryption	[33], [9], [35], [137], [226], [229], [231], [230] [232], [233]	V01.3, V01.4, V05.1, V05.2	R01, R02, R03, R04, R06, R07
	Digital signature with SSO and LDAP, Group signature, ID-based proxy signatures	[25], [227], [228]		
Intrusion Detection and Prevention System (M04)	Network based intrusion detection and prevention system	[238], [239], [240], [241], [242], [243], [244], [245]	V01.1, V01.2, V01.3, V04.1, V04.2, V04.3, V05.2, V08.1	R01, R02, R03
	Host based intrusion detection and prevention system	[333], [246], [247], [248]		
	Distributed intrusion detection and prevention system	[256], [249], [250], [254]		
	Hypervisor based intrusion detection and prevention system	[251], [252], [33]		
	Structured prevention, detection and mitigation methods	[257]		
	Middleware approach, SDN based approach, additional resource allocation	[256], [260], [259], [258]		
	Machine learning algorithm based IDPS	[261], [262], [263], [264], [265]		
Web Applications, Services and Interfaces security measures (M05)	Use of web services security standards and recommendations — SAML, XACML, XKMS, WS-Security, WS-Federation, WS-Secure Conversation, XML Digital Signature, XML Encryption, WS-Security Policy and WS-Trust	[268], [27], [166], [269], [270], [266], [267], [271], [272], [273], [274], [275] and [276]	V01.1, V01.2,	R01, R02, R04, R05, R07
	Web application scanner, firewall and one-time cookies	[278], [279], [280], [281], [282]		
	Application Programming Interface (API) management	[10], [467]		
	Security aware web application development, periodic penetration testing	[89], [20]		
	Proactive vulnerabilities identification and applying countermeasure	[283], [284], [285], [286]		
Software development environment security measures (M06)	Software Development Life Cycle (SDLC), SDL, SecDLC, user experience	[89], [289], [55], [288], [290]	V02.1, V02.2, V02.3	R01, R02, R03, R04, R05, R06, R07
	OS level isolation to support multi-tenancy	[92]		
	OS level hardening and monitoring, monitoring malicious admin	Spring (2011), [93], [94], [54]		
	Best programming practices, training, awareness and collaboration	McGraw (2006), [9], [89], [292], [291]		

(*continued on next page*)

Table 12 (*continued*).

Countermeasure	Security solution approach	Related survey and study	Addressed vulnerabilities(s)	Addressed requirements(s)
Virtual environment security measures (M07)				
Trusted computing (M07.1)	Hardware supported trusted platforms — TPM, vTPM, TCCP, Excalibur, MyCloud	[293], [294], [137], [295], [296], [297], [298]	V01.3, V01.4, V03.1, V03.4, V03.5, V06.1	R01, R02, R03, R04, R07
	Secured hardware architecture and infrastructure	[299], [300]		
Virtual Machine and Hypervisor security (M07.2)	VM introspection	[311], [312], [251]	V03.1, V03.5	R01, R02, R03, R07
	Hardware-assisted VMM secure execution framework — HyperCheck, HA-VMSI	[313], [317]		
	VM isolation schemes — HyperLock, CloudVisor	[315], [316]		
	VMM reduced/eliminated attack surface — DeHype, NoHype, SplitVisor	[277], [116], [314]		
	Standards and recommendations	[318]		
Virtual Image security (M07.3)	Regulated access control and image filtering for VM sharing	[104]	V03.2	R01, R02, R03, R06, R07
	Provenance tracking mechanism	[104]		
	Repository maintenance services — patching, virus scanning etc.	[104], [320], [321], [113]		
	Using encryption at rest	[319]		
VM Migration and Rollback security (M07.4)	Secured pre-copy and live migration techniques	[331], [332], [333], [107]	V03.3	R01, R02, R03, R04, R05, R06, R07
	Trusted computing migration techniques	[324], [327], [328], [330], [329]		
	Secured framework for migration	[326], [325]		
	Rollback protection framework	[335], [334]		
Virtual network communication security (M07.5)	Secured virtual network architecture	[112], [337]	V04.1, V04.3	R01, R02, R03
	Trusted Virtual domains and sandboxes	[338], [339]		
	Secured routing and firewall protection in virtual network	[340], [337], [341], [105]		
	SDN based approach — DCPortalsNG	[342]		
Network communication security measures (M08)	Use combination of Firewalls, IDS, IPS and virtual LANs	[20], [344], measures mentioned in 4.6.7, 4.6.4 and 4.6.5.	V04.1, V04.2	R01, R02, R03
	Network performance assessment and measures	[8]		
Data storage security measures (M09)				
Data classification and access control (M09.1)	Confidentiality level based data classification and encryption	[345]	V05.2	R01, R05
	Parameterized (access control, content, storage) data classification	[346]		
Data integrity and availability (M09.2)	Provable Data Possession (PDP)	[348], [351]	V05.1	R02, R03
	Dynamic Provable Data Possession (DPDP)	[352], [353], [354] [355]		
	Proof of Retrievability (POR)	[349], [347], [350]		
Location, backup and recovery transparency (M09.3)	Transparent de-duplication	[357]	V05.3	R03
	Encrypted multi-location transparent data backup	[356], [358]		
Data sanitization (M09.4)	Systematic stepwise Physical deletion of data	[360], [359], [361]	V05.4	R01, R07
Hardware security measures (M10)	Fault tolerant high availability and scalable hardware	[133], [362]	V06.1	R01, R02, R03
	Load balancing	[133]		
	Hardware-Enhanced security and hardware cryptography	[300], [363], [364]		
Physical security measures (M11)				
Physical access control (M11.1)	Strong physical identification, authorization and access control (like biometric access control)	[365], [367], [366]	V07.1	R04 R05
Business continuity and disaster recovery planning (M11.2)	Multiple cloud provider (intercloud solution to avoid lock-in)	[370], [369]	V07.2	R03
	Multi-site cloud provider (software, application and data)	[9]		
	Resource allocation re-prioritization	[368]		

(*continued on next page*)

Table 12 (*continued*).

Countermeasure	Security solution approach	Related survey and study	Addressed vulnerabilities(s)	Addressed requirements(s)
Assurance and Compliance measures (M12)				
Service Level Agreement (M12.1)	Consideration of security requirements in SLA document	[372], [373], [10]	V08.1	R03
Monitoring and Incident Response (M12.2)	Tools — Varanus, DARGOS, GMonE, cloudinit.d, CloudSense, SQRT-C — for Monitoring cloud resources and report incidents	[389], [385], [386] [381], [384], [383]	V08.1	R01, R02, R03, R04, R05, R06, R07
	Monitoring intrusions and report security incidents	[154], [392], [393]		
	Logging to monitor and audit security events	[160], [399], [398]		
Verification and Validation (M12.3)	Cloud infrastructure and software testing mechanism	[400], [401], [402], [403]	V01.1, V01.2, V02.1, V02.2, V02.3, V03.5, V04.1, V04.2, V04.3 V08.1	R01, R02, R03, R04, R05, R06, R07
	Penetration testing	[405], [113]		
	Software and performance testing	[407], [406], [404]		
	Testing-as-a-Service	[408], [409]		
Trust framework (M12.4)	Trusted cloud computing platform: TPM, vTPM, TCCP, TCCI	[293], [294] [412]	V01.3, V01.4, V05.1, V05.2, V08.1, V08.2,	R01, R02, R03, R04, R05, R06, R07
	Trust based confidentiality, integrity, availability	[413], [297], [296]		
	Trust based privacy	[298]		
	Trust based authentication, authorization, accountability	[295], [414]		
Certification and Audits (M12.5)	Cloud services certification	[148], [415], [416], [417], [418], [419], [420], [421], [422], [423]	V08.2	R01, R02, R06, R07
	Cloud remote data auditing (RDA)	[425], [426], [424], [427], [433], [435], [436]		
	Replication-based RDA	[351], [348], [428], [354], [429], [434]		
	Erasure-coding-based RDA	[347], [468]		
	Network-coding-based RDA	[430], [431], [264], [432]		
	Activity, event and traffic records logging	[395], [396], [397], [398], [399], [160]		
Legal and regulatory compliances (M12.6)	Compliance to legal and regulatory policies, laws and authorities	[437], [447]	V08.2	R06
	Forensic investigation mechanism	[438], [439], [440], [441],[442], [443], [444], [445]		
	Metering and billing of resource usage	[446], [357]		
Data privacy (M12.7)	Privacy-preserving policies, laws and regulations	[447], [30]	V08.2	R01, R02, R04, R05, R07
	Privacy-preserving encryption techniques	[449], [452], [454], [206], [455], [227]		
	Privacy-preserving authentication and authorization techniques	[448], [451], [458], [457]		
	Privacy-preserving IDS, audits and trust mechanisms	[456], [450], [453], [298]		

R01: Confidentiality
R02: Integrity
R03: Availability
R04: Authentication
R05: Authorization
R06: Accountability
R07: Privacy

V01.1: Web Services and Interfaces vulnerabilities; V01.2: Web client data manipulation vulnerabilities; V01.3: User Identity and Access vulnerabilities; V01.4: Encryption and Keys vulnerabilities; V02.1: Software development framework and practices vulnerabilities; V02.2: Software code vulnerabilities; V02.3: Operating system traditional vulnerabilities; V03.1: Virtual Machine traditional vulnerabilities; V03.2: VM Image vulnerabilities; V03.3: VM Migration and Rollback vulnerabilities; V03.4: Multi-tenancy environment vulnerabilities; V03.5: Hypervisor vulnerabilities; V04.1: Network communication vulnerabilities; V04.2: Shared network vulnerabilities; V04.3: Virtual network vulnerabilities; V05.1: Data storage cryptography vulnerabilities; V05.2: Data access vulnerabilities; V05.3: Data storage location, backup and recovery vulnerabilities; V05.4: Data sanitization vulnerabilities; V06.1: Hardware vulnerabilities; V07.1: Physical access vulnerabilities; V07.2: Natural disasters; V08.1: Assurance vulnerabilities; V08.2: Compliance vulnerabilities

architecture. The SDN centralized control plane, Deterministic Virtual Networks (DVNs), and lightweight encryption at layer-2 works together to achieve expected level of security and privacy with acceptable performance and energy efficiencies in the cloud IoT [500].

5.7.3. 5G, SDN, NFV and cloud computing security

SDN and NFV, complementing each other, drives the future network powered by cloud computing and 5G. Softwarization of network functions using SDN separates network control and data forwarding planes. NFV enables network functions to be

Table 13
Trust based security and privacy countermeasures.

Cloud security requirement	Trust based security and privacy countermeasures approach	Related study
Confidentiality	Public Key Infrastructure (PKI), TTP, Hybrid cryptography, PKI trusted CA certificate enabled IPSec or SSL communication, and Hardware enabled trusted computing platform — TPM, vTPM, TCCP, Excalibur	[25], [470], [413], [293], [294], [137], [296]
Integrity	Public Key Infrastructure (PKI), TTP, Hybrid cryptography, and Trusted computing platform — VM Migration	[25], [470], [295], [327], [330], [328]
Availability	Continuous monitoring of attributes to enforce SLAs, Fault tolerant mechanism, and Hardware enabled trusted computing platform — VM Machine replication, Framework for enhanced hardware and attribute based adaptive trust management scheme for SLA guarantee	[418], [22], [298], [133], [362], [297], [300], [373]
Authentication	Public Key Infrastructure (PKI), TTP, Security domains with common security tokens (Federated Clouds), Digital signatures with SSO and LDAP, and Trusted computing platform	[25], [295]
Authorization	Public Key Infrastructure (PKI), TTP, Security domains with common security tokens (Federated Clouds), Attribute based certificates by CA, and Hardware enabled Access Control	[25], [299]
Accountability	TTP Certificates from CA used in communication chain of TrustActivity, event and traffic logging	[25], [414], [411], [399], [398]
Privacy	Public Key Infrastructure (PKI), TTP, Hybrid cryptography Trusted computing platform — MyCloud, User Trusted Entity (UTE), and Privacy preserving access control in SOA, public auditing and data anonymization	[25], [470], [298], [412], [451], [450], [30]

placed anywhere in the perimeter of the network on a need basis and reduces dependencies from network function-specific hardware. Future network technology enablers cloud computing, SDN, NFV and IoT are maturing to use 5G. Soldani et al. [501] mentioned the widespread adoption and utilization of services, SDN, NFV, and cloud computing at the edge will make the 5G infrastructure technically feasible and business viable. However, with the upcoming fifth-generation wireless network (5G) the security threat vector has become bigger. Ahmad et al. [502] discussed multiple security and privacy challenges for 5G and affected enabling technologies of cloud computing, IoT, SDN, and NFV. They also explained the technologies to use for addressing these security challenges. Liyanage et al. [503] highlighted Software Defined Mobile Network (SDMN) security challenges and a mechanism to address the same that includes security enabling features of NFV. Tian et al. [504] have discussed security issues and possible solution for Cloud Radio Access Network (C-RAN) being used in 5G. Monshizadeh et al. [505], in order to detect and prevent security attacks and malicious traffic, have proposed for centralized monitoring along with to use dynamicity and programmability of SDN, clustering mechanisms for load balancing and traffic filtering capabilities of IDS.

6. Conclusion and further research opportunity

In the last ten years, there has been enormous growth for cloud-based business opportunities. However, the cloud threat spectrum also has been widened. This narrative review examines the cloud service and deployment models, cloud architectural components, cloud security taxonomy, security requirements, CSA's treacherous twelve threats, known vulnerabilities in cloud architectural components and suggested countermeasures. This survey has provided some of the missing aspects of previous works on security and privacy for a cloud computing system, especially the formulation of a unified cloud security taxonomy to analyze the end-to-end inter-related mapping between cloud security requirements to identified threats, known vulnerabilities, and suggested countermeasures. The inter-related analysis of security requirements, threats, vulnerabilities and countermeasures presented here will assist in choosing the appropriate countermeasures to mitigate the risks associated with the threats due to vulnerabilities in the cloud component. These implemented countermeasures will limit the attack vectors for identified threats and fulfill the desired level of security and privacy requirements.

Apart from different countermeasures suggested, implementation priority should be given to those measures which can build trust and confidence in cloud-based solutions and systems to its users. Like implementing countermeasures providing control and visibility on data life-cycle management to users for their outsourced data, a proven user identity, authentication and authorization mechanism, and use of software engineering and system design principles for cloud platforms and applications software used in delivering cloud services. It will help in building trust in cloud computing solutions and accelerate its adoption. Trust-based countermeasures seem to be promising for addressing cloud security requirements. Hard Trust approach uses vTPM and TTP with certificates, and Soft Trust evaluates the trust factor dynamically from user behavior perspective using reputation-based, content-based, context-based, or evidence-based approaches.

The work presented here, however, is limited to the narrative review of research works from academia, industry, and recommendations of the standards organizations. This work scoped itself for modeling security in cloud computing based on the published works and analyzed mappings can be used as a quick reference for effective planning the implementation of recommended countermeasures to address the vulnerabilities in cloud computing architectural components.

To cater the changing landscape of threats and dynamism of cloud computing environment, security countermeasures should be implemented in a self-adaptive way. The statically beforehand selected security mechanism will not be sufficient and effective to address evolving threat vectors. So, adaptive security, especially trust-based adaptive security, for cloud computing systems seems to be an exciting area for future research that can enable the secure and innovative business service offerings from the cloud provider to leverage technological evolution of IoT, Big Data, 5G, SDN, and NFV based applications and services.

Acknowledgments

The authors would like to convey their appreciation and gratitude to the anonymous reviewers. Their remarks and suggestions were extremely insightful and enabled us to improve the quality of manuscript.

Declaration of competing interest

The authors declare that there is no conflict of interest in this paper.

References

[1] statista, Size of the cloud computing and hosting market market worldwide from 2010 to 2020, URL https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/, [Accessed on 07-Jul-2018], 2017.

[2] J. Willis, Who Coined The Phrase Cloud Computing? URL http://www.johnmwillis.com/cloud-computing/who-coined-the-phrase-cloud-computing, [Accessed on 26-Jan-2018], 2008.

[3] A. Regalado, Who Coined 'Cloud Computing'? URL https://www.technologyreview.com/s/425970/who-coined-cloud-computing, [Accessed on 26-Jan-2018], 2011.

[4] K. Gill, The history of Cloud Computing and Cloud Storage, URL https://www.linkedin.com/pulse/20140602173917-185626188-the-history-of-cloud-computing-and-cloud-storage, [Accessed on 26-Jan-2018], 2014.

[5] P.M. Mell, T. Grance, The NIST Definition of Cloud Computing (SP 800-145), Tech. Rep., National Institute of Standards & Technology, Gaithersburg, MD, United States, URL http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, [Accessed on 10-Feb-2018], 2011.

[6] Gartner, Gartner Forecasts Worldwide Public Cloud Services Revenue, URL https://www.gartner.com/newsroom/id/3815165, [Accessed on 08-Apr-2018], 2017.

[7] Q. Zhang, L. Cheng, R. Boutaba, Cloud computing: state-of-the-art and research challenges, J. Internet Serv. Appl. (ISSN: 1869-0238) 1 (1) (2010) 7–18, http://dx.doi.org/10.1007/s13174-010-0007-6.

[8] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. (ISSN: 1084-8045) 34 (1) (2011) 1–11, http://dx.doi.org/10.1016/j.jnca.2010.07.006.

[9] N. Phaphoom, X. Wang, P. Abrahamsson, Foundations and technological landscape of cloud computing, ISRN Softw. Eng. 2013 (2013) http://dx.doi.org/10.1155/2013/782174, [Accessed on 10-Feb-2018].

[10] M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: Opportunities and challenges, Inform. Sci. (ISSN: 0020-0255) 305 (2015) 357–383, http://dx.doi.org/10.1016/j.ins.2015.01.025.

[11] B. Robertson, Top Five Cloud-Computing Adoption Inhibitors, URL https://www.gartner.com/doc/977217/top-cloudcomputing-adoption-inhibitors, [Accessed on 08-Apr-2018], 2009.

[12] M. Avram, Advantages and challenges of adopting cloud computing from an enterprise perspective, Procedia Technol. (ISSN: 2212-0173) 12 (2014) 529–534, http://dx.doi.org/10.1016/j.protcy.2013.12.525.

[13] N. Phaphoom, X. Wang, S. Samuel, S. Helmer, P. Abrahamsson, A survey study on major technical barriers affecting the decision to adopt cloud services, J. Syst. Softw. (ISSN: 0164-1212) 103 (2015) 167–181, http://dx.doi.org/10.1016/j.jss.2015.02.002.

[14] C.-L. Hsu, J.C.-C. Lin, Factors affecting the adoption of cloud services in enterprises, Inf. Syst. E-bus. Manag. (ISSN: 1617-9846) 14 (4) (2016) 791–822, http://dx.doi.org/10.1007/s10257-015-0300-9.

[15] Forbes Technology Council, 13 Biggest Challenges When Moving Your Business To The Cloud, URL https://www.forbes.com/sites/forbestechcouncil/2017/06/05/13-biggest-challenges-when-moving-your-business-to-the-cloud/#3a8e0e219b0e, 2017.

[16] S.A. Alatresh, A.B. Ali, M.A. Ambarek, Cloud computing adoption by business organization: A systematic review, Aust. J. Basic Appl. Sci. 11 (13) (2017) 17–28, http://dx.doi.org/10.22587/ajbas.2017.11.13.3.

[17] RightScale, RightScale 2018 State of the Cloud Report, URL https://www.rightscale.com/lp/state-of-the-cloud?campaign=7010g0000016JiU, [Accessed on 08-Apr-2018], 2018.

[18] B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, IEEE Secur. Priv. (ISSN: 1540-7993) 9 (2) (2011) 50–57, http://dx.doi.org/10.1109/MSP.2010.115.

[19] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf, NIST Cloud Computing Reference Architecture (SP 500-292), National Institute of Standards & Technology, Gaithersburg, MD 20899-8930, USA, 2011, URL http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505, [Accessed on 10-Feb-2018].

[20] R. Mogull, J. Arlen, A. Lane, G. Peterson, M. Rothman, D. Mortman, Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance, 2017, URL https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf, [Accessed on 10-Feb-2018].

[21] M.A. Morsy, J. Grundy, I. Müller, An analysis of the cloud computing security problem, in: Proceedings of APSEC 2010 Cloud Workshop, 2010, pp. 1–6, URL https://www.cs.auckland.ac.nz/~john-g/papers/cloud2010_1.pdf, [Accessed on 11-Feb-2018].

[22] H. Takabi, J.B.D. Joshi, G.-J. Ahn, Security and privacy challenges in cloud computing environments, IEEE Secur. Priv. (ISSN: 1540-7993) 8 (6) (2010) 24–31, http://dx.doi.org/10.1109/MSP.2010.186.

[23] L.M. Vaquero, L. Rodero-Merino, D. Morán, Locking the sky: a survey on IaaS cloud security, Computing (ISSN: 1436-5057) 91 (1) (2011) 93–118, http://dx.doi.org/10.1007/s00607-010-0140-x.

[24] K. Dahbur, B. Mohammad, A.B. Tarakji, A survey of risks, threats and vulnerabilities in cloud computing, in: Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, in: ISWSA '11, ACM, New York, NY, USA, ISBN: 978-1-4503-0474-0, 2011, pp. 1–6, http://dx.doi.org/10.1145/1980822.1980834.

[25] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst. (ISSN: 0167-739X) 28 (3) (2012) 583–592, http://dx.doi.org/10.1016/j.future.2010.12.006.

[26] S. Pearson, Privacy, security and trust in cloud computing, in: S. Pearson, G. Yee (Eds.), Privacy and Security for Cloud Computing, Springer, London, UK, ISBN: 978-1-4471-4189-1, 2013, pp. 3–42, http://dx.doi.org/10.1007/978-1-4471-4189-1_1.

[27] K. Hashizume, D.G. Rosado, E. Fernández-Medina, E.B. Fernandez, An analysis of security issues for cloud computing, J. Internet Serv. Appl. (ISSN: 1869-0238) 4 (1) (2013) 1–13, http://dx.doi.org/10.1186/1869-0238-4-5.

[28] Z. Xiao, Y. Xiao, Security and privacy in cloud computing, IEEE Commun. Surv. Tutor. (ISSN: 1553-877X) 15 (2) (2013) 843–859, http://dx.doi.org/10.1109/SURV.2012.060912.00182.

[29] C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan, A survey on security issues and solutions at different layers of cloud computing, J. Supercomput. (ISSN: 1573-0484) 63 (2) (2013) 561–592, http://dx.doi.org/10.1007/s11227-012-0831-5.

[30] D.A.B. Fernandes, L.F.B. Soares, J.V. Gomes, M.M. Freire, P.R.M. Inácio, Security issues in cloud environments: a survey, Int. J. Inf. Secur. (ISSN: 1615-5270) 13 (2) (2014) 113–170, http://dx.doi.org/10.1007/s10207-013-0208-7.

[31] E. Aguiar, Y. Zhang, M. Blanton, An overview of issues and recent developments in cloud computing and storage security, in: K.J. Han, B.-Y. Choi, S. Song (Eds.), High Performance Cloud Auditing and Applications, Springer, New York, NY, USA, ISBN: 978-1-4614-3296-8, 2014, pp. 3–33, http://dx.doi.org/10.1007/978-1-4614-3296-8_1.

[32] I.M. Khalil, A. Khreishah, M. Azeem, Cloud computing security: A survey, Computers (ISSN: 2073-431X) 3 (1) (2014) 1–35, http://dx.doi.org/10.3390/computers3010001.

[33] C.A. Ardagna, R. Asal, E. Damiani, Q.H. Vu, From security to assurance in the cloud: A survey, ACM Comput. Surv. (ISSN: 0360-0300) 48 (1) (2015) 1–50, http://dx.doi.org/10.1145/2767005.

[34] W. Huang, A. Ganjali, B.H. Kim, S. Oh, D. Lie, The state of public infrastructure-as-a-service cloud security, ACM Comput. Surv. (ISSN: 0360-0300) 47 (4) (2015) 1–31, http://dx.doi.org/10.1145/2767181.

[35] S. Singh, Y.-S. Jeong, J.H. Park, A survey on cloud computing security: Issues, threats, and solutions, J. Netw. Comput. Appl. 75 (2016) 200–222, http://dx.doi.org/10.1016/j.jnca.2016.09.002.

[36] N. Khan, A. Al-Yasiri, Identifying cloud security threats to strengthen cloud computing adoption framework, Procedia Comput. Sci. (ISSN: 1877-0509) 94 (2016) 485–490, http://dx.doi.org/10.1016/j.procs.2016.08.075.

[37] A. Singh, K. Chatterjee, Cloud security issues and challenges: A survey, J. Netw. Comput. Appl. (ISSN: 1084-8045) 79 (2017) 88–115, http://dx.doi.org/10.1016/j.jnca.2016.11.027.

[38] G. Ramachandra, M. Iftikhar, F.A. Khan, A comprehensive survey on security in cloud computing, Procedia Comput. Sci. (ISSN: 1877-0509) 110 (2017) 465–472, http://dx.doi.org/10.1016/j.procs.2017.06.124.

[39] L. Coppolino, S. DAntonio, G. Mazzeo, L. Romano, Cloud security: Emerging threats and current solutions, Comput. Electr. Eng. (ISSN: 0045-7906) 59 (2017) 126–140, http://dx.doi.org/10.1016/j.compeleceng.2016.03.004.

[40] N. Subramanian, A. Jeyaraj, Recent security challenges in cloud computing, Comput. Electr. Eng. (ISSN: 0045-7906) 71 (2018) 28–42, http://dx.doi.org/10.1016/j.compeleceng.2018.06.006.

[41] J.B. Hong, A. Nhlabatsi, D.S. Kim, A. Hussein, N. Fetais, K.M. Khan, Systematic identification of threats in the cloud: A survey, Comput. Netw. (ISSN: 1389-1286) 150 (2019) 46–69, http://dx.doi.org/10.1016/j.comnet.2018.12.009.

[42] R. Patil, C. Modi, An exhaustive survey on security concerns and solutions at different components of virtualization, ACM Comput. Surv. (ISSN: 0360-0300) 52 (1) (2019) 12:1–12:38, http://dx.doi.org/10.1145/3287306.

[43] A. Shawish, M. Salama, Cloud computing: Paradigms and technologies, in: F. Xhafa, N. Bessis (Eds.), Inter-Cooperative Collective Intelligence: Techniques and Applications, Springer, Berlin, Heidelberg, ISBN: 978-3-642-35016-0, 2014, pp. 39–67, http://dx.doi.org/10.1007/978-3-642-35016-0_2.

[44] A. Gajbhiye, K.M.P. Shrivastva, Cloud computing: Need, enabling technology, architecture, advantages and challenges, in: 2014 5th International Conference - Confluence the Next Generation Information Technology Summit (Confluence), 2014, pp. 1–7, http://dx.doi.org/10.1109/CONFLUENCE.2014.6949224.

[45] I. Foster, Y. Zhao, I. Raicu, S. Lu, Cloud computing and grid computing 360-degree compared, in: 2008 Grid Computing Environments Workshop, 2008, pp. 1–10, http://dx.doi.org/10.1109/GCE.2008.4738445, ISSN 2152-1085.

[46] L. Youseff, M. Butrico, D.D. Silva, Toward a unified ontology of cloud computing, in: 2008 Grid Computing Environments Workshop, 2008, pp. 1–10, http://dx.doi.org/10.1109/GCE.2008.4738443, ISSN 2152-1085.

[47] CSA, The Treacherous 12 - Cloud Computing Top Threats in 2016, Tech. Rep., Cloud Security Alliance, URL https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf, [Accessed on 10-Feb-2018], 2016.

[48] R. Kissel, Glossary of Key Information Security Terms, in: NISTIR 7298 Revision 2, National Institute of Standards and Technology, 2013, URL http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, [Accessed on 10-Feb-2018].

[49] CSA, Top Threats to Cloud Computing, Tech. Rep. V1.0, Cloud Security Alliance, URL https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, [Accessed on 10-Feb-2018], 2010.

[50] CSA, The Treacherous 12 - Cloud Computing Top Threats in 2016, Tech. Rep., Cloud Security Alliance, URL https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf, [Accessed on 10-Feb-2018], 2016.

[51] X. Chen, J. Andersen, Z.M. Mao, M. Bailey, J. Nazario, Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware, in: 2008 IEEE International Conference on Dependable Systems and Networks with FTCS and DCC (DSN), 2008, pp. 177–186, http://dx.doi.org/10.1109/DSN.2008.4630086, ISSN 1530-0889.

[52] N. Gruschka, M. Jensen, Attack surfaces: A taxonomy for attacks on cloud services, in: 2010 IEEE 3rd International Conference on Cloud Computing, 2010, pp. 276–279, http://dx.doi.org/10.1109/CLOUD.2010.23, ISSN 2159-6182.

[53] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, L. Lo Iacono, All your clouds are belong to us: Security analysis of cloud management interfaces, in: Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, ACM, New York, NY, USA, ISBN: 978-1-4503-1004-8, 2011, pp. 3–14, http://dx.doi.org/10.1145/2046660.2046664.

[54] G. Porter, Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase I, Tech. Rep. CMU/SEI-2013-TN-020, Software Engineering Institute, URL https://resources.sei.cmu.edu/asset_files/technicalnote/2013_004_001_69713.pdf, [Accessed on 15-Apr-2018], 2013.

[55] J. Rittinghouse, J. Ransome, Cloud Computing: Implementation, Management, and Security, first ed., CRC Press, Inc., Boca Raton, FL, USA, 2009, ISBN 1439806802, 9781439806807.

[56] M. Jensen, N. Gruschka, R. Herkenhöner, A survey of attacks on web services, Comput. Sci. - Res. Dev. (ISSN: 0949-2925) 24 (4) (2009) 185–197, http://dx.doi.org/10.1007/s00450-009-0092-6.

[57] OWASP, Top 10 Most Critical Web Application Security Risks, Tech. Rep. Top 10 - 2017, The OWASP Foundation, URL https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf, [Accessed on 11-Feb-2018], 2017.

[58] M. Doroodchi, A. Iranmehr, S.A. Pouriyeh, An investigation on integrating XML-based security into web services, in: 2009 5th IEEE GCC Conference Exhibition, 2009, pp. 1–5, http://dx.doi.org/10.1109/IEEEGCC.2009.5734300.

[59] N. Gruschka, L.L. Iacono, Vulnerable cloud: SOAP message security validation revisited, in: 2009 IEEE International Conference on Web Services, 2009, pp. 625–631, http://dx.doi.org/10.1109/ICWS.2009.70.

[60] M. Jensen, J. Schwenk, N. Gruschka, L.L. Iacono, On technical security issues in cloud computing, in: 2009 IEEE International Conference on Cloud Computing, 2009a, pp. 109–116, http://dx.doi.org/10.1109/CLOUD.2009.60, ISSN 2159-6182.

[61] A.K. Sood, R.J. Enbody, Targeted cyberattacks: A superset of advanced persistent threats, IEEE Secur. Priv. (ISSN: 1540-7993) 11 (1) (2013) 54–61, http://dx.doi.org/10.1109/MSP.2012.90.

[62] MANDIANT, M-TRENDS 2018, URL https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf, [Accessed on 13-Apr-2018], 2018.

[63] M. Jensen, C. Meyer, Expressiveness considerations of XML signatures, in: 2011 IEEE 35th Annual Computer Software and Applications Conference Workshops, 2011, pp. 392–397, http://dx.doi.org/10.1109/COMPSACW.2011.72.

[64] OWASP, The OWASP Top 10 Most Critical Web Application Security Risks, Tech. Rep. Top 10 - 2013, The OWASP Foundation, URL https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf, [Accessed on 11-Feb-2011], 2013.

[65] OWASP, The OWASP Top 10 Most Critical Web Application Security Risks, Tech. Rep. Top 10 - 2010, The OWASP Foundation, URL https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/owasptop10/OWASP%20Top%2010%20-%202010.pdf, [Accessed on 11-Feb-2018], 2010.

[66] A. Panah, O. Panah, S. Fallahpour, Challenges of security issues in cloud computing layers, Rep Opin. (ISSN: 1553-9873) 4 (2012) 25–29, http://dx.doi.org/10.7537/marsroj041012.07.

[67] Symantec, Internet Security Threat Report, URL https://img03.en25.com/Web/Symantec/%7Bf8ca1fb2-b73c-46d0-ae9e-17456c45df87%7D_ISTR23-FINAL.pdf?aid=elq_, [Accessed on 13-Apr-2018], 2018.

[68] F.B.M. Nor, K.A. Jalil, J. l. Ab Manan, An enhanced remote authentication scheme to mitigate man-in-the-browser attacks, in: Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012, pp. 271–276, http://dx.doi.org/10.1109/CyberSec.2012.6246086.

[69] T. Dougan, K. Curran, Man in the browser attacks, Int. J. Ambient Comput. Intell. (ISSN: 1941-6237) 4 (1) (2012) 29–39, http://dx.doi.org/10.4018/jaci.2012010103.

[70] W.A. Jansen, Cloud hooks: Security and privacy issues in cloud computing, in: 2011 44th Hawaii International Conference on System Sciences, 2011, pp. 1–10, http://dx.doi.org/10.1109/HICSS.2011.103, ISSN 1530-1605.

[71] T. Jung, X.Y. Li, Z. Wan, M. Wan, Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption, IEEE Trans. Inf. Forensics Secur. (ISSN: 1556-6013) 10 (1) (2015) 190–199, http://dx.doi.org/10.1109/TIFS.2014.2368352.

[72] S.A. Almulla, C.Y. Yeun, Cloud computing security management, in: 2010 Second International Conference on Engineering System Management and Applications, 2010, pp. 1–7, URL https://ieeexplore.ieee.org/document/5542654/.

[73] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, J. Molina, Controlling data in the cloud: Outsourcing computation without outsourcing control, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, in: CCSW '09, ACM, New York, NY, USA, ISBN: 978-1-60558-784-4, 2009, pp. 85–90, http://dx.doi.org/10.1145/1655008.1655020.

[74] PayPal, Integrate Log In with PayPal, URL https://developer.paypal.com/docs/integration/direct/identity/log-in-with-paypal/, [Accessed on 13-Apr-2018], 2018.

[75] Google, OpenID Connect, URL https://developers.google.com/identity/protocols/OpenIDConnect, [Accessed on 13-Apr-2018], 2018.

[76] Microsoft, Authorize access to web applications using OpenID Connect and Azure Active Directory, URL https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-protocols-openid-connect-code, [Accessed on 24-Apr-2018], 2018.

[77] W. Li, C.J. Mitchell, Analysing the security of google's implementation of OpenID connect, in: J. Caballero, U. Zurutuza, R.J. Rodríguez (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, Cham, ISBN: 978-3-319-40667-1, 2016, pp. 357–376.

[78] N. Naik, P. Jenkins, Securing digital identities in the cloud by selecting an apposite federated identity management from SAML, OAuth and OpenID connect, in: 2017 11th International Conference on Research Challenges in Information Science (RCIS), 2017, pp. 163–174, http://dx.doi.org/10.1109/RCIS.2017.7956534.

[79] D. Fett, R. Küsters, G. Schmitz, A comprehensive formal security analysis of oauth 2.0, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, in: CCS '16, ACM, ISBN: 978-1-4503-4139-4, 2016, pp. 1204–1215, http://dx.doi.org/10.1145/2976749.2978385.

[80] W. Li, C.J. Mitchell, Addressing threats to real-world identity management systems, in: H. Reimer, N. Pohlmann, W. Schneider (Eds.), ISSE 2015, Springer, Wiesbaden, 2015, pp. 251–259, http://dx.doi.org/10.1007/978-3-658-10934-9_21.

[81] C. Mainka, V. Mladenov, J. Schwenk, On the security of modern Single Sign-On Protocols Second-Order Vulnerabilities in OpenID Connect, CoRR URL https://arxiv.org/pdf/1508.04324.pdf, [Accessed on 13-Apr-2018].

[82] D. Fett, R. Küsters, G. Schmitz, The web SSO standard openid connect: In-depth formal security analysis and security guidelines, in: 2017 IEEE 30th Computer Security Foundations Symposium (CSF), 2017, pp. 189–202, http://dx.doi.org/10.1109/CSF.2017.20.

[83] S. Sengupta, V. Kaulgud, V.S. Sharma, Cloud computing security–trends and research directions, in: Proceedings of the 2011 IEEE World Congress on Services, in: SERVICES '11, IEEE Computer Society, Washington, DC, USA, 2011, pp. 524–531, http://dx.doi.org/10.1109/SERVICES.2011.20.

[84] X. Ding, L. Zhang, Z. Wan, M. Gu, De-anonymizing dynamic social networks, in: 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, 2011, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2011.6133607, ISSN 1930-529X.

[85] A. Narayanan, V. Shmatikov, De-anonymizing social networks, in: Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, in: SP '09, IEEE Computer Society, Washington, DC, USA, ISBN: 978-0-7695-3633-0, 2009, pp. 173–187, http://dx.doi.org/10.1109/SP.2009.22.

[86] A. Behl, Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation, in: 2011 World Congress on Information and Communication Technologies, 2011, pp. 217–222, http://dx.doi.org/10.1109/WICT.2011.6141247.

[87] N. Heninger, Z. Durumeric, E. Wustrow, J.A. Halderman, Mining your ps and qs: Detection of widespread weak keys in network devices, in: Proceedings of the 21st USENIX Conference on Security Symposium, in: Security'12, USENIX Association, Berkeley, CA, USA, 2012, pp. 35–35. URL https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf.

[88] H. Yu, N. Powell, D. Stembridge, X. Yuan, Cloud computing and security challenges, in: Proceedings of the 50th Annual Southeast Regional Conference, in: ACM-SE '12, ACM, New York, NY, USA, ISBN: 978-1-4503-1203-5, 2012, pp. 298–302, http://dx.doi.org/10.1145/2184512.2184581.

[89] D. Martin, Implementing effective controls in a mobile, agile, cloud-enabled enterprise, IEEE Secur. Priv. (ISSN: 1540-7993) 11 (1) (2013) 13–14, http://dx.doi.org/10.1109/MSP.2013.1.

[90] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, E. Dubois, Security transparency: the next frontier for security research in the cloud, J. Cloud Comput. (ISSN: 2192-113X) 4 (1) (2015) 1–14, http://dx.doi.org/10.1186/s13677-015-0037-5.

[91] G. McGraw, Software Security: Building Security In, Addison-Wesley Professional, ISBN: 0321356705, 2006, URL https://www.pearson.com/us/higher-education/program/Mc-Graw-Software-Security-Building-Security-In/PGM55117.html, [Accessed on 15-Apr-2018].

[92] L. Rodero-Merino, L.M. Vaquero, E. Caron, A. Muresan, F. Desprez, Building safe paas clouds: A survey on security in multitenant software platforms, Comput. Secur. 31 (1) (2012) 96–108, http://dx.doi.org/10.1016/j.cose.2011.10.006.

[93] W.R. Claycomb, A. Nicoll, Insider threats to cloud computing: Directions for new research challenges, in: Proceedings of the 2012 IEEE 36th Annual Computer Software and Applications Conference, in: COMPSAC '12, IEEE Computer Society, Washington, DC, USA, ISBN: 978-0-7695-4736-7, 2012, pp. 387–394, http://dx.doi.org/10.1109/COMPSAC.2012.113.

[94] B.M. Babu, M.S. Bhanu, Prevention of insider attacks by integrating behavior analysis with risk based access control model to protect cloud, Procedia Comput. Sci. 54 (2015) 157–166, http://dx.doi.org/10.1016/j.procs.2015.06.018.

[95] J. Spring, Monitoring cloud computing by layer, part 1, IEEE Secur. Priv. (ISSN: 1540-7993) 9 (2) (2011) 66–68, http://dx.doi.org/10.1109/MSP.2011.33.

[96] C. Manes, 2015's MVPs – The most vulnerable players, URL https://techtalk.gfi.com/2015s-mvps-the-most-vulnerable-players/?_ga=2.122131789.771011896.1523716786-780905549.1523716786, [Accessed on 14-Apr-2018], 2016.

[97] M. Pearce, S. Zeadally, R. Hunt, Virtualization: Issues, security threats, and solutions, ACM Comput. Surv. (ISSN: 0360-0300) 45 (2) (2013) 1–39, http://dx.doi.org/10.1145/2431211.2431216.

[98] Trend Micro, Cloud Computing Security: Making Virtual Machines Cloud-Ready, URL http://www.trendmicro.com.cn/cloud-content/us/pdfs/business/white-papers/wp_cloud-computing-security.pdf, [Accessed on 25-Mar-2018], 2009.

[99] L.M. Kaufman, Can public-cloud security meet its unique challenges? IEEE Secur. Priv. (ISSN: 1540-7993) 8 (2010) 55–57, http://dx.doi.org/10.1109/MSP.2010.120.

[100] K. Okamura, Y. Oyama, Load-based covert channels between xen virtual machines, in: Proceedings of the 2010 ACM Symposium on Applied Computing, in: SAC '10, ACM, New York, NY, USA, ISBN: 978-1-60558-639-7, 2010, pp. 173–180, http://dx.doi.org/10.1145/1774088.1774125.

[101] A. Aviram, S. Hu, B. Ford, R. Gummadi, Determinating timing channels in compute clouds, in: Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, in: CCSW '10, ACM, New York, NY, USA, ISBN: 978-1-4503-0089-6, 2010, pp. 103–108, http://dx.doi.org/10.1145/1866835.1866854.

[102] Y. Zhang, A. Juels, M.K. Reiter, T. Ristenpart, Cross-VM side channels and their use to extract private keys, in: Proceedings of the 2012 ACM Conference on Computer and Communications Security, in: CCS '12, ACM, New York, NY, USA, ISBN: 978-1-4503-1651-4, 2012, pp. 305–316, http://dx.doi.org/10.1145/2382196.2382230.

[103] A. Jasti, P. Shah, R. Nagaraj, R. Pendse, Security in multi-tenancy cloud, in: 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, 2010, pp. 35–41, http://dx.doi.org/10.1109/CCST.2010.5678682, ISSN 1071-6572.

[104] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, Managing security of virtual machine images in a cloud environment, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, in: CCSW '09, New York, NY, USA, ISBN: 978-1-60558-784-4, 2009, pp. 91–96, http://dx.doi.org/10.1145/1655008.1655021.

[105] S. Luo, Z. Lin, X. Chen, Z. Yang, J. Chen, Virtualization security for cloud computing service, in: Proceedings of the 2011 International Conference on Cloud and Service Computing, in: CSC '11, IEEE Computer Society, Washington, DC, USA, ISBN: 978-1-4577-1635-5, 2011, pp. 174–179, http://dx.doi.org/10.1109/CSC.2011.6138516.

[106] T. Garfinkel, M. Rosenblum, When virtual is harder than real: Security challenges in virtual machine based computing environments, in: Proceedings of the 10th Conference on Hot Topics in Operating Systems - Volume 10, in: HOTOS'05, USENIX Association, Berkeley, CA, USA, 2005, pp. 20–20. URL https://www.usenix.org/legacy/event/hotos05/final_papers/full_papers/garfinkel/garfinkel_old.pdf, [Accessed on 25-Mar-2018].

[107] F. Zhang, H. Chen, Security-preserving live migration of virtual machines in the cloud, J. Netw. Syst. Manage. (ISSN: 1064-7570) 21 (4) (2013) 562–587, http://dx.doi.org/10.1007/s10922-012-9253-1.

[108] W. Dawoud, I. Takouna, C. Meinel, Infrastructure as a service security: Challenges and solutions, in: 2010 the 7th International Conference on Informatics and Systems (INFOS), 2010, pp. 1–8, URL ieeexplore.ieee.org/iel5/5457305/5461721/05461732.pdf.

[109] J. Oberheide, E. Cooke, F. Jahanian, Empirical exploitation of live virtual machine migration, in: BlackHat DC Briefings, Washington DC, 2008, pp. 1–6, URL http://vhosts.eecs.umich.edu/fjgroup/pubs/blackhat08-migration.pdf, [Accessed on 26-Mar-2018].

[110] A. Duncan, S. Creese, M. Goldsmith, J.S. Quinton, Cloud computing: Insider attacks on virtual machines during migration, in: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 493–500, http://dx.doi.org/10.1109/TrustCom.2013.62, ISSN 2324-898X.

[111] H. Tsai, R. Steinmetz, Y. Huang, M. Siebenhaar, A. Miede, Threat as a service?: Virtualization's impact on cloud security, IT Prof. (ISSN: 1520-9202) 14 (2011) 32–37, http://dx.doi.org/10.1109/MITP.2011.117.

[112] H. Wu, Y. Ding, C. Winer, L. Yao, Network security for virtual machine in cloud computing, in: 5th International Conference on Computer Sciences and Convergence Information Technology, 2010, pp. 18–21, http://dx.doi.org/10.1109/ICCIT.2010.5711022.

[113] R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, B. Freisleben, Increasing virtual machine security in cloud environments, J. Cloud Comput. Adv. Syst. Appl. (ISSN: 2192-113X) 1 (1) (2012) 1–12, http://dx.doi.org/10.1186/2192-113X-1-12.

[114] W. Liu, S. Peng, W. Du, W. Wang, G.S. Zeng, Security-aware intermediate data placement strategy in scientific cloud workflows, Knowl. Inf. Syst. (ISSN: 0219-1377) 41 (2) (2014) 423–447, http://dx.doi.org/10.1007/s10115-014-0755-x.

[115] M.H. Song, Analysis of risks for virtualization technology, in: Advanced Engineering Solutions, Vol. 539, Trans Tech Publications, 2014, pp. 374–377, http://dx.doi.org/10.4028/www.scientific.net/AMM.539.374, [Accessed on 01-Apr-2018].

[116] J. Szefer, E. Keller, R.B. Lee, J. Rexford, Eliminating the hypervisor attack surface for a more secure cloud, in: Proceedings of the 18th ACM Conference on Computer and Communications Security, in: CCS '11, ACM, New York, NY, USA, ISBN: 978-1-4503-0948-6, 2011, pp. 401–412, http://dx.doi.org/10.1145/2046707.2046754.

[117] V. Varadharajan, U. Tupakula, Counteracting security attacks in virtual machines in the cloud using property based attestation, J. Netw. Comput. Appl. (ISSN: 1084-8045) 40 (2014) 31–45, http://dx.doi.org/10.1016/j.jnca.2013.08.002.

[118] D. Perez-Botero, J. Szefer, R.B. Lee, Characterizing hypervisor vulnerabilities in cloud computing servers, in: Proceedings of the 2013 International Workshop on Security in Cloud Computing, in: Cloud Computing '13, ACM, New York, NY, USA, ISBN: 978-1-4503-2067-2, 2013, pp. 3–10, http://dx.doi.org/10.1145/2484402.2484406.

[119] Z. Wang, X. Jiang, Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity, in: Proceedings of the 2010 IEEE Symposium on Security and Privacy, IEEE Computer Society, Washington, DC, USA, ISBN: 978-0-7695-4035-1, 2010, pp. 380–395, http://dx.doi.org/10.1109/SP.2010.30.

[120] S. Stamm, Z. Ramzan, M. Jakobsson, Drive-by pharming, in: S. Qing, H. Imai, G. Wang (Eds.), Information and Communications Security, Springer Berlin Heidelberg, Berlin, Heidelberg, ISBN: 978-3-540-77048-0, 2007, pp. 495–506, URL https://link.springer.com/chapter/10.1007/978-3-540-77048-0_38.

[121] T. Hunt, 5 ways to implement HTTPS in an insufficient manner (and leak sensitive data), URL https://www.troyhunt.com/5-ways-to-implement-https-in/, [Accessed on 17-Apr-2018], 2013.

[122] M. Prandini, M. Ramilli, W. Cerroni, F. Callegati, Splitting the HTTPS stream to attack secure web connections, IEEE Secur. Priv. (ISSN: 1540-7993) 8 (6) (2010) 80–84, http://dx.doi.org/10.1109/MSP.2010.190.

[123] M. Marlinspike, More tricks for defeating SSL in practice, URL https://www.blackhat.com/presentations/bh-usa-09/MARLINSPIKE/BHUSA09-Marlinspike-DefeatSSL-SLIDES.pdf, [Accessed on 17-Apr-2018], 2009.

[124] B. Pfaff, J. Pettit, T. Koponen, K. Amidon, M. Casado, S. Shenker, Extending networking into the virtualization layer, in: Proc. of Workshop on Hot Topics in Networks (HotNets-VIII, New York City, NY, 2009, pp. 1–6, URL http://conferences.sigcomm.org/hotnets/2009/papers/hotnets2009-final143.pdf, [Accessed on 15-Apr-2018].

[125] S.J. Vaughan-Nichols, Virtualization sparks security concerns, Computer (ISSN: 0018-9162) 41 (8) (2008) 13–15, http://dx.doi.org/10.1109/MC.2008.276.

[126] G. Xiaopeng, W. Sumei, C. Xianqin, VNSS: A network security sandbox for virtual computing environment, in: 2010 IEEE Youth Conference on Information, Computing and Telecommunications, 2010, pp. 395–398.

[127] J.S. Reuben, A survey on virtual machine security, in: TKK T-110.5290 Seminar on Network Security, Helsinki, Finland, 2007, pp. 1–5, URL http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf, [Accessed on 15-Apr-2015.

[128] M. Almorsy, A. Ibrahim, J. Grundy, Adaptive security management in saas applications, in: S. Nepal, M. Pathan (Eds.), Security, Privacy and Trust in Cloud Systems, Springer, ISBN: 978-3-642-38586-5, 2014, pp. 73–102, http://dx.doi.org/10.1007/978-3-642-38586-5_3.

[129] D. Chen, H. Zhao, Data security and privacy protection issues in cloud computing, in: 2012 International Conference on Computer Science and Electronics Engineering, Vol. 1, 2012, pp. 647–651, http://dx.doi.org/10.1109/ICCSEE.2012.193.

[130] S.K. Sood, A combined approach to ensure data security in cloud computing, J. Netw. Comput. Appl. (ISSN: 1084-8045) 35 (6) (2012) 1831–1838, http://dx.doi.org/10.1016/j.jnca.2012.07.007.

[131] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing, in: SAC '12, ACM, New York, NY, USA, ISBN: 978-1-4503-0857-1, 2012, pp. 1427–1434, http://dx.doi.org/10.1145/2245276.2232005.

[132] V. Getov, Cloud adoption issues: interoperability and security, Clouds Big Data Data-intensive Comput. 23 (2013) 53–65, http://dx.doi.org/10.3233/978-1-61499-322-3-53,

[133] B.P. Rimal, A. Jukan, D. Katsaros, Y. Goeleven, Architectural requirements for cloud computing systems: An enterprise cloud approach, J. Grid Comput. (ISSN: 1572-9184) 9 (1) (2011) 3–26, http://dx.doi.org/10.1007/s10723-010-9171-y.

[134] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, A view of cloud computing, Commun. ACM 53 (4) (2010) 50–58, http://dx.doi.org/10.1145/1721654.1721672.

[135] S.P. Ahuja, B. Moore, A survey of cloud computing and social networks, Netw. Commun. Technol. 2 (2) (2013) http://dx.doi.org/10.5539/nct.v2n2p11.

[136] F. Rocha, M. Correia, Lucy in the sky without diamonds: Stealing confidential data in the cloud, in: 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), 2011, pp. 129–134, http://dx.doi.org/10.1109/DSNW.2011.5958798, ISSN 2325-6648.

[137] N. Santos, K.P. Gummadi, R. Rodrigues, Towards trusted cloud computing, in: Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, in: HotCloud'09, USENIX Association, Berkeley, CA, USA, 2009, pp. 1–5, URL https://www.usenix.org/legacy/event/hotcloud09/tech/full_papers/santos.pdf, [Accessed on 24-Feb-2018].

[138] Z. Tan, Y. Niu, Y. Liu, G. Yang, A novel trust model based on SLA and behavior evaluation for clouds, in: 2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016, pp. 581–587, http://dx.doi.org/10.1109/PST.2016.7907020.

[139] G. Aceto, A. Botta, W. De Donato, A. Pescapè, Survey cloud monitoring: A survey, Comput. Netw. (ISSN: 1389-1286) 57 (9) (2013) 2093–2115, http://dx.doi.org/10.1016/j.comnet.2013.04.001.

[140] J.S. Ward, A. Barker, Observing the clouds: a survey and taxonomy of cloud monitoring, J. Cloud Comput. (ISSN: 2192-113X) 3 (1) (2014) 1–30, http://dx.doi.org/10.1186/s13677-014-0024-2.

[141] A.F. Mohammad, H. Mcheick, Cloud services testing: An understanding, Procedia Comput. Sci. (ISSN: 1877-0509) 5 (2011) 513–520, http://dx.doi.org/10.1016/j.procs.2011.07.066.

[142] S. Nachiyappan, S. Justus, Cloud testing tools and its challenges: A comparative study, Procedia Comput. Sci. (ISSN: 1877-0509) 50 (2015) 482–489, http://dx.doi.org/10.1016/j.procs.2015.04.018.

[143] P.T. Endo, M. Rodrigues, G.E. Gonçalves, J. Kelner, D.H. Sadok, C. Curescu, High availability in clouds: systematic review and research challenges, J. Cloud Comput. (ISSN: 2192-113X) 5 (1) (2016) 1–15, http://dx.doi.org/10.1186/s13677-016-0066-8.

[144] M. Jensen, J. Schwenk, The accountability problem of flooding attacks in service-oriented architectures, in: 2009 International Conference on Availability, Reliability and Security, 2009, pp. 25–32, http://dx.doi.org/10.1109/ARES.2009.11.

[145] J. Idziorek, M. Tannian, Exploiting cloud utility models for profit and ruin, in: 2011 IEEE 4th International Conference on Cloud Computing, 2011, pp. 33–40, http://dx.doi.org/10.1109/CLOUD.2011.45, ISSN 2159-6182.

[146] J.C. Roberts II, W. Al-Hamdani, Who Can you trust in the cloud?: A review of security issues within cloud computing, in: Proceedings of the 2011 Information Security Curriculum Development Conference, in: InfoSecCD '11, ACM, New York, NY, USA, ISBN: 978-1-4503-0812-0, 2011, pp. 15–19, http://dx.doi.org/10.1145/2047456.2047458.

[147] H. Thompson, The human element of information security, IEEE Secur. Priv. (ISSN: 1540-7993) 11 (1) (2013) 32–35, http://dx.doi.org/10.1109/MSP.2012.161.

[148] G. Spanoudakis, E. Damiani, A.M. na, Certifying services in cloud: The case for a hybrid, incremental and multi-layer approach, in: 2012 IEEE 14th International Symposium on High-Assurance Systems Engineering, 2012, pp. 175–176, http://dx.doi.org/10.1109/HASE.2012.16, ISSN 1530-2059.

[149] R. Marchini, Cloud Computing: A Practical Introduction to the Legal Issues, BSI, London, ISBN: 978-0580703225, 2010.

[150] P.K. McKinley, F.A. Samimi, J.K. Shapiro, C. Tang, Service clouds: A distributed infrastructure for constructing autonomic communication services, in: 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, 2006, pp. 341–348, http://dx.doi.org/10.1109/DASC.2006.44.

[151] D. Yimam, E.B. Fernandez, A survey of compliance issues in cloud computing, J. Internet Serv. Appl. (ISSN: 1869-0238) 7 (1) (2016) 1–12, http://dx.doi.org/10.1186/s13174-016-0046-8.

[152] K.M. Khan, Q. Malluhi, Establishing trust in cloud computing, IT Prof. (ISSN: 1520-9202) 12 (5) (2010) 20–27, http://dx.doi.org/10.1109/MITP.2010.128.

[153] L.M. Kaufman, Data security in the world of cloud computing, IEEE Secur. Priv. (ISSN: 1540-7993) 7 (4) (2009) 61–64, http://dx.doi.org/10.1109/MSP.2009.87.

[154] A.T. Monfared, M.G. Jaatun, Monitoring intrusions and security breaches in highly distributed cloud environments, in: 2011 IEEE Third International Conference on Cloud Computing Technology and Science, 2011, pp. 772–777, http://dx.doi.org/10.1109/CloudCom.2011.119.

[155] S.M. Habib, S. Ries, M. Muhlhauser, Towards a trust management system for cloud computing, in: 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 2011, pp. 933–939, http://dx.doi.org/10.1109/TrustCom.2011.129, ISSN 2324-898X.

[156] M. Damshenas, A. Dehghantanha, R. Mahmoud, S. bin Shamsuddin, Forensics investigation challenges in cloud computing environments, in: Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012, pp. 190–194, http://dx.doi.org/10.1109/CyberSec.2012.6246092.

[157] S. Hraiz, Challenges of digital forensic investigation in cloud computing, in: 2017 8th International Conference on Information Technology (ICIT), 2017, pp. 568–571, http://dx.doi.org/10.1109/ICITECH.2017.8080060.

[158] M. Taylor, J. Haggerty, D. Gresty, D. Lamb, Forensic investigation of cloud computing systems, Netw. Secur. (ISSN: 1353-4858) 2011 (3) (2011) 4–10, http://dx.doi.org/10.1016/S1353-4858(11)70024-1.

[159] V.M. Katilu, V.N.L. Franqueira, O. Angelopoulou, Challenges of data provenance for cloud forensic investigations, in: 2015 10th International Conference on Availability, Reliability and Security, 2015, pp. 312–317, http://dx.doi.org/10.1109/ARES.2015.54.

[160] S. Sundareswaran, A. Squicciarini, D. Lin, Ensuring distributed accountability for data sharing in the cloud, IEEE Trans. Dependable Secure Comput. (ISSN: 1545-5971) 9 (4) (2012) 556–568, http://dx.doi.org/10.1109/TDSC.2012.26.

[161] V. Sekar, P. Maniatis, Verifiable resource accounting for cloud computing services, in: Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, in: CCSW '11, ACM, New York, NY, USA, ISBN: 978-1-4503-1004-8, 2011, pp. 21–26, http://dx.doi.org/10.1145/2046660.2046666.

[162] Amazon Web Services, AWS Security Best Practices, URL https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf, [Accessed on 12-May-2018], 2016.

[163] Trend Micro, Best Practices for Security and Compliance with Amazon Web Services, URL http://www.trendmicro.it/media/wp/best-practices-security-and-compliance-with-amazon-web-services-whitepaper-en.pdf, [Accessed on 12-May-2018], 2013.

[164] Gartner, IT Glossary, URL https://www.gartner.com/it-glossary/identity-and-access-management-iam/, [Accessed on 05-May-2018], 2018.

[165] A. Buecker, K. Lodewijkx, H. Moss, K. Skapinetz, M. Waidner, Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security, IBM Redpaper, 2009, URL http://www.redbooks.ibm.com/redpapers/pdfs/redp4614.pdf, [Accessed on 05-May-2018].

[166] OASIS, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS, 2005, URL https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, [Accessed on 05-May-2018].

[167] D. Hardt, The OAuth 2.0 Authorization Framework, Tech. Rep. RFC 6749, Internet Engineering Task Force (IETF), URL https://tools.ietf.org/html/rfc6749, [Accessed on 05-May-2018], 2012.

[168] W. Denniss, J. Bradley, OAuth 2.0 for Native Apps, Tech. Rep. RFC 8252, Internet Engineering Task Force (IETF), URL https://tools.ietf.org/html/rfc8252, [Accessed on 05-May-2018], 2017.

[169] N. Sakimura, J. Bradley, M.B. Jones, B. de Medeiros, C. Mortimore, OpenID Connect Core 1.0, Tech. Rep., The OpenID Foundation, URL http://openid.net/specs/openid-connect-core-1_0.html, [Accessed on 05-May-2018], 2014.

[170] Wikipedia, JSON, URL https://en.wikipedia.org/w/index.php?title=JSON&oldid=839464344, [Accessed on 05-May-2018], 2018.

[171] E. T. Bray, The JavaScript Object Notation (JSON) Data Interchange Format, Tech. Rep. RFC 8259, Internet Engineering Task Force (IETF), URL https://tools.ietf.org/html/rfc8259, [Accessed on 12-Jun-2018], 2017.

[172] Wikipedia, Representational state transfer, URL https://en.wikipedia.org/wiki/Representational_state_transfer, [Accessed on 05-May-2018], 2018.

[173] R. Fielding, Architectural Styles and the Design of Network-based Software Architectures, Tech. Rep., University of California, Irvine, URL http://roy.gbiv.com/pubs/dissertation/top.htm, [Accessed on 12-Jun-2018], 2000.

[174] J. Lu, J. Zhang, J. Li, Z. Wan, B. Meng, Automatic verification of security of openid connect protocol with proverif, in: F. Xhafa, L. Barolli, F. Amato (Eds.), Advances on P2P, Parallel, Grid, Cloud and Internet Computing, Springer, Cham, ISBN: 978-3-319-49109-7, 2017, pp. 209–220, URL https://link.springer.com/chapter/10.1007%2F978-3-319-49109-7_20.

[175] B. Blanchet, An efficient cryptographic protocol verifier based on prolog rules, in: Proceedings. 14th IEEE Computer Security Foundations Workshop, 2001, 2001, pp. 82–96, http://dx.doi.org/10.1109/CSFW.2001.930138, ISSN 1063-6900.

[176] P. Siriwardena, Advanced API Security, Apress, Berkeley, CA, ISBN: 978-1-4302-6817-8, 2014.

[177] M. Jones, J. Hildebrand, JSON Web Encryption (JWE), Tech. Rep. RFC 7516, Internet Engineering Task Force (IETF), URL https://tools.ietf.org/html/rfc7516, [Accessed on 12-Jun-2018], 2015.

[178] M. Jones, J. Bradley, N. Sakimura, JSON Web Signature (JWS), Tech. Rep. RFC 7515, Internet Engineering Task Force (IETF), URL https://tools.ietf.org/html/rfc7515, [Accessed on 12-Jun-2018], 2015.

[179] C. Mainka, V. Mladenov, J. Schwenk, T. Wich, Sok: Single sign-on security, in: 2017 IEEE European Symposium on Security and Privacy (EuroS P), 2017, pp. 251–266, http://dx.doi.org/10.1109/EuroSP.2017.32.

[180] E. P. Hunt, K. Grizzle, M. Ansari, E. Wahlstroem, C. Mortimore, System for Cross-domain Identity Management: Protocol (SCIM), Tech. Rep. RFC 7644, Internet Engineering Task Force (IETF), URL https://tools.ietf.org/html/rfc7544, [Accessed on 12-Jun-2018], 2015.

[181] Google, Security Whitepaper: Google Apps Messaging and Collaboration Products, URL https://cryptome.org/2012/12/google-cloud-sec.pdf, [Accessed on 05-May-2018], 2011.

[182] Google, Google Cloud Security Whitepapers, URL https://services.google.com/fh/files/misc/security_whitepapers_march2018.pdf, [Accessed on 11-Jun-2018], 2018.

[183] Microsoft, Securing Microsofts Cloud Infrastructure, URL https://cloudsecurityalliance.org/securing-the-MS-Cloud.pdf, [Accessed on 05-May-2018], 2009.

[184] A. Abdellaoui, Y.I. Khamlichi, H. Chaoui, A novel strong password generator for improving cloud authentication, Procedia Comput. Sci. (ISSN: 1877-0509) 85 (2016) 293–300, http://dx.doi.org/10.1016/j.procs.2016.05.236.

[185] U. Habiba, R. Masood, M.A. Shibli, M.A. Niazi, Cloud identity management security issues & solutions: a taxonomy, Complex Adapt. Syst. Model. (ISSN: 2194-3206) 2 (1) (2014) 1–37, http://dx.doi.org/10.1186/s40294-014-0005-9.

[186] L. Xie, C. Wang, Cloud multidomain access control model based on role and trust-degree, J. Electr. Comput. Eng. 2016 (2016) http://dx.doi.org/10.1155/2016/9820590.

[187] B. Tang, Q. Li, R. Sandhu, A multi-tenant RBAC model for collaborative cloud services, in: 2013 Eleventh Annual Conference on Privacy, Security and Trust, 2013, pp. 229–238, http://dx.doi.org/10.1109/PST.2013.6596058.

[188] K. Beaty, A. Kundu, V. Naik, A. Acharya, Network-level access control management for the cloud, in: 2013 IEEE International Conference on Cloud Engineering (IC2E), 2013, pp. 98–107, http://dx.doi.org/10.1109/IC2E.2013.18.

[189] J. Rosenberg, R. Mahy, P. Matthews, D. Wing, Session Traversal Utilities for NAT (STUN), Tech. Rep. RFC 5389, Internet Engineering Task Force (IETF), URL https://tools.ietf.org/html/rfc5389, [Accessed on 07-Jul-2018], 2008.

[190] N.M. Gonzalez, M.A.T. Rojas, M.V.M. da Silva, F. Redígolo, T.C.M. d. B. Carvalho, C.C. Miers, M. Näslund, A.S. Ahmed, A framework for authentication and authorization credentials in cloud computing, in: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 509–516, http://dx.doi.org/10.1109/TrustCom.2013.63, ISSN 2324-898X.

[191] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, Q. Zhou, FEACS: A flexible and efficient access control scheme for cloud computing, in: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 2014, pp. 310–319, http://dx.doi.org/10.1109/TrustCom.2014.42, ISSN 2324-898X.

[192] X. Liu, Y. Xia, S. Jiang, F. Xia, Y. Wang, Hierarchical attribute-based access control with authentication for outsourced data in cloud computing, in: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 477–484, http://dx.doi.org/10.1109/TrustCom.2013.60, ISSN 2324-898X.

[193] M. Habiba, M.R. Islam, A.B.M.S. Ali, Access control management for cloud, in: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 485–492, http://dx.doi.org/10.1109/TrustCom.2013.61, ISSN 2324-898X.

[194] L. Martin, XTS: A mode of AES for encrypting hard disks, IEEE Secur. Priv. (ISSN: 1540-7993) 8 (3) (2010) 68–69, http://dx.doi.org/10.1109/MSP.2010.111.

[195] H.Y. Lin, W.G. Tzeng, A secure erasure code-based cloud storage system with secure data forwarding, IEEE Trans. Parallel Distrib. Syst. (ISSN: 1045-9219) 23 (6) (2012) 995–1003, http://dx.doi.org/10.1109/TPDS.2011.252.

[196] M. Ahmed, Q.H. Vu, R. Asal, H. Muhairi, C.Y. Yeun, Lightweight secure storage model with fault-tolerance in cloud environment, Electron. Commer. Res. (ISSN: 1389-5753) 14 (3) (2014) 271–291, http://dx.doi.org/10.1007/s10660-014-9140-9.

[197] M. van Dijk, A. Juels, A. Oprea, R.L. Rivest, E. Stefanov, N. Triandopoulos, Hourglass schemes: How to prove that cloud files are encrypted, in: Proceedings of the 2012 ACM Conference on Computer and Communications Security, in: CCS '12, ACM, New York, NY, USA, ISBN: 978-1-4503-1651-4, 2012, pp. 265–280, http://dx.doi.org/10.1145/2382196.2382227.

[198] M. Naehrig, K. Lauter, V. Vaikuntanathan, Can homomorphic encryption be practical? in: Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, in: CCSW '11, ACM, New York, NY, USA, ISBN: 978-1-4503-1004-8, 2011, pp. 113–124, http://dx.doi.org/10.1145/2046660.2046682.

[199] J. Li, S. Chen, D. Song, Security structure of cloud storage based on homomorphic encryption scheme, in: 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, Vol. 01, 2012, pp. 224–227, http://dx.doi.org/10.1109/CCIS.2012.6664401, ISSN 2376-5933.

[200] M. Mani, Enabling secure query processing in the cloud using fully homomorphic encryption, in: Proceedings of the Second Workshop on Data Analytics in the Cloud, in: DanaC '13, ACM, New York, NY, USA, ISBN: 978-1-4503-2202-7, 2013, pp. 36–40, http://dx.doi.org/10.1145/2486767.2486775.

[201] M. Louk, H. Lim, Homomorphic encryption in mobile multi cloud computing, in: 2015 International Conference on Information Networking (ICOIN), 2015, pp. 493–497, http://dx.doi.org/10.1109/ICOIN.2015.7057954, ISSN 1550-445X.

[202] K.E. Makkaoui, A. Ezzati, A.B. Hssane, Challenges of using homomorphic encryption to secure cloud computing, in: 2015 International Conference on Cloud Technologies and Applications (CloudTech), 2015, pp. 1–7, http://dx.doi.org/10.1109/CloudTech.2015.7337011.

[203] Y. Bensitel, R. Romadi, Secure data storage in the cloud with homomorphic encryption, in: 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), 2016, pp. 1–6, http://dx.doi.org/10.1109/CloudTech.2016.7847680.

[204] M.M. Potey, C. Dhote, D.H. Sharma, Homomorphic encryption for security of cloud data, Procedia Comput. Sci. (ISSN: 1877-0509) 79 (2016) 175–181, http://dx.doi.org/10.1016/j.procs.2016.03.023.

[205] I. Jabbar, S. Najim, Using fully homomorphic encryption to secure cloud computing, Internet Things Cloud Comput. (ISSN: 2376-7731) 4 (2) (2016) 13–18, http://dx.doi.org/10.11648/j.iotcc.20160402.12.

[206] M.H. Diallo, B. Hore, E.C. Chang, S. Mehrotra, N. Venkatasubramanian, Cloudprotect: Managing data privacy in cloud applications, in: 2012 IEEE Fifth International Conference on Cloud Computing, 2012, pp. 303–310, http://dx.doi.org/10.1109/CLOUD.2012.122, ISSN 2159-6182.

[207] C. Wang, N. Cao, K. Ren, W. Lou, Enabling secure and efficient ranked keyword search over outsourced cloud data, IEEE Trans. Parallel Distrib. Syst. (ISSN: 1045-9219) 23 (8) (2012) 1467–1479, http://dx.doi.org/10.1109/TPDS.2011.282.

[208] J. Yu, P. Lu, Y. Zhu, G. Xue, M. Li, Toward secure multikeyword top-k retrieval over encrypted cloud data, IEEE Trans. Dependable Secure Comput. (ISSN: 1545-5971) 10 (4) (2013) 239–250, http://dx.doi.org/10.1109/TDSC.2013.9.

[209] L. Wei, M.K. Reiter, Ensuring file authenticity in private DFA evaluation on encrypted files in the cloud, in: J. Crampton, S. Jajodia, K. Mayes (Eds.), Computer Security – ESORICS 2013, Springer, Berlin, Heidelberg, ISBN: 978-3-642-40203-6, 2013, pp. 147–163, http://dx.doi.org/10.1007/978-3-642-40203-6_9.

[210] E. Pattuk, M. Kantarcioglu, V. Khadilkar, H. Ulusoy, S. Mehrotra, Bigsecret: A secure data management framework for key-value stores, in: 2013 IEEE Sixth International Conference on Cloud Computing, 2013, pp. 147–154, http://dx.doi.org/10.1109/CLOUD.2013.37, ISSN 2159-6182.

[211] P.K. Tysowski, M.A. Hasan, Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds, IEEE Trans. Cloud Comput. 1 (2) (2013) 172–186, http://dx.doi.org/10.1109/TCC.2013.11.

[212] C.K. Chu, S.S.M. Chow, W.G. Tzeng, J. Zhou, R.H. Deng, Key-aggregate cryptosystem for scalable data sharing in cloud storage, IEEE Trans. Parallel Distrib. Syst. (ISSN: 1045-9219) 25 (2) (2014) 468–477, http://dx.doi.org/10.1109/TPDS.2013.112.

[213] S. Jajodia, W. Litwin, T. Schwarz S.J., Recoverable encryption through a noised secret over a large cloud, in: A. Hameurlain, J. Küng, R. Wagner (Eds.), Transactions on Large-Scale Data- and Knowledge-Centered Systems IX, Springer, Berlin, Heidelberg, ISBN: 978-3-642-40069-8, 2013, pp. 42–64, http://dx.doi.org/10.1007/978-3-642-40069-8_3.

[214] G. Wang, Q. Liu, J. Wu, Hierarchical attribute-based encryption for fine-grained access control in cloud storage services, in: Proceedings of the 17th ACM Conference on Computer and Communications Security, in: CCS '10, ACM, New York, NY, USA, ISBN: 978-1-4503-0245-6, 2010, pp. 735–737, http://dx.doi.org/10.1145/1866307.1866414.

[215] N.S. Kumar, G.R. Lakshmi, B. Balamurugan, Enhanced attribute based encryption for cloud computing, Procedia Comput. Sci. (ISSN: 1877-0509) 46 (2015) 689–696, http://dx.doi.org/10.1016/j.procs.2015.02.127.

[216] H. Hong, Z. Sun, An efficient and traceable KP-ABS scheme with untrusted attribute authority in cloud computing, J. Cloud Comput. (ISSN: 2192-113X) 5 (1) (2016) 1–8, http://dx.doi.org/10.1186/s13677-016-0052-1.

[217] Q. Gan, X. Wang, D. Wu, Revocable key-aggregate cryptosystem for data sharing in cloud, Secur. Commun. Netw. 2017 (2017) 1–11, http://dx.doi.org/10.1155/2017/2508693.

[218] Y. Wang, D. Yan, F. Li, H. Xiong, A key-insulated proxy re-encryption scheme for data sharing in a cloud environment, Int. J. Netw. Secur. 19 (4) (2017) 623–630, http://dx.doi.org/10.6633/IJNS.201707.19(4).16.

[219] C. Yang, Y. Sun, Q. Wu, Batch attribute-based encryption for secure clouds, Information (ISSN: 2078-2489) 6 (4) (2015) 704–718, http://dx.doi.org/10.3390/info6040704.

[220] Wikipedia, Cryptographic hash function (Message digest), URL https://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=835740775, [Accessed on 6-May-2018], 2018.

[221] Wikipedia, Digital signature, URL https://en.wikipedia.org/w/index.php?title=Digital_signature&oldid=838549835, [Accessed on 6-May-2018], 2018.

[222] Wikipedia, Message authentication code, URL https://en.wikipedia.org/w/index.php?title=Message_authentication_code&oldid=839074550, [Accessed on 6-May-2018], 2018.

[223] A. Singh, K. Chatterjee, A multi-dimensional trust and reputation calculation model for cloud computing environments, in: 2017 ISEA Asia Security and Privacy (ISEASP), 2017, pp. 1–8, http://dx.doi.org/10.1109/ISEASP.2017.7976983.

[224] Wikipedia, MD5, URL https://en.wikipedia.org/w/index.php?title=MD5&oldid=839116210, [Accessed on 6-May-2018], 2018.

[225] Wikipedia, Secure Hash Algorithms, URL https://en.wikipedia.org/w/index.php?title=Secure_Hash_Algorithms&oldid=837517049, [Accessed on 6-May-2018], 2018.

[226] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky, D. Shaket, Venus: Verification for untrusted cloud storage, in: Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, in: CCSW '10, ACM, New York, NY, USA, ISBN: 978-1-4503-0089-6, 2010, pp. 19–30, http://dx.doi.org/10.1145/1866835.1866841.

[227] S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, R.H. Deng, Dynamic secure cloud storage with provenance, in: D. Naccache (Ed.), Cryptography and Security: From Theory to Applications, Springer, Berlin, Heidelberg, 2012, pp. 442–464, http://dx.doi.org/10.1007/978-3-642-28368-0_28.

[228] L. Xu, X. Cao, Y. Zhang, W. Wu, Software service signature (S3) for authentication in cloud computing, Cluster Comput. (ISSN: 1386-7857) 16 (4) (2013) 905–914, http://dx.doi.org/10.1007/s10586-013-0262-y.

[229] B. Wang, S.S.M. Chow, M. Li, H. Li, Storing shared data on the cloud via security-mediator, in: 2013 IEEE 33rd International Conference on Distributed Computing Systems, 2013, pp. 124–133, http://dx.doi.org/10.1109/ICDCS.2013.60, ISSN 1063-6927.

[230] V. Attasena, J. Darmont, N. Harbi, Secret sharing for cloud data security: a survey, VLDB J. (ISSN: 0949-877X) 26 (5) (2017) 657–681, http://dx.doi.org/10.1007/s00778-017-0470-9.

[231] V. Attasena, N. Harbi, J. Darmont, A novel multi-secret sharing approach for secure data warehousing and on-line analysis processing in the cloud, Int. J. Data Warehousing Min. (IJDWM) 11 (2) (2015) 22–43, URL https://EconPapers.repec.org/RePEc:igg:jdwm00:v:11:y:2015:i:2:p:22-43.

[232] R. Shiny, R.S. Shaji, J.P. Jayan, Signature based data auditing under mobile cloud system, in: 2015 Global Conference on Communication Technologies (GCCT), 2015, pp. 565–570.

[233] S. Dey, S. Sampalli, Q. Ye, MDA: message digest-based authentication for mobile cloud computing, J. Cloud Comput. (ISSN: 2192-113X) 5 (1) (2016) 1–13, http://dx.doi.org/10.1186/s13677-016-0068-6.

[234] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, A survey of intrusion detection techniques in Cloud, J. Netw. Comput. Appl. (ISSN: 1084-8045) 36 (1) (2013) 42–57, http://dx.doi.org/10.1016/j.jnca.2012.05.003.

[235] A. Patel, M. Taghavi, K. Bakhtiyari, J.C. Júnior, An intrusion detection and prevention system in cloud computing: A systematic review, J. Netw. Comput. Appl. (ISSN: 1084-8045) 36 (1) (2013) 25–41, http://dx.doi.org/10.1016/j.jnca.2012.08.007.

[236] Z. Chiba, N. Abghour, K. Moussaid, A.E. Omri, M. Rida, A survey of intrusion detection systems for cloud computing environment, in: 2016 International Conference on Engineering MIS (ICEMIS), 2016, pp. 1–13, http://dx.doi.org/10.1109/ICEMIS.2016.7745295.

[237] N. Keegan, S.-Y. Ji, A. Chaudhary, C. Concolato, B. Yu, D.H. Jeong, A survey of cloud-based network intrusion detection analysis, Hum.-Centric Comput. Inf. Sci. (ISSN: 2192-1962) 6 (1) (2016) 1–16, http://dx.doi.org/10.1186/s13673-016-0076-z.

[238] A. Bakshi, Y.B. Dujodwala, Securing cloud from DDOS attacks using intrusion detection system in virtual machine, in: 2010 Second International Conference on Communication Software and Networks, 2010, pp. 260–264, http://dx.doi.org/10.1109/ICCSN.2010.56.

[239] C. Mazzariello, R. Bifulco, R. Canonico, Integrating a network IDS into an open source cloud computing environment, in: 2010 Sixth International Conference on Information Assurance and Security, 2010, pp. 265–270, http://dx.doi.org/10.1109/ISIAS.2010.5604069.

[240] H. Hamad, M. Al-hoby, Managing intrusion detection as a service in cloud networks, Int. J. Comput. Appl. (ISSN: 09758887) 41 (1) (2012) 35–40, URL https://research.ijcaonline.org/volume41/number1/pxc3877533.pdf.

[241] C.N. Modi, D.R. Patel, A. Patel, M. Rajarajan, Integrating signature apriori based network intrusion detection system (NIDS) in cloud computing, Procedia Technol. (ISSN: 2212-0173) 6 (2012) 905–912, http://dx.doi.org/10.1016/j.protcy.2012.10.110.

[242] T. Alharkan, P. Martin, Idsaas: Intrusion detection system as a service in public clouds, in: 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (Ccgrid 2012), 2012, pp. 686–687, http://dx.doi.org/10.1109/CCGrid.2012.81.

[243] J.K. Khatri, M.G. Khilari, Advancement in virtualization based intrusion detection system in cloud environment, Int. J. Sci. Eng. Technol. Res. (IJSETR) (ISSN: 2278-7798) 4 (2015) 1510–1514, URL http://ijsetr.org/wp-content/uploads/2015/05/IJSETR-VOL-4-ISSUE-5-1510-1514.pdf.

[244] D. Singh, D. Patel, B. Borisaniya, C. Modi, Collaborative IDS framework for cloud, Int. J. Netw. Secur. 18 (4) (2016) 699–709, URL http://ijns.femto.com.tw/contents/ijns-v18-n4/ijns-2016-v18-n4-p699-709.pdf.

[245] C.N. Modi, D. Patel, A novel hybrid-network intrusion detection system (H-NIDS) in cloud computing, in: 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2013, pp. 23–30, http://dx.doi.org/10.1109/CICYBS.2013.6597201.

[246] K. Vieira, A. Schulter, C. Westphall, C. Westphall, Intrusion detection for grid and cloud computing, IT Prof. (ISSN: 1520-9202) 12 (4) (2010) 38–43, http://dx.doi.org/10.1109/MITP.2009.89.

[247] J.H. Lee, M.W. Park, J.H. Eom, T.M. Chung, Multi-level intrusion detection system and log management in cloud computing, in: 13th International Conference on Advanced Communication Technology (ICACT2011), 2011, pp. 552–555, ISSN 1738-9445.

[248] J. Arshad, P. Townend, J. Xu, An abstract model for integrated intrusion detection and severity analysis for clouds, Int. J. Cloud Appl. Comput. (ISSN: 2156-1834) 1 (1) (2011) 1–16, http://dx.doi.org/10.4018/ijcac.2011010101.

[249] C.C. Lo, C.C. Huang, J. Ku, A cooperative intrusion detection system framework for cloud computing networks, in: 2010 39th International Conference on Parallel Processing Workshops, 2010, pp. 280–284, http://dx.doi.org/10.1109/ICPPW.2010.46.

[250] A.V. Dastjerdi, K.A. Bakar, S.G.H. Tabatabaei, Distributed intrusion detection in clouds using mobile agents, in: 2009 Third International Conference on Advanced Engineering Computing and Applications in Sciences, 2009, pp. 175–180, http://dx.doi.org/10.1109/ADVCOMP.2009.34.

[251] T. Garfinkel, M. Rosenblum, et al., A virtual machine introspection based architecture for intrusion detection., in: Ndss, Vol. 3, 2003, pp. 191–206, URL http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/13.pdf.

[252] N. Pandeeswari, G. Kumar, Anomaly detection system in cloud environment using Fuzzy clustering based ANN, Mobile Networks Appl. 21 (3) (2016) 494–505, http://dx.doi.org/10.1007/s11036-015-0644-x.

[253] SNORT, SNORT User Manual (2.9.11), URL https://www.snort.org/, [Accessed on 05-May-2018], 2017.

[254] S. Teng, C. Zheng, H. Zhu, D. Liu, W. Zhang, A cooperative intrusion detection model for cloud computing networks, Int. J. Secur. Appl. 8 (3) (2014) 107–118, http://dx.doi.org/10.14257/ijsia.2014.8.3.12.

[255] C. Kahn, D. Bolinger, D. Schnackenberg, Communication in the Common Intrusion Detection Framework (v0.7), URL http://gost.isi.edu/cidf/drafts/communication.txt [Accessed on 05-May-2018], 1998.

[256] M. Ficco, L. Tasquier, R. Aversa, Intrusion detection in federated clouds, Int. J. Comput. Sci. Eng. 13 (3) (2016) 219–232, http://dx.doi.org/10.1504/IJCSE.2016.078929.

[257] G. Somani, M.S. Gaur, D. Sanghi, M. Conti, M. Rajarajan, R. Buyya, Combating ddos attacks in the cloud: Requirements, trends, and future directions, IEEE Cloud Comput. (ISSN: 2325-6095) 4 (1) (2017) 22–32, http://dx.doi.org/10.1109/MCC.2017.14.

[258] S. Yu, Y. Tian, S. Guo, D.O. Wu, CaN we beat ddos attacks in clouds? IEEE Trans. Parallel Distrib. Syst. (ISSN: 1045-9219) 25 (9) (2014) 2245–2254, http://dx.doi.org/10.1109/TPDS.2013.181.

[259] T. Xing, Z. Xiong, D. Huang, D. Medhi, SDNIPS: Enabling software-defined networking based intrusion prevention system in clouds, in: 10th International Conference on Network and Service Management (CNSM) and Workshop, 2014, pp. 308–311, http://dx.doi.org/10.1109/CNSM.2014.7014181, ISSN 2165-9605.

[260] T. Xing, D. Huang, L. Xu, C.J. Chung, P. Khatkar, Snortflow: A openflow-based intrusion prevention system in cloud environment, in: 2013 Second GENI Research and Educational Experiment Workshop, 2013, pp. 89–92, http://dx.doi.org/10.1109/GREE.2013.25.

[261] Y. Lee, W. Kang, H. Son, An internet traffic analysis method with mapreduce, in: 2010 IEEE/IFIP Network Operations and Management Symposium Workshops, 2010, pp. 357–361, http://dx.doi.org/10.1109/NOMSW.2010.5486551.

[262] K. Singh, S.C. Guntuku, A. Thakur, C. Hota, Big data analytics framework for peer-to-peer botnet detection using random forests, Inform. Sci. (ISSN: 0020-0255) 278 (2014) 488–497, http://dx.doi.org/10.1016/j.ins.2014.03.066.

[263] A.H. Bhat, S. Patra, D. Jena, Machine learning approach for intrusion detection on cloud virtual machines, Int. J. Appl. Innovation Eng. Manage. (IJAIEM) (ISSN: 2319-4847) 2 (2013) 57–66, URL http://ijaiem.org/Volume2Issue6/IJAIEM-2013-06-09-029.pdf.

[264] H.C.H. Chen, P.P.C. Lee, Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation, IEEE Trans. Parallel Distrib. Syst. (ISSN: 1045-9219) 25 (2) (2014) 407–416, http://dx.doi.org/10.1109/TPDS.2013.164.

[265] S. Muthurajkumar, K. Kulothungan, M. Vijayalakshmi, N. Jaisankar, A. Kannan, A rough set based feature selection algorithm for effective intrusion detection in cloud model, in: Proc. of Int. Conf. on Advances in Communication, Network, and Computing, 2013, pp. 8–13, URL https://pdfs.semanticscholar.org/518c/43dd6ac4119e992fea5e5e69783ef5754d2c.pdf, [Accessed on 13-May-2018].

[266] OASIS, Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS, 2006, URL https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf, [Accessed on 12-May-2018].

[267] Wikipedia, WS-Security, URL https://en.wikipedia.org/w/index.php?title=WS-Security&oldid=840710777, [Ac- cessed on 12-May-2018], 2018.

[268] E.B. Fernandez, O. Ajaj, I. Buckley, N. Delessy-Gassant, K. Hashizume, M.M. Larrondo-Petrie, A survey of patterns for web services security and reliability standards, Future Internet 4 (2) (2012) 430–450, http://dx.doi.org/10.3390/fi4020430.

[269] OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0 Plus Errata 01, OASIS, URL http://docs.oasis-open.org/xacml/3.0/errata01/os/xacml-3.0-core-spec-errata01-os-complete.pdf, [Accessed on 12- May-2018], 2017.

[270] W3C, XML Key Management Specification (XKMS 2.0), Tech. Rep., The World Wide Web Consortium (W3C), URL https://www.w3.org/TR/xkms2/, [Accessed on 12-May-2018], 2005.

[271] OASIS, Web Services Federation Language (WS-Federation) Version 1.2, OASIS, URL http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf, [Accessed on 12-May-2018], 2009.

[272] OASIS, WS-SecureConversation 1.3, OASIS, URL http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.pdf, [Accessed on 12-May-2018], 2007.

[273] W3C, XML Signature Syntax and Processing Version 1.1, Tech. Rep., The World Wide Web Consortium (W3C), https://www.w3.org/TR/xmldsig-core/, [Accessed on 12-May-2018], 2013.

[274] W3c, xml signature syntax and processing version 1.1, tech. rep., the world wide web consortium (w3c), url , [accessed on 12-may-2018], 2013, 2013, https://www.w3.org/tr/xmldsig-core/.

[275] OASIS, WS-SecurityPolicy 1.2, OASIS, URL http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.2/errata01/os/ws-securitypolicy-1.2-errata01-os-complete.pdf, [Accessed on 12-May-2018], 2012.

[276] OASIS, WS-Trust 1.3, OASIS, URL http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf, [Ac- cessed on 12-May-2018], 2007.

[277] C. Wu, Z. Wang, X. Jiang, Taming hosted hypervisors with (mostly) deprivileged execution, in: NDSS, 2013, pp. 1–15, URL http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/03_3_0.pdf.

[278] E. Fong, V. Okun, Web application scanners: Definitions and functions, in: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007, pp. 1–7, http://dx.doi.org/10.1109/HICSS.2007.611, ISSN 1530-1605.

[279] Wikipedia, Web application security scanner, URL https://en.wikipedia.org/w/index.php?title=Web_application_security_scanner&oldid=834251813, [Accessed on 12-May-2018], 2018.

[280] Wikipedia, Web application security scanner, URL https://en.wikipedia.org/w/index.php?title=Web_application_security_scanner&oldid=834251813, [Accessed on 12-May-2018], 2018.

[281] OWASP, Best Practices: Use of Web Application Firewalls, URL https://www.owasp.org/images/b/b0/Best_ Practices_WAF_v105.en.pdf, [Accessed on 12-May-2018], 2008.

[282] I. Dacosta, S. Chakradeo, M. Ahamad, P. Traynor, One-time cookies: Preventing session hijacking attacks with stateless authentication tokens, ACM Trans. Internet Technol. (ISSN: 1533-5399) 12 (1) (2012) 1–24, http://dx.doi.org/10.1145/2220352.2220353.

[283] S. Gupta, B. Gupta, CSSXC: Context-sensitive sanitization framework for web applications against XSS vulnerabilities in cloud environments, Procedia Comput. Sci. (ISSN: 1877-0509) 85 (2016) 198–205, http://dx.doi.org/10.1016/j.procs.2016.05.211.

[284] R. Akrout, E. Alata, M. Kaaniche, V. Nicomette, An automated black box approach for web vulnerability identification and attack scenario generation, J. Braz. Comput. Soc. (ISSN: 1678-4804) 20 (1) (2014) 1–16, http://dx.doi.org/10.1186/1678-4804-20-4.

[285] D. Mitropoulos, D. Spinellis, Fatal injection: a survey of modern code injection attack countermeasures, Peer J. Comput. Sci. (ISSN: 2376-5992) 3 (2017) 1–36, http://dx.doi.org/10.7717/peerj-cs.136.

[286] J. Mao, Y. Chen, F. Shi, Y. Jia, Z. Liang, Toward exposing timing-based probing attacks in web applications, Sensors (ISSN: 1424-8220) 17 (3) (2017) http://dx.doi.org/10.3390/s17030464.

[287] E.W. Felten, M.A. Schneider, Timing attacks on web privacy, in: Proceedings of the 7th ACM Conference on Computer and Communications Security, in: CCS '00, ACM, New York, NY, USA, 2000, pp. 25–32, http://dx.doi.org/10.1145/352600.352606.

[288] L. Chung, J.C.S. do Prado Leite, On non-functional requirements in software engineering, in: A.T. Borgida, V.K. Chaudhri, P. Giorgini, E.S. Yu (Eds.), Conceptual Modeling: Foundations and Applications: Essays in Honor of John Mylopoulos, Springer, Berlin, Heidelberg, ISBN: 978-3-642-02463-4, 2009, pp. 363–379, http://dx.doi.org/10.1007/978-3-642-02463-4_19.

[289] M. Howard, S. Lipner, The Security Development Lifecycle, Microsoft Press, Redmond, WA, USA, ISBN: 0735622140, 2006.

[290] P. Kashfi, A. Nilsson, R. Feldt, Integrating user experience practices into software development processes: implications of the UX characteristics, PeerJ. Comput. Sci. (ISSN: 2376-5992) 3 (2017) http://dx.doi.org/10.7717/peerj-cs.130.

[291] S. Park, M. Hwang, S. Lee, Y.B. Park, A generic software development process refined from best practices for cloud computing, Sustainability (ISSN: 2071-1050) 7 (5) (2015) 5321–5344, http://dx.doi.org/10.3390/su7055321.

[292] R. Bachmann, A.D. Brucker, Developing secure software, Datenschutz und Datensicherheit - DuD (ISSN: 1862-2607) 38 (4) (2014) 257–261, http://dx.doi.org/10.1007/s11623-014-0102-0.

[293] T. Morris, Trusted platform module, in: H.C.A. van Tilborg, S. Jajodia (Eds.), Encyclopedia of Cryptography and Security, Springer, Boston, MA, ISBN: 978-1-4419-5906-5, 2011, pp. 1332–1335, http://dx.doi.org/10.1007/978-1-4419-5906-5_796.

[294] S. Berger, R. Cáceres, K.A. Goldman, R. Perez, R. Sailer, L. van Doorn, Vtpm: Virtualizing the trusted platform module, in: Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15, in: USENIX-SS'06, USENIX Association, Berkeley, CA, USA, 2006, pp. 305–320, URL https://www.usenix.org/legacy/event/sec06/tech/full_papers/berger/berger.pdf.

[295] P.A. Boampong, L.A. Wahsheh, Different facets of security in the cloud, in: Proceedings of the 15th Communications and Networking Simulation Symposium, in: CNS '12, Society for Computer Simulation International, San Diego, CA, USA, ISBN: 978-1-61839-785-0, 2012, pp. 1–7, URL http://dl.acm.org/citation.cfm?id=2331762.2331767.

[296] N. Santos, R. Rodrigues, K.P. Gummadi, S. Saroiu, Policy-sealed data: A new abstraction for building trusted cloud services, in: Proceedings of the 21st USENIX Conference on Security Symposium, in: Security'12, USENIX Association, Berkeley, CA, USA, 2012, pp. 10–10. URL Accessedon01-Apr-2018.

[297] W. Ma, X. Li, Y. Shi, Y. Guo, A virtual machine cloning approach based on trusted computing, Indonesian Journal of Electrical Engineering and Computer Science 11 (11) (2013) 6935–6942, URL https://pdfs.semanticscholar.org/f6e4/5a77af3298f3ea01bb922e4c5c99998d6bd3.pdf, [Accessed on 02-Mar-2018].

[298] M. Li, W. Zang, K. Bai, M. Yu, P. Liu, Mycloud: Supporting user-configured privacy protection in cloud computing, in: Proceedings of the 29th Annual Computer Security Applications Conference, in: ACSAC '13, ACM, New York, NY, USA, 2013, pp. 59–68, http://dx.doi.org/10.1145/2523649.2523680.

[299] R.B. Lee, Hardware-enhanced access control for cloud computing, in: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies, in: SACMAT '12, ACM, New York, NY, USA, ISBN: 978-1-4503-1295-0, 2012, pp. 1–2, http://dx.doi.org/10.1145/2295136.2295138.

[300] J. Szefer, R.B. Lee, Hardware-enhanced security for cloud computing, in: S. Jajodia, K. Kant, P. Samarati, A. Singhal, V. Swarup, C. Wang (Eds.), Secure Cloud Computing, Springer, New York, NY, USA, ISBN: 978-1-4614-9278-8, 2014, pp. 57–76, http://dx.doi.org/10.1007/978-1-4614-9278-8_3.

[301] Intel, Intel®Software Guard Extensions (Intel®SGX), URL https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html, [Accessed on 11-Apr-2019], 2019.

[302] S. Arnautov, B. Trach, F. Gregor, T. Knauth, A. Martin, C. Priebe, J. Lind, D. Muthukumaran, D. O'Keeffe, M.L. Stillwell, D. Goltzsche, D. Eyers, R. Kapitza, P. Pietzuch, C. Fetzer, SCONE: Secure linux containers with intel SGX, in: 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16), USENIX Association, Savannah, GA, ISBN: 978-1-931971-33-1, 2016, pp. 689–703, URL https://www.usenix.org/conference/osdi16/technical-sessions/presentation/arnautov.

[303] S. Brenner, T. Hundt, G. Mazzeo, R. Kapitza, Secure cloud micro services using intel SGX, in: L.Y. Chen, H.P. Reiser (Eds.), Distributed Applications and Interoperable Systems, Springer International Publishing, Cham, 2017, pp. 177–191.

[304] C. che Tsai, D.E. Porter, M. Vij, Graphene-SGX: A practical library OS for unmodified applications on SGX, in: 2017 USENIX Annual Technical Conference (USENIX ATC 17), USENIX Association, Santa Clara, CA, ISBN: 978-1-931971-38-6, 2017, pp. 645–658, URL https://www.usenix.org/conference/atc17/technical-sessions/presentation/tsai.

[305] F. Campanile, L. Coppolino, S. DAntonio, L. Lev, G. Mazzeo, L. Romano, L. Sgaglione, F. Tessitore, Cloudifying critical applications: A use Case from the power grid domain, in: 2017 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2017, pp. 363–370, http://dx.doi.org/10.1109/PDP.2017.50, ISSN 2377-5750.

[306] SecureCloud, URL https://www.securecloudproject.eu/index.html [Accessed on 11-Apr-2019], 2019.

[307] H. Sun, R. He, Y. Zhang, R. Wang, W.H. Ip, K.L. Yung, Etpm: A trusted cloud platform enclave TPM scheme based on intel sgx technology, Sensors (ISSN: 1424-8220) 18 (11) (2018) http://dx.doi.org/10.3390/s18113807.

[308] D. Kaplan, J. Powell, T. Woller, AMD Memory Encryption, URL http://amd-dev.wpengine.netdna-cdn.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf, [Accessed on 11-Apr-2019], 2016.

[309] R. Boivie, P. Williams, SecureBlue++ : CPU Support for Secure Executables, URL https://domino.research.ibm.com/library/cyberdig.nsf/papers/BE73A643EFE8274B85257B51006760C0/File/rc25369.pdf, [Accessed on 11-Apr-2019], 2013.

[310] S. Mofrad, F. Zhang, S. Lu, W. Shi, A comparison study of intel SGX and AMD memory encryption technology, in: Hardware and Architectural Support for Security and Privacy (HASP'18) , in Conjunction with the 45th International Symposium on Computer Architecture (ISCA'18), Los Angeles, California, 2018, p. 8.

[311] M. Christodorescu, R. Sailer, D.L. Schales, D. Sgandurra, D. Zamboni, Cloud security is not (just) virtualization security: A short paper, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, in: CCSW '09, ACM, New York, NY, USA, ISBN: 978-1-60558-784-4, 2009, pp. 97–102, http://dx.doi.org/10.1145/1655008.1655022.

[312] J. Pfoh, C. Schneider, C. Eckert, A formal model for virtual machine introspection, in: Proceedings of the 1st ACM Workshop on Virtual Machine Security, in: VMSec '09, ACM, New York, NY, USA, ISBN: 978-1-60558-780-6, 2009, pp. 1–10, http://dx.doi.org/10.1145/1655148.1655150.

[313] F. Zhang, J. Wang, K. Sun, A. Stavrou, Hypercheck: A hardware-assisted integrity monitor, IEEE Trans. Dependable Secure Comput. (ISSN: 1545-5971) 11 (4) (2014) 332–344, http://dx.doi.org/10.1109/TDSC.2013.53.

[314] W. Pan, Y. Zhang, M. Yu, J. Jing, Improving virtualization security by splitting hypervisor into smaller components, in: Data and Applications Security and Privacy XXVI, Springer, Berlin, Heidelberg, 2012, pp. 298–313.

[315] Z. Wang, C. Wu, M. Grace, X. Jiang, Isolating commodity hosted hypervisors with hyperlock, in: Proceedings of the 7th ACM European Conference on Computer Systems, in: EuroSys '12, ACM, New York, NY, USA, ISBN: 978-1-4503-1223-3, 2012, pp. 127–140, http://dx.doi.org/10.1145/2168836.2168850.

[316] F. Zhang, J. Chen, H. Chen, B. Zang, Cloudvisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization, in: Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, in: SOSP '11, ACM, New York, NY, USA, ISBN: 978-1-4503-0977-6, 2011, pp. 203–216, http://dx.doi.org/10.1145/2043556.2043576.

[317] M. Zhu, B. Tu, W. Wei, D. Meng, HA-VMSI: A lightweight virtual machine isolation approach with commodity hardware for ARM, in: Proceedings of the 13th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, in: VEE '17, ACM, New York, NY, USA, 2017, pp. 242–256, http://dx.doi.org/10.1145/3050748.3050767.

[318] R. Chandramouli, Security Recommendations for Hypervisor Deployment on Servers (Special Publication 800-125A), National Institute of Standards & Technology, Gaithersburg, MD 20899-8930, USA, 2018, http://dx.doi.org/10.6028/NIST.SP.800-125A, [Accessed on 13-May-2018].

[319] M. Kazim, R. Masood, M.A. Shibli, Securing the virtual machine images in cloud computing, in: Proceedings of the 6th International Conference on Security of Information and Networks, in: SIN '13, ACM, New York, NY, USA, ISBN: 978-1-4503-2498-4, 2013, pp. 425–428, http://dx.doi.org/10.1145/2523514.2523576.

[320] K. Fan, D. Mao, Z. Lu, J. Wu, OPS: Offline patching scheme for the images management in a secure cloud environment, in: 2013 IEEE International Conference on Services Computing, 2013, pp. 587–594, http://dx.doi.org/10.1109/SCC.2013.57.

[321] D. Jeswani, A. Verma, P. Jayachandran, K. Bhattacharya, Imageelves: Rapid and reliable system updates in the cloud, in: 2013 IEEE 33rd International Conference on Distributed Computing Systems, 2013, pp. 390–399, http://dx.doi.org/10.1109/ICDCS.2013.33, ISSN 1063-6927.

[322] A. Choudhary, M.C. Govil, G. Singh, L.K. Awasthi, E.S. Pilli, D. Kapil, A critical survey of live virtual machine migration techniques, J. Cloud Comput. (ISSN: 2192-113X) 6 (1) (2017) 1–41, http://dx.doi.org/10.1186/s13677-017-0092-1.

[323] V. Medina, J.M. García, A survey of migration mechanisms of virtual machines, ACM Comput. Surv. (ISSN: 0360-0300) 46 (3) (2014) 1–33, http://dx.doi.org/10.1145/2492705.

[324] B. Danev, R.J. Masti, G.O. Karame, S. Capkun, Enabling secure VM-vtpm migration in private clouds, in: Proceedings of the 27th Annual Computer Security Applications Conference, in: ACSAC '11, ACM, New York, NY, USA, ISBN: 978-1-4503-0672-0, 2011, pp. 187–196, http://dx.doi.org/10.1145/2076732.2076759.

[325] M. Kazim, R. Masood, M.A. Shibli, A.G. Abbasi, Security aspects of virtualization in cloud computing, in: K. Saeed, R. Chaki, A. Cortesi, S. Wierzchoń (Eds.), Computer Information Systems and Industrial Management, Springer, Berlin, Heidelberg, ISBN: 978-3-642-40925-7, 2013, pp. 229–240, URL https://link.springer.com/content/pdf/10.1007%2F978-3-642-40925-7_22.pdf.

[326] Z. Tavakoli, S. Meier, A. Vensmer, A framework for security context migration in a firewall secured virtual machine environment, in: R. Szabó, A. Vidács (Eds.), Information and Communication Technologies, Springer, Berlin, Heidelberg, ISBN: 978-3-642-32808-4, 2012, pp. 41–51.

[327] X. Wan, X. Zhang, L. Chen, J. Zhu, An improved vtpm migration protocol based trusted channel, in: 2012 International Conference on Systems and Informatics (ICSAI2012), 2012, pp. 870–875, http://dx.doi.org/10.1109/ICSAI.2012.6223146.

[328] M. Aslam, C. Gehrmann, M. Bjorkman, Security and trust preserving VM migrations in public clouds, in: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications(TRUSTCOM), Vol. 00, 2012, pp. 869–876, http://dx.doi.org/10.1109/TrustCom.2012.256.

[329] P. Fan, B. Zhao, Y. Shi, Z. Chen, M. Ni, An improved vtpm-VM live migration protocol, Wuhan Univ. J. Nat. Sci. (ISSN: 1993-4998) 20 (6) (2015) 512–520, http://dx.doi.org/10.1007/s11859-015-1127-4.

[330] H. Zhou, J. Wang, H. Zhang, A trusted VM-vtpm live migration protocol in clouds, Adv. Intell. Syst. Res. (ISSN: 1951-6851) (2013) http://dx.doi.org/10.2991/ccis-13.2013.70, [Accessed on 01-Apr-2018].

[331] S. Sharma, M. Chawla, A three phase optimization method for precopy based VM live migration, Springer Plus (ISSN: 2193-1801) 5 (1) (2016) 1–24, http://dx.doi.org/10.1186/s40064-016-2642-2.

[332] J. Song, W. Liu, F. Yin, C. Gao, TSMC: A novel approach for live virtual machine migration, J. Appl. Math. 2014 (2014) http://dx.doi.org/10.1155/2014/297127, [Accessed on 01-Apr-2018].

[333] M.R. Anala, J. Shetty, G. Shobha, A framework for secure live migration of virtual machines, in: 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013, pp. 243–248, http://dx.doi.org/10.1109/ICACCI.2013.6637178.

[334] Y. Xia, Y. Liu, H. Chen, Architecture support for guest-transparent VM protection from untrusted hypervisor and physical attacks, in: 2013 IEEE 19th International Symposium on High Performance Computer Architecture (HPCA), 2013, pp. 246–257, http://dx.doi.org/10.1109/HPCA.2013.6522323, ISSN 1530-0897.

[335] M.I. Gofman, R. Luo, P. Yang, K. Gopalan, SPARC: A security and privacy aware virtual machinecheckpointing mechanism, in: Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society, in: WPES '11, ACM, New York, NY, USA, ISBN: 978-1-4503-1002-4, 2011, pp. 115–124, http://dx.doi.org/10.1145/2046556.2046571.

[336] L.R. Bays, R.R. Oliveira, M.P. Barcellos, L.P. Gaspary, E.R. Mauro Madeira, Virtual network security: threats, countermeasures, and challenges, J. Internet Serv. Appl. (ISSN: 1869-0238) 6 (1) (2015) 1–19, http://dx.doi.org/10.1186/s13174-014-0015-z.

[337] N.C. Fernandes, O.C.M.B. Duarte, Xnetmon: A network monitor for securing virtual networks, in: 2011 IEEE International Conference on Communications (ICC), 2011, pp. 1–5, http://dx.doi.org/10.1109/icc.2011.5963443, ISSN 1550-3607.

[338] S. Cabuk, C.I. Dalton, H. Ramasamy, M. Schunter, Towards automated provisioning of secure virtualized networks, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, in: CCS '07, ACM, New York, NY, USA, ISBN: 978-1-59593-703-2, 2007, pp. 235–245, http://dx.doi.org/10.1145/1315245.1315275.

[339] D.I. Wolinsky, A. Agrawal, P.O. Boykin, J.R. Davis, A. Ganguly, V. Paramygin, Y.P. Sheng, R.J. Figueiredo, On the design of virtual machine sandboxes for distributed computing in wide-area overlays of virtual workstations, in: First International Workshop on Virtualization Technology in Distributed Computing (VTDC 2006), 2006, http://dx.doi.org/10.1109/VTDC.2006.8, 8–8.

[340] D. Huang, S. Ata, D. Medhi, Establishing secure virtual trust routing and provisioning domains for future internet, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2010.5683661, ISSN 1930-529X.

[341] W.-L. Yeow, C. Westphal, U. Kozat, Designing and embedding reliable virtual infrastructures, in: Proceedings of the Second ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures, in: VISA '10, ACM, New York, NY, USA, ISBN: 978-1-4503-0199-2, 2010, pp. 33–40, http://dx.doi.org/10.1145/1851399.1851406.

[342] H. Moraes, R. Nunes, D. Guede, Dcportalsng: efficient isolation of tenant networks in virtualized datacenters, ICN 2014 : The Thirteenth Int. Conf. Networks (ISSN: 2308-4413) (2014) 230–235, URL http://www.thinkmind.org/download.php?articleid=icn_2014_9_50_30192, [Accessed on 29-Apr-2018].

[343] F. Lombardi, R. Di Pietro, Secure virtualization for cloud computing, J. Netw. Comput. Appl. 34 (4) (2011) 1113–1122, http://dx.doi.org/10.1016/j.jnca.2010.06.008.

[344] X. He, T. Chomsiri, P. Nanda, Z. Tan, Improving cloud network security using the tree-rule firewall, Future Gener. Comput. Syst. (ISSN: 0167-739X) 30 (2014) 116–126, http://dx.doi.org/10.1016/j.future.2013.06.024.

[345] L. Tawalbeh, N.S. Darwazeh, R.S. Al-Qassas, F. AlDosari, A secure cloud computing model based on data classification, Procedia Comput. Sci. (ISSN: 1877-0509) 52 (2015) 1153–1158, http://dx.doi.org/10.1016/j.procs.2015.05.150.

[346] R. Shaikh, M. Sasikumar, Data classification for achieving security in cloud computing, Procedia Comput. Sci. (ISSN: 1877-0509) 45 (2015) 493–498, http://dx.doi.org/10.1016/j.procs.2015.03.087.

[347] K.D. Bowers, A. Juels, A. Oprea, HAIL: A high-availability and integrity layer for cloud storage, in: Proceedings of the 16th ACM Conference on Computer and Communications Security, in: CCS '09, ACM, New York, NY, USA, ISBN: 978-1-60558-894-0, 2009, pp. 187–198, http://dx.doi.org/10.1145/1653662.1653686.

[348] A.F. Barsoum, M.A. Hasan, Provable Possession and Replication of Data over Cloud Servers, Tech. Rep. Report 32, University of Waterloo, URL http://cacr.uwaterloo.ca/techreports/2010/cacr2010-32.pdf, [Accessed on 03-Mar-2018], 2010.

[349] A. Juels, B.S. Kaliski Jr., Pors: Proofs of retrievability for large files, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, in: CCS '07, ACM, New York, NY, USA, 2007, pp. 584–597, http://dx.doi.org/10.1145/1315245.1315317.

[350] H. Shacham, B. Waters, Compact proofs of retrievability, in: J. Pieprzyk (Ed.), Advances in Cryptology - ASIACRYPT 2008, Springer, Berlin, Heidelberg, ISBN: 978-3-540-89255-7, 2008, pp. 90–107, URL https://link.springer.com/content/pdf/10.1007%2F978-3-540-89255-7_7.pdf.

[351] R. Curtmola, O. Khan, R. Burns, Robust remote data checking, in: Proceedings of the 4th ACM International Workshop on Storage Security and Survivability, in: StorageSS '08, ACM, New York, NY, USA, 2008, pp. 63–68, http://dx.doi.org/10.1145/1456469.1456481.

[352] G. Ateniese, R. Di Pietro, L.V. Mancini, G. Tsudik, Scalable and Efficient Provable Data Possession, in: SecureComm '08, ACM, New York, NY, USA, ISBN: 978-1-60558-241-2, 2008, pp. 1–10, http://dx.doi.org/10.1145/1460877.1460889.

[353] C. Erway, A. Küpçü, C. Papamanthou, R. Tamassia, Dynamic provable data possession, in: Proceedings of the 16th ACM Conference on Computer and Communications Security, in: CCS '09, ACM, New York, NY, USA, ISBN: 978-1-60558-894-0, 2009, pp. 213–222, http://dx.doi.org/10.1145/1653662.1653688.

[354] Y. Zhu, H. Hu, G.J. Ahn, M. Yu, Cooperative provable data possession for integrity verification in multicloud storage, IEEE Trans. Parallel Distrib. Syst. 23 (12) (2012) 2231–2244, http://dx.doi.org/10.1109/TPDS.2012.66.

[355] S.A. Ali, M. Ramakrishnan, Secure provable data possession scheme with replication support in the cloud using tweaks, Cluster Comput. (ISSN: 1573-7543) (2017) http://dx.doi.org/10.1007/s10586-017-1075-1.

[356] M.D.H. Parekh, D.R. Sridaran, An analysis of security challenges in cloud computing, International Journal of Advanced Computer Science and Applications 4 (1) (2013) http://dx.doi.org/10.14569/IJACSA.2013.040106.

[357] F. Armknecht, J.-M. Bohli, G.O. Karame, F. Youssef, Transparent data deduplication in the cloud, in: Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security, in: CCS '15, ACM, New York, NY, USA, ISBN: 978-1-4503-3832-5, 2015, pp. 886–900, http://dx.doi.org/10.1145/2810103.2813630.

[358] R. Wang, Research on data security technology based on cloud storage, Procedia Eng. (ISSN: 1877-7058) 174 (2017) 1340–1355, http://dx.doi.org/10.1016/j.proeng.2017.01.286.

[359] J. Reardon, D. Basin, S. Capkun, Sok: Secure data deletion, in: Proceedings of the 2013 IEEE Symposium on Security and Privacy, in: SP '13, IEEE Computer Society, Washington, DC, USA, 2013, pp. 301–315, http://dx.doi.org/10.1109/SP.2013.28.

[360] R. Kissel, A. Regenscheid, M. Scholl, K. Stine, Guidelines for Media Sanitization (NIST SP 800-88 Revision 1), Information Technology Laboratory, NIST, http://dx.doi.org/10.6028/NIST.SP.800-88r1, [Accessed on 12-Mar-2018], 2014.

[361] S.M. Diesburg, A.-I. Wang, A survey of confidential data storage and deletion methods, ACM Comput. Surv. (ISSN: 0360-0300) 43 (1) (2010) 1–37, http://dx.doi.org/10.1145/1824795.1824797.

[362] P.K. Patra, H. Singh, G. Singh, Fault tolerance techniques and comparative implementation in cloud computing, Int. J. Comput. Appl. 64 (14) (2013) 37–41, http://dx.doi.org/10.5120/10705-5643.

[363] H. Hacigumus, B. Iyer, S. Mehrotra, Providing database as a service, in: Proceedings 18th International Conference on Data Engineering, 2002, pp. 29–38, http://dx.doi.org/10.1109/ICDE.2002.994695.

[364] K. Dharsee, E. Johnson, J. Criswell, A software solution for hardware vulnerabilities, in: 2017 IEEE Cybersecurity Development (SecDev), 2017, pp. 27–33, http://dx.doi.org/10.1109/SecDev.2017.18.

[365] G.L. Masala, P. Ruiu, E. Grosso, Biometric authentication and data security in cloud computing, in: K. Daimi (Ed.), Computer and Network Security Essentials, Springer, Cham, 2018, pp. 337–353, http://dx.doi.org/10.1007/978-3-319-58424-9_19.

[366] G. Naveed, R. Batool, Biometric authentication in cloud computing, J. Biometrics Biostat. 06 (05) (2015) http://dx.doi.org/10.4172/2155-6180.1000258.

[367] P. Padma, S. Srinivasan, A survey on biometric based authentication in cloud computing, in: 2016 International Conference on Inventive Computation Technologies (ICICT), IEEE, 2016, pp. 1–5, http://dx.doi.org/10.1109/inventive.2016.7823273.

[368] Y. Nakajima, H. Masutani, W. Shen, H. Tanaka, O. Kamatani, K. Shimano, M. Fukui, R. Kawamura, Design and implementation of virtualized ICT resource management system for carrier network services toward cloud computing era, in: 2013 Proceedings of ITU Kaleidoscope: Building Sustainable Communities, 2013, pp. 1–8.

[369] D. Bernstein, D. Vij, Intercloud security considerations, in: 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 2010, pp. 537–544, http://dx.doi.org/10.1109/CloudCom.2010.82.

[370] C. Rong, S.T. Nguyen, M.G. Jaatun, Beyond lightning: A survey on security challenges in cloud computing, Comput. Electr. Eng. (ISSN: 0045-7906) 39 (1) (2013) 47–54, http://dx.doi.org/10.1016/j.compeleceng.2012.04.015.

[371] R. Kumar, R. Goyal, Assurance of data security and privacy in the cloud: A three-dimensional perspective, Softw. Qual. Prof. 21 (2019) URL http://asq.org/software-quality/2019/03/software-quality/assurance-of-data-security-and-privacy-in-the-cloud-a-three-dimensional-perspective.pdf, [Accessed on 11-Apr-2019].

[372] B.R. Kandukuri, R.P. V., A. Rakshit, Cloud security issues, in: 2009 IEEE International Conference on Services Computing, 2009, pp. 517–520, http://dx.doi.org/10.1109/SCC.2009.84.

[373] X. Li, J. Du, Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing, IET Inf. Secur. (ISSN: 1751-8709) 7 (1) (2013) 39–50, http://dx.doi.org/10.1049/iet-ifs.2012.0232.

[374] M. L.M.assie, B. N.C.hun, D. E.C.uller, The ganglia distributed monitoring system: design, implementation, and experience, Parallel Comput. (ISSN: 0167-8191) 30 (7) (2004) 817–840, http://dx.doi.org/10.1016/j.parco.2004.04.001.

[375] Gangila Project, URL https://github.com/ganglia, [Accessed on 25-Feb-2018], 2018.

[376] Nagios - The Industry Standard In IT Infrastructure Monitoring, URL https://www.nagios.org/, [Accessed on 25-Feb-2018], 2018.

[377] R. Van Renesse, K.P. Birman, W. Vogels, Astrolabe: A robust and scalable technology for distributed system monitoring, management, and data mining, ACM Trans. Comput. Syst. (ISSN: 0734-2071) 21 (2) (2003) 164–206, http://dx.doi.org/10.1145/762483.762485.

[378] collectd – The system statistics collection daemon, URL https://collectd.org/, [Accessed on 25-Feb-2018], 2018.

[379] Riemann, Riemann monitors distributed systems, URL http://riemann.io/, [Accessed on 25-Feb-2018], 2018.

[380] Zabbix, Zabbix - Monitor anything, URL https://www.zabbix.com/, [Accessed on 25-Feb-2018], 2018.

[381] J. Bresnahan, T. Freeman, D. LaBissoniere, K. Keahey, Managing appliance launches in infrastructure clouds, in: Proceedings of the 2011 TeraGrid Conference: Extreme Digital Discovery, in: TG '11, ACM, New York, NY, USA, ISBN: 978-1-4503-0888-5, 2011, pp. 1–7, http://dx.doi.org/10.1145/2016741.2016755.

[382] Sensu, Sensu - Full-stack monitoring for todays business, URL https://sensuapp.org/, [Accessed on 25-Feb-2018], 2018.

[383] K. An, S. Pradhan, F. Caglar, A. Gokhale, A publish/subscribe middleware for dependable and real-time resource monitoring in the cloud, in: Proceedings of the Workshop on Secure and Dependable Middleware for Cloud Monitoring and Management, ACM, New York, NY, USA, ISBN: 978-1-4503-1615-6, 2012, pp. 1–6, http://dx.doi.org/10.1145/2405186.2405189.

[384] B. Konig, J.M.A. Calero, J. Kirschnick, Elastic monitoring framework for cloud infrastructures, IET Commun. (ISSN: 1751-8628) 6 (10) (2012) 1306–1315, http://dx.doi.org/10.1049/iet-com.2011.0200.

[385] J. Povedano-Molina, J.M. Lopez-Vega, J.M. Lopez-Soler, A. Corradi, L. Foschini, DARGOS: A highly adaptable and scalable monitoring architecture for multi-tenant clouds, Future Gener. Comput. Syst. (ISSN: 0167-739X) 29 (8) (2013) 2041–2056, http://dx.doi.org/10.1016/j.future.2013.04.022.

[386] J. Montes, A. Sánchez, B. Memishi, M. Pérez, G. Antoniu, Gmone: A complete approach to cloud monitoring, Future Gener. Comput. Syst. (ISSN: 0167-739X) 29 (8) (2013) 2026–2040, http://dx.doi.org/10.1016/j.future.2013.02.011.

[387] OpenNebula, The simplest cloud management experience, URL https://opennebula.org/, [Accessed on 25-Feb-2018], 2018.

[388] H.T. Kung, C.-K. Lin, D. Vlah, Cloudsense: Continuous fine-grain cloud monitoring with compressive sensing, in: Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing, in: HotCloud'11, USENIX Association, Berkeley, CA, USA, 2011, pp. 21–21. URL https://www.usenix.org/legacy/events/hotcloud11/tech/final_files/Kung.pdf, Acessed on: 25-Feb-2018].

[389] J.S. Ward, A. Barker, Cloud cover: monitoring large-scale clouds with varanus, J. Cloud Comput. (ISSN: 2192-113X) 4 (1) (2015) 1–28, http://dx.doi.org/10.1186/s13677-015-0041-9.

[390] Amazon, Amazon CloudWatch, URL https://aws.amazon.com/cloudwatch/, [Accessed on 25-Feb-2018], 2018.

[391] Google, Google Stackdriver - Monitoring, logging, and diagnostics for applications on Cloud Platform and AWS, URL https://cloud.google.com/stackdriver/, [Accessed on 25-Feb-2018], 2018.

[392] S. Shin, G. Gu, Cloudwatcher: Network security monitoring using openflow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?), in: 2012 20th IEEE International Conference on Network Protocols (ICNP), 2012, pp. 1–6, http://dx.doi.org/10.1109/ICNP.2012.6459946, ISSN 1092-1648.

[393] S. Cai, B. Gallina, D. Nyström, C. Seceleanu, A. Larsson, Design of cloud monitoring systems via DAGGTAX: a Case study, Procedia Comput. Sci. (ISSN: 1877-0509) 109 (2017) 424–431, http://dx.doi.org/10.1016/j.procs.2017.05.412.

[394] S. Cai, B. Gallina, D. Nyström, C. Seceleanu, DAGGTAX: A taxonomy of data aggregation processes, in: Y. Ouhammou, M. Ivanovic, A. Abelló, L. Bellatreche (Eds.), Model and Data Engineering, Springer International Publishing, Cham, 2017, pp. 324–339, URL https://link.springer.com/chapter/10.1007/978-3-319-66854-3_25.

[395] S. Shetty, Auditing and analysis of network traffic in cloud environment, in: 2013 IEEE Ninth World Congress on Services, 2013, pp. 260–267, http://dx.doi.org/10.1109/SERVICES.2013.42, ISSN 2378-3818.

[396] M. Lemoudden, M. Amar, B.E. Ouahidi, A binary-based mapreduce analysis for cloud logs, Procedia Comput. Sci. (ISSN: 1877-0509) 83 (2016) 1213–1218, http://dx.doi.org/10.1016/j.procs.2016.04.253.

[397] S. Muthurajkumar, S. Ganapathy, M. Vijayalakshmi, A. Kannan, Secured temporal log management techniques for cloud, Procedia Comput. Sci. (ISSN: 1877-0509) 46 (2015) 589–595, http://dx.doi.org/10.1016/j.procs.2015.02.098.

[398] H. Chen, S. Tu, C. Zhao, Y. Huang, Provenance cloud security auditing system based on log analysis, in: 2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS), 2016, pp. 155–159, http://dx.doi.org/10.1109/ICOACS.2016.7563069.

[399] C.H. Suen, R.K.L. Ko, Y.S. Tan, P. Jagadpramana, B.S. Lee, S2logger: End-to-end data tracking mechanism for cloud data provenance, in: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 594–602, http://dx.doi.org/10.1109/TrustCom.2013.73, ISSN 2324-898X.

[400] P. Zech, Risk-based security testing in cloud computing environments, in: 2011 Fourth IEEE International Conference on Software Testing, Verification and Validation, 2011, pp. 411–414, http://dx.doi.org/10.1109/ICST.2011.23, ISSN 2159-4848.

[401] W.T. Tsai, P. Zhong, J. Balasooriya, Y. Chen, X. Bai, J. Elston, An approach for service composition and testing for cloud computing, in: 2011 Tenth International Symposium on Autonomous Decentralized Systems, 2011, pp. 631–636, http://dx.doi.org/10.1109/ISADS.2011.90, ISSN 1541-0056.

[402] J. Moreno, A testing framework for cloud storage systems, (Master's thesis), ETH Zürich, URL https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/152294/eth-1987-01.pdf?sequence=1&isAllowed=y, [Accessed on 02-Mar-2018], 2010.

[403] C. Pham, D. Chen, Z. Kalbarczyk, R.K. Iyer, Cloudval: A framework for validation of virtualization environment in cloud infrastructure, in: 2011 IEEE/IFIP 41st International Conference on Dependable Systems Networks (DSN), 2011, pp. 189–196, http://dx.doi.org/10.1109/DSN.2011.5958218, ISSN 1530-0889.

[404] T. Siddiqui, R. Ahmad, A review on software testing approaches for cloud applications, Perspectives Sci. (ISSN: 2213-0209) 8 (2016) 689–691, http://dx.doi.org/10.1016/j.pisc.2016.06.060.
[405] D. Dalalana Bertoglio, A.F. Zorzo, Overview and open issues on penetration test, J. Braz. Comput. Soc. (ISSN: 1678-4804) 23 (1) (2017) 1–16, http://dx.doi.org/10.1186/s13173-017-0051-1.
[406] P. Ping, Z. Xuan, M. Xinyue, Research on security test for application software based on SPN, Procedia Eng. (ISSN: 1877-7058) 174 (2017) 1140–1147, http://dx.doi.org/10.1016/j.proeng.2017.01.267.
[407] D. Jayasinghe, G. Swint, S. Malkowski, J. Li, Q. Wang, J. Park, C. Pu, Expertus: A generator approach to automate performance testing in iaas clouds, in: 2012 IEEE Fifth International Conference on Cloud Computing, 2012, pp. 115–122, http://dx.doi.org/10.1109/CLOUD.2012.98, ISSN 2159-6182.
[408] G. Candea, S. Bucur, C. Zamfir, Automated software testing as a service, in: Proceedings of the 1st ACM Symposium on Cloud Computing, in: SoCC '10, ACM, New York, NY, USA, 2010, pp. 155–160, http://dx.doi.org/10.1145/1807128.1807153.
[409] L. Yu, W.T. Tsai, X. Chen, L. Liu, Y. Zhao, L. Tang, W. Zhao, Testing as a service over cloud, in: 2010 Fifth IEEE International Symposium on Service Oriented System Engineering, 2010, pp. 181–188, http://dx.doi.org/10.1109/SOSE.2010.36.
[410] B. Jin, Y. Wang, Z. Liu, J. Xue, A trust model based on cloud model and Bayesian networks, Procedia Environ. Sci. (ISSN: 1878-0296) 11 (2011) 452–459, http://dx.doi.org/10.1016/j.proenv.2011.12.072.
[411] N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho, M. Simplicio, M. Naslund, M. Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing, in: 2011 IEEE Third International Conference on Cloud Computing Technology and Science, 2011, pp. 231–238, http://dx.doi.org/10.1109/CloudCom.2011.39.
[412] H. Banirostam, A. Hedayati, A.K. Zadeh, E. Shamsinezhad, A trust based approach for increasing security in cloud computing infrastructure, in: 2013 UKSim 15th International Conference on Computer Modelling and Simulation, 2013, pp. 717–721, http://dx.doi.org/10.1109/UKSim.2013.39.
[413] S. Rizvi, K. Cover, C. Gates, A trusted third-party (TTP) based encryption scheme for ensuring data confidentiality in cloud environment, Procedia Comput. Sci. (ISSN: 1877-0509) 36 (2014) 381–386, http://dx.doi.org/10.1016/j.procs.2014.09.009.
[414] D. Contractor, D.R. Patel, Accountability in cloud computing by means of chain of trust, Int. J. Network Secur. 19 (2017) 251–259, URL http://ijns.femto.com.tw/contents/ijns-v19-n2/ijns-2017-v19-n2-p251-259.pdf, [Accessed on 02-Mar-2018].
[415] S. Cimato, E. Damiani, F. Zavatarelli, R. Menicocci, Towards the certification of cloud services, in: 2013 IEEE Ninth World Congress on Services, 2013, pp. 92–97, http://dx.doi.org/10.1109/SERVICES.2013.16, ISSN 2378-3818.
[416] S. Katopodis, G. Spanoudakis, K. Mahbub, Towards hybrid cloud service certification models, in: 2014 IEEE International Conference on Services Computing, 2014, pp. 394–399, http://dx.doi.org/10.1109/SCC.2014.59.
[417] P. Stephanow, K. Khajehmoogahi, Towards continuous security certification of software-as-a-service applications using web application testing techniques, in: 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), 2017, pp. 931–938, http://dx.doi.org/10.1109/AINA.2017.107, ISSN 1550-445X.
[418] M. Anisetti, C. Ardagna, E. Damiani, F. Gaudenzi, A semi-automatic and trustworthy scheme for continuous cloud service certification, IEEE Trans. Serv. Comput. PP (99) (2017) http://dx.doi.org/10.1109/TSC.2017.2657505, 1–1.
[419] M. Anisetti, C.A. Ardagna, E. Damiani, A.M. na, G. Spanoudakis, Towards transparent and trustworthy cloud, IEEE Cloud Comput. 4 (3) (2017b) 40–48, http://dx.doi.org/10.1109/MCC.2017.51.
[420] H. Foster, G. Spanoudakis, K. Mahbub, Formal certification and compliance for run-time service environments, in: 2012 IEEE Ninth International Conference on Services Computing, 2012, pp. 17–24, http://dx.doi.org/10.1109/SCC.2012.23.
[421] M. Anisetti, C.A. Ardagna, E. Damiani, A low-cost security certification scheme for evolving services, in: 2012 IEEE 19th International Conference on Web Services, 2012, pp. 122–129, http://dx.doi.org/10.1109/ICWS.2012.53.
[422] M. Anisetti, C.A. Ardagna, E. Damiani, F. Saonara, A test-based security certification scheme for web services, ACM Trans. Web (ISSN: 1559-1131) 7 (2) (2013) 1–41, http://dx.doi.org/10.1145/2460383.2460384.
[423] M. Anisetti, C.A. Ardagna, E. Damiani, A test-based incremental security certification scheme for cloud-based systems, in: 2015 IEEE International Conference on Services Computing, 2015, pp. 736–741, http://dx.doi.org/10.1109/SCC.2015.104.
[424] M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S.U. Khan, R. Buyya, A.Y. Zomaya, Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues, ACM Comput. Surv. 47 (4) (2015) 1–34, http://dx.doi.org/10.1145/2764465.
[425] C. Wang, K. Ren, W. Lou, J. Li, Toward publicly auditable secure cloud data storage services, IEEE Network (ISSN: 0890-8044) 24 (4) (2010) 19–24, http://dx.doi.org/10.1109/MNET.2010.5510914.
[426] K. Yang, X. Jia, An efficient and secure dynamic auditing protocol for data storage in cloud computing, IEEE Trans. Parallel Distrib. Syst. (ISSN: 1045-9219) 24 (9) (2013) 1717–1726, http://dx.doi.org/10.1109/TPDS.2012.278.
[427] D. Xiao, Y. Yang, W. Yao, C. Wu, J. Liu, Y. Yang, Multiple-file remote data checking for cloud storage, Comput. Secur. (ISSN: 0167-4048) 31 (2) (2012) 192–205, http://dx.doi.org/10.1016/j.cose.2011.12.005.
[428] R. Mukundan, S. Madria, M. Linderman, Efficient integrity verification of replicated data in cloud using homomorphic encryption, Distrib. Parallel Databases (ISSN: 1573-7578) 32 (4) (2014) 507–534, http://dx.doi.org/10.1007/s10619-014-7151-0.
[429] M. Yi, J. Wei, L. Song, Efficient integrity verification of replicated data in cloud computing system, Comput. Secur. (ISSN: 0167-4048) 65 (2017) 202–212, http://dx.doi.org/10.1016/j.cose.2016.11.003.
[430] B. Chen, R. Curtmola, G. Ateniese, R. Burns, Remote data checking for network coding-based distributed storage systems, in: Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, in: CCSW '10, ACM, New York, NY, USA, ISBN: 978-1-4503-0089-6, 2010, pp. 31–42, http://dx.doi.org/10.1145/1866835.1866842.
[431] L. Anh, A. Markopoulou, NC-Audit: Auditing for network coding storage, in: 2012 International Symposium on Network Coding (NetCod), 2012, pp. 155–160, http://dx.doi.org/10.1109/NETCOD.2012.6261901, ISSN 2374-9660.
[432] Y. Hu, H.C.H. Chen, P.P.C. Lee, Y. Tang, Nccloud: Applying network coding for the storage repair in a cloud-of-clouds, in: Proceedings of the 10th USENIX Conference on File and Storage Technologies, in: FAST'12, USENIX Association, Berkeley, CA, USA, 2012, pp. 21–21. URL http://www.usenix.net/legacy/events/fast12/tech/full_papers/Hu.pdf, [Accessed on 03-Mar-2018].
[433] R. Saxena, S. Dey, Cloud audit: A data integrity verification approach for cloud computing, Procedia Comput. Sci. (ISSN: 1877-0509) 89 (2016) 142–151, http://dx.doi.org/10.1016/j.procs.2016.06.024.
[434] O. Kwon, D. Koo, Y. Shin, H. Yoon, A secure and efficient audit mechanism for dynamic shared data in cloud storage, The Scientific World Journal 2014 (2014) 1–10, URL http://downloads.hindawi.com/journals/tswj/2014/820391.pdf, [Accessed on 03-Mar-2014].
[435] D. Kim, I.R. Jeong, Certificateless public auditing protocol with constant verification time, Secur. Commun. Netw. 2017 (2017) 1–14, http://dx.doi.org/10.1155/2017/6758618, [Accessed on 03-Mar-2018].
[436] H. Tian, Y. Chen, C.C. Chang, H. Jiang, Y. Huang, Y. Chen, J. Liu, Dynamic-hash-table based public auditing for secure cloud storage, IEEE Trans. Serv. Comput. (ISSN: 1939-1374) 10 (5) (2017) 701–714, http://dx.doi.org/10.1109/TSC.2015.2512589.
[437] M. Zhou, R. Zhang, W. Xie, W. Qian, A. Zhou, Security and privacy in cloud computing: A survey, in: 2010 Sixth International Conference on Semantics, Knowledge and Grids, 2010, pp. 105–112, http://dx.doi.org/10.1109/SKG.2010.19.
[438] S. Zawoad, A.K. Dutta, R. Hasan, Seclaas: Secure logging-as-a-service for cloud forensics, in: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, in: ASIA CCS '13, ACM, New York, NY, USA, ISBN: 978-1-4503-1767-2, 2013, pp. 219–230, http://dx.doi.org/10.1145/2484313.2484342.
[439] B. Martini, K.K.R. Choo, Remote programmatic vcloud forensics: A six-step collection process and a proof of concept, in: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 2014, pp. 935–942, http://dx.doi.org/10.1109/TrustCom.2014.124, ISSN 2324-898X.
[440] V. Roussev, S. McCulley, Forensic analysis of cloud-native artifacts, Digit. Investigation 16 (2016) S104–S113, http://dx.doi.org/10.1016/j.diin.2016.01.013.
[441] S. Khan, A. Gani, A.W.A. Wahab, M.A. Bagiwa, M. Shiraz, S.U. Khan, R. Buyya, A.Y. Zomaya, Cloud log forensics: Foundations, state of the art, and future directions, ACM Comput. Surv. (ISSN: 0360-0300) 49 (1) (2016) 1–42, http://dx.doi.org/10.1145/2906149.
[442] J. Dykstra, A.T. Sherman, Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques, Digit. Investigation 9 (2012) S90–S98, http://dx.doi.org/10.1016/j.diin.2012.05.001.
[443] K.K.R. Choo, C. Esposito, A. Castiglione, Evidence and forensics in the cloud: Challenges and future research directions, IEEE Cloud Comput. 4 (3) (2017) 14–19, http://dx.doi.org/10.1109/MCC.2017.39.
[444] N.H.A. Rahman, W.B. Glisson, Y. Yang, K.K.R. Choo, Forensic-by-design framework for cyber-physical cloud systems, IEEE Cloud Comput. (ISSN: 2325-6095) 3 (1) (2016) 50–59, http://dx.doi.org/10.1109/MCC.2016.5.

[445] S. Nanda, R.A. Hansen, Forensics as a service: Three-tier architecture for cloud based forensic analysis, in: 2016 15th International Symposium on Parallel and Distributed Computing (ISPDC), 2016, pp. 178–183, http://dx.doi.org/10.1109/ISPDC.2016.31.
[446] K.W. Park, J. Han, J. Chung, K.H. Park, THEMIS: A mutually verifiable billing system for the cloud computing environment, IEEE Trans. Serv. Comput. (ISSN: 1939-1374) 6 (3) (2013) 300–313, http://dx.doi.org/10.1109/TSC.2012.1.
[447] T. Mather, S. Kumaraswamy, S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, Inc., 2009, ISBN 0596802765, 9780596802769.
[448] L. Malina, J. Hajny, P. Dzurenda, V. Zeman, Privacy-preserving security solution for cloud services, J. Appl. Res. Technol. (ISSN: 1665-6423) 13 (1) (2015) 20–31, http://dx.doi.org/10.1016/S1665-6423(15)30002-X.
[449] M.I. Salam, W.-C. Yau, J.-J. Chin, S.-H. Heng, H.-C. Ling, R.C.-W. Phan, G.S. Poh, S.-Y. Tan, W.-S. Yap, Implementation of searchable symmetric encryption for privacy-preserving keyword search on cloud storage, Human-centric Comput. Inf. Sci. 5 (1) (2015) 1–16, http://dx.doi.org/10.1186/s13673-015-0039-9.
[450] T. Tu, L. Rao, H. Zhang, Q. Wen, J. Xiao, Privacy-preserving outsourced auditing scheme for dynamic data storage in cloud, Secur. Commun. Netw. 2017 (2017) 1–17, http://dx.doi.org/10.1155/2017/4603237, [Accessed on 04-Mar-2018].
[451] R. Ranchal, B. Bhargava, R. Fernando, H. Lei, Z. Jin, Privacy preserving access control in service-oriented architecture, in: 2016 IEEE International Conference on Web Services (ICWS), 2016, pp. 412–419, http://dx.doi.org/10.1109/ICWS.2016.60.
[452] F. Hörandner, S. Krenn, A. Migliavacca, F. Thiemer, B. Zwattendorfer, Credential: A framework for privacy-preserving cloud-based data sharing, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 742–749, http://dx.doi.org/10.1109/ARES.2016.79.
[453] A. Razaque, S.S. Rizvi, Privacy preserving model: a new scheme for auditing cloud stakeholders, J. Cloud Comput. (ISSN: 2192-113X) 6 (1) (2017) 1–17, http://dx.doi.org/10.1186/s13677-017-0076-1.
[454] M.Q. Hong, P.Y. Wang, W.B. Zhao, Homomorphic encryption scheme based on elliptic curve cryptography for privacy protection of cloud computing, in: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016, pp. 152–157, http://dx.doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.51.
[455] N. Kaaniche, A. Boudguiga, M. Laurent, ID Based cryptography for cloud data storage, in: 2013 IEEE Sixth International Conference on Cloud Computing, 2013, pp. 375–382, http://dx.doi.org/10.1109/CLOUD.2013.80, ISSN 2159-6182.
[456] F. Benali, N. Bennani, G. Gianini, S. Cimato, A distributed and privacy-preserving method for network intrusion detection, in: R. Meersman, T. Dillon, P. Herrero (Eds.), On the Move To Meaningful Internet Systems, OTM 2010, Springer, Berlin, Heidelberg, ISBN: 978-3-642-16949-6, 2010, pp. 861–875.
[457] U. Khalid, A. Ghafoor, M. Irum, M.A. Shibli, Cloud based secure and privacy enhanced authentication & authorization protocol, Procedia Comput. Sci. (ISSN: 1877-0509) 22 (2013) 680–688, http://dx.doi.org/10.1016/j.procs.2013.09.149.
[458] T. Jung, X.Y. Li, Z. Wan, M. Wan, Privacy preserving cloud data access with multi-authorities, in: 2013 Proceedings IEEE INFOCOM, 2013, pp. 2625–2633, http://dx.doi.org/10.1109/INFCOM.2013.6567070, ISSN 0743-166X.
[459] Wikipedia, STRIDE (security), URL https://en.wikipedia.org/wiki/STRIDE_(security), [Accessed on 10-Jul-2018], 2018.
[460] Microsoft, The STRIDE Threat Model, URL https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20), [Accessed on 10-Jul-2018], 2009.
[461] R. Scandariato, K. Wuyts, W. Joosen, A descriptive study of microsoft's threat modeling technique, Requir. Eng. (ISSN: 0947-3602) 20 (2) (2015) 163–180, http://dx.doi.org/10.1007/s00766-013-0195-2.
[462] A. Abraham, A. Happe, A. Hudic, S. Krenn, N. McDonnell, C. Striecks, F. Thiemer, CREDENTIAL - D2.2 System Security Requirements, Risk and Threat Analysis, Tech. Rep. 653454: H2020-DS-2014-1, CREDENTIAL Consortium, URL https://credential.eu/wp-content/uploads/2017/06/CREDENTIAL-D2.2-System-security-requirements-v1.0.pdf, [Accessed on 10-Jul-2018], 2016.
[463] S. Krishnan, A Hybrid Approach to Threat Modelling, URL https://blogs.sans.org/appsecstreetfighter/files/2017/03/A-Hybrid-Approach-to-Threat-Modelling.pdf, [Accessed on 10-Jul-2018], 2017.
[464] L. Desmet, B. Jacobs, F. Piessens, W. Joosen, Threat modelling for web services based web applications, in: D. Chadwick, B. Preneel (Eds.), Communications and Multimedia Security, Springer US, 2005, pp. 131–144.
[465] CSA, Top Threats to Cloud Computing Plus: Industry Insights, Tech. Rep., Cloud Security Alliance, URL https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf, [Accessed on 10-Feb-2018], 2017.
[466] S.P. Ahuja, D. Komathukattil, A survey of the state of cloud security, Network Commun. Technol. 1 (2) (2012) 66–75, http://dx.doi.org/10.5539/nct.v1n2p66, ISSN 1927-064X, 1927-0658.
[467] M.Y. Wu, T.H. Lee, Design and implementation of cloud API access control based on oauth, in: IEEE 2013 Tencon - Spring, 2013, pp. 485–489, http://dx.doi.org/10.1109/TENCONSpring.2013.6584492.
[468] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. Serv. Comput. (ISSN: 1939-1374) 5 (2) (2012) 220–232, http://dx.doi.org/10.1109/TSC.2011.24.
[469] R.N. Akram, R.K.L. Ko, Digital trust - trusted computing and beyond: A position paper, in: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 2014, pp. 884–892, http://dx.doi.org/10.1109/TrustCom.2014.116, ISSN 2324-898X.
[470] C.P. Pfleeger, S.L. Pfleeger, J. Margulies, Security in Computing, fifth ed., Prentice Hall, ISBN: 978-0-13-408504-3, 2015.
[471] P. Manuel, A trust model of cloud computing based on quality of service, Ann. Oper. Res. (ISSN: 1572-9338) 233 (1) (2015) 281–292, http://dx.doi.org/10.1007/s10479-013-1380-x.
[472] N. Iltaf, A. Ghafoor, M. Hussain, Modeling interaction using trust and recommendation in ubiquitous computing environment, EURASIP J. Wireless Commun. Networking (ISSN: 1687-1499) 2012 (1) (2012) 1–13, http://dx.doi.org/10.1186/1687-1499-2012-119.
[473] S. Shenai, M. Aramudhan, A federated cloud computing model with self-organizing capability using trust negotiation, in: 2017 International Conference on IoT and Application (ICIOT), 2017, pp. 1–6, http://dx.doi.org/10.1109/ICIOTA.2017.8073605.
[474] A. Ali, M. Ahmed, A. Khan, M. Ilyas, M.S. Razzaq, A trust management system model for cloud, in: 2017 International Symposium on Networks, Computers and Communications (ISNCC), 2017, pp. 1–6, http://dx.doi.org/10.1109/ISNCC.2017.8072029.
[475] E.G. Abdallah, M. Zulkernine, Y.X. Gu, C. Liem, TRUST-CAP: A trust model for cloud-based applications, in: 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Vol. 2, 2017, pp. 584–589, http://dx.doi.org/10.1109/COMPSAC.2017.256, ISSN 0730-3157.
[476] M.J. Sule, M. Li, G. Taylor, Trust modeling in cloud computing, in: 2016 IEEE Symposium on Service-Oriented System Engineering (SOSE), 2016, pp. 60–65, http://dx.doi.org/10.1109/SOSE.2016.32.
[477] G. D' Angelo, S. Rampone, F. Palmieri, An artificial intelligence-based trust model for pervasive computing, in: 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015, pp. 701–706, http://dx.doi.org/10.1109/3PGCIC.2015.94.
[478] S. Rizvi, J. Ryoo, Y. Liu, D. Zazworsky, A. Cappeta, A centralized trust model approach for cloud computing, in: 2014 23rd Wireless and Optical Communication Conference (WOCC), 2014, pp. 1–6, http://dx.doi.org/10.1109/WOCC.2014.6839923.
[479] S.M. Habib, S. Hauke, S. Ries, M. Mühlhäuser, Trust as a facilitator in cloud computing: a survey, J. Cloud Comput.: Adv. Syst. Appl. (ISSN: 2192-113X) 1 (1) (2012) 1–18, http://dx.doi.org/10.1186/2192-113X-1-19.
[480] J. Huang, D.M. Nicol, Trust mechanisms for cloud computing, J. Cloud Comput.: Adv. Syst. Appl. (ISSN: 2192-113X) 2 (1) (2013) 1–14, http://dx.doi.org/10.1186/2192-113X-2-9.
[481] C. Lynch, Big data: How do your data grow? Nature 455 (7209) (2008) 28–29, http://dx.doi.org/10.1038/455028a, [Accessed on 21-Mar-2018].
[482] Apache, Apache Hadoop, Tech. Rep. 2.9.1, Apache Software Foundation, URL http://hadoop.apache.org/docs/stable/index.html, [Accessed on 10-Jul-2018], 2018.
[483] Apache, Hadoop Distributed File System (HDFS), Tech. Rep. 2.9.1, Apache Software Foundation, URL http://hadoop.apache.org/docs/stable/hadoop-project-dist/hadoop-hdfs/HdfsDesign.html, [Accessed on 10-Jul-2018], 2018.
[484] Apache, MapReduce, Tech. Rep. 2.9.1, Apache Software Foundation, URL http://hadoop.apache.org/docs/stable/hadoop-mapreduce-client/hadoop-mapreduce-client-core/MapReduceTutorial.html, [Accessed on 10-Jul-2018], 2018.
[485] S. Ghemawat, H. Gobioff, S.-T. Leung, The google file system, in: Proceedings of the 19th ACM Symposium on Operating Systems Principles, 2003, pp. 20–43, URL https://storage.googleapis.com/pub-tools-public-publication-data/pdf/035fc972c796d33122033a0614bc94cff1527999.pdf.
[486] A. Gholami, E. Laure, Big data security and privacy issues in the cloud, Int. J. Network Secur. Appl. (IJNSA) (2016) URL http://aircconline.com/ijnsa/V8N1/8116ijnsa04.pdf, [Accessed on 21-Mar-2018].
[487] K.A. Salleh, L. Janczewski, Technological, organizational and environmental security and privacy issues of big data: A literature review, Procedia Comput. Sci. (ISSN: 1877-0509) 100 (2016) 19–28, http://dx.doi.org/10.1016/j.procs.2016.09.119.

[488] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, J. Al-Jaroodi, Applications of big data to smart cities, J. Internet Serv. Appl. (ISSN: 1869-0238) 6 (1) (2015) 1–15, http://dx.doi.org/10.1186/s13174-015-0041-5.

[489] S. Li, T. Zhang, J. Gao, Y. Park, A sticky policy framework for big data security, in: Proceedings of the 2015 IEEE First International Conference on Big Data Computing Service and Applications, in: BIGDATASERVICE '15, IEEE Computer Society, Washington, DC, USA, ISBN: 978-1-4799-8128-1, 2015, pp. 130–137, http://dx.doi.org/10.1109/BigDataService.2015.71.

[490] S. Pearson, M.C. Mont, Sticky policies: An approach for managing privacy across multiple parties, Computer (ISSN: 0018-9162) 44 (2011) 60–68, http://dx.doi.org/10.1109/MC.2011.225.

[491] K. Gai, M. Qiu, H. Zhao, Security-aware efficient mass distributed storage approach for cloud systems in big data, in: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), Vol. 00, 2016, pp. 140–145, http://dx.doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.68.

[492] T.Y. Win, H. Tianfield, Q. Mair, Big data based security analytics for protecting virtualized infrastructures in cloud computing, IEEE Trans. Big Data (ISSN: 2332-7790) 4 (1) (2018) 11–25, http://dx.doi.org/10.1109/TBDATA.2017.2715335.

[493] K. Abouelmehdi, A. Beni-Hessane, H. Khaloufi, Big healthcare data: preserving security and privacy, J. Big Data (ISSN: 2196-1115) 5 (1) (2018) 1–18, http://dx.doi.org/10.1186/s40537-017-0110-7.

[494] G. Manogaran, C. Thota, M.V. Kumar, Metaclouddatastorage architecture for big data security in cloud computing, Procedia Comput. Sci. (ISSN: 1877-0509) 87 (2016) 128–133, http://dx.doi.org/10.1016/j.procs.2016.05.138.

[495] S. Sahmim, H. Gharsellaoui, Privacy and security in internet-based computing: Cloud computing, internet of things, cloud of things: a review, Procedia Comput. Sci. (ISSN: 1877-0509) 112 (2017) 1516–1522, http://dx.doi.org/10.1016/j.procs.2017.08.050.

[496] P.P. Ray, A survey of iot cloud platforms, Future Comput. Inf. J. (ISSN: 2314-7288) 1 (1) (2016) 35–46, http://dx.doi.org/10.1016/j.fcij.2017.02.001.

[497] A. Nordrum, Popular internet of things forecast of 50 billion devices by 2020 is outdated, IEEE Spectrum Online (2016) URL https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated, [Accessed on 24-Mar-2018].

[498] D. Evans, The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, URL https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, [Accessed on 24-Mar-2018], 2011.

[499] O. Salman, I. Elhajj, A. Chehab, A. Kayssi, Software defined iot security framework, in: 2017 Fourth International Conference on Software Defined Systems (SDS), 2017, pp. 75–80, http://dx.doi.org/10.1109/SDS.2017.7939144.

[500] T.H. Szymanski, Security and privacy for a green internet of things, IT Prof. (ISSN: 1520-9202) 19 (5) (2017) 34–41, http://dx.doi.org/10.1109/MITP.2017.3680952.

[501] D. Soldani, K. Pentikousis, R. Tafazolli, D. Franceschini, 5g networks: End-to-end architecture and infrastructure, IEEE Commun. Mag. (ISSN: 0163-6804) 52 (11) (2014) 62–64, http://dx.doi.org/10.1109/MCOM.2014.6957144.

[502] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, 5g security: Analysis of threats and solutions, in: 2017 IEEE Conference on Standards for Communications and Networking (CSCN), 2017, pp. 193–199, http://dx.doi.org/10.1109/CSCN.2017.8088621.

[503] M. Liyanage, A.B. Abro, M. Ylianttila, A. Gurtov, Opportunities and challenges of software-defined mobile networks in network security, IEEE Secur. Priv. (ISSN: 1540-7993) 14 (4) (2016) 34–44, http://dx.doi.org/10.1109/MSP.2016.82.

[504] F. Tian, P. Zhang, Z. Yan, A survey on c-RAN security, IEEE Access 5 (2017) 13372–13386, http://dx.doi.org/10.1109/ACCESS.2017.2717852.

[505] M. Monshizadeh, V. Khatri, R. Kantola, An adaptive detection and prevention architecture for unsafe traffic in SDN enabled mobile networks, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 883–884, http://dx.doi.org/10.23919/INM.2017.7987395.