The Journal of Supercomputing (2020) 76:9493–9532
https://doi.org/10.1007/s11227-020-03213-1

A survey on security challenges in cloud computing: issues, threats, and solutions

Hamed Tabrizchi[1] · Marjan Kuchaki Rafsanjani[1]

Published online: 28 February 2020

Abstract

Cloud computing has gained huge attention over the past decades because of continuously increasing demands. There are several advantages to organizations moving toward cloud-based data storage solutions. These include simplified IT infrastructure and management, remote access from effectively anywhere in the world with a stable Internet connection and the cost efficiencies that cloud computing can bring. The associated security and privacy challenges in cloud 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 provides cloud security issues and requirements, identified threats, and known vulnerabilities. In fact, this work aims to analyze the different components of cloud computing as well as present security and privacy problems that these systems face. Moreover, this work presents new classification of recent security solutions that exist in this area. Additionally, this survey introduced various types of security threats which are threatening cloud computing services and also discussed open issues and propose future directions. This paper will focus and explore a detailed knowledge about the security challenges that are faced by cloud entities such as cloud service provider, the data owner, and cloud user.

Keywords Cloud computing · Security · Threats · Vulnerabilities · Data protection

1 Introduction

Large rooms and the huge amounts of electricity play an important role in the history of the technology so that they are widely used to get only a little processing output. In the last decades, small and more efficient computers have gradually taken the place of huge (in some cases, room-size) computers. In recent years, the demand

✉ Marjan Kuchaki Rafsanjani
kuchaki@uk.ac.ir

[1] Department of Computer Science, Faculty of Mathematics and Computer, Shahid Bahonar University of Kerman, Kerman, Iran

for data has dramatically raised and the number of online users has increased behind belief. Also, traditional computing infrastructure has become expensive and difficult to be managed so that accessing data has become impossible by traditional computing anywhere and at any time. Therefore, the external storage system has turned out to be a necessity for saving data. That traditional computing is now unable to handle the increased number of online users on networking sites, social networking, multimedia broadcasting, etc. Since global Internet usage has dramatically grown step by step, the volume of the uses and availability of services led to a new concept called cloud computing. Figure 1 indicates the progress that the computing infrastructure and platforms are provisioned.

Cloud computing has brought a lot of benefits like many other technological services. For instance, it made it possible to store a large amount of data and various services. Furthermore, this platform solved the problem of limited resources and reduced the cost of services by sharing valuable resources among multiple users. Resource reliability and performance require the platform to be robust against security threats [1]. In recent years, cloud computing has become one of the most significant topics in security researches. These researches include data storage security, network security, and software security. The National Institute of Standards and Technology (NIST) defines the cloud computing as [2], “a model for enabling convenient, resource pooling, ubiquitous, on-demand access which can be easily delivered with different types of service provider interaction.” The procedure of cloud computing follows Pay as You Go (PAYG), which the customers only pay the services they use. PAYG model provides customers with the ability to customize software, storage, development platform, and computing resources according to the customer or end-user demands. These benefits are the reason that the research community has dedicated many efforts to this state-of-the-art concept [3].

The virtualization technique has increased the availability of the resources for the end users. The manageability, scalability, and availability are the main attributes of cloud computing. In fact, these techniques combine the available resources in a network by splitting up the available bandwidth into separate and distinguished channels in order to assign to a specific server or device or stay unassigned totally [4]. Furthermore, it provides demand service, elasticity, and stability very economically.

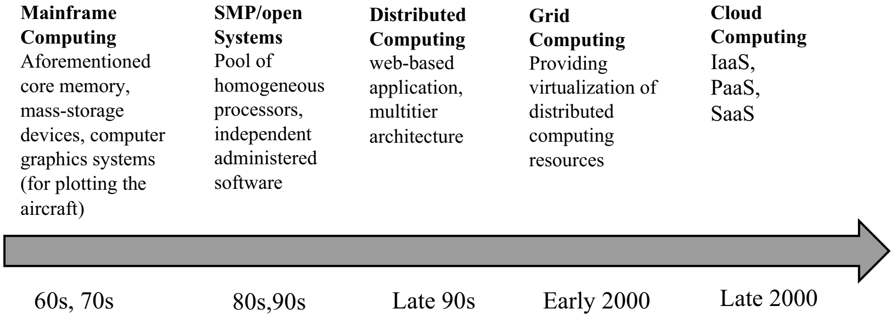
Mainframe Computing
Aforementioned core memory, mass-storage devices, computer graphics systems (for plotting the aircraft)
SMP/open Systems
Pool of homogeneous processors, independent administered software
Distributed Computing
web-based application, multitier architecture
Grid Computing
Providing virtualization of distributed computing resources
Cloud Computing
IaaS, PaaS, SaaS
60s, 70s
80s,90s
Late 90s
Early 2000
Late 2000

Fig. 1 The computing architecture evolution

Fundamentally, cloud computing provides three different models of service delivery, called software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS). SaaS model emphasizes on access management tasks in applications like policy controls. For instance, a person is only allowed to download certain information from applications. In this way, multiple end users benefit from a single instance of the service. Today, companies like Google, Microsoft Office 365, Dropbox, etc., offer SaaS. In PaaS, a layer of the development environment is used as a service and other higher level of service can be built. In the PaaS model, the customer creates their own applications running on the provider's infrastructure. In fact, PaaS offers a combination of OS and application servers like Microsoft Azure, Google App Engine, LAMP platform (Linux, Apache, MySQL, and PHP), etc. It is worth noting that one of the main focuses of the PaaS model is data protection. This becomes notably important in the case of storage as a service. It should be considered that this model should be able to encrypt data while storing them on a third-party platform and should be aware of the regulatory issues that may impress data availability in different geographies. IaaS offers computing capabilities and essential storage as standardized services across the network. The inherent strategy of virtualization is to arrange independent virtual machines (VM) and isolate them from both the underlying hardware and other VMs. IaaS also emphasizes on security fields like firewall, intrusion detection, prevention (IDS/IPS), and virtual machine monitor. Cloud computing is considerably and rapidly growing and more and more organizations adopted cloud technology every day. However, there are several parallel security issues that should be taken care of. Organizations pick out some secure infrastructures when transmitting their data to remote destinations. In this way, each customer would typically use his own software on the infrastructure [5]. Google Compute Engine (GCE), Amazon Web Services (AWS), Cisco Metapod, and Microsoft Azure are among the most important examples of IaaS.

Cloud computing has many aspects including cloud development model that provides a certain type of cloud environment, mainly distinguished by its size, ownership, and accessibility. In fact, cloud computing is empowered by sharing resources among individual devices or local servers. The purpose and nature of the cloud are associated with deployment model. Deployment model includes three types, namely public cloud, private cloud, and hybrid cloud [6].

In the private cloud, cloud computing deal with the data center of an organization. In this model, resources are allocated to a single organization or multiple ones and work inter-functionally. For this reason, infrastructure is owned and operated by the same organization in this type of cloud. Also, customer and vendor relationship identification and security risk detection are much easier. In the second model, government, business or academies own and operate a public cloud. Also, organizations could provide open access over the Internet or another portal in this model. In this type of cloud, many challenges appear in the field of resource location and ownership detection. Furthermore, it is very complicated and difficult to protect resources against various types of intrusions and attacks. However, the third deployment model, the hybrid cloud, is the best one in terms of advantages. This model offers private cloud associated with one or more external cloud services, while the data and application are bound together and managed centrally. It is worth noting that hybrid cloud security is more reliable than the public cloud's if the entities access across the Internet. However, each of deployment models has their specific advantages and disadvantages. In fact, each deployment model has a specific advantage and disadvantage with regard to user experience. The private cloud provides complete control over the user experience. However, in some cases, the public cloud has no control over the user experience and hybrid cloud admit control over the user experience relies on the agreement have placed with the consumer [7]. In addition, Table 1 illustrates the advantages and disadvantages of public clouds, private cloud, and hybrid cloud.

However, there is a shared responsibility security model behind all services provided by cloud computing. Both the provider and cloud consumer have a role in the security of cloud-resident infrastructure and cloud-delivered applications. The responsibility for security is different in each delivery model. In some services, the customer is responsible for data security like user access and identity management in any case of delivery models (IaaS, PaaS, and SaaS) as shown in Fig. 2.

To release the security patches or updates, they should be comprehensively tested, repackaged, and stored in the repository. However, customers have some responsibilities like collaborating with provider regarding to system maintenance. In this regard, they should install patches on the operating system (OS) and application stack and act the role of the system administrator in the cloud by patching and updating operating systems and various applications [8]. Other customer responsibilities are user account creation management, provisioning, and destruction, server-level account authentication mechanisms, password policies, etc. Customers' data activity can be monitored using the logs automatically delivered to their accounts. However, both the cloud provider and cloud customer are responsible for different aspects of the system and both must take some actions to secure the service properly.

According to Oracle and KPMG Cloud Threat Report (2018) [9], only 43% of respondents were able to correctly recognize the most common IaaS shared responsibility security model. Organizations should employ various network security controls like physical and VM-based firewalls, intrusion detection and prevention systems, and gateways as well as the purposeful workload and cloud application controls. Also, 66% of respondents said they faced a cyber security incident

Table 1 The pros and cons of public, private, and hybrid clouds

Cloud development models	Advantages	Disadvantages
Public cloud	Scalability and reliability with on-demand resources	Can be unreliable
	Easy to use	Less secure
Private cloud	Organization-specific	More costly
	Customizable	Requires IT expertise
Hybrid cloud	Flexible infrastructure	Lack of visibility
	Cost controls	Potential challenges in application and data integration
	Faster speeds	

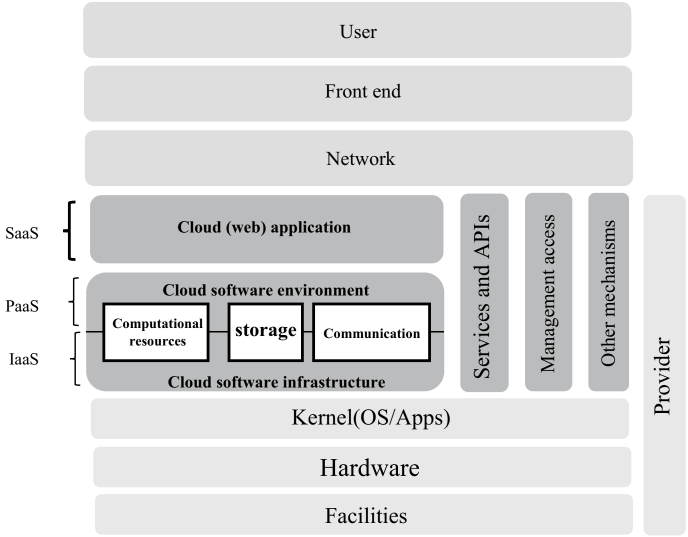

Fig. 2 Configuration of cloud delivery model [2]

affecting their business operations over the past 2 years. These effects were standard business operation disruption, service providing disruption, employee productivity loss, and delays in IT projects. In fact, cloud companies have provided a lot of attributions like global availability of high-performance services, support of a large number of services, storing a large amount of data [10].

The rest of the paper is organized as follows. A background of main security services and the main known techniques to fulfill each service is presented in Sect. 2. In Sect. 3, the main cloud security issues and challenges are classified and described. Also, we present our new classification of security solutions in this section. In Sect. 4, different security threats threatening cloud computing services are introduced. Then, in Sect. 5, the importance of cloud security issues in the future is discussed. Finally, conclusions are presented in Sect. 6.

1.1 Contributions on this survey

Given the undeniable need for computation and storage resources in today's world, many new technologies have decided to consider cloud computing as the main computing or storage component. However, this popular phenomenon suffers from various security challenges and vulnerabilities. It is a vivid fact that cloud environment faces many threats. For this reason, using this phenomenon requires sufficient knowledge and the best possible solution to deal with each of these threats.. In the current study, several studies are reviewed and some of them having more importance will be discussed. In fact, this work deals with the expression of security issues, challenges, and threats in cloud computing.

The main contributions of this work can be summarized as follows:

- The basic concepts of cloud computing and all entities associated with the architecture of cloud computing systems are introduced.
- We provide a new classification of cloud security issues and challenges based on the security state of cloud environments into five categories.
- We provide an overview of the cloud security threats model, recent computing threat based on the STRIDE threat model and also categorize attacks based on the OWASP attack classification.

2 Literature review

2.1 Background

The Background section discusses issues such as data security preliminaries and presents some information about the architecture of cloud computing systems.

2.1.1 Security service

Security includes all the approaches aiming to preserve, restore, and guarantee the protection of information in computer systems against various threats. In fact, the security services implemented by security mechanisms execute security policies. As shown in Table 2, the security of computer networks and information systems is provided by services like integrity, confidentiality, authentication, non-repudiation, and availability [11].

- *Confidentiality* ensures that information is not disclosed and available to unauthorized individuals, entities, or processes. In fact, data should be sent (and received) data without being accessed by unauthorized entities during the transmission. Data encryption is a good way to realize confidentiality. Encryption can be accomplished by symmetric or asymmetric key paradigm.
- *Integrity* ensures the data received by an authorized person is same as the sent data without any modification. In other words, it guarantees that data have not been modified by a third party (intentionally or accidentally). When an intrusion occurs, the connection is dropped and the invalid information transmission is canceled.
- *Availability* ensures the availability of services for rightful users and makes data accessible and useable upon demand by an authorized entity. For instance, when a distributed denial-of-service (DDoS) attack occurs in a system, it will lose its ability to transfer data.
- *Authentication* confirms the identity of the information transmitter and recipient. In fact, the integrity and confidentiality of information are meaningful just when the identities of senders and receivers are properly verified.
- *Non-repudiation ensures that* the actions taken cannot be denied by senders or receivers. There are two kinds of repudiations—source repudiation and destination repudiation. In the former, sender or receiver cannot deny the transmission of a message, and in the latter, they cannot deny the delivery of a message.

Table 2 Security services and mechanisms

Security services	Security mechanisms	Some examples
Confidentiality	Data encryption (cryptography, quantum cryptography), secure sockets layer (SSL)	Symmetric cryptographic mechanisms (AES, CBC, etc.) asymmetric mechanisms (RSA, DSA, etc.), post-quantum cryptography
Integrity	Hash functions, message signature, message authentication code	Hash functions (SHA-256, MD5, etc.), message authentication codes (HMAC), public blockchains [ethereum (platform)]
Availability	Intrusion detection and prevention systems, firewalls, packet filters	Signature-based intrusion detection, statistical anomaly-based intrusion detection, etc.
Authentication	Digital signature, secure sockets layer (SSL), endorsing certificate	HMAC, CBC-MAC, ECDSA, certified signatures, SSL certificate
Non-repudiation	Digital signatures, notary, public, and private blockchains	Email tracking, capturing unique biometric information and other data about the sender or signer

2.1.2 Cloud configuration

For a better understanding of security issues, we should first understand the cloud configuration we have discussed in the following paragraphs. A cloud company is made of the resources dedicated to demands. According to NITS, cloud computing configuration has five major actors listed in the following table [12, 13]. The classification focuses on cloud customer's and cloud provider's threats and risk-awareness. The actors mentioned in Table 3 are the entities taking part in a process or transaction and/or playing a role in cloud computing.

2.1.2.1 Cloud consumer A cloud consumer is a person or organization that gets some services from a cloud provider. In fact, a cloud consumer can opt the most fitting services by scrutinizing the services offered by cloud providers and closing a contract. To close this contract, a cloud consumer has to determine the technical performance by signing a service-level agreement (SLA) with a cloud provider. SLAs (as an agreement) cover things like consistency of the quality of services, security, prevention, and performance failure. However, a cloud consumer is able to choose providers offering more favorable services and better prices.

2.1.2.2 Cloud provider A cloud provider is a person or organization making a service available to a cloud consumer. The cloud provider organize and arrange cloud software by acquiring and managing the cloud infrastructure. In SaaS, the cloud provider provides services at expected service levels through deploying, configuring, maintaining, and updating the software applications. According to the limited administrative applications of cloud, most of the managing and controlling responsibilities in the infrastructure and application are on SaaS provider's shoulders. In PaaS, the cloud provider manages the computing infrastructure of the platform and the components of the platform (such as runtime software, database, or other middleware components) are provided by cloud software. In IaaS, the cloud provider acquires the physical computing resources including the networks, storages, servers, and hosting infrastructure.

Table 3 Different actors in cloud computing

Actor	Definition
Cloud consumer	A person or organization that maintains a business relationship with, and uses service from, cloud providers
Cloud provider	A person, organization, or entity responsible for making a service available to interested parties
Cloud auditor	A party that can conduct an independent assessment of cloud services, information system operations, performance and security of the cloud implementation
Cloud broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers
Cloud carrier	An intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers

2.1.2.3 Cloud auditor A cloud auditor is responsible to examine the cloud services independently. The auditor checks the conformance to standards by reviewing various objective evidence. The services offered by cloud providers can be assessed by cloud auditor regarding their privacy impacts, security controls, performance, etc.

2.1.2.4 Cloud broker As the integration of cloud services is too complicated to be managed by cloud consumers, they acquire the cloud services via a cloud broker instead of contacting with cloud provider directly. In fact, the cloud broker is responsible for managing the usage, performance, and delivery of cloud services as well as the relationships among the cloud consumers and cloud providers. The services offered by cloud brokers can be categorized into three categories:

- *Service intermediation* A cloud broker can enhance a certain service by improving some specific capabilities and providing value-added services to cloud consumers. These improvements include cloud services' access management, performance reporting, identity management, enhanced security, etc.
- *Service aggregation* refers to the actions taken by a cloud broker to combine or merge multiple services into one or more new services. In fact, the cloud broker integrates data and plays the role of a bridge between the cloud consumer and multiple cloud providers.
- *Service arbitrage* performs like service aggregation, but services are not aggregated to be fixed. In fact, service arbitrage gives the broker the flexibility to pick services from several agencies. For example, a cloud broker can use a credit-scoring service to assess and select the best agency.

2.1.2.5 Cloud carrier A cloud carrier intermediates between cloud consumer and cloud provider to deliver cloud services. Cloud carriers get access to consumers through the network and other access devices. As discussed earlier, by establishing SLAs with a cloud carrier, the cloud provider can bring services consistent with the SLAs to cloud consumers. Furthermore, cloud carrier is responsible for dedicating secured connections to cloud consumer and the cloud provider.

In Fig. 3, the diagram indicates an overview of the NIST cloud computing configuration [13] including its major actors, their activities and functions in cloud computing. According to the mentioned contents, the diagram characterizes the requirements, characteristics, and standards of cloud computing.

2.2 Existing review papers on security challenges in cloud computing

Cloud computing is an emerging computing paradigm that brings great deals of new challenges for data security, access control, etc. [14]. During the last decade, a lot of survey papers focus on the security challenges in cloud computing. Moreover, it is undeniable that most of the presented reviewed papers play a valuable role in cloud security issues and these noticeable reviewed works had been a lot of valuable and comprehensive research in this area.

Sgandurra and Lupu [15] have presented a taxonomy of attacks in virtualized systems in terms of the target at the different levels, the source and goals of the attackers. In fact, they aim to illustrate the evolution of the threats, related security, and trust assumptions in virtualized systems at the different layers such as hardware, OS, and application.

Kaur and Singh [16] presented a review of cloud computing security issues. This work has discussed the issues related to data location, storage, security, availability, and integrity. In fact, this review focuses on one of the significant security concerns, although it is vital to note that the authors only address security issues without discussing the possible solutions.

Kumar et al. [17] have demonstrated diverse kinds of data security issues in cloud computing and also presented an approach to overcome security issues in a multi-tenant environment. In fact, this paper completely focuses on data security issues and also presents methods to protect the data and its privacy.

Khalil et al. [18] present a review study of cloud computing security and privacy concerns. In this work, various types of known security threats and attacks are classified and also different kinds of cloud vulnerabilities identified. Moreover, this review work investigates the drawbacks of the current solutions and discuss future security perspectives.

Bashir and Haider [19] provide a review study in order to indicate the most vulnerable security threats in cloud computing. In addition, this review work considers both end users' and vendors' key security threats associated with cloud computing by providing analysis related to the different security models and tools.

Ryan [20] present a survey with vital research directions such as protecting data method that aims to keep safe data from a cloud infrastructure provider. Moreover, this work describes a browser key translation method that allows a software-as-a-service application to provide confidentiality service.

Table 4 indicates a summary of the contributions of some of the recent surveys reviewing security challenges, attacks, and threats in the cloud environments.

One of the long-dreamed vision of computing as a utility, where users can remotely store their data, is cloud computing which provides high-quality services from a shared pool of configurable computing resources [21]. Due to the fact that the majority of technologies related to cloud phenomenon witnessed many signs of progress in today's world, security risks become more advanced and new challenges arise. For this reason, comprehensive research is needed along with identifying potential challenges and providing new solutions. In addition, the majority of the mentioned surveys have discussed the aspect of security issues about clouds without considering a comprehensive review of issues, challenges, and threats in the cloud environment. We have focused on all detail related to cloud security and challenges and discuss existing solutions as much as possible.

Table 4 Summary of existing surveys

References	Years	Objective	Remarks
Sgandurra and Lupu [15]	2016	Taxonomy of attacks	Evolution of the threats and of the related security and trust assumptions
			Categorize threat models, security and trust assumptions, and attacks
			Focused on hardware, virtualization, OS, and application
Kaur and Singh [16]	2015	Cloud data storage	Focused on data location, storage, security, availability, and integrity
Kumar et al. [17]	2018	Cloud data security issues	Explores the diverse data security issues in a multi-tenant environment
			Proposes methods to overcome the security issues
			Describes cloud computing models such as the deployment models and the service delivery models
Khalil et al. [18]	2014	Cloud security and privacy	Identify cloud vulnerabilities
			Classify known security threats and attacks
			Present the state-of-the-art practices to control the vulnerabilities, threats, and attacks
Bashir and Haider [19]	2011	Identification of security threats in cloud computing	Focused on both end users and vendors key security threats associated with cloud computing
			Identify vulnerable security threats in cloud computing
Ryan [20]	2013	Cloud security challenge and a survey of solutions	Explain some difficulties with using fully homomorphic encryption for cloud computing applications
			Describe a method in which in-browser key translation allows a software-as-a-service application to run with confidentiality from the service provider
			Explore trusted hardware used to protect cloud-based data

3 Cloud security issues and challenges

Although cloud computing has brought a variety of beneficial services, it also involves many security threats and challenges. Since a lot of information is transferred through the network and stored in specific resources in the cloud, there are many vulnerabilities that can be exploited by malicious actors. In this section, we discuss the security state of cloud environments classified into five categories [22, 23]. It should be noted that each subsection of this section is allocated to a common security property. As illustrated in Fig. 4, cloud security issues can be categorized into the following five categories: security policies, user-oriented security, data storage security, application security, and network security.

3.1 Security policies

Security policies include the standards necessary to prevent attacks by taking precautionary measures. These standards should secure the working environment in cloud without compromising its performance and reliability [7, 24]. Security policies work based on regulatory authorities and involve various service-level agreements (SLAs), client management issues, and antecedent trust.

3.1.1 Service-level agreement (SLA)

A service-level agreement is associated with the relationship between customers and providers and includes both. Service providers are expected SLAs to manage customer expectations. In fact, SLAs establish the circumstances under which providers are not responsible for outages or performance issues. Also, SLAs represent the

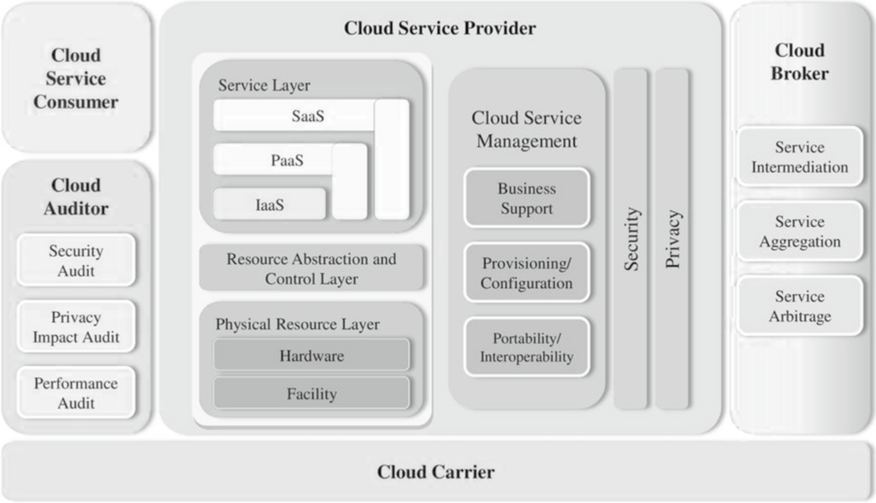

Fig. 3 NIST cloud computing configuration [13]

performance characteristics of services which can be used for comparison purposes. However, SLA cannot guarantee that a particular service will be achieved. In other words, SLA does not eliminate the risk of choosing a bad service and is not able to turn a bad service into a good one. In general, SLA consists of a statement of objections and a list of the services covered by the agreement. Also, at the same time, it determines the responsibilities of the service provider and customer under the SLA. SLA specifies availability, usage statistics, service provider response time, and specific performance benchmarks that will be provided [25].

3.1.2 Client management issue

In recent years, most organizations have attempted to focus on the customer. The client management issue as one of the most significant concerns in cloud security has many different aspects including client experiences, client-centric privacy, client authentication system, and client service-level agreement. These different aspects of security in cloud business will be discussed in the following paragraphs [26].

3.1.2.1 Client experience (CX) Customers expect their providers to recognize their special demands, personal conditions, and life difficulties. To offer better services, providers must know their customers' needs and deliver customized solutions for them. The customer experience plays a vital role in cloud. This experience makes companies able to deliver products and services according to customer's values. For example, there are some advantages of cloud that are derived from a user's search history and its connection with the provider. In recent years, the cloud-based services have improved the customer experiences in the market so that many companies are in trouble because of the lack of cloud-based customer system, whereas choosing a secure cloud provider company will be difficult for customers with experiences in security areas.

3.1.2.2 Client authentication Ensures that users get access to a server or remote computer by presenting a digital certificate. This digital certificate acts as a "Digital ID," and its function is to cryptographically bind a customer and employee's identities. The digital certificate makes cloud resources able to control accesses and pre-

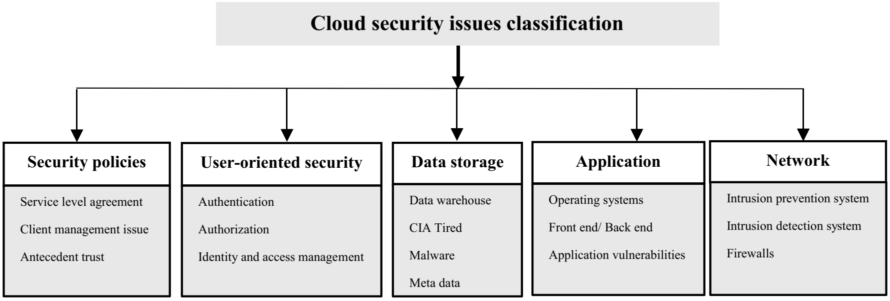

Fig. 4 Different categories of cloud security issues

vents non-rightful users to get access to cloud services. Users should be able to get access to their applications from anywhere and any device like cell phones, tablets, laptops, smart televisions, etc.; however, it is a challenge for cloud service providers to guarantee that only rightful users get access to their services. Nevertheless, it is worth noting that there are various authentication threats and attacks in cloud environment including password discovery attacks, cookies reply attack, credential theft (for instance, phishing or social engineering), man in the middle attack, and many other ones [27].

3.1.2.3 Client-centric privacy Nowadays, the most significant vulnerabilities in the cloud appear when privacy is lost and data leakage arises [28]. In fact, data processing by provider causes this challenge and compromises client-centric privacy. This challenge is a critical barrier to adapt cloud services. For example, when a user submitted the data into the cloud machine for processing, it has no control on processing procedure. In fact, the users have not any knowledge about where their data reside and are stored and used. For example, the service provider is able to share the sensitive data with unallowable individuals without user permission leading to privacy loss and data leakage. As a result, we need a client-centric solution to solve this challenge. This solution should make the users able to control their submitted data. Therefore, a client-centric approach is required to solve this problem. This problem can cause many issues like security, privacy, trust, and customer relationship management (CRM) issues.

3.1.2.4 Service-level management As mentioned, SLA is used to provide the agreements and their costs. In fact, service-level management (SLM) is the process in which the benchmarks for level of service are arranged. This process measures the performance compliance expected by customer. Also, in an SLM process, different services are structurally defined and service levels needed to maintain business processes are agreed upon. The definition structure should contain the security responsibilities of both internal and external service providers and customers. In this regard, service-level management covers the role and define the organization structure.

3.1.3 Antecedent trust

Trust is one of most important facilitators to make business relationships strong. Since trust has received a pale attention in cloud computing, as a result, the lack of trust understanding in cloud services has caused huge challenges for the adoption of cloud computing. This challenge has created a gap between adoption and innovation and caused the cloud computing consumers not to fully trust this new way of computing. To fill this gap, the trust issue related to could computing should be recognized from both technological and business perspectives [29, 30].

3.1.3.1 Human factor At the first glance, reinforcing the security of the cloud provides a secure infrastructure for information. However, considering the human factor of the cloud security is a necessity for organizations. To characterize the human role in the security aspect of the cloud, it should be noted that human is able to create various innovations and solve all the problems. In cloud systems, human access level to the system is different, so that an employee or costumer with administrator access level can play a critical role in saving or damaging system security. To fix security threats and eliminate vulnerabilities, in addition to technological defects, human mistakes, and behaviors should definitely be considered. With more emphasis on human behavior, a vulnerability pattern (such as social engineering) can be found. Then, social engineering attacks will be monitored and studied in more detail.

3.1.3.2 Digital forensics The more the network applications, the more the digital crimes. Digital forensics play a vital role in protecting and restoring operational data. In other words, digital forensics is the process used to uncover and interpret electronic data. With increased number of users in the digital worlds, it is more likely that non-rightful malicious users exploit the cloud services. Furthermore, this issue is propagated to wider bounds when costumers bring their own accessible devices including PC Windows, MACs, iPhones, and Android smart phones. However, the digital forensics have encountered many challenges including the wider range and increased number of devices operating in the cloud have made it more difficult to archive and encrypt data from different operating systems in different platforms.

3.1.3.3 Costumer trust status According to a recently published report [31], many organizations are concerned about their personal and sensitive data kept by companies. They are worry that these companies can use the data for purposes other than what they collected for. According to this report, although 93% of organizations use cloud services at the moment, only 23% of them completely trust public clouds to keep their data secure. When moving to IaaS, the most important desire of related authorities is to have stable security controls providing integrated security with central management across all cloud and traditional data center infrastructure. However, although the trust in public cloud services continues to improve year by year, the reports published on cloud security topic should always be reviewed.

3.1.3.4 Trust third party (TTP) One of the main concerns of cloud users is about how their data are used because it is possible that malicious data centers exploit these data. In this regard, trust third party (TTP) can authenticate, audit, and authorize the confidential data and protect information against unauthorized malicious people. Therefore, when the third party is discredited, the cloud environment will be severely threatened and many security properties will be compromised. In fact, the starting point of the challenge is where users do not know the location the resource allocated to store their data [32]. Therefore, this problem can be basically solved by the following steps. First, the data submitted by cloud customers should be encrypted using symmetric key encryption algorithms. In this step, TTP asks secret key and holds it to perform data verification or identification tasks. Finally, the service provider is able to ask secret key and perform the data processing task.

3.1.3.5 Governance Cloud computing governance as an aspect of information technology governance presents integrated management with automated performance resolution, balancing resources in a cloud environment. Unfortunately, many organizations adopt cloud environment without understanding the governance importance in the modern life of IaaS. If this issue is disregarded, the administrator operations and access security controls will be lost. In summary, cloud computing governance creates the policies and principles that control the lifecycle of services offered in the cloud. Governance can solve the problem of losing administrative operations and access security controls that may be resulted from the lack of well-established standards. As a result, it is clear that incorrect governance can lead to weakening financial capabilities of the cloud providers, complicating the time management to recovery, and increasing the possibility of data breaches and service terminations [33].

3.2 User-oriented security

Due to the complexity of usage, cloud computing requires extensive user-oriented security to make its data and resources secure. In fact, one of the most important issues in cloud security is that cloud service providers can control the storing and processing steps of information submitted by users. This aspect of security includes identification, authentication, authorization, and access management issues.

3.2.1 Authentication

As you know, cloud computing benefits businesses by storing large amount of data by less cost. Fortunately, as necessity, service providers should guarantee that users are authenticated by specific methods. This authentication is completely or partly done by a software. In a cloud environment, a simple authentication mechanism is not suitable for the costumers accessing and composing services from multiple cloud providers. The privileged user access is an event happening when these kinds of accesses have caused an inherent level of risk. However, there are various authentication methods that can be used to solve this problem. Generally, access permission is dedicated when the users present something they individually know, such as their card number or a password defined by them. In total, these methods can be divided into two categories, namely physical security authentication mechanisms and digital security authentication mechanisms [34].

3.2.1.1 Physical security authentication mechanism One of the recent attractions for organizations is to provide their customers with easy access to their cloud resources at any time. This can be provided with the help of the cloud data centers centralizing old servers, networks, and applications that users are able to access them at anytime and anywhere. In fact, physical security authentication mechanisms such as access cards and biometrics (including retina recognition, fingerprint recognition, and face recognition) are used to prevent unauthorized access. In this regard, some certain usage and governance policies should be considered with respect to physical security [35].

3.2.1.2 Digital security authentication mechanisms Similarly, digital authentication is used when an individual or online entity is honest with the server provider or when it seems that the mechanism is suitably established [36, 37]. One of the mathematical schemes that provide verification and authentication of any kind of digital message is a digital signature. In fact, the name of the digital signature is inspired by handwritten signatures in the physical world. In real life, it is common to use handwritten signatures on the paper's messages. In a similar way, a digital signature is a particular form of procedure that binds a sender entity to the digital data based on cryptography concepts. In other words, the digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer. Apart from the ability to provide non-repudiation of the message, the digital signature also provides message authentication (he message was created by a known sender) and data integrity (the message was not altered in transit). For example, some of the most common digital authentication methods in a cloud environment are credentials, secure shell keys, multi-factor authentication, personal identification number, and single sign-on (SSO).

Credentials: Credentials work as evidences of authority, entitlements, status, and access rights. They provide particular users with an evidence to prove that they are rightful to use resources and services. In fact, taking advantage of credentials (such as one-time passwords, patterns, and captchas) is a traditional way of securing malicious activities. Since the management overhead of the credentials is high, it is necessary to add, disable, modify, or remove accounts whenever any user enters or leaves the service (or organization). On the other hand, when a weak password recovery mechanism is used, the credential reset vulnerability appears. In this way, hackers can monitor or manipulate data in the cloud with malicious activities when the credentials are at the risk of abuse. By encrypting and signing the authentication server, the credentials help the communication among the clients and terminals. The asymmetric encryption technology is able to use public and private keys as a personal identification number (PIN). The advantage of using PINs is that they are used in multiple types of network systems and websites. However, credentials simplify information privacy management while preventing unauthorized access by abusing lost credit/debit cards or usernames/passwords. In this way, a PIN is responsible to authenticate the client/terminal for getting access to user data and keys from the chip.

Single sign-on: The conventional authentication mechanisms are not always suitable for remote authentication because a centralized monitoring system is required for SaaS applications, limiting the software policies. In other words, the existence of multiple services causes that the cloud customers need multiple login requirements and make various problems because only a single user may be forced to maintain a large number of credentials. Because of these reasons, the possible solution is to take advantage of single sign-on (SSO) technique. SSO provision provides one password to get access to all applications and services in the cloud environment.

Secure shell (SSH): SSH is a network protocol that provides a secure way to get access to a remote computer. SSH keys respond to SSH server identification with public key cryptography or challenge authentication with the SSH. In this regard, all user file transfers, commands, and authentications are encrypted to protect users against attacks in the network. The main benefit of SSH key is that the authentication process is accomplished without passing the password over the network. In fact, SSH can prevent the interception or cracking of the passwords by a person leading unauthorized access to data and provides a secure channel based on client–server model by considering the unsecured network in a client–server architecture. However, one of the most critical aspects of SSH is key management. It should be noted that when the suitable centralized creation, rotation, and elimination of SSH key are ignored, the system can lose its control on resource access management.

Multi-factor authentication: Another method to secure digital assets and transactions in the Internet is the multi-factor authentication. This method has many kinds like One-Time Password (OTP), Captchas, or patterns that all of them are involved in the secondary authentication mechanism. The multi-factor authentication can recognize the trustworthy users through their information clarification. In fact, the more the number of the factors used to clarify the user identity, the greater the authentication. It should be noted that with the advent of mobile networks, second-factor authentication has taken the form of SMS, push notification, and mobile OATH tokens.

Personal identification number (PIN): A person identification number is a secure alphanumeric or numeric code that is used to authenticate the access requests. Since different applications and resources follow various authentication mechanisms, single sign-on can internally save the credentials used for primary authentication and translate them into the credentials required for a variety of mechanisms. However, to highlight the advantages of the cloud, it is better that users not specify their credentials whenever they get access to different cloud web services. In this regard, single sign-on (SSO) can reduce password fatigue from different username and password combinations.

3.2.2 Authorization

Authorization is a method which gives permission or prevents the access to a particular resource according to an authorized user's entitlements. In the systems in which users are permitted to access to the system, a system administrator is specified. According to the fact that a cloud network consists of different service providers, there is a common situation in which a single user is able to access different types of services at the moment, so that each service is provided by a different service provider and with a different security level. For example, when the user authorizes the application, cloud-hosted applications are permitted to be accessible from outside the application. In this situation, authorization is done by either access right delegation or access control policies. In fact, through the cloud environment, the cloud service provider presents and executes access control policies like the services and resources should only be accessed by the authorized users [37, 38]. Some of the advantages of centralized access mechanisms include securing the sensitive information and reducing several management and security tasks. However, there are many authorization mechanisms including MAC, DAC, RBAC, and ABAC. In addition, Table 5 indicates the advantages and disadvantages of these authorization mechanisms [39].

3.2.2.1 Mandatory access control (MAC) MAC makes it possible to get access through the operating system or security kernel. The system manager, its security policy, and all access control rights determine the usage of resources and their access policies which cannot be overridden by the end users. Therefore, these policies will slow who has the authority to access the particular programs and files. MAC is widely employed in the systems in which the confidentiality is a priority. Although MAC is a secure way for resource access management, it is less flexible to process the access rights.

3.2.2.2 Discretionary access control (DAC) DAC mechanism is vice versa, regarding MAC. As mentioned earlier, MAC policies are determined by user permission while validation of the username and password in DAC is to specify the access right of each user. Because data owners exist in DAC, data access policies are supervised by them. Generally, DAC is more flexible, but less secure compared to MAC.

3.2.2.3 Role-based access control (RBAC) Role-based access control restricts system access to authorized users. In RBAC, each role is statically specified by the system administrator. In fact, access to the computer or network resources is

Table 5 Advantages and disadvantages of these authorization mechanisms

Authorization mechanisms	Advantages	Disadvantages
MAC	Easy to scale	Limited user functionality
	High security	Not flexible
DAC	Easy implementation	Does not support dynamic alteration
	Flexibility	Requires a high system management
RBAC	Independence authorization management	Not preferred in a dynamic environment
	Separation of duties	Not possible to change access rights without changing the roles
	Hierarchy of roles	
	Least privilege	
ABAC	High flexibility in a distributed and dynamic environment	Require the central database
	Central storage for user attributes	High complexity

mostly controlled by RBAC based on users in an organization. In RBAC, several parameters are considered to give the permission to the user; including role permission, user–role, and role–role relationship. These roles can be categorized into two categories, namely application/technical roles and organizational/business roles. RBAC provides the systems having large number of users and permissions with appropriate administration security. One of the advantages of RBAC is its highly secured environment for allocating access permissions. On the other hand, the main defect of RBAC is that the assigned roles might change over the time, requiring real-time environment for validation and investigation of changes.

3.2.2.4 Attribute-based access control (ABAC) ABAC presents a control over the access where rights are granted to users using the policies combining attributes together. The polices follow any type of attributes like user attributes, resource attributes, object attributes, environment attributes, etc. Generally, since roles and privileges of any individual user are pre-defined in the ABAC mode, it eliminates many authorization problems, gains an effective regulatory compliance, and provides implementation flexibility [40].

3.2.3 Identity and access management

Identity and access management is a framework consisting of the organizational policies for managing digital identity at the condition that technology is supported well enough to find the ability for identity management [41]. Also, it is necessary for identity access management systems to have all the required controls and tends to save and record user login information, manage the enterprise database of user identities and manage assignments and elimination of access privileges. In other words, identification and access management system has the responsibility to prepare a centralized directory service by considering all aspects of the company's user base. However, the identity and access management system is currently unable to directly enhance either profitability or functionality. Therefore, it is very difficult to take funds for these projects. However, with the lake of impressive identity and access management situation, there would be a huge risk for organizations' compliance and overall security.

3.3 Data storage

In physical cloud storage model, data are stored in logical pools. The physical storages span various servers so that each of them is owned and operated by a separate hosting company. By taking into account the significant growth in various online applications and multiple Internet devices, data storage and its security over distributed computing environments is a vital issue. In fact, cloud providers should take the responsibility for the data availability and accessibility at any time [42]. The defects that come about to control the data have caused some security issues like warehouses, availability, confidentiality, integrity management (CIA), etc.

3.3.1 Data warehouse

Data warehouses are the huge central repositories of integrated data having disparate sources. In fact, all data collected by enterprises and various operational systems are integrated in physical or logical data warehouses. These data warehouses use various sources for giving priority on the access and analysis rather than transaction processing [43]. Typically, data warehouse security is an important requirement for implementation and maintenance. It is worth noting that storage security is a critical aspect of the quality of services (QoS). In this regard, data warehouses are encountering three fundamental security issues, namely availability, integrity, and confidentiality.

3.3.2 CIA tired in data security

The main challenges of cloud storage can be categorized into three aspects, namely confidentiality, integrity, and availability (CIA). As mentioned earlier, the most important factor in information systems is to protect the data against any unauthorized data modification, addition, or deletion. Since the data are moving through insecure media, considering the confidentiality before uploading the data to the cloud servers is a necessity [44, 45]. ACID property to ensure the integrity has four contributions to the ability of a transaction to ensure data integrity. Cloud data can follow ACID property to guarantee the integrity and confidentiality. For better understanding of these four qualities, it should be noted that ACID is an acronym for atomicity, consistency, isolation, and durability. In summary, atomicity is a transaction in a situation to exhibit all or none of the treatments. In this regard, consistency is based on the state of the data before or after the transaction is processed. Next property is the isolation that is related to the transaction permitted to run at the same moment. Any transaction running in parallel has the isolation property in the absence of any concurrency. Finally, durability refers to the influence of the success or failure on a processing transaction. There are many challenges in cloud data security that are related to the four above-mentioned properties. In fact, when the security parameters or VM configuration are described incorrectly, the multi-tenant nature of the cloud significantly impresses the integrity and conditionality; in addition, the increased number of users will increase security risks in the cloud. Unfortunately, these two aspects are not enough to protect data in the cloud. One of the important goals in cloud services is to provide the clients with excellent availability. In the field of cloud availability, we should consider not only the software aspect of data, but also the hardware aspect of data for authorized users. However, there are many various methods to violate the availability of services including system errors, hardware and software constraints, and malicious attacks from outside.

As a result, we conclude although data confidentiality is important, two other factors have more importance. In some cases, cloud service providers do not provide cryptographic protection for stored data. For example, Microsoft One Drive does not provide any encryption services to assign data confidentiality.

3.3.3 Metadata

In simple terms, metadata means data about data. Metadata contains confidential and sensitive information, and by taking into account the importance of cloud services, it plays a much more important role and is becoming more complex. In fact, metadata includes information related to data events, something was done, where it was done, the file type and the format of the data, etc. The metadata contains valuable information that can be exploited by attackers. However, organizations use the data in metadata to extract new business values from the information. Furthermore, metadata includes confidential and sensitive information so it is very important to use appropriate encryption mechanism to make these data secure. Unfortunately, encryption only hides the data of massage, not the metadata of communication [46, 47]. An efficient way to protect this sensitive content against abusing is to employ virtual private networks (VPN) that will guarantee data privacy and metadata confidentiality.

3.4 Application security

One of the most important and vulnerable areas of information security is software application security. Most of the applications have different platforms, frameworks, and various types of vulnerabilities [48, 49]. One of the most important challenges in cloud computing security is the vulnerabilities in the application security aspect. In this regard, it should be considered that the software application has a million lines of programming codes written by different programmers in different programming languages and each has its own vulnerabilities. Since the developers are responsible for dealing with cloud application security, they need to understand the security aspects of cloud application programming and networking before developing a software application. As discussed in detail in above, to define cloud application security requirements with regard to data, a developer needs to focus on some areas like encryption identity management services, authentication services, and identity and access management services. However, in this section, we discuss the different types of cloud application security issues. Nowadays, many application developers use programming languages with default functions and classes having various vulnerabilities. For example, a programmer needs to know the security aspects of the web-developing languages like HTML/CSS/PHP/JS to mitigate injection masked code. From another point of view, SQL injection attacks abuse the back-end application weaknesses. The Open Web Application Security Project (OWASP) targets aspects like back-end security and development hardening and testing. Additionally, by taking into account the security issue in cloud applications, trust mechanism in web-based business services plays a critical role in protecting sensitive information. Unfortunately, these web-based services create some opportunities for malicious attackers.

Generally, to perform tasks over the Internet, one of the most commonly used methods is web applications, but the security aspect of web application vulnerabilities has faced a wide variety of shortfalls. In fact, hackers find some ways to insert malicious executable codes into legitimate traffic sent to an endpoint. This process is called code injection. Furthermore, similar to code injection, the cross-site scripting also provides some ways to insert malicious executable codes. However, its difference is that it is involving scripts. As a result, lousy programming of things like boundaries, exceptions, and credentials can make web applications vulnerable. Sometimes, administrative issues cause configuration failures or lead to incomplete component updates. As a result, special programming languages are designed in a way making it harder to ensure them. The security of web application also complicates other challenges and causes a lot of problems like Internet service security issues.

In addition to security problems in applications, operating systems (OSs) also play an important role in the security of the cloud [50]. There is a relationship between an application program and its operating system. In fact, the operating system is defined as an application which is run on a computer and also responsible for the management and control of all the resources (memory, hard drives, monitors, etc.) running different applications at the same time and sharing the tasks among themselves. Cloud computing utilizes many virtual machines and different kinds of servers in different networks and operating systems. This brings in many security challenges and vulnerabilities on different operating systems used in cloud computing, such as desktop OS, server OS, network OS, and smartphone OS.

3.5 Network

Since cloud computing has been significantly dependent on the network, it has faced a major challenge called network security. In fact, the main similarity between network security and cloud security is an evolving sub-area of computer security, network security, and information security. In the real world, networks encounter many security challenges. As a result, network administrators must take appropriate security policies and use preventive mechanisms and services to protect data and cloud infrastructure [51]. Unfortunately, network security has encountered significant connection availability threats such as the denial of service (DoS), distributed denial of service (DDoS), flooding attack, and Internet protocol vulnerabilities. One of the most effective and common methods to prevent these threats is to employ firewalls. In the cloud, to check the safety of data, they are exchanged among the end users, servers, and routers in cyberspace. Firewall-as-a-service (FWaaS) offers the same protection as traditional firewalls. However, when a service is hosted in the cloud, it means that it is available in all places on any device [52]. Since FWaaS is cheaper, more efficient, and more flexible than traditional firewalls, it is a beneficial choice for any company concerned about network security. Generally, using firewalls is not a perfect way to defend cloud systems against threats but a strong firewall can reduce vulnerabilities and branches. In simple terms, a firewall can block backdoor access via a Trojan, but cannot tackle viruses, worms, and other malware. For this reason, it is necessary that a firewall interacts with other systems [53]. In comparison, a firewall only analyzes packet headers and implements policies based on protocol type, secure address, destination address, and secure port while intrusion detection system (IDS) detects and logs any malicious access to the network. IDS is designed not only to prevent attacks, but also to log useful data for future security analyses. In addition, the intrusion prevention system (IPS) is a network tool preventing any malicious access to the network. IPS is designed not only to detect and log attacks, but also to prevent malware or other types of intrusions. Eventually, it is worth noting that network security needs a broader overview which can be comprehensively included in this survey. Therefore, it is suggested to refer to other specialized papers for more information.

4 Security attacks and threats in cloud computing

The infrastructure of cloud computing with a great deal of hardware and software components suffers from various security issues arising from the existing and new threats. In the context of computer security, anything that has the potential to cause serious damage to a computer system is called a threat. In other words, threats are able to lead attacks on computer systems, networks, and other communication infrastructures. Threats can include everything from viruses, trojans, back doors to outright attacks from hackers. Due to the fact that each kind of public, private, or hybrid cloud provides a flexible model for simplified management and cost efficiency, a privacy of data and security of software becomes considerable growing concerns.

4.1 Threat model and compromised attribute

Cloud computing provides many advantages, such as speed and efficiency via dynamic scaling. But it also raises a host of concerns about security threats, such as data breaches, human error, malicious insiders, and DDoS attacks. A threat model, or threat risk model, is a process that reviews the security of any web-based system, identifies problem areas, and determines the risk associated with each area. Threat model considered identifying steps in the process such as identify security objectives, identify threats, and identify vulnerabilities. In fact, threat models are a systematic and structured way to identify and mitigate security risks in systems. Preeti [54] presents a threat model for the attacks from one VM to another VM. In fact, two VMs in the same tenant or different tenant with the same physical server is able to become a victim of the attacks. Moreover, a malicious tenant user is able to set up an attack by generating traffic floods with ICMP/UDP packets having a spoofed source address and also it can exhaust the resources of the server at the virtualization layer. STRIDE is a model of threats developed by Praerit Garg and Loren Kohnfelder at Microsoft [55] for identifying computer security threats and provides an overview of threats in a given system by categorizing them into six categories (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege). Each category of the STRIDE captures individual features of the attacks that pose a particular type of threat. In fact, the STRIDE threat model categorizes the threats regarding the result or effect of their realization. The STRIDE threat model has been captured the high-level view of the threats posed. Furthermore, this survey extends the threat classification to the cloud component level advanced.

4.1.1 Spoofing

The act of disguising a communication from an unfamiliar source as being from a known trusted source is called spoofing. In fact, spoofing aims to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack [56]. Spoofing is able to apply to emails and websites with a lot of technical aspects, such as a computer spoofing an IP address, or domain name system (DNS) server. Since IP spoofing is not able to be prevented, measures can be taken to prevent spoofed packets from infiltrating a network. A well-known defense against spoofing is ingress filtering which is a form of packet filtering. In addition, ingress filtering usually implemented on a network edge device that examines incoming IP packets and looks at their source headers. If the source headers on those packets do not match their origin or they otherwise look fishy, the packets have to reject.

4.1.2 Tampering

Attackers may maliciously modify the data to interfere with operations. Unlike spoofing, this threat directly modifies the system such as XML poisoning which is able to change commands and codes to make the system malfunction [57]. One type of data tampering is ransomware. In this attack, cybercriminals encrypt an organization's data and demand payment of a ransom to obtain the decryption key. In fact, it is vital that organizations are able to identify successful and unsuccessful attempts to change critical files with a security control known as file integrity monitoring (FIM). In other words, FIM is the process of examining critical files to know when and how they changed. This system can compare the current state of a file to a known, typically using a cryptographic algorithm to generate a mathematical value. Due to a large amount of data stored by organizations today, monitoring all files typically is not practical. For this reason, FIM systems generally are used to monitor user identities, security settings, operating system and application files, configuration files, and encryption key stores. In addition, the monitoring of log files plays a noticeable role in systems and applications which write data to logs and that log files are frequently collected and stored in a separate management system.

4.1.3 Repudiation

When an application or system cannot adapt controls to properly track and log users' actions, a repudiation attack is able to happen. This attack can be used to modify the authoring information of actions executed by a malicious user in order to log the wrong data to log files. Unfortunately, the repudiation attackers can deny actions that cannot be proven due to the lack of ability to provide evidence [58]. In fact, non-repudiation refers to the ability of a system to counter repudiation threats. In cloud security, non-repudiation means a service that provides proof of the integrity and origin of data which brings authentication with high reliability.

4.1.4 Information disclosure

Information can leak to unintended individuals due to malicious activities. There are various ways information can leak from the system, such as VM configuration stealing [59, 60] and scanning for open ports to discover services and their associated vulnerabilities [61]. There are two main types of disclosures that can happen in cloud system: internal and external. An internal disclosure is when an employee or administrator inadvertently makes private information public. This could happen from lack of shredding, carelessness, mistakes, or not understanding the sensitivity of information. An external information disclosure attack is aimed at acquiring system specific information about a provider, including software distribution, version numbers, and patch levels. The acquired information might also contain the location of backup files or temporary files. To prevent disclosure of information attacks, methods such as encryption and third-party authentication are used.

4.1.5 Denial of service

A denial-of-service attack is a security event that happens when an attacker prevents legitimate users from accessing particular services or resources. In other words, valid users are denied from the service due to malicious activities caused by cyber attacks. DoS and DDoS attacks often use the vulnerability of how network protocols handle network traffic by transferring large numbers of packets to a vulnerable network service from different Internet Protocol (IP) addresses to overwhelm the service to deny legitimate users from accessing services or resources. To prevent this kind of attack, various precautionary actions can be taken. Using multiple data centers in different countries with a good load balancing system to distribute traffic between them is a reasonable action to prevent DDoS attacks. Further action can also be taken considering network firewalls and more specialized web application firewalls. It is undeniable that software protection against DDoS attacks plays an important role in the prevention of this kind of attack. These software protection methods are able to monitor a number of incomplete connections that exist and flushing them when the number reaches a configurable threshold value [62, 63].

4.1.6 Elevation of privilege

In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats includes those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed. Vulnerabilities in the system can be exploited by attackers to bypass the system authentication, and various attack types can be used to exploit those vulnerabilities. One of the most common tactics an attacker could use to escalate privileges in cloud environments is abuse overly permissive identity and access policies for cloud users and services. These techniques involve policy creation and manipulation, profile changes, the ability to pass roles that may be in use and more [64]. To prevent privilege escalation in the cloud, organizations can take a number of steps to help prevent escalation of privilege attacks against their cloud environments. First, track any vulnerability announcements from providers that may require an emergency patch to prevent exploitation of flaws that could elevate privileges for attackers and insiders. This should fall under the helm of vulnerability management programs already in place. Next, perform regular audits of any policies and roles defined within the cloud service environments by considering a penetration testing tool that can be run against the considered environment to find out if any policy settings may enable privilege escalation. Scanning tools from third-party providers can also be used to scan cloud configurations for security issues. Finally, scan the environment for exposed APIs using traditional network scanners and security query tools and monitor cloud environments for suspicious network traffic or user activities.

Figure 5 illustrates the mappings of threats, attacks, and cloud components in order to trace the existing vulnerabilities of the cloud components that provide opportunity attacks. In addition, this figure categorizes threats based on the STRIDE threat model and also categorizes attacks based on the OWASP attack classification.

STRIDE is an acronym that stands for six categories of security threat. Table 6 indicates that each category of threat aims to address one aspect of security. In fact, threat modeling is a process by which potential threats, such as structural

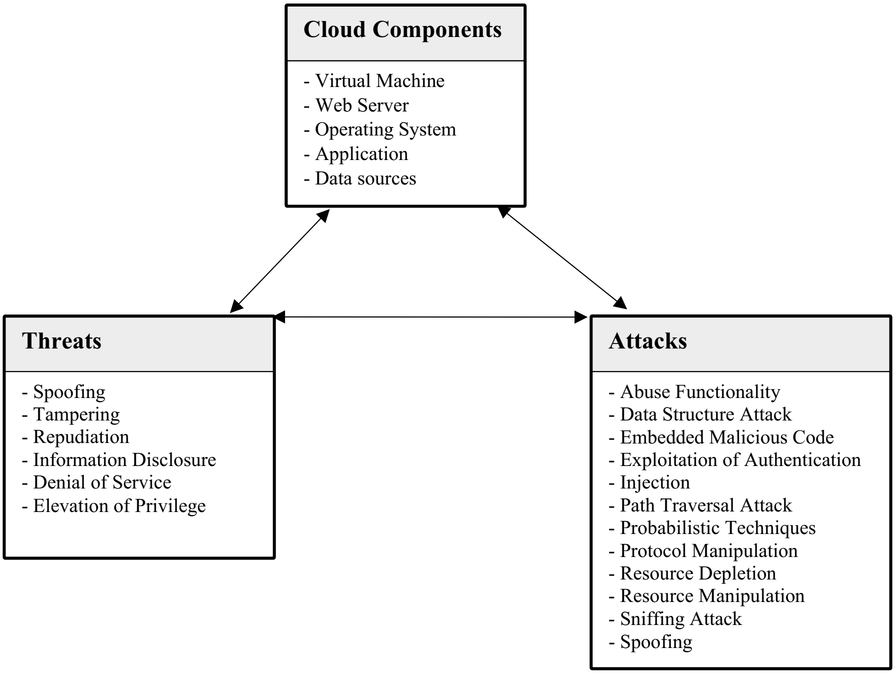

Fig. 5 Classification of cloud component, threat, and attack

Table 6 The STRIDE threat model

Threat	Desired property	Examples
Spoofing	Authenticity	User spoofs the identify of another user by brute-forcing username/password credentials
Tampering	Integrity	A user performs injection attacks on the cloud application
Repudiation	Non-repudiability	Attackers commonly erase or truncate log files as a technique for hiding their tracks
Information disclosure	Confidentiality	A user is able to eavesdrop, sniff, or read sensitive data in a database
Denial of service	Availability	The cloud storage becomes too full
Elevation of privilege	Authorization	A user takes advantage of a buffer overflow to gain root-level privileges on a system

vulnerabilities, can be identified, enumerated, and prioritized—all from a hypothetical attacker's point of view. The purpose of threat modeling is to provide defenders with a systematic analysis of the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker [65].

4.2 Cloud computing threats and risks

The Global Threat Report is an annual study published by the companies. This type of report helps shine a light on current challenges and provides a useful roadmap for your cloud security future. According Symantec's inaugural Cloud Security Threat Report (CSTR) 2019 [66], new forms of cross-cloud attacks are on the rise even as malware and DDOS attacks. The report indicates that cloud malware injection is ranked second among cloud threats after data breaches. With more workloads shifting to IaaS and PaaS, it becomes critical to take a consistent approach to discovering, monitoring, and remediating service misconfigurations, malware, and inappropriate access and privileges. In a lot of recent studies, great importance has been given to threats such as data breaches, hacked interface and application program interfaces, exploited system vulnerabilities, account hijacking, malicious insiders, denial-of-service (DOS) attacks [67, 68].

4.2.1 Data breaches

The risk of a data breach is a top concern for cloud customers. In fact, a data breach means releasing, viewing, stealing, or using protected or confidential information like personal information such as credit card numbers, Social Security numbers for any purpose which was not authorized to do. Unfortunately, there is not just one control way to prevent data breaches. The most reasonable means for preventing data breaches involve common sense security practices. This includes well-known security basics, such as conducting ongoing vulnerability and penetration testing, applying for proven malware protection, using strong passwords and consistently applying the necessary software patches on all systems. Furthermore, in the event of a successful intrusion into the environment, encryption will prevent threat actors from accessing the actual data [69].

4.2.2 Hacked interface and application program interfaces

Application programming interface (API) also known as a user interface is the way that provides access to the service. It is a program that you can operate from a remote location. This interface provides key security that can be exploited because some API's give access to the cloud customer's system and also every system has specific vulnerabilities. For this reason, staying up to date with the latest patches for software services is important. The difficulty is that this is all going on behind the scenes [70]. The client may have been hacked and even may not know it, yet identify what information was compromised, and the weak point in the cloud system that allowed for the breach, is a crucial part of keeping a competitive edge in the world today. A lot of the prevention can seem vague or unnecessary to keep data safe, but it is vital to understand security and cloud providers.

4.2.3 Account hijacking

Cloud account hijacking is a process of stealing or hijacking a cloud account by an attacker. Cloud account hijacking is a common tactic in identity theft schemes in which the attacker uses the stolen account information to carry out the malicious or unauthorized activity. In fact, when cloud account hijacking occurs, an attacker typically uses stolen credentials to impersonate the account owner. Using stolen credentials, attackers may gain access to critical areas of cloud computing services, compromising the confidentiality, integrity, and availability of those services. There are a lot of effective steps that are able to keep data secure on the cloud such as require multi-factor authentication and data security platforms. It is clear that several tools exist that require users to enter static passwords as well as dynamic one-time passwords, which can be delivered via SMS or other schemes. For bolstered data theft protection, companies should choose security platforms that extend to the cloud and mobile. These types of data security platforms should include cloud security capabilities such as end-to-end encryption, application control, continuous data monitoring, and the ability to control or block risky data activity based on behavioral and contextual factors involving the user, event, and data access type. This data-aware and comprehensive approach enables organizations to manage cloud security risks [41].

4.2.4 Malicious insiders

A malicious insider is a current or former employee or any business partner that has or had authorized access to information system creates a threat if he or she intentionally misused that access to negatively impact the security and privacy aspects of the information system. Malicious insider is a person that gains access to an organization's network, system, or data and releases this information without permission by the organization. There are many reasons an insider can be or become malicious including revenge, coercion, ideology, ego, or seeking financial gain through intellectual property theft or espionage. Protecting against malicious insiders will depend on organizations, systems, culture and business processes, and how well this is communicated and understood by staff [71]. A malicious insider's system access and knowledge of business processes can make them hard to detect. But practices can be put in place to reduce the risk of a malicious insider in organizations such as controlling removable storage, controlling outbound emails and files, requiring strong passwords, and using multi-factor authentication, access controls, etc.

4.2.5 Distributed denial-of-service attacks

DDoS attacks are able to make significant risks to cloud customers and providers, including reputational damage and exposure of customer data. DDoS stands for distributed denial of service which refers to the deployment of large numbers of

Internet bots, anywhere from hundreds to hundreds of thousands. These bots are designed to attack a single server, network, or application with an overwhelming number of requests, packets, or messages, thereby denying service to legitimate users such as employees or customers [51, 72]. To prevent this type of attack, the provider needs a battle plan, as well as reliable DDoS prevention and mitigation solutions. In fact, the provider needs an integrated security strategy that protects all infrastructure levels. Integrated security strategies such as develop a denial-of-service response plan, secure network infrastructure, and maintain strong network architecture. Threat detection is one of the most efficient ways to prevent the attack. Denial of service can come in multiple forms, and it is critical to recognize its visual indication. Any dramatic slowdown in network performance or an increase in the number of spam emails can be a sign of an intrusion. These should be addressed as soon as they are noticed, even if deviations do not look that important at first. Businesses also need to understand their equipment's capabilities to identify both network-layer and application-layer attacks with ISP, data center, or security vendor to get advanced protection resources.

4.3 Attack in the cloud

It is undeniable that cloud computing aims to provide great deals of computing resources over the Internet. While cloud computing models are full of advantages, this valuable phenomenon susceptible to both inside and outside attacks. For this reason, cloud developers improve their knowledge about key vulnerabilities, the most common types of attacks and security measures in the cloud. Due to a noticeable relationship between threats and attacks, this survey presents a top-down categorization of attack based on the OWASP regarding attack characteristics. In the following, each attack described in detail.

4.3.1 Abuse functionality

Abuse of Functionality is an attack method using the own features and functionality of any aspect of computing to attack itself or others. For example, one infrastructure that provides services in the cloud environment without the authentication method might allow any users (including the attacker or real user) to utilize the cloud computing resources to launch malicious attacks. In fact, the abuse of an application's intended functionality to perform an undesirable outcome called abuse of functionality. These attacks have various types of results such as consuming resources, circumventing access controls, or leaking information. In addition, most of the time the abuse of functionality attacks uses a combination of other types of attacks such as denial-of-service attacks, protocol exploitation, application flaws, stealing or modifying VM configuration and launching a malicious VM [73, 74].

4.3.2 Data structure attack

Data structure attacks exploit characteristics of the system by exploiting the existing vulnerabilities in data structures related to the process of system management. In addition, attackers are able to access the system data directly and encourage a violation of normal usage by running the attacks like reference manipulation, attacking shared memory and buffer overflow attacks. In fact, one of the common software coding mistakes that provide an opportunity for an attacker to obtain access to the system is a buffer overflow. To effectively alleviate buffer overflow vulnerabilities, it is vital to understand buffer overflows, their possible dangers and other techniques used to successfully exploit these vulnerabilities [75, 76].

4.3.3 Embedded malicious code

Each application might contain code that becomes malicious. In fact, the malicious code may subvert the security of the application in a noticeable way. There are various types of attacks that directly manipulate the system with malicious code including Trojan horse, trapdoor, timebomb, and logic bomb. It is always possible for a developer to insert malicious code with the intent to subvert the security of an application at the present time or in the future [77]. In addition, one embedded malicious code will not be executed until the user executes the application with the malicious code [78]. In today's world, cloud computing is interacting with its users using applications based on frameworks and programming languages that suffer from significant vulnerabilities. For this reason, cloud computing witnessed the attacks that cause VMs to escape where the attacker can access and manipulate the VM and another component of the cloud.

4.3.4 Exploitation of authentication

It is undeniable that system identification and authentication mechanisms have to deal with vulnerabilities to prevent exposing sensitive data. Moreover, these types of attacks exposed administration and management interfaces, redundant user profiles, and improper authentication and authorization can allow attackers to exploit backdoor vulnerabilities [79]. Due to the fact that in many of today's cloud computing applications, web-based applications are commonplace among developer companies. In addition, web-based applications are prime candidates for authentication brute force attempts.

4.3.5 Injection

Attackers can inject code or query into a program, or by injecting one or multiple malware onto a computer in order to modify a database. A code injection attack appears in different forms relying on the execution context of the application and the location of the programming flaw that leads to the attack [80]. This type of attack plays a noticeable role in system hacking or cracking, unauthorized access to a system in order to gain information. Moreover, the most widespread injection attacks among the other injection attacks are SQL injection and cross-site scripting (XSS).

4.3.6 Path traversal attack

The main object of path traversal attack is access files and directories that are stored outside the web-root folder. This attack accesses arbitrary files and directories stored on the file system by manipulating variables that reference files with "dot-dot-slash" sequences. In addition, this type of attacks tends to access critical system files including application source code or configuration [81, 82]. However, path traversal attack provides unauthorized access through shared folders to manipulate cloud settings such as allowing VM escape.

4.3.7 Probabilistic techniques

Probabilistic techniques refer to probability-based attacks. This kind of attack considers a probability that the attack would be successful, where other attack categories would either succeed or fail regarding reasonable reason. In fact, the attacker is able to exploit weak cryptographic systems by using different statistical and analytical approaches [83]. There various types of probability-based attacks such as attacks include bruteforce attack, side-channel attack, man in the middle attack, and misconfiguration of the client-side validation to bypass authentication.

4.3.8 Protocol manipulation

That network protocols are able to be vulnerable to well-known attacks such as attacks include denial of service, exploiting application communication flaws and modifying the contents of the XML information passed among the users and the servers to discover the security of the target [84]. In fact, incorrect implementation relating to the protocols leads to this type of attack by sending malformed messages exploiting bugs in protocol implementations, and adversaries can crash or hijack victims.

4.3.9 Resource depletion

Resource depletion attack is the attack that uses a compromised node involving in generating more network traffic which consumes the energy of the nodes. In fact, resource depletion attacks at the routing protocol layer, trying to disable networks by exhausting the energy of the nodes. Attackers are able to exhaust any computational resources like cloud resources, such as network bandwidth, memory, and other computing capabilities [85]. Due to the fact that the cloud provides scalability to deal with the workload size, the cloud is still likely to suffer from resource depletion types of attacks such as volume-based flooding protocol exploitations or exploiting application communication flaws.

4.3.10 Resource manipulation

Resource manipulation focuses on the way that manipulates one or more resources in order to violate the integrity with planned changes in systems like cloud systems. This type of attack can change the availability of resources including files, applications, libraries, infrastructure, and configuration information and also information integrity [86]. Moreover, attackers are able to break down the data and resources of the cloud by using parameter tampering. In fact, parameter tampering is one form of a web-based attack that aims to change certain parameters in the web page form field data without user authorization. There are diverse kinds of resource manipulation attacks such as manipulating a direct object reference to access unauthorized data and also modifying the XML content information between the user to server communication.

4.3.11 Sniffing attacks

Sniffing attacks can capture network traffic using a sniffer. In fact, the sniffer is an application that aims to capture network transmitted packets across networks. Moreover, if security mechanisms are misconfigured, this type of attack is able to collect sensitive data by sniffing network traffic or allowing remotely stored user data in the cloud environment [87]. Sniffing attacks are divided into passive sniffing and active sniffing. The passive sniffing captures data communicating between the two parties, and active sniffing uses tools and techniques to find information about the system. This kind of attack is able to reveal existing vulnerabilities and misconfiguration in the system. These attacks aim to obtain sensitive information on the network by scanning for open ports to find services and any vulnerabilities associated with these services. In addition, attackers are able to sniff features, parameters, and profiles in order to bypass normal authentication in a customer device. However, one of the reasonable methods that lead to good prevention against a packet sniffer is encryption. Encryption provides security for private data against malicious intruders by keeping devices safe on the network.

4.3.12 Spoofing

In the area of network security, and in particular cloud security, a spoofing attack is a set of situations in which a person or program successfully spoofs another to gain an illegitimate advantage such as spoofing metadata by impersonating a trusted email sender, DNS spoofing, IP spoofing, and phishing [88, 89]. In addition, DDoS attacks often employ spoofing in order to overwhelm a target with traffic while masking the identity of the malicious source, preventing mitigation efforts. However, this attack is able to conduct "cross-site request forgery" by forcing "the user's browser" to transmit an unauthorized command, such as forged HTTP request, forcing the user to execute malicious actions on a web application.

5 Cloud security issues in the future

Cloud computing is an emerging paradigm that involves all the basic components of computing such as end-user machines, communication networks, access management systems, and cloud infrastructures. In addition, with the emergence of new phenomena such as the 5G Internet, Internet of Things (IoT), and smart cities, the role of cloud computing will be more vital for processing and storing more information than ever before. The heterogeneity of the modern enterprise environment has added a broader set of vulnerabilities and security concerns. In recent years, organizations in the dark about how much and where data and workloads reside, making it harder to identify and mitigate mounting security risks. Without a clear picture into the cloud infrastructure, security organizations are grappling with issues from data duplication to the inability to identify threats in a timely manner, with a loss of control over data access and the protection to meet regulatory compliance. To achieve comprehensive cloud security, the data and cloud infrastructure must be protected against known/unknown attacks across all cloud components. There are several research gives her effort to solve the security problems in a cloud environment. But, still there are many open issues are present that is needed to be solved for providing a secure cloud infrastructure. The security issues related to cloud communication, network, data privacy, application, and web services are some traditional issues that are present at the beginning of cloud computing. Security issues that emerge due to multi-tenancy, virtualization, and shared pool resources are innovative security issues. In a cloud computing environment, several services and resources are available, but security level of the resources depends upon the sensitivity and value level of the resource. The privacy of the computation is open issue in cloud computing. In the storage, most of the data are in an encrypted form. But, in the storage all the operations are not performed over the encrypted data. Most of the operations required plain text data during computation. The memory assigned to the within or outside processor used for storing temporary data may be the target of attack. Therefore, research endeavors in this respect to find a broad solution that provides privacy during computation time. The cloud computing also needs a security solution against insider threat. Many solutions are available and still applicable to the cloud. But, the available solutions are not sufficient to solve the insider threat. In these phenomena, identification of the insider attack in cloud computing is an open area of research. In this scenario, an indicator is developed that helps to find the insider attacks. This indicator will increase the potential of securing the cloud system. Similarly, another open issue, to identify who is the normal user and who is the malicious user, still has a problem in a cloud environment. A growing number of security platforms have incorporated AI and machine learning to automate tasks and bring a higher level of intelligence to identify insider or outsider attack. This includes user behavior analytics, used to identify potential security risks by establishing a usage baseline over time to identify abnormal cloud activity. Too many companies are not acknowledging the perception gap in cloud security and are vastly underestimating today's threats, leaving themselves vulnerable to cloud account compromises and data exposures that pose substantial reputational and financial risk. Investment in cloud cyber security platforms that leverage automation and AI to supplement limited human resources is a clear way to automate defenses and enforce data governance principles. Automating the compilation and modeling of existing network data using behavioral analytics not only helps organizations more readily identify and classify potential threats, and it also makes them more efficient.

6 Conclusion

Cloud services are now a vital part of corporate life, bringing a momentous opportunity to accelerate business through their ability to quickly scale, allowing us to be agile with our resources, and providing new opportunities for collaboration. In fact, cloud brings many benefits to companies, organizations, and even countries. Despite bringing several advantages, the cloud still is vulnerable to many security challenges. This is why, security is the major challenge in the adoption of the cloud. The customer and vendors are well aware of security threats. In other words, the main purpose of the current study is to present all possible security challenges in the cloud computing environment and provide appropriate solution to resolve these issues. In fact, this research attempted to show various security challenges, vulnerabilities, attacks, and threats that hamper the adoption of cloud computing. Our paper provided a survey on cloud security issues and challenges that arise from the unique characteristics of the cloud. A generalized view of these issues has been presented here to enhance the importance of understanding the security flaws of the cloud computing framework and devising suitable countermeasures for them. From this line of research, we propose a review of recent security frameworks in terms of reducing vulnerabilities in order to prevent possible attacks. Throughout the article, we present a series of documented policies, procedures, and processes that define the secure management way in the cloud environment in order to reduce risk and vulnerability and increase confidence in an ever-connected world. These issues encompass the security of data and services on cloud platforms. We categorize security challenges and perform a comparative analysis of security issues and the countermeasures suggested to cope with these issues.

References

1. Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng 71:28–42
2. Mell P, Grance T (2018) SP 800-145, The NIST Definition of cloud computing | CSRC (online) Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-145/final. Accessed 11 Dec 2018
3. Xu X (2012) From cloud computing to cloud manufacturing. Robot Comput Integr Manuf 28(1):75–86
4. Pippal SK, Kushwaha DS (2013) A simple, adaptable and efficient heterogeneous multi-tenant database architecture for ad hoc cloud. J Cloud Comput Adv Syst Appl 2(1):5

5. Shi B, Cui L, Li B, Liu X, Hao Z, Shen H (2018) Shadow monitor: an effective in-VM monitoring framework with hardware-enforced isolation. In: International Symposium on Research in Attacks, Intrusions, and Defenses. Springer, Berlin, pp 670–690
6. Bhamare D, Samaka M, Erbad A, Jain R, Gupta L, Chan HA (2017) Optimal virtual network function placement in multi-cloud service function chaining architecture. Comput Commun 102:1–16
7. Alzahrani A, Alalwan N, Sarrab M (2014) Mobile cloud computing. In: Proceedings of the 7th Euro American Conference on Telematics and Information Systems (EATIS'14)
8. Deka GC, Das PK (2018) Application of virtualization technology in IaaS cloud deployment model. In: Design and Use of Virtualization Technology in Cloud Computing: IGI Global, pp 29–99
9. Oracle.com (2018) The Oracle and KPMG Cloud Threat Report 2018 ǀ Oracle (online). https://www.oracle.com/cloud/cloud-threat-report.html. Accessed 11 Dec 2018
10. Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A, Khan SU (2015) The rise of "big data" on cloud computing: review and open research issues. Inf Syst 47:98–115
11. Roman R, Lopez J, Mambo M (2018) Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future Gener Comput Syst 78:680–698
12. Ramachandra G, Iftikhar M, Khan FA (2017) A comprehensive survey on security in cloud computing. Proc Comput Sci 110:465–472
13. Csrc.nist.gov (2018) SP 500-299 (DRAFT), NIST Cloud Computing Security Reference Architecture ǀ CSRC (online). https://csrc.nist.gov/publications/detail/sp/500-299/draft. Accessed 11 Sept 2018
14. Yu S, Wang C, Ren K, Lou W (Mar 2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: Proceedings of the IEEE INFOCOM
15. Sgandurra D, Lupu E (2016) Evolution of attacks, threat models, and solutions for virtualized systems. ACM Comput Surv 48(3):1–38
16. Kaur M, Singh H (2015) A review of cloud computing security issues. Int J Adv Eng Technol 8(3):397–403
17. Kumar PR, Raj PH, Jelciana P (2018) Exploring data security issues and solutions in cloud computing. Proc Comput Sci 125:691–697
18. Khalil I, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35
19. Bashir SF, Haider S (Dec 2011) Security threats in cloud computing. In: Proceedings of the International Conference for Internet Technology and Secured Transactions, pp 214–219
20. Ryan MD (2013) Cloud computing security: the scientific challenge, and a survey of solutions. J Syst Softw 86(9):2263–2268
21. Wang C, Wang Q, Ren K, Lou W (Mar 2010) Privacy-preserving public auditing for data storage security in cloud computing. In: Proceedings of the IEEE INFOCOM
22. Singh S, Jeong Y-S, Park JH (2016) A survey on cloud computing security: issues, threats, and solutions. J Netw Comput Appl 75:200–222
23. Khalil IM, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35
24. Ahmed M, Litchfield AT (2018) Taxonomy for identification of security issues in cloud computing environments. J Comput Inf Syst 58(1):79–88
25. Fotiou N, Machas A, Polyzos GC, Xylomenos G (2015) Access control as a service for the Cloud. J Internet Serv Appl 6(1):11
26. Sumitra B, Pethuru C, Misbahuddin M (2014) A survey of cloud authentication attacks and solution approaches. Int J Innov Res Comput Commun Eng 2(10):6245–6253
27. Fernandes DA, Soares LF, Gomes JV, Freire MM, Inácio PR (2014) Security issues in cloud environments: a survey. Int J Inf Secur 13(2):113–170
28. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11
29. Zhang Y, Chen X, Li J, Wong DS, Li H, You I (2017) Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Inf Sci 379:42–61
30. Abbas H, Maennel O, Assar S (2017) Security and privacy issues in cloud computing. Springer, Berlin
31. TechRepublic (2018) Building Trust in a Cloudy Sky (online). https://www.techrepublic.com/resource-library/whitepapers/building-trust-in-a-cloudy-sky/. Accessed 11 Sept 2018
32. Basu S et al (2018) Cloud computing security challenges and solutions—a survey. In: Proceedings of the IEEE 8th Annual on Computing and Communication Workshop and Conference (CCWC), pp 347–356

33. Dzombeta S, Stantchev V, Colomo-Palacios R, Brandis K, Haufe K (2014) Governance of cloud computing services for the life sciences. IT Prof 16(4):30–37
34. Butun I, Erol-Kantarci M, Kantarci B, Song H (2016) Cloud-centric multi-level authentication as a service for secure public safety device networks. IEEE Commun Mag 54(4):47–53
35. Saevanee H, Clarke N, Furnell S, Biscione V (2015) Continuous user authentication using multimodal biometrics. Comput Secur 53:234–246
36. Khalil I, Khreishah A, Azeem M (2014) Consolidated identity management system for secure mobile cloud computing. Comput Netw 65:99–110
37. Faber T, Schwab S, Wroclawski J (2016) Authorization and access control: ABAC. In: McGeer R, Berman M, Elliott C, Ricci R (eds) The GENI book. Springer, Berlin, pp 203–234
38. Khan MA (2016) A survey of security issues for cloud computing. J Netw Comput Appl 71:11–29
39. Cai F, Zhu N, He J, Mu P, Li W, Yu Y (2018) Survey of access control models and technologies for cloud computing. Clust Comput 22(S3):6111–6122
40. Joshi MP, Joshi KP, Finin T (2018) Attribute based encryption for secure access to cloud based EHR systems. In: Proceedings of the International Conference on Cloud Computing
41. Indu I, Anand PR, Bhaskar V (2018) Identity and access management in cloud environment: mechanisms and challenges. Eng Sci Technol Int J 21(4):574–588
42. Mohit P, Biswas G (2017) Confidentiality and storage of data in cloud environment. In: Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications. Springer, Berlin, pp 289–295
43. Khan SI, Hoque ASL (2016) Privacy and security problems of national health data warehouse: a convenient solution for developing countries. In: Proceedings of the IEEE International Conference on Networking Systems and Security (NSysS), pp 1–6
44. Tang J, Cui Y, Li Q, Ren K, Liu J, Buyya R (2016) Ensuring security and privacy preservation for cloud data services. ACM Comput Surv (CSUR) 49(1):13
45. Islam MA, Vrbsky SV (2017) Transaction management with tree-based consistency in cloud databases. Int J Cloud Comput 6(1):58–78
46. Ku C-Y, Chiu Y-S (2013) A novel infrastructure for data sanitization in cloud computing. In: Diversity, Technology, and Innovation for Operational Competitiveness: Proceedings of the 2013 International Conference on Technology Innovation and Industrial Management, pp 3–25
47. Singh HJ, Bawa S (2018) Scalable metadata management techniques for ultra-large distributed storage systems—a systematic review. ACM Comput Surv (CSUR) 51(4):82
48. Sehgal NK, Bhatt PCP (2018) Cloud computing concepts and practics. Springer
49. Prokhorenko V, Choo K-KR, Ashman H (2016) Web application protection techniques: a taxonomy. J Netw Comput Appl 60:95–112
50. Shin S et al (2014) Rosemary: a robust, secure, and high-performance network operating system. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, New York, pp 78–89
51. Somani G, Gaur MS, Sanghi D, Conti M, Buyya R (2017) DDoS attacks in cloud computing: issues, taxonomy, and future directions. Comput Commun 107:30–48
52. Sattar K, Salah K, Sqalli M, Rafiq R, Rizwan M (2017) A delay-based countermeasure against the discovery of default rules in firewalls. Arab J Sci Eng 42(2):833–844
53. Iqbal S, Kiah ML, Dhaghighi B, Hussain M, Khan S, Khan MK, Choo KKR (2016) On cloud security attacks: a taxonomy and intrusion detection and prevention as a service. J Netw Comput Appl 74:98–120
54. Mishra P, Pilli ES, Varadharajan V, Tupakula U (2017) Intrusion detection techniques in cloud environment: a survey. J Netw Comput Appl 77:18–47
55. Kohnfelder L, Garg P (1999) The threats to our products. Microsoft Interface, Microsoft Corporation, New York, p 33
56. Tounsi W, Rais HJC (2018) A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput Secur 72:212–233
57. Meinig M, Sukmana MI, Torkura KA, Meinel CJPCS (2019) Holistic strategy-based threat model for organizations. Proc Comput Sci 151:100–107
58. Mokhtar B, Azab MJAEJ (2015) Survey on security issues in vehicular ad hoc networks. Alex Eng J 54(4):1115–1126
59. Tan Y, Wu F, Wu Q, Liao XJTJOS (2019) Resource stealing: a resource multiplexing method for mix workloads in cloud system. J Supercomput 75(1):33–49

60. Hong JB, Nhlabatsi A, Kim DS, Hussein A, Fetais N, Khan KMJCN (2019) Systematic identification of threats in the cloud: a survey. Comput Netw 150:46–69
61. Haber MJ, Hibbert B (2018) Asset attack vectors. Apress, Berkeley, CA
62. Rai S, Sharma K, Dhakal D (2019) A survey on detection and mitigation of distributed denial-of-service attack in named data networking. In: Sarma H, Borah S, Dutta N (eds) Advances in communication, cloud, and big data. Lecture notes in networks and systems, vol 31. Springer, Singapore
63. Bojović P, Bašičević I, Ocovaj S, Popović M (2019) A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. Comput Electr Eng 73:84–96
64. Eldewahi AE, Hassan A, Elbadawi K, Barry BI (2018) The analysis of MATE attack in SDN based on STRIDE model. In: Proceedings of the International Conference on Emerging Internetworking, Data and Web Technologies, pp 901–910
65. Tuma K, Scandariato R (2018) Two architectural threat analysis techniques compared. In: Proceedings of the European Conference on Software Architecture. Springer, Berlin, pp 347–363
66. Symantec.com (2019) Cloud Security Threat Report (CSTR) 2019 | Symantec (online). https://www.symantec.com/security-center/cloud-security-threat-report. Accessed 19 July 2019
67. Akshaya MS, Padmavathi G (2019) Taxonomy of security attacks and risk assessment of cloud computing. In: Peter J, Alavi A, Javadi B (eds) Advances in big data and cloud computing. Advances in intelligent systems and computing, vol 750. Springer, Singapore
68. Subramanian N, Jeyaraj AJC, Engineering E (2018) Recent security challenges in cloud computing. Comput Electr Eng 71:28–42
69. Tan CB, Hijazi MHA, Lim Y, Gani A (2018) A survey on proof of retrievability for cloud data integrity and availability: cloud storage state-of-the-art, issues, solutions and future trends. J Netw Comput Appl 110:75–86
70. Ghafir I, Jibran S, Mohammad H, Hanan F, Vaclav P, Sardar J, Sohail J, Thar B (2018) Security threats to critical infrastructure: the human factor. J Supercomput 74(10):4986–5002
71. Yamin MM, Katt B, Sattar K, Ahmad MB (2019) Implementation of insider threat detection system using honeypot based sensors and threat analytics. In: Future of Information and Communication Conference. Springer, Berlin, pp 801–829
72. Osanaiye O, Choo K-KR, Dlodlo MJJON (2016) Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. J Netw Comput Appl 67:147–165
73. Alsmadi I (2019) Incident response. In: The NICE Cyber Security Framework, pp 331–346
74. Fernandes G, Rodrigues JJPC, Carvalho LF, Al-Muhtadi JF, Proença ML (2018) A comprehensive survey on network anomaly detection. Telecommun Syst 70(3):447–489
75. Nashimoto S, Homma N, Hayashi Y, Takahashi J, Fuji H, Aoki T (2016) Buffer overflow attack with multiple fault injection and a proven countermeasure. J Cryptogr Eng 7(1):35–46
76. Chen Z, Han H (2017) Attack mitigation by data structure randomization. In: Cuppens F, Wang L, Cuppens-Boulahia N, Tawbi N, Garcia-Alfaro J (eds) Foundations and practice of security. FPS 2016. Lecture notes in computer science, vol 10128. Springer, Cham
77. Cohen A, Nissim N, Rokach L, Elovici Y (2016) SFEM: structural feature extraction methodology for the detection of malicious office documents using machine learning methods. Expert Syst Appl 63:324–343
78. Sangeetha R (Feb 2013) Detection of malicious code in user mode. In: Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES)
79. Lichtman M, Poston JD, Amuru S, Shahriar C, Clancy TC, Buehrer RM, Reed JH (2016) A communications jamming taxonomy. IEEE Secur Priv 14(1):47–54
80. Wu M, Moon YB (2017) Taxonomy of cross-domain attacks on cyber manufacturing system. Proc Comput Sci 114:367–374
81. Bhagwani H, Negi R, Dutta AK, Handa A, Kumar N, Shukla SK (2019) Automated classification of web-application attacks for intrusion detection. In: Lecture notes in computer science, pp 123–141
82. Chen M-S, Park JS, Yu PS (1996) Data mining for path traversal patterns in a web environment. In: Proceedings of 16th International Conference on Distributed Computing Systems, pp 385–392
83. Murugan K, Suresh P (2018) Efficient anomaly intrusion detection using hybrid probabilistic techniques in wireless ad hoc network. Int J Netw Secur 20(4):730–737
84. Ghose N, Lazos L, Li M (2018) Secure device bootstrapping without secrets resistant to signal manipulation attacks. In: Proceedings of the IEEE Symposium on Security and Privacy (SP), pp 819–835
85. Osanaiye O, Choo K-KR, Dlodlo M (2016) Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. J Netw Comput Appl 67:147–165

86. Zhang X, Zhang Y, Mo Q, Xia H, Yang Z, Yang M, Wang X, Lunand L, Duan H (2018) An empirical study of web resource manipulation in real-world mobile applications. In: Proceedings of the 27th Security Symposium (Security 18), pp 1183–1198

87. Coppolino L, D'Antonio S, Mazzeo G, Romano L (2017) Cloud security: emerging threats and current solutions. Comput Electr Eng 59:126–140

88. Gumaei A, Sammouda R, Al-Salman AMS, Alsanad A (2019) Anti-spoofing cloud-based multispectral biometric identification system for enterprise security and privacy-preservation. J Parallel Distrib Comput 124:27–40

89. Vlajic N, Chowdhury M, Litoiu M (2019) IP Spoofing in and out of the public cloud: from policy to practice. Computers 8(4):81

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