Advances in Networks
2018; 6(1): 1-13
http://www.sciencepublishinggroup.com/j/net
doi: 10.11648/j.net.20180601.11
ISSN: 2326-9766 (Print); ISSN: 2326-9782 (Online)

Identifying the Top Threats in Cloud Computing and Its Suggested Solutions: A Survey

Najib A. Kofahi, Areej Rasmi Al-Rabadi

Department of Computer Sciences, Yarmouk University, Irbid, Jordan

Email address:
nkofahi@yu.edu.jo (N. A. Kofahi), areeg.rabadi@yahoo.com (A. R. Al-Rabadi)

To cite this article:
Najib A. Kofahi, Areej Rasmi Al-Rabadi. Identifying the Top Threats in Cloud Computing and Its Suggested Solutions: A Survey. *Advances in Networks.* Vol. 6, No. 1, 2018, pp. 1-13. doi: 10.11648/j.net.20180601.11

Received: February 14, 2018; **Accepted**: March 1, 2018; **Published**: March 20, 2018

Abstract: The interest in cloud computing has increased rapidly in the last two decades. This increased interest is attributed to the important role played by cloud computing in the various aspects of our life. Cloud computing is recently emerged as a new paradigm for hosting and delivering services over the Internet. It is attractive to business owners as well as to researchers as it eliminates the requirement for users to plan ahead for provisioning, and allows enterprises to start from the small and increase resources only when there is a rise in service demand. As cloud computing is done through the Internet, it faces several kinds of threats due to its nature, where it depends on the network and its users who are distributed around the world. These threats differ in type, its side effect, its reasons, and its main purposes. This survey presents the most critical threats to cloud computing with its impacts, its reasons, and some suggested solutions. In addition, this survey determines what the main aspects of the cloud and the security attributes that are affected by each one of these threats. As a result of this survey, we order the most critical threats according to the level of its impact.

Keywords: Cloud Computing, Threats, Attacks, Deployment Models, Service Models, Networks

1. Introduction

These days, cloud computing which is also called “Cloud” plays an important role in the technology environment. It has several characteristics like on-demand self-service and broad network which increased its advantages and its benefits like scalability, availability, portability and other features that come clearly with the nature of CC and may be considered as big motivation for technology adaption. Cloud computing has received a huge attention from different people in different areas of interest due to its aforementioned advantages in addition to the huge storage and powerful computational power on different scales that it provides to its users and its services that are available at all time.

Cloud computing is a new environmental model for information and services using existing technologies like virtualization. Cloud computing environment represents a large pool of resources that can be accessed remotely by a huge number of individuals and organizations [1]. In this environment, several types of users (called customers) from different locations accesses shared resources such as memory storage, virtual servers and many other services.

It is used by several kinds of people in different ages for different purposes; some of them use the cloud to start their own business, others just want to use the services provided by service providers as on-demand services like using a free software to convert from Microsoft Word to PDF or vice versa...etc. The cloud environment has several important characteristics which include:

1. On On-demand self-service, where the customers can use the cloud services by themselves without the need to interact with the cloud provider.
2. Broad network access which means the cloud services can be used and accessed from all over the world.
3. Resource pooling, where the cloud resources are collected together to service a huge number of users.
4. Rapid elasticity which means that the number of cloud resources can be increased and decreased as needed.
5. Measured service, this means that the cloud pay as much as they use from the cloud services.

In addition to these characteristics, cloud computing environment has several benefits and advantages. Some of these advantages are [2]:

1. Cost Effective: Several organizations depend on the in-

frastructure that is provided by the cloud to build and offer its services to reduce the cost of building an infrastructure. This motivated a lot of organizations to start their own business such as Google, Amazon, and Microsoft.

2. Scalability: The cloud can provide resources with high specifications such as high memory capacity and a high computational power, which allowing users to easily expand their own business compared with the traditional technology.
3. The Speed of Implementation: One of the main advantages of cloud computing it has a high computational power. This advantage solved problems for a lot of users and business organizations especially the organizations that need a high computational power to perform services.
4. Flexibility: The cloud computing depends on the network to offer its services and to communicate with its customers. This enables the users to access the cloud from anywhere as long as they have an internet connection. This advantage increased the number of cloud customers, where anyone can access the cloud environment and use its services.

The cloud computing model consists of two main components shown in Figure 1 as presented in [3] affront end, and a back end.

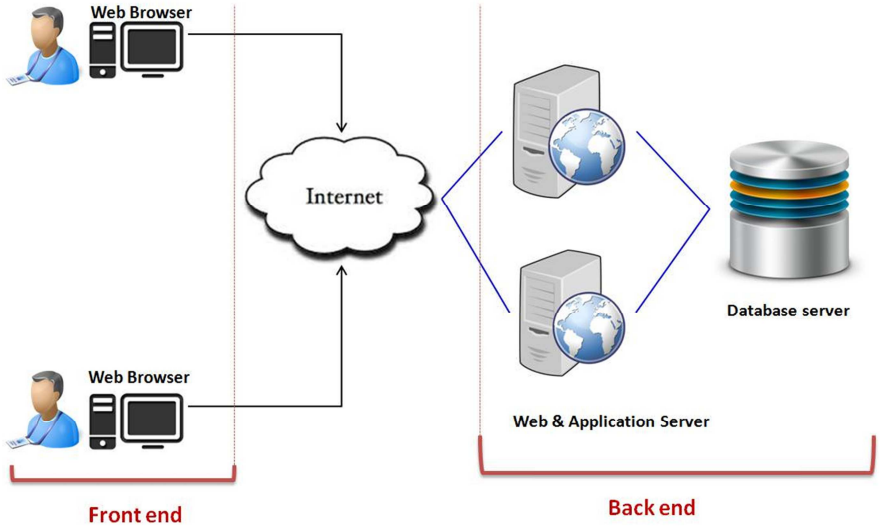

Figure 1. *The Cloud Computing Components.*

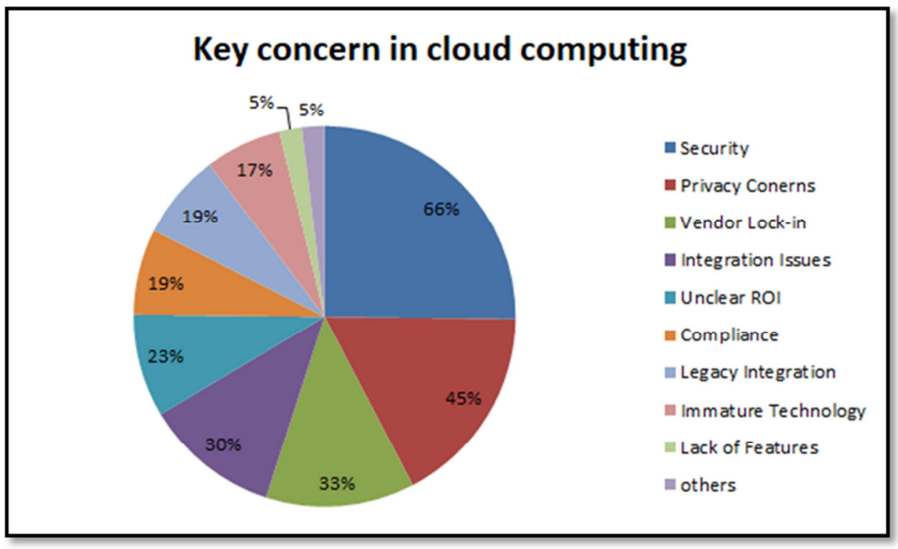

Figure 2. *Cloud Computing Issues [1].*

The front end represents the side that can be seen by the users like the computer and the applications. The back end represents the cloud system and that cannot be seen by the users like the storage medium and the cloud servers.

In addition to the previous components, the cloud environment consists of five layers presented in [4], [5]. These layers are client layer which include laptops through which cloud users can run the methods to access cloud services; cloud services and the applications that are used by cloud users are represented by the application layer; platform layer

which provides the cloud applications; infrastructure layer represents the cloud storage, database etc.; and the server layer.

Although cloud computing environment provide several advantages to its users, where it reduces the cost, increases the scalability, and it is easy to use, it also has several disadvantages. In addition to the technical problems that may occur in the cloud environment like overheating, power outages, hardware failure, and miss-configuration servers [3], it is facing several types of threats and challenges due to the distributed and dynamic nature of the infrastructure. Security and privacy is considered as one of the main challenges that cloud computing is facing. Figure 2 shows the main challenges that are related to cloud computing. As can be noticed from the figure, the security occupies the highest percentage value (66%) compared with the other challenges [1].

The security in the cloud environment is faced by the threats that threaten its users. Among these threats are malicious insiders, abuse of cloud Service, account hijacking, and denial of Services [4]. The Cloud Security Alliance in [4] identified 12 critical threats that threaten the cloud environment security. In this survey the most critical threats will be presented and evaluated according to the cloud security alliance (CSA) in [4]. Some of these threats have been considered by many researchers as top threats to cloud computing [5], [6].

The rest of the paper is organized as follows: Section 2, the Background section, introduces the main aspects of the cloud environment and the impacts of cloud environment's threats on these aspects. The related work is presented in Section 3. Section 4 describes the problem statement. The top threats to cloud computing, their main effects, the aspects of the cloud affected by each threat and other issues are discussed in section 5. Finally, Section 6 gives a general discussion and conclusions of the paper.

2. Background

The cloud environment consists of different aspects. The main aspects of the cloud environment are the deployment models, and the service models [7]. In addition to these aspects, there are cloud stakeholders and the security attributes which will be presented in the following subsections to show the impacts of cloud environment's threats on them.

2.1. Deployment Models

As presented in [8] there are four deployment models of the cloud computing: private, public, community, and the hybrid model.

1. Private Cloud: In this type, the services and the data are available only within one organization which has a set of customers. This type is used by more than 33% of organizations [8]. Examples of private clouds include: VMware Cloud Infrastructure Suite, Amazon VPC (Virtual Private Cloud) and Microsoft ECI data center.
2. Public Cloud: Services provided in this model are generally offered to public users and not to specific users. This model is usually used by the governments, academic organizations and individuals who did not need the level of security and infrastructure provided by the private model. Services in this type can be on a pay-per-use or free. Examples of this model include Google AppEngine, Amazon Elastic Compute Cloud (EC2), Sun Cloud, IBM Blue Cloud, etc.
3. Community Cloud: In this model, a set of organizations communicate and share the cloud environment infrastructure. The services are provided by a set of communicated organizations and the cloud is owned by one of these organizations. Examples of community clouds include Microsoft Government Community Cloud and Google Apps for Government.
4. Hybrid cloud: This model merges two or more of the previous models together. Some of the offered services are available to the public and some are available only to the authorized users. Examples of hybrid cloud include VMware vCloud (Hybrid Cloud Services) and Windows Azure (capable of Hybrid Cloud).

2.2. Service Models

The cloud environment has three well-known service models namely, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [9], [10].

1. Software as a Service (SaaS): In the SaaS model, the cloud provider is responsible for deploying the applications on the cloud. The cloud customers can use these applications using any web browser such as Google without installing them. The cloud provider is the only one who is responsible for these applications and the cloud infrastructure. SaaS examples include Amazon web services which include several dozens of services, online mail with spam protection, project management systems and many other services.
2. Platform as a Service (PaaS): In this model, the cloud customers can deploy and install their own applications on the cloud using tools that are offered by the cloud provider. The cloud customers can control only their own applications, where the cloud infrastructure is controlled and managed by the cloud provider. Google App Engine and Windows are examples of the customers who use the cloud to deploy and offer their own services to the public. Examples of the PaaS are Databases and web servers.
3. Infrastructure as a Service (IaaS): In this model, the cloud customers can deploy their own applications in addition to their own operating systems on the cloud by renting a cloud infrastructure from the cloud provider. The customers in this model have the whole controlling on the cloud infrastructure. Examples of IaaS providers include Amazon web services, Windows Azure, Google Compute Engine, etc. Servers, storage and networks examples of the infrastructures that can be provided by the cloud.

2.3. Cloud Computing Stakeholders

The major players of the cloud environment are classified into three categories as follows: cloud provider (Provider), the

service provider (Broker), and service customer (Consumer) [10]–[12].

1. The Service Provider (Provider): This category includes all parties that use the cloud infrastructure to offer their services like computing, networking and the storage services. Examples of cloud providers are Amazon and Terremark organizations.
2. Service Customer (Consumer): Involves any player uses the cloud services. The customers are divided into two major groups; end users, and application developer. NASA is one of the organizations that use the cloud to benefit from its high computational power.
3. The Cloud Provider (Broker): The broker is responsible for providing an appropriate environment for both service provider and service customer to communicate. Brokers provide the computing, storage, and network services. The cloud provider is like a third party who provides the PaaS and SaaS services like Salesforce.com, Amazon.com [10].

2.4. Cloud Security Attributes

The cloud stores information for a lot of users who use the cloud services, some of this information is very sensitive and very important. The attackers regardless if they are insider workers or outsiders are trying to compose this information and use it for their personal purposes. Not only the stored information need to be secret and protected but also the cloud services must be safe to motivate the customers to use it. Among the most important security attributes that must be achieved by the cloud providers are confidentiality, availability, integrity, privacy, and accountability [3], [9].

1. Confidentiality: Ensures that the stored data in the cloud are not read or accessed by any unauthorized users. This attribute can be achieved by using a strong authentication and access control mechanism [9].
2. Availability: The owners of the stored information wants to access to their information whenever they want, and to achieve this the cloud services must be available at all time to its customers. The availability can be affected by several factors like hard disk damage, and network failures [9].
3. Integrity: This attribute gives the customers of the cloud the ability to ensure the accuracy of the stored data and check if it has been modified by unauthorized users. This attribute can be achieved using a strong authentication.
4. Accountability: It refers to the tracking of which users use how much and what kind of cloud services to prevent any user from accessing any data or services that do not belong to him. At the same time, it can protect the stored data from being used by unauthorized users.
5. Privacy: This attribute focuses on the fact that cloud resources are accessed legally and used ethically by the individuals. The malicious attacker can act an ethical customer to access cloud resources and use them for their unethical purposes.

3. Related Work

Cloud computing has attracted the attention of many researchers in the last few decades. Different researchers are interested in different aspects of the cloud computing environment. Many of the researchers were interested in data security and privacy in the cloud like the research carried out in[5], [9]. These researchers considered that the data is the main resource that must be protected in the cloud due to its importance. They presented some of the techniques that can be used to protect data. Other researchers like in [12] proposed a scheme that can be used to protect the data stored in the cloud. In [3] the researchers focused on the threats and the challenges that exist in the cloud computing.

The security issue considered as a main issue in the cloud computing. The authors in [13] stated that the security issue in 2013 has occupied the highest value (87%) compared with the other issues that exist in the cloud computing. In 2016 the authors in [1] stated that the security issue occupied the highest value (66%) compared with the other issues. The security issue is determined by the number of threats that exist in the cloud computing and the level of its impacts. These threats differ in their reasons, the level of its impacts, and its purposes.

Different researchers in the cloud computing environment were interested in different types of threats and they presented and discussed different sides of these threats. The researchers in [8] defined five different types of threats, where in [3] the researchers presented 26 threats along with potential challenges and suggested solutions. Other researcher presented only the top threats to cloud computing like the researchers in [14] The threats they presented are data breaches, data loss, account hijacking, insecure API's, denial-of-service, malicious insiders, abuse of service, insufficient due-diligence, and shared technology as top threats to cloud computing. In [5] the researchers discussed data breaches, data loss, account or service hijacking, insecure interfaces and APIs, denial-of-service, data location, and malicious insiders as top threats to cloud computing.

The researchers in [6] classified the top threats to cloud computing into three categories; network, data, and cloud environment specific threats. The researchers in [15] identified 28 cloud security threat and classified them into five categories: security standards, network, access control, cloud infrastructure, and data.

The cloud security alliance (CSA) in 2010 in [16] determined that the Abuse and Nefarious Use of Cloud Computing, Insecure Interfaces and APIs, Malicious Insiders, Data Loss or Leakage, and Account or Service Hijacking as top threats to cloud computing. In 2016, the authors in [4] determined that Data Breaches, Weak Identity, Credential and Access Management, Insecure APIs, System and Application Vulnerabilities, Account Hijacking,. Malicious Insiders, Advanced Persistent Threats (APTs), Data Loss, Insufficient Due Diligence, Abuse and Nefarious Use of Cloud Services, Denial of Service, and Shared Technology as top threats to cloud computing. The cloud security alliance is not a profit organization, it just aims

to provide guides for users who want to adapt and use the cloud computing.

4. Problem Statement

In this paper we presents a survey which focuses on the most critical threats facing the use of cloud computing. These threats present a serious challenge to those who are interested in the use of the cloud computing environment. These threats are: (1) Data Breaches, (2) Insecure APIs, (3) Account Hijacking, (4) Malicious Insiders, (5) Data Loss, (6) Denial of Service, (7) Insufficient Due Diligence, (8) Shared Technology Vulnerabilities, (9) Advanced Persistent Threats, (10) Abuse Use of Cloud Services,(11) System and Application Vulnerabilities, and (12) Weak Identity, and Access Management. Each threat will be discussed as follows: describe it, list its main effects, determine what the cloud's aspects that are affected by each one of these threats, its reasons, and finally some of the suggested solutions for these threats will be presented. Figure 3 shows how each threat will be discussed.

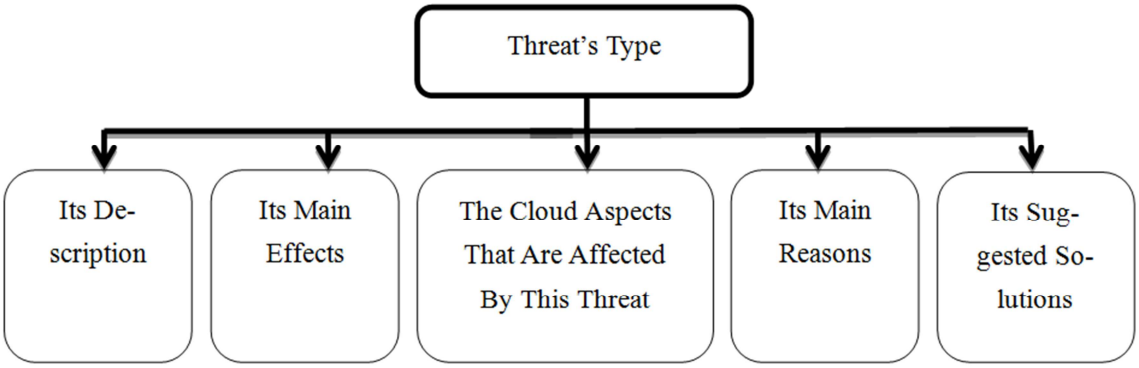

Figure 3. *The Analysis Side of each Threat.*

5. Top Threats to Cloud Computing

Since cloud computing is carried out through the use of the Internet, it is facing several threats. These threats are increasing in number and in type. This survey focuses on the most critical threats that exist in the cloud computing as presented by the Cloud Security Alliance in [4]. These threats are classified into four types in this survey. These types are: (1) Data threats including Data Loss and Data Breaches, (2) Access threats including Malicious Insiders, Weak Identity and Access Management, and Account or Service Hijacking, (3) Cloud Environment specific threats including Insecure interfaces and APIs, Insufficient Due Diligence, Shared Technology Vulnerabilities, Advanced Persistent Threats, Abuse Use of Cloud Services, System and Application Vulnerabilities, and (4) Network Threats including Denial of Service.

5.1. Data Threats

The threats that threaten the data stored in the cloud are continuously increasing. The data can be deleted, altered, used illegally by the unauthorized users, and it can be removed accidentally either by the cloud provider or by its owners. The data security is one of the biggest challenges the cloud faces. This type includes two important kinds of the threats that threaten the data loss and data breach as presented in [4], [5].

The data goes through 7 steps shown in Figure 4 to be in the cloud and available to its owners [17]; (1) Create the data, (2) Migrate it to cloud, (2) Use it, (3) Share it with specific parties, (4) Store the data on cloud using an encryption mechanism, (5) Archive the data on off-site storage media in case the cloud storage media is being out of control, (6) Destroy it when the data become unnecessary.

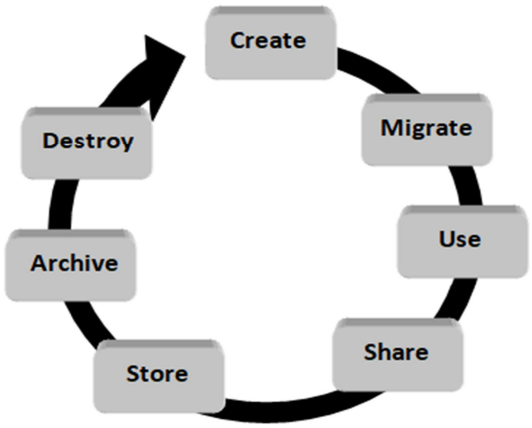

Figure 4. *Data Life Cycle In Cloud.*

5.1.1. Data Loss

In this case, the customers can lose their data either intentionally, or accidentally. Intentionally like when the malicious attackers steal the data to use it for their purposes. Accidental loss of data may be due to the occurrence of natural disaster.

5.1.2. Data Breaches

The data breach threat occurs when the customer's sensitive data is used by an unauthorized person. This threat impacts on the organizations more than the individual users especially if the organizations are large and have a huge number of customers. Because the organizations will not only lose its data but also its customers data which will cause a big loss for the organization [18]. The data security can be broken by several ways; it may occur when a virtual machine access the data of another machine, or it may occur when a recovery tool is used to erased or overwritten data [19].

The data threats regardless if data is lost or stolen by unauthorized users, its main impacts on Data Loss, and Data Breach are as follows [4]:

1. The data owners may lose their reputation.
2. The organizations may face big losses including finance, trust, and its customers.
3. It may lead the data owners to be a subject of civil and criminal lawsuits.

The number of customers using cloud computing to store their own data is increasing daily [6]. The data owners lose their control over these data when they share it with the cloud computing. The most common procedures that can be used to prevent the data from being lost or breached are as follows:

1. The Data Backup is the main preventive mechanism that can be used by cloud stakeholders. The sensitive data can be backed up in a secure manner. The problem with this solution is it increases the attacker's chance to reach the sensitive data that are backed up especially if it is not protected efficiently [6].
2. Using powerful application programming interfaces (API) for access control [5].
3. The Data Sanitization is a process used to remove the data from all storage medium. If the data is not used anymore it is removed to protect its owner. The problems with this solution are: the attacker can use a recovery tool to overwrite the data, and it is not easy to delete the data that is backed up on multimedia.
4. The Encryption mechanism. It involves encrypting the data when it is stored in the cloud or is sent through the network [6], [14]. But if the customer loses his key, then he will lose his data [4].
5. Digital Signature using the RSA algorithm to encrypt and decrypt the data and the messages [14]. The RSA algorithm is an encryption mechanism depends on the asymmetric cryptographic algorithm.

There are two main problems with both the Encryption mechanism and the Digital Signature solutions. The first problem is that these they will not work if the multi-tenant service provider database (where several users access the same database) is weak and is not designed properly, and therefore, any customer may access the other customer's data. The second problem is the appropriate key management scheme that should be used like how can securely generate and store the secret key [11].

1. Multi-factor authentication [4]. It is an access control mechanism, where the users have to provide several evidences to authenticate themselves.
2. Fine-grained data access control mechanism in [20], [21]. It is an encryption mechanism that includes a set of access policies depending on the data file attributes.
3. The Authentication Logic Model in [22]. In this model the authors use four functions to protect the data at the login time and during the usage time; Authentication function to control the user's requests to access the data, requirement function checks the conditions before the usage, authorization (for the Right requests) and obligation functions (for the obligation fulfillment) during the data usage.
4. Cloud service provider must separate the physical location of the stored data and shared computing resources [17].
5. The cloud provider can provide a permanent monitoring of access to protect the stored data like using video monitoring systems and movement sensors.
6. Using strong passwords to protect the data from the unauthorized users. The strong passwords usually include the password that has a length exceed 12 characters, and it is formed from letters and numbers [14].

5.2. Access Threats

This second class of threat involves the types of threats related to access the information of the users and their services. This type includes three kinds of threats, namely: Malicious Insiders, Weak Identity and Access Management, and Account or Service Hijacking.

5.2.1. Malicious Insiders

The insider worker may be one of the employees of the cloud or one of the business partners who has an authorized access to a cloud network. They can access cloud services and the client's data directly. These insiders may want to steal the data for the purpose of buying it or just to hurt the data owners. This threat may occur accidentally by any insider employee who upload a customer database to a public repository [4]. The level of the impact of the malicious insiders depends upon the ability that they have and the level of their authority. The side effects of the malicious insiders include the following:

1. They may lead to expose the client's sensitive data [3].
2. They have a monetary impact [3], [23].
3. Impact negatively on the productivity of the organizations who depend completely on the cloud to offer their services [23]. This may cause brand damage to these organizations.

Some of the procedures that can be followed to prevent malicious insiders from accessing wherever they want on the cloud are:

1. Define and enforce privilege rights management systems, where the insiders can access a specific data according to their IDs [3], [4].
2. Restrict the amount of information the users can access and the functions they can do [3].
3. Multi-factor authentication [23].
4. Strict Supply chain management and assessment [3], [16]. The supply chain is a relation between two or more parties who may be related by a flow of services, funds or information [24].
5. The cloud service provider's policies and procedures must be known to the cloud customers like the information security [3], [16].
6. The Encryption and key management mechanism [4].
7. Define the procedures that will be followed to notify the data owners when the data breach happens [5].

5.2.2. Weak Identity and Access Management

This threat happens if the identity system or the access management system of the cloud computing is not efficient and weak. This can lead to steal the identity of users easily by the malicious attackers and use it illegally. Since the users depend on their identities to get the cloud services and access their resources, the main impact of this threat is that the identity of the users may be stolen and used by unauthorized users. This can lead to occur other threats like the account or service hijacking which in turn can lead to other threats like data breach, spoofing…etc.

The identity system of the cloud must have the ability to handle the identity of millions of users and prevent accessing cloud resources immediately when personal changes like job termination. Some of the procedures that can be followed by the cloud service providers and the brokers to provide a strong identity system to its users are:

1. Use an efficient multifactor authentication mechanism.
2. Cryptographic keys and passwords must be changed periodically. This is useful when the keys and passwords are accessed or known by unauthorized users.
3. Try to keep the cryptographic keys, passwords, and certificates secured and do not distribute them in a public repository like GitHub.
4. Notify the users when their data or account has been breached by unauthorized users.

5.2.3. Account or Service Hijacking

This type of threats happens when the user credentials are used illegally by an authorized user. The users may be responsible for stealing their credential information like their passwords. But the cloud service provider is still responsible for providing a secure interface to its customers. The phishing is one of the methods that are used by the malicious attackers to steal the user credentials. Some of the impacts of this threat are:

1. The attacker can eavesdrop on the user activities and transactions.
2. Manipulate the user sensitive data such as alter it, use it, or delete it.
3. For the organizations that depend on the cloud computing to offer its services the attackers send falsified information to its customers or redirect them to illegitimate sites.
4. The attackers can use the user credentials to access critical areas of cloud computing.

This type of threats is very dangerous because the cloud service providers depend on the user credentials to allow them to access their own data and its services. Some of the suggested solutions to this threat are:

1. Use a strong password because now the modern password-cracking programs can easily find out and break the weak passwords [19].
2. Prevent sharing the user credential information between cloud stakeholders.
3. Use the intrusion detection systems (IDS). This system is used to verify the cloud requests (the request source) before they reach the cloud servers [6], [25]. The authors in [26] presented an IDS on the virtual machine. This system keeps monitoring the network traffic to capture the attacker addresses and block it. In [27] the authors proposed another IDS called Intrusion Prevention System (IPS). This system monitors all the incoming requests and allocates the extra resources from the available ones.
4. Multi-Level Authentication technique. The user uses the password in multi-levels to access the cloud services such as enter a password to access the cloud and enter another password to access the cloud service. Or they can give several evidences to authenticate themselves. These evidences contain at least two of the following categories: something they have, something they know, or something they are [28].
5. Two-way authentication technique. Each party authenticates himself to the other party at the same time [29].
6. The customers must understand all the security policies of the cloud computing [5].
7. Cryptographic keys and passwords must be changed periodically. This is useful when the keys and passwords are accessed or have been known by unauthorized users.
8. Notify the users when their accounts are accessed by unusual devices.

5.3. Cloud Environment Specific Threats

The cloud service providers are responsible for providing a secure environment for their users. This type includes threats that do not go to a specific type like the data type.

5.3.1. Insecure Interfaces and APIs

Application Programming Interface (API) contains a set of protocols and data formats that are used by the users to communicate with the cloud service provider. The users use it to manage and control their own data on the cloud or use its services. The APIs must be protected and controlled, where the availability of the cloud services and its security depends on its interfaces. This threat impacts on all cloud stakeholders [4]. The main impact of this threat is that it may build a barrier between the cloud service providers and their customers, which may increase the probabilities of the other threats like denial of service and data loss.

The cloud service providers are responsible for providing secure interfaces to its customers. Some of the solutions and procedures the cloud service providers can do to protect their APIs are:

1. Allow their customers to perform penetration tests against the APIs and return the results to the customers [14]. So the customer can ensure that the interfaces are safe.
2. A strong secure authentication and control access to cloud services with encryption mechanism [3], [29], like the two-way authentication technique.
3. Allow their customers to recognize and understand the dependency chain associated with the API [29].
4. Keep updating the APIs by the cloud service provider to

fix any vulnerabilities that may exist in their APIs [14].

5.3.2. Insufficient Due Diligence

Due diligence as a term means that the cloud customers have a complete information about the nature of the cloud computing [6]. Lack of understanding of cloud environment may put the cloud customers in a critical situation especially the business organizations. This threat happens due to three reasons; when the cloud service providers do not illustrate the main risk and challenges of the cloud computing [6], the cloud customers do not understand the nature of the cloud operations [30], or the customers do not have the desired expertise to deal with complex structure. The main effects of this threats are:

1. The cloud customers may face financial, legal, and commercial problems especially the business organizations [4].
2. The data and service owners may lose their controls over these data and services.

The cloud customers are responsible as well as the cloud service providers for this kind of threats. Some of the procedures that can be followed are:

1. The cloud customers must have the desired expertise to work on the cloud and deal with its complex architecture.
2. The cloud customers must have a complete information about the nature of the risks and the threats that exist in the cloud computing.
3. The cloud service providers should provide logs and detailed information about the nature of its infrastructure to their customers.
4. The cloud service providers should use the industry standards to implement the cloud applications and services like the Cloud Security Alliance guidelines.
5. Notify the users of any changes or updating in the cloud operations such as when making changes in the cloud operations.

5.3.3. Hared Technology Vulnerabilities

Vulnerability as a term means any hole or weakness that can be used by the malicious attackers. Cloud computing depends on the sharing idea, where its services and applications are shared by several users. Using shared technologies and architectures without using the appropriate protection mechanisms may cause several problems to cloud users. These vulnerabilities motivated the malicious attackers to access cloud resources as authorized users to install their own codes or to get the users data…etc. Databases and CPUs are examples of shared services. The main impacts of this type of attack are:

1. If one component is compromised, then the entire environment will be compromised. For example, if a database is compromised, then all data stored in this database will be compromised.
2. The malicious users can access cloud computing as authorized users to use its services or to install their own codes. This may be a cause for other threats like denial of service.

The cloud providers must have the ability to isolate the users who access the same resources. Some of the mechanisms that can be followed to protect the users from this kind of threats are:

1. Multi-factor authentication, where the users must go through several phases to authenticate themselves [4].
2. Host-based Intrusion Detection System (HIDS). It is an intrusion detection system that is controlled by the cloud service provider. Examples of the HIDS include the security access control policies and user login information [31].
3. Network-based Intrusion Detection Systems (NIDS). It is like the HIDS but it monitors the network traffic and monitors more than one user. The problem with this mechanism is that it cannot open the encrypted packets to check it. Example of the techniques that are used in NIDS is the signature mechanism [31].
4. Using an access control list.
5. Apply a strong compartmentalization to separate and isolate the users.

5.3.4. System and Application Vulnerabilities

The attackers can take advantage from any hole that can exist in the applications and the systems of the cloud computing. These holes can be used as a road to attack the cloud stakeholders to access their sensitive data, steal it, or to control the cloud operations [4]. The vulnerabilities that exist in the internal system of the cloud and its applications may put the cloud services and the customer's data in a critical situation. These vulnerabilities and holes called bugs and these bugs are not new and it came with the computers. Example of these bugs that can be exploited by the attackers including when several organizations and users access the same memory without taking the appropriate mechanism by the cloud service providers to isolate them.

Some of the procedures that can be followed by the cloud service providers and the cloud brokers to provide secure applications to its customers are:

1. Scan the systems and the applications periodically for any bugs that can exist.
2. Try to build and design a secure architecture to reduce the attacker's chances to access the cloud system.

5.3.5. Abuse Use of Cloud Services

This threat occurs by the purchaser and the customers when they exploit their access to the cloud services and misuse their legal access. The attackers in this threat can build their own module and services and act as legitimate providers [32]. This threat can lead to denial of service attack. Examples of this threat including send several e-mail spams to the cloud servers, brute-force password attack to guess the passwords, or SQL injection attacks to exploit the bugs that exist in the systems. Some of the suggested solutions for this threat are:

1. Network intrusion detection system.

Impose strict rules for registration and validation process.

2. Monitor the credit card transactions to capture the fraud transactions.
3. Intrusion detection system, like the system presented in [33]. This system is used to monitor the behaviors of the customers to identify the malicious behaviors.

4. The system that is presented in [34]. This system imposes the users pay a small deposit before using the service and if later, it turned out they are not malicious attackers they will get back their deposit.

5.4. Network Threats

Because the cloud computing depends on the network completely, it is normal to face all the possible threats that can exist on the network. This type concerns on threats that happen due to the nature of the network. The brokers and the cloud service providers depend on the network to offer their services and to communicate with the customers. The network threats type contains two important threats [9], [35].

5.4.1. Denial of Service

The cloud services must be available at all time to the customers. This threat can happen when the attackers keep cloud resources busy to perform specific services that need a high computational power and memory storage. This attack may lead to consume cloud resources like the servers power, memory, and network bandwidth [3]. Therefore, the users will not be able to access cloud services. Recently, there are 81 percent of the cloud users consider this threat as a significant threat [6], [8]. The most popular example of this threat is the Distributed Denial Of Service (DDOF) when a user or a set of users send a large number of requests to cloud to consume its resources [36].

The main impact of this threat is that it consume the cloud resources [22] which lead to waste the customers time and frustrate them while they are waiting for their processes to be finished [4]. The main resources that are affected by this type of threats are:

1. Memory: The attacker can send several messages and requests to the cloud server to fill its buffer. When the server buffer became full, it will be unable to receive any new request.
2. Network Bandwidth: When the attacker sends several requests to cloud server more than the network bandwidth, a lot of requests will be dropped including the legal requests.
3. Cloud Server Computing Time: It occurs when the attacker makes the cloud server busy to perform services that need a high computational power. An example of this request is when the attacker sends a message to the cloud server that contains a large number of references to external entities. This will force the server to be busy to open all of these references to download the external entities.

Several solutions have been proposed to protect the cloud computing from this kind of threats. Some of the suggested solutions for this threat are:

1. The cloud service provider should be aware of the implementation of the application. The applications should not have any loop that can be used by the attackers [6].
2. The intrusion detection systems (IDS). This system monitors all incoming requests and allocated the extra resources from the available ones.
3. Increase the network bandwidth to increase the chances of cloud customers to access cloud services [6].
4. Service Level Agreement (SLA) technique. It is like a contract between the cloud service provider and its customers to prevent this attack. It protects the cloud resources like the Data Segregation, and the Data Location [25].
5. The Network Firewall. The firewall is the first line to protect the cloud server from the unknown requests [37]. In [38] the authors proposed a clustering firewall. They divided the cloud servers into clusters and each cluster has a firewall to protect the applications in that cluster.
6. The virtual machine monitor that is presented in [39]. This machine is used to monitor the available resources and compares it with a specific value to determine if there is an attack.
7. DDoS Attack Mitigation Architecture. The authors in [40] proposed a new architecture to defend against DDoS. In this architecture, they merged a highly programmable network monitoring (The Software-Defined Networking (SDN)) to enable attack detection with a flexible control structure to allow fast and specific attack reaction. The SDN is an approach that provides the ability to change the network infrastructure and manage its services [25], [41].
8. In [40] the authors proposed a multilayered security architecture based on the IDS, honeypots (it is a computer detection mechanism used to detect and face the unauthorized users), and firewalls. The architecture layers are: (1) the perimeter defense; (2) the deceptive; (3) the detection and (4) the cryptography.

5.4.2. Advanced Persistent Threats (APTs)

This threat refers to a group of people or organizations that target the Business organizations and companies through the network. The attackers in this threat attack the infrastructure of the companies and set up their own codes to monitor their objectives for a long period of time [42]. These attackers have specific targets, they may want to steal secret files, fabricate files…etc. A good example of this threat is the attack that happens on the companies that are responsible for the intellectual properties to produce fake patents.

Some of the means that can be used by APT attackers to get access to the network of the target companies are: unsecured links or files, Spear-Phishing (it is an email-spoofing attack), through the USB devices that have the attacker code, or any other means that can help to distribute and transfer the attack code. So the staff should be careful when they want to open files or links that exist on the network. The usual defense means like the anti-viruses and the firewalls cannot face and detect this kind of threats. The most important defense means that are used to face this attack are [42]:

1. Hardware-based. In this solution, a special hardware is placed on the edge of the network to monitor its traffic to protect it and to inform the target companies about any unusual or suspected movements on the network. But the problems with this solution are its costly which limits its

numbers, and it cannot monitor and record all the network traffic due to the high number of the remote devices and the workstations.

2. Cloud-based. This solution came to solve the limitations of the Hardware-based solution. It is implemented as a multi-user platform to monitor the network traffic efficiently and provide a real-time analysis of the network traffic.
3. Defense-in-depth strategy. It provides protection for each layer of the network (the people, the devices, and the applications). It monitors the network traffic and the security control permanently.
4. Train the staff of the companies very well especially the IT staff.

In addition to the previous solutions, there are other solutions that can be followed to minimize the lost as much as possible like Isolate the core network, Disconnect from the infected host, and analyze the attacking routine [43].

It is important to note that, all the previous solutions will not work if the cloud service provider and the brokers do not provide the appropriate physical security like:

1. Provide the appropriate level of the security for the server rooms and the dedicated computers using physical barriers like doors, fences or any access control mechanism.
2. The location of the cloud center must be safe and far enough geographically from any location that is exposed to any natural disasters like flooding.

A list of the top 12 threats and the relation of these threats with the cloud aspects are presented in Table 1 below:

Table 1. *The Relation Between Threats and The Cloud Aspects.*

Threat Name	Deployment Models	Service Models	Security Attributes	Cloud Stakeholders
Data Loss	-Private Cloud - Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Paas	- Availability.	-Customers. -Service providers.
Data Breach	- Private Cloud - Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas - Paas	- Confidentiality. - Integrity.	-Customers. -Service providers.
Insecure API	- Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas - Paas	- Confidentiality. - Availability. - Integrity. - Accountability.	-Customers. -Service providers.
Malicious insiders	- Private Cloud - Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas - Paas	- Confidentiality. - Availability. - Integrity. - Privacy.	-Customers. -Service providers.
Denial of service	- Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas - Paas	- Privacy - Availability.	-Customers. -Service providers.
Account or Service Hijacking	- Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas - Paas	- Confidentiality. - Availability. - Integrity. - Privacy.	-Customers.
Insufficient Due Diligence	- Private Cloud - Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas - Paas	- Confidentiality. - Availability. - Integrity.	-Customers. -Service providers.
Shared Technology Vulnerabilities	- Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas - Paas	- Confidentiality. - Availability. - Integrity.	-Customers. -Service providers.
Weak Identity and Access management	- Private Cloud - Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas - Paas	- Confidentiality. - Availability. - Integrity.	-Customers. -Service providers.
System and Application Vulnerabilities	- Private Cloud - Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas - Paas	- Confidentiality. - Availability. - Integrity. - Accountability.	-Customers. -Service providers. -Brokers
Advanced Persistent Threats (APTs)	- Private Cloud - Public Cloud - Community Cloud. - Hybrid cloud.	- Saas - Iaas	- Confidentiality. - Privacy.	-Brokers. -Service providers.
Abuse Use of Cloud Services	- Public Cloud - Community Cloud. - Hybrid cloud.	- Iaas - Paas	- Confidentiality. - Availability. - Privacy.	-Brokers. -Service providers.

There are several reasons that stand behind each threat. These reasons may happen either intentionally, or accidentally. Throughout the years, the researchers have tried to find solutions to face these threats and make the cloud more secure and trustable. Some of these solutions did not work very well. Table 2 below shows a summary of the main reasons for each threat with suggested solutions that have been mentioned previously in this survey.

Table 2. *List Of The Top Threats With A Few Of Its Reasons And It Suggested Solutions.*

Threat Name	Its Reasons	Its Main Suggested Solutions
Data Loss	- Delete it or alter it without backup it. - Natural disasters like Earthquake. -Side factors like disk failure, the customer loses his encryption key.	- Data backup. - Encryption. - Authentication mechanism.
Data Breach	- A virtual machine has ability to access the data stored on another machine. - It may occur when a recovery tool is used to erase or overwritten data. - A poor multi-tenant database.	- Access Control. - Digital Signature and Encryption. - Strong passwords.
Insecure API	- Anyone can use the cloud service provider's APIs.	-Monitoring process. -Encryption mechanism. -Access control. -Authentication mechanism.
Malicious insiders	- The insider workers have a direct access to the data stored in the cloud and its services.	-Identify the cloud service provider's policies. -Encryption mechanism. -Access control. -Authentication mechanism.
Denial of service	- When the attacker sends a large number of requests that need a high computational power to the cloud servers.	- Access control. - Avoiding the applications that have a loop or requests that need a huge number of references. - IDS
Account or Service Hijacking	- Phishing, Fraud…etc.	- IDS. - Strong passwords. - Authentication mechanism. - Prevent the users from sharing their credentials.
Insufficient Due Diligence	- The customers start working on the cloud computing without knowing its challenges and its nature. - The customers do not have the desired expertise to work on it.	- Using industry standard to implement the cloud applications and services. - perform a risk assessment of the cloud resources. - notify the user if there any updating in the cloud operations. - Monitor the cloud resources.
Shared Technology Vulnerabilities	- The cloud computing architecture is not designed properly to enforce a strong isolation between the users.	- Apply a strong compartmentalization to separate and isolate the users. - Access control. - Authentication mechanism. - HIDS and NIDS.
Weak Identity and Access management	- Weak passwords. - The cryptographic keys, passwords, and certificates are not changed periodically. - The multifactor authentication do not used efficiently. - The identity system of the cloud and its identity access management are weak and they are not updated efficiently.	- Try to keep the cryptographic keys, passwords, and certificates secure and do not distribute them in a public repository like GitHub. - Cryptographic keys and passwords must be changed periodically. - Multifactor authentication. - Notify the users when their data or account has been breached by unauthorized users.
System and Application Vulnerabilities	- Vulnerabilities that can exist in the operating system of the cloud, its applications, and its system.	- Scan the systems and the applications periodically for any bugs or any vulnerabilities.
Advanced Persistent Threats (APTs)	- Unsecured links and files. - Spear-Phishing. - The USB devices that have the attacker code.	- Hardware-based. - Cloud-based - Defense-in-depth strategy. - Staff training. -Intrusion detection system
Abuse Use of Cloud Services	- Unsecured services. - free trail services.	- Impose strict rules for registration and validation process. - Monitor the credit card transactions to capture the fraud transactions.

5. Discussion

The threats that have been presented in this survey can be ordered according to the dangers they present as follows: (1) insecure interfaces and the APIs, (2) Weak Identity and Access management, (3) System and Application Vulnerabilities, (4) Shared Technology Vulnerabilities, (5) Advanced Persistent Threats (APTs), (6) Malicious insiders, (7) Account or Service Hijacking, (8) Data Breach, (9) Insufficient Due Diligence, (10) Data Loss, (11) Abuse Use of Cloud Services, and (12) Denial of service.

The interfaces take the first rank because they are the main means that are used by the cloud service providers to communicate with their customers. They have also several benefits. They are used by the users to access their data and services. The users also pay for services through the interfaces. Insecure interfaces may be a reason to cause other threats to occur. It may prevent the customers from reaching their services or data causing the denial of service. Then the weak identity system threat is the next critical one as it may help the unauthorized users to access the accounts and the data of other users and use it for their purposes. So this threat can be a reason for other threats like account hijacking and data breach. Then the Advanced Persistent Threat take the next rank because this type of threats is not easy to be detected. But in this threat, the attackers take advantage of the vulnerabilities that exist in the cloud system.

The data is the main resource that must be protected in the cloud environment and its protection depends on the cloud service providers and the owners of these data. The owners of the data are responsible for losing their data or being breached if they start working on the cloud and store their sensitive data on it without knowing how to work with the cloud or they were careless about their passwords or any other protection key they used.

6. Conclusion

In this survey, the most critical threats that exist in cloud computing with their side effects and its suggested solutions have been presented. The level of the impact of these threats depends on the power of the attackers, and their purposes. Some of these threats may be a cause for other threats like the insecure APIs may increase the probability of the account or service hijacking threat. Another example is the account hijacking threat may increase the probability of the data lose beach threats. Confronting these threats does not depend only on the cloud service provider and the brokers, but also depends on the cloud customers. For example in the Insufficient Due Diligence threat, the users must be ready to work on the cloud architecture and they must be aware of its threats and risks. There is no complete solution that can prevent the cloud threats and give its customers a full security. These solutions can reduce the level of the impact of these threats and give its customers some kind of protection.

References

[1] C. T. S. Xue and F. T. W. Xin, “Benefits and Challenges of the Adoption of Cloud Computing in Business,” *Int. J. Cloud Comput. Serv. Archit.*, vol. 6, no. 6, pp. 01–15, 2016.

[2] S. Kaisler, W. H. Money, and S. J. Cohen, “A Decision Framework for Cloud Computing,” *2012 45th Hawaii Int. Conf. Syst. Sci.*, pp. 1553–1562, 2012.

[3] I. Ahmad, H. Bakht, and U. Mohan, “Cloud Computing – Threats and Challenges,” *J. Comput. Manag. Stud.*, vol. 1, no. 1, 2017.

[4] Cloud Security Alliance, “The Treacherous 12 Cloud Computing Top Threats in 2016,” *Security*, no. February, pp. 1–34, 2016.

[5] S. Aldossary and W. Allen, “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 4, pp. 485–498, 2016.

[6] M. Kazim and S. Zhu, “A Survey on Security Threats in Cloud Computing Technology,” *Int. J. Res.*, vol. 1, no. 8, pp. 1071–1081, 2015.

[7] T. Islam, D. Manivannan, and S. Zeadally, “A Classification and Characterization of Security Threats in Cloud Computing A Classification and Characterization of Security Threats in Cloud Computing,” no. March, 2016.

[8] G. Aswini and R. Mervin, “A Survey on Cloud Security Issues and Techniques,” *Int. J. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 125–132, 2016.

[9] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, “Data Security and Privacy in Cloud Computing,” *Int. J. Distrib. Sens. Networks*, vol. 2014, 2014.

[10] K. M. Khan, “Security dynamics of cloud computing,” *Cut. IT J.*, vol. 22, no. 6–7, pp. 38–43, 2009.

[11] M. Al Morsy, J. Grundy, and I. Müller, “An analysis of the cloud computing security problem,” *17th Asia-Pacific Softw. Eng. Conf. (APSEC 2010) Cloud Work. Aust.*, no. December, p. 7, 2010.

[12] I. Iyoob, E. Zarifoglu, and A. B. Dieker, “Cloud Computing Operations Research,” *Serv. Sci.*, vol. 5, no. 2, pp. 88–101, 2013.

[13] a Omotunde, O. Awodele, O. Kuyoro, and C. Ajaegbu, “Survey of Cloud Computing Issues at Implementation Level,” *CIS J.*, vol. 4, no. 1, pp. 91–96, 2013.

[14] S. Pandey and M. Farik, “Cloud Computing Security : Latest Issues & Countermeasures,” *Int. J. Sci.*, vol. 4, no. 11, pp. 3–6, 2015.

[15] I. Khalil, A. Khreishah, and M. Azeem, “Cloud Computing Security: A Survey,” *Computers*, vol. 3, no. 1, pp. 1–35, 2014.

[16] Cloud Security Alliance, “Top Threats to Cloud Computing,” *Security*, no. March, pp. 1–14, 2010.

[17] P. Sareen and T. Singh, “Data Security in Cloud Computing,” *Int. J. Comput. Sci. Eng.*, vol. 2, no. 1, pp. 1–169, 2015.

[18] P. Kumar and L. Kumar, “Threats to Cloud Computing Security,” *Int. Technol. Conf.*, vol. 2014, no. 3, pp. 79–84, 2014.

[19] Y. McDermott, “Conceptualising the right to data protection in an era of Big Data,” *Big Data Soc.*, vol. 4, no. 1, p. 205395171668699, 2017.

[20] M. Xiao, M. Wang, X. Liu, and J. Sun, “Efficient distributed access control for big data in clouds,” *Proc. - IEEE INFOCOM*, vol. 2010–Augus, no. BigSecurity, pp. 202–207, 2015.

[21] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” in *2010 Proceedings IEEE INFOCOM*, 2010, pp. 1–9.

[22] M. Shahpasand, M.. Rana, R. Mahmod, and N.. Udzir, “Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014),” in *An Evidence Collection and Analysis of Ubuntu File System*, 2016, no. JUNE 2014, pp. 105–112.

[23] A. Mahajan and S. Sharma, “The Malicious Insiders Threat in the Cloud,” *Int. J. Eng. Res. Gen. Sci.*, vol. 3, no. 2, pp. 245–256, 2015.

[24] M. Lindner, C. Chapman, S. Clayman, D. Henriksson, and E. Elmorth, “The Cloud Supply Chain : A Framework for Information, Monitoring, Accounting and Billing,” *2nd Int. ICST Conf. Cloud Comput.*, 2010.

[25] A. Bonguet and M. Bellaiche, “A survey of Denial-of-Service and distributed Denial of Service attacks and defenses in cloud computing,” *Futur. Internet*, vol. 9, no. 3, 2017.

[26] A. Bakshi and Y. B. Dujodwala, “Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine,” in *2010 Second International Conference on Communication Software and Networks*, 2010, pp. 260–264.

[27] S. Yu, Y. Tian, S. Guo, and D. O. Wu, “Can We Beat DDoS Attacks in Clouds?,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2245–2254, Sep. 2014.

[28] W. Liu, A. S. Uluagac, and R. Beyah, “MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data,” *Proc. - IEEE INFOCOM*, pp. 518–523, 2014.

[29] M.. Potey, D. Dhote, and D.. Sharma, “Cloud Computing – Understanding Risk, Threats, Vulnerability and Controls : A Survey What Comprises Cloud Computing ?,” *Int. J. Comput. Appl.*, vol. 67, no. 3, pp. 9–14, 2013.

[30] C. Racuciu, “Security Threats And Risks In Cloud Computing,” *Nav. Acad. Sci. Bull.*, vol. XVIII, no. 1, pp. 105–108, 2015.

[31] Y. Tayyeb and D. S. Bhilare, “Cloud security through Intrusion Detection System (IDS): Review of Existing Solutions,” *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 4, no. 6, pp. 213–215, 2015.

[32] Y. A. Hamza and M. D. Omar, “Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing,” *Int. J. Comput. Eng. Res.*, vol. 3, no. 6, pp. 22–27, 2017.

[33] F. Doelitzscher, M. Knahl, C. Reich, and N. Clarke, “Anomaly Detection in IaaS Clouds,” in *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*, 2013, pp. 387–394.

[34] J. Szefer and R. B. Lee, “BitDeposit: Deterring attacks and abuses of cloud computing services through economic measures,” *Proc. - 13th IEEE/ACM Int. Symp. Clust. Cloud, Grid Comput. CCGrid 2013*, no. May, pp. 630–635, 2013.

[35] Cloud Security Alliance, “The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.” 2013.

[36] M. Ficco and M. Rak, “Stealthy denial of service strategy in cloud computing,” *IEEE Trans. Cloud Comput.*, vol. 3, no. 1, pp. 80–94, 2015.

[37] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in Cloud,” *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, Jan. 2013.

[38] M. Liu, W. Dou, S. Yu, and Z. Zhang, “A clusterized firewall framework for cloud computing,” in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 3788–3793.

[39] S. Zhao, K. Chen, and W. Zheng, “Defend Against Denial of Service Attack with VMM,” in *2009 Eighth International Conference on Grid and Cooperative Computing*, 2009, pp. 91–96.

[40] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, “DDoS attack protection in the era of cloud computing and Software-Defined Networking,” *Comput. Networks*, vol. 81, pp. 308–319, Apr. 2015.

[41] D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” *Proc. IEEE*, vol. 103, pp. 1–61, 2014.

[42] A. Rot and B. Olszewski, “Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection,” in *In 2017 Federated Conference on Computer Science and Information Systems*, 2017, vol. 13, pp. 113–117.

[43] G. Yang, Z. Tian, and W. Duan, “The prevent of advanced persistent threat,” *J. Chem. Pharm. Res.*, vol. 6, no. 7, pp. 572–576, 2014.