applied sciences

MDPI

Review

Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges

Yara Alghofaili [1], Albatul Albattah [1], Noura Alrajeh [1], Murad A. Rassam [1,2,*] and Bander Ali Saleh Al-rimy [3]

[1] Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia; 411207305@qu.edu.sa (Y.A.); 411207333@qu.edu.sa (A.A.); 411200195@qu.edu.sa (N.A.)
[2] Faculty of Engineering and Information Technology, Taiz University, Taiz 6803, Yemen
[3] Faculty of Engineering, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia; bander@utm.my
* Correspondence: m.qasem@qu.edu.sa

Abstract: Cloud computing is currently becoming a well-known buzzword in which business titans, such as Microsoft, Amazon, and Google, among others, are at the forefront in developing and providing sophisticated cloud computing systems to their users in a cost-effective manner. Security is the biggest concern for cloud computing and is a major obstacle to users adopting cloud computing systems. Maintaining the security of cloud computing is important, especially for the infrastructure. Several research works have been conducted in the cloud infrastructure security area; however, some gaps have not been completely addressed, while new challenges continue to arise. This paper presents a comprehensive survey of the security issues at different cloud infrastructure levels (e.g., application, network, host, and data). It investigates the most prominent issues that may affect the cloud computing business model with regard to infrastructure. It further discusses the current solutions proposed in the literature to mitigate the different security issues at each level. To assist in solving the issues, the challenges that are still unsolved are summarized. Based on the exploration of the current challenges, some cloud features such as flexibility, elasticity and the multi-tenancy are found to pose new challenges at each infrastructure level. More specifically, the multi-tenancy is found to have the most impact at all infrastructure levels, as it can lead to several security problems such as unavailability, abuse, data loss and privacy breach. This survey concludes by giving some recommendations for future research.

Keywords: cloud computing; secure cloud infrastructure; application security; network security; host security; data security

check for updates

Citation: Alghofaili, Y.; Albattah, A.; Alrajeh, N.; Rassam, M.A.; Al-rimy, B.A.S. Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. *Appl. Sci.* **2021**, *11*, 9005. https://doi.org/10.3390/app11199005

Academic Editors: Gianluca Lax and Antonia Russo

Received: 1 September 2021
Accepted: 23 September 2021
Published: 27 September 2021

1. Introduction

The idea behind cloud computing is to provide all possible facilities such as software, IT infrastructure, and services to its customers for use over the internet. Cloud computing systems are large-scale, heterogeneous collections of autonomous systems and flexible computational architecture. This technology is emerging, as it is considered the first choice for businesses that do not want to deal with the in-house maintenance of systems and a development team [1]. Many businesses, such as Amazon AWS, Google, IBM, Sun, Microsoft, and many others, are developing efficient cloud products and technology [2]. In cloud technology, data are shared via virtual data centers from the customers and the organization [2].

Cloud computing has evolved as a popular and universal paradigm for service-oriented computing where computing infrastructure and solutions are delivered as a service. The cloud has revolutionized the abstraction and use of computing infrastructure through its features (e.g., self-service on-demand, broad network access, resource pooling, etc.), making cloud computing desirable [3]. However, security is the biggest challenge, and concerns regarding cloud computing continue to arise as we witness an increasing number of new developments in cloud computing platforms [4]. In the post-COVID-19 world, it is clear that more people and businesses are adopting cloud services, software, and infrastructure, as they can be accessed anytime, and from anywhere. To handle security risks, several research works and developments, such as in [5–8], have been proposed. Nonetheless, there are still more opportunities for new techniques to make the cloud more secure. Most of the existing techniques for securing the cloud do not focus on the new types of security risks that might face the cloud computing infrastructure. Hence, they cannot detect attacks or vulnerabilities that might come from the cloud service provider's side or the consumer's side. Furthermore, very few existing works have examined the different levels of cloud infrastructure altogether. Due to the high importance of investigating such issues, this paper conducted an extensive survey on the issues that the cloud computing infrastructure faces at different levels (application, host, network, and data level). It also presents the existing solutions used to mitigate these issues. Additionally, this paper highlights some open challenges that still need to be solved and suggest directions for future work. To the best of our knowledge, this study is the first effort to provide a systematic review of associated security issues and solutions based on cloud levels (application, host, network, and data level). The following are the main contributions of this study:

1. Conducting a systematic evaluation of 103 articles on cloud infrastructure in connection with attacks and defenses.
2. Providing a new taxonomy for a systematic review of cloud infrastructure levels.
3. Investigating four levels that aim to cover all vulnerabilities that might come from the cloud service provider's side or the consumer's side.
4. Identifying the limitations of the examined studies and highlighting the open research challenges and proposed directions for future work.

The rest of this paper is divided into eight sections: the methodology of this study is presented in Section 2. The background on cloud computing is given in Section 3. The current security issues that cloud infrastructure faces at different levels are investigated in Section 4. Section 5 presents the solutions proposed to solve the related security issues in the literature. The open challenges that still need to be solved are presented in Section 6. Section 7 suggests some future directions. The paper is concluded in Section 8.

2. Methodology

This study was based on the systematic literature review (SLR). The phases in this study are divided into three, which are depicted in Figure 1.

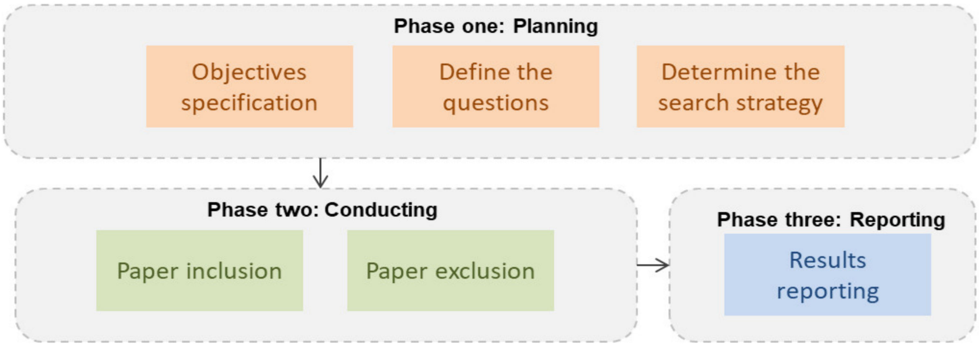

Figure 1. The methodology of the study.

2.1. Planning the Review Phase

This phase contains three sub-phases: obtaining the research objectives, defining the research questions, and determining the search strategy used in the study.

2.1.1. Research Objectives

The following are the study's primary objectives:

1. To quantify and expand upon the current state-of-the-art literature on secure cloud infrastructure to provide a new taxonomy.
2. To present an in-depth review of various issues and solutions that are used in cloud infrastructure at various levels (application, host, network, and data).
3. To highlight the limitations and pitfalls of the current solutions in terms of research challenges and future opportunities.

2.1.2. Research Questions

The study considers answering two important questions, which are described below, to achieve the objectives.

Q1: What are the well-known issues and the proposed solutions in cloud infrastructure at its various levels?

Q2: What are some of the security issues that could stymie widespread cloud computing adoption?

2.1.3. Search Strategy

During this study, various academic digital databases are used to extract related studies, including Springer, IEEE Xplore, ScienceDirect, ACM Digital Library, Arxiv, and some other related international conferences, as shown in Figure 2. These databases are considered to be sufficient for covering the most up-to-date and reliable literature on cloud infrastructure issues and existing security solutions. The literature search was extensively conducted from 2011 to 2020, as shown in Figure 3. This study queried major libraries, utilizing a combination of various search keywords that evolved utilizing a reduplicate operation to maximize the number of pertinent studies in order to obtain accurate search results (optimal results). Therefore, the most used combinations of words included: “Cloud Computing”, “Secure Cloud Infrastructure”, “Application Security”, “Network Security”, “Host Security”, and “Data Security”. Based on these keywords, the studies were grouped into different categories to map the pertinent studies based on cloud infrastructure levels, such as application, network, host, and data. This procedure includes extracting from the abstracts of the studies some keywords and concepts that reflect the contributions of the studies.

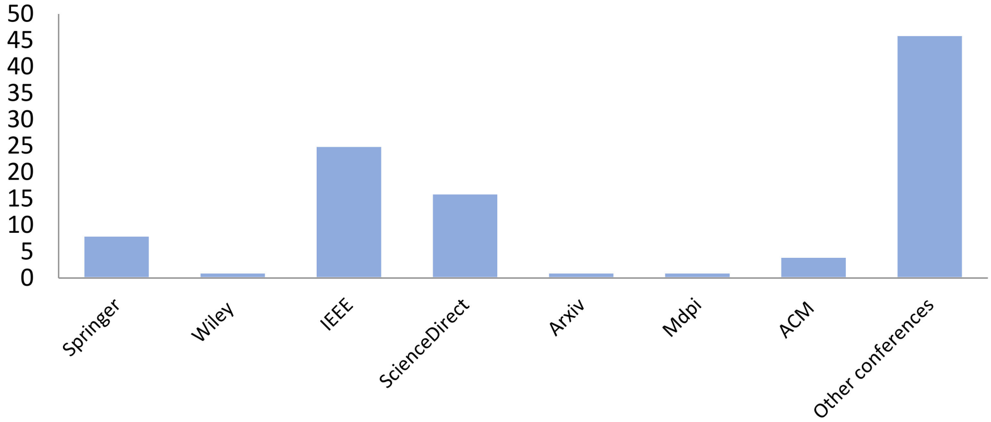

Figure 2. Number of papers selected from each academic database.

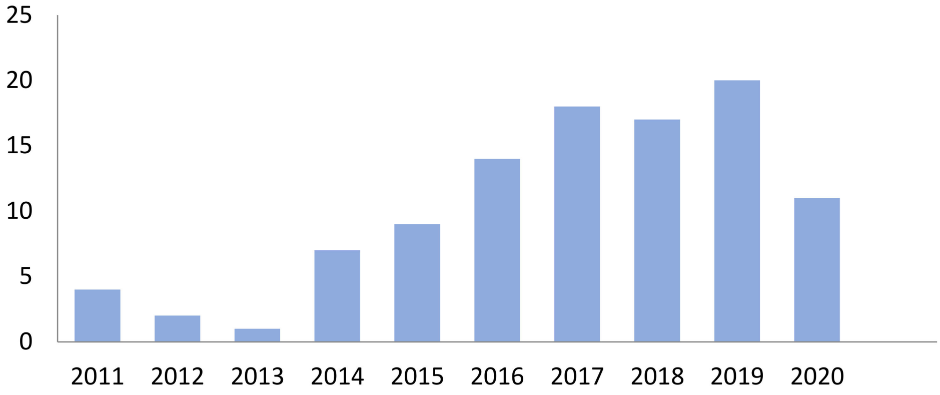

Figure 3. Number of papers selected over years.

2.2. Conducting the Review Phase

This phase defines the criteria of inclusion and exclusion followed in this study.

For inclusion,

1. The publication was written in English.
2. The publication addressed the issue or solutions for cloud infrastructure security covering one or more levels.
3. The publication was more than 4 pages.

For exclusion,

1. The publication was written in a language other than English.
2. The publication discussed cloud infrastructure from a non-secure side.
3. The publication did not cover any level of cloud infrastructure.
4. The publication was less than 4 pages.

2.3. Reporting the Results Phase

The search yielded a total of 531 publications. After eliminating duplicated publications, the total number decreased to 326. A total of 74 publications did not fulfill the inclusion criteria and were thus eliminated. Among the remaining 252 publications, 149 did not cover the security of cloud infrastructure at any level and thus were removed. A total of 103 publications are recognized as being relevant among the remaining publications.

3. Cloud Computing Background and Terminologies

The idea behind cloud computing is not new. In the 1960s, John McCarthy envisioned that computing services will be offered to the general public as a utility [3]. The term "cloud" has also been used in various aspects, such as the concept of widespread ATM networks in the 1990s and the e-commerce outlets currently used by hundreds of millions of people around the world. However, the term only started to gain momentum after Google's CEO Eric Schmidt defined a "cloud" as the business model of offering services across the Internet in 2006 [9]. In 2011, the National Institute of Standards and Technology (NIST) defined cloud computing as a paradigm for allowing convenient, ubiquitous, and on-demand network access to a shared pool of configurable computing resources such as servers, storage, services, applications, and networks that can be quickly provisioned and released with minimal interaction or management effort from service providers. This cloud paradigm consists of five essential attributes, three service delivery models, and four deployment models [3], as shown in Figure 4 (which is adapted from the study in [10]).

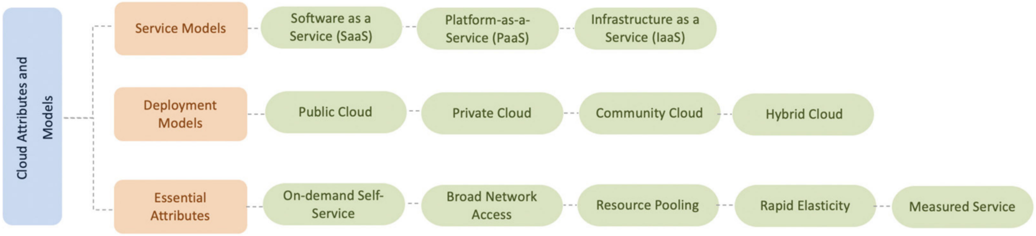

Figure 4. Cloud attributes and models.

3.1. Cloud Essential Attributes

NIST summarized the cloud computing attributes as the following [3]:

On-demand self-service (Pay-as-you use): A consumer will be able to unilaterally save on computing capabilities such as network storage and server time as the consumer's needs will be satisfied automatically without the need for human interaction with all service providers.

Broad network access: Some capabilities are available through the network and can be accessed through standard techniques that promote utilization via thick client platforms or heterogeneous devices such as laptops, tablets, mobile phones, and workstations.

Resource pooling (multi-tenancy): Service providers are involved in pooling computing resources to several multiple consumers through a multi-tenant model. It is also defined by various virtual and physical resources assigned and reassigned approbate to consumer demand.

Rapid elasticity: The capabilities are released and provided rapidly to scale both internally and externally commensurate to a request. Additionally, the consumer has some capabilities for provisioning, although they often appear to be unlimited. They can be assigned in any quantity and at any time.

Measured service: Cloud systems can automatically control and optimize resource utilization by leveraging metering to services such as active user accounts processing, storage, and bandwidth. Resource use can also be controlled, reported, and monitored to provide transparency for both consumers and providers.

3.2. Cloud Stockholders

Many actors play a major role in cloud computing, as shown in Table 1.

Table 1. Cloud Stakeholders.

Stakeholders in Cloud	Definition
Service Providers	The cloud computing systems are owned and operated by service providers and deliver service to third parties. The providers will be responsible for maintaining and upgrading systems, such as Google, Microsoft, IBM, Oracle, Amazon, and Sun [11].
Consumers	The effective subscribers purchase the services and use the system based on their operational expenses from service providers [11].
Enablers	Organizations that facilitate adoption, utilization and delivery to selling services in cloud computing [11].
Regulators	International entities that penetrate the other stakeholders [11].

3.3. Cloud Computing Services Delivery Models

A cloud services delivery model consists of three primary models that become more established and formalized. These models are software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). These three primary models are commonly referred to as an SPI model.

3.3.1. Software as a Service (SaaS)

Software as a service (SaaS) is a software distribution model that allows the consumer to access applications hosted by service provider infrastructure over a network. Concretely, the SaaS model provides software to customers, which are mostly end users who subscribe to ready-to-use applications (Bokhari et al., 2018). Moreover, the SaaS model has been associated with a pay-as-you-go attribute that offers cloud consumers a service that enables them to access the software from a web browser without any complexity regarding installation, maintenance, and high initial cost [12,13]. MS Office 365, Google Apps, Salesforce, CISCO Webex and DropBox are examples of SaaS's real-world applications. From a security standpoint, user awareness is the major contributor to SaaS security. Nevertheless, the SaaS provider needs to impose a set of security policies like multi-factor authentication, password complexity, and retention to make sure that users follow the due security requirements. Security measures are another aspect that SaaS providers should have in place to protect users' data and make them accessible for legitimate use all the time.

3.3.2. Platform-as-a-Service (PaaS)

Platform-as-a-service (PaaS) refers to a group of software and development tools hosted by the provider's servers. It offers developers a platform to build their applications without any concern about what lies underneath the service. The PaaS model also facilitates the effective management of the software development life cycle from the planning until maintenance phases. Furthermore, the platform uses programming languages such as Java, Python, and Net, among other tools that enable consumers to create custom applications [12,13]. WordPress, GoDaddy, and AWS are examples of PaaS products that many developers and programmers rely upon nowadays. In the PaaS paradigm, security is a shared responsibility between the developers and service providers. On the one hand, developers need to adopt security standards and best practices when building their applications. For instance, the developer needs to make sure that the application is free from bugs and flaws. It is also necessary to test and mitigate any vulnerability that attackers could exploit to break into and compromise users' data. On the other hand, the reliability of PaaS technology is crucial for a safe and secure application development environment. For instance, some application development environments such as C++ are infamous in memory management, leaving the window open for attackers to carry out several attacks, such as stack overflow. Another vulnerability that attackers could exploit is the lack of proper authentication inherited from some RDBMSs such as Oracle, which allows users authenticated at the OS level to login the database with admin privileges with no username/password.

3.3.3. Infrastructure as a Service (IaaS)

Infrastructure as a service (IaaS) is a single-tenant model where the cloud computing service provider dedicates resources that are only shared with contracted consumers based on pay-per-use fees. The IaaS model helps to minimize the need for a large initial investment in computing hardware such as networking devices, processing power, and servers. The model can also add or release computing resources quickly and cost-effectively [12]. With the spreading of multiple cloud delivery models, it is often difficult to identify the limits of security accountability. Both cloud service providers (CSPs) and customers are responsible for security. Figure 5 (which is adapted from [14]) shows cloud computing services delivery models' responsibilities. Examples of the IaaS include Amazon Web Services, CISCO Meta-cloud, MS Azure, and Google Compute Engine (GCE). Again, the security of the infrastructure used by customers is imperative, as it is the first line of defense that protects the system's perimeter. In this regard, attackers could target the infrastructure in many ways, such as denial of service (DoS) and malware, and most of the time, the PaaS security is the responsibility of the service provider.

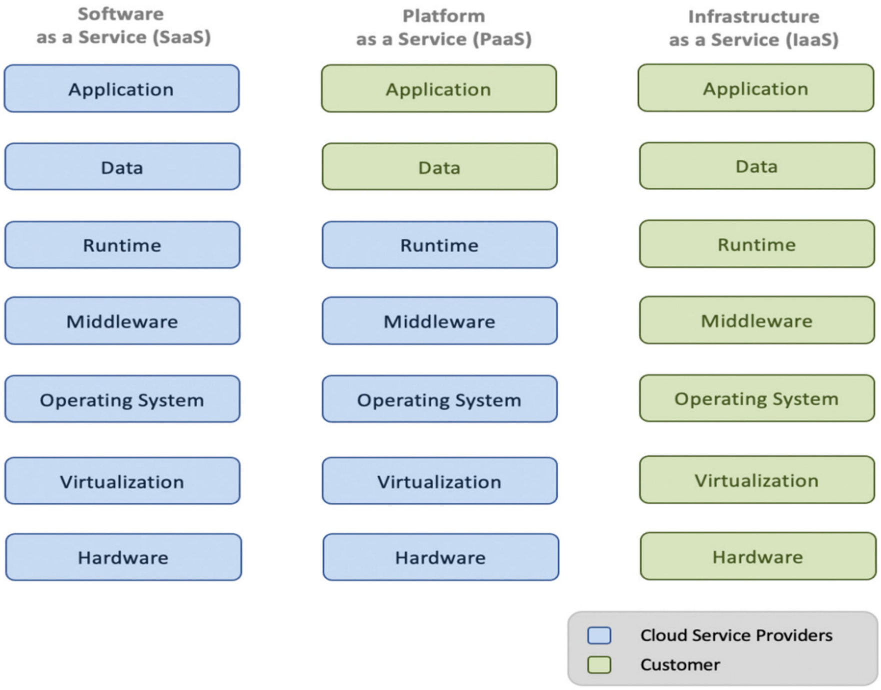

Figure 5. Cloud computing services delivery models' responsibilities.

3.4. Cloud Computing Deployment Models

The first critical step to take is to choose the appropriate type of cloud to be implemented by an institution, as it guarantees an effective implementation process [14]. According to [15], institutions that have been unsuccessful in implementing a deployment model have done so by choosing the wrong type of cloud. Before determining the best form of cloud to use, institutions must first analyze their data to avoid chances of failure. However, the security aspect is overlooked by many of the customers when opting-in for cloud services due to the misconception about the efficacy of the security embedded into cloud services. Many organizations that adopt cloud computing rely totally on the security applied by the cloud service providers. Consequently, malicious actors could exploit client-side vulnerability to compromise the systems of one or more tenants. Four models have been completely incorporated in every type of cloud-based system in accordance with management requirements and the senility of data. These models include public cloud, private cloud, community cloud, and hybrid cloud.

3.4.1. Public Cloud

The public cloud is often referred to as an external cloud. This type of cloud is open to all users or large groups of users via the Internet, with ownership being retained by cloud service providers. It is run by the provider and enables users to access any data through the internet. The public cloud offers cost-effective and elastic ways of deploying IT solutions [10,16]. However, Internet connectivity imposes many security threats to the services and systems hosted by the cloud, including, but not limited to, DoS, malware, ransomware, and advanced persistent threat (APT) attacks.

3.4.2. Private Cloud

The private cloud is often referred to as the internal cloud. This type is dedicated to a single user, group, or institution. It may be operated by the service provider or a third party and may work on-site or off-site. Although more secure, private clouds are more costly. A private cloud is also hosted within the institution's firewall; thus, users within an institution can access it over the intranet [14]. In contrast to public clouds, private clouds are less secure due to the limitation in resources and expertise dedicated to the services and systems, let alone the security. As a result, some components might not be well-protected, which allows malicious actors to carry out attacks by exploiting these weakly secured components.

3.4.3. Community Cloud

The community cloud serves specific communities with shared interests, such as missions, policies, security requirements, and compliance considerations. It can be managed by institutions themselves or by a third party on-site or off-site. The community cloud provides greater privacy, protection, and policy compliance standards [16]. The security of community clouds relies on the degree of security-awareness of the community and how critical the security is for community business. For instance, a cloud for federal agencies contains sensitive data that, if exposed, could compromise national security. As such, the security measures should be intrinsic to such clouds.

3.4.4. Hybrid Cloud

This type of cloud deployment occurs due to the diversity of an institution's requirements. It is a mix of two or more models (public, private, or community) to implement cloud services. It allows institutions to host sensitive data or applications on the private cloud and non-sensitive data or applications on the public cloud [16]. However, the hybridization between clouds poses several security risks due to the federation between clouds with different and incompatible security measures. Attackers, consequently, expose vulnerabilities in one or more clouds to break into the entire system.

3.5. Existing Surveys

Various survey papers have analyzed the security concerns relating to cloud computing over the last decade. Most of the reviewed literature has contributed significantly to the management of cloud security issues [17]. One such survey in [18] explored the common security concerns of cloud use. In addition, the authors presented some solutions to security risks according to user data sensitivity in cloud architecture.

A study by [19] highlighted the security issues for data transfer in a cloud. This survey provided sensible solutions for tackling possible threats. A survey in [20] presented a taxonomy and survey of cloud services in terms of cloud infrastructure vendors and revenue. It proposed a taxonomy of the services containing some categories such as computing, networking services, databases, storage, analytics, and machine learning. The computing, networking, and storage of all cloud vendors provide a strong product in terms of functionality and are considered the core of cloud computing. On the other hand, the databases, machine learning, and data analytics products of all cloud vendors offer a variety of different choices concerning streaming capabilities, data processing and orchestration, building blocks, and machine learning.

A survey in [21] focused on the security issues facing cloud entities. The entities involved the cloud customer, the cloud service provider, and the data owner. Additionally, the study focused on the crypto cloud with various communication-, storage-, and service-level agreements. Additionally, it included the necessary updates to research the causes and effects of different cyber-attacks.

A study by [22] discussed the various data protection issues in a multi-tenant system in cloud computing and suggested approaches to address security issues. This survey, however, focused more on data privacy rather than security.

A study in [23] provided a proper definition of cloud computing and different cloud architecture layers. Additionally, the study compared three service models (SaaS, PaaS, and IaaS) with deployment models (private, public, and community). The authors discussed the information security requirements of the private and public cloud. In addition, they discussed the main issues and challenges of cloud computing related to security.

A survey in [24] focused more on how we can recognize many forms of threats that often occur in cloud computing environments. In this paper, the author's contribution was in classifying the types of threats based on service resources in the context of the cloud. Based on the description and scope of the types of threats, this classification was defined.

A study in [25] discussed the design of software-defined networks (SDNs) and cloud computing environments with regard to DDoS attack situations and recognition instruments in cloud computing conditions. Additionally, this survey study discussed how to fabricate exploratory conditions and utilize simulation instruments for DDoS attacks and identification.

In the study of [26], a survey reviewed and evaluated major attacks targeting the security of Cloud Computing and presented solutions and potential countermeasures to serve as a benchmark for comparative research. This study lacked techniques to solve some major security challenges.

The authors in [27] reviewed technologies that allow for privacy-aware outsourcing of storage and processing of sensitive data to public clouds. The authors reviewed masking methods for outsourced data based on data splitting and anonymization, in addition to cryptographic methods covered by other surveys. These methods were then compared in terms of operations supported by masked outsourced data, overheads, and the impact on data management.

A narrative review by [28] showed integral end-to-end mapping of cloud security requirements, identifying threats, known vulnerabilities, and recommended remedies. It also contributed to the identification of a unified taxonomy for security requirements, threats, vulnerabilities, and countermeasures for end-to-end mapping. It also highlighted security challenges in other related fields, such as trust-based security models, cloud-enabled big data applications, the Internet of Things (IoT), the software defined network (SDN), and network function virtualization (NFV).

The study in [29] conducted a systematic literature review of the integration as a service between trusted computing and cloud computing for infrastructure as a service (IaaS). Cloud computing integration and trusted computing can create a new infrastructure architecture as a service that encourages more cloud service tenants to trust cloud service providers.

A survey in [17] provided security issues and requirements for the cloud and identified threats and known vulnerabilities. The work presented a new classification of recent security solutions that exist in this area. It presented a series of documented policies, procedures and processes that define a secure way to manage the cloud environment to identify the vulnerability and increase confidence in an ever-connected world.

In [30], the authors investigated the key contemporary security problem in cloud computing and provided the best practices for service providers and organizations hoping to manage cloud services. Table 2 presents a summary of the existing related surveys in terms of their contributions and the levels of infrastructure they covered. It summarizes existing survey papers in cloud infrastructure over the period from 2016 to 2020. As noticed, most of these surveys were conducted at only one level of cloud infrastructure. For instance, the surveys in [19,20,23,28], focused on only the data level, while the survey in [24] focused on only the application level. Moreover, a survey [26] was conducted on the network level and another paper [30] on the host level.

There have been some works performed at two or more levels in cloud infrastructure, such as the studies conducted in [18,22,25]. In addition, the studies in [21,27,29,31], considered all infrastructure levels. Nevertheless, [20] considered a public cloud only, and also for cloud services in terms of cloud infrastructure vendors and revenue. Meanwhile the survey in [27] focused more on how to manage the data in the public cloud. The study in [29] was a narrative review without any analyses of the reviewed materials. Lastly, the survey in [31] was limited to the analyses of security from the provider's perspective.

To conclude, the existing survey papers in cloud infrastructure security are not comprehensive enough. They do not cover the security of all levels of cloud infrastructure, i.e., host, network, application and data. Some of the reported surveys are limited to one or more levels. In addition, some surveys do not consider all perspectives of customers and service providers. Our proposed survey is different, such that it conducts an extensive review of issues that faced all levels of cloud computing infrastructure with a proper analysis of such issues. Then, it discusses the existing solutions used to mitigate these issues. Finally, the survey highlights the open issues and challenges, and gives directions for future research.

Table 2. Summary of existing surveys.

Reference	Contribution	Data	Application	Host	Network
[18]	The study reviewed the security issues regarding user data sensitivity on cloud architecture.	√			
[19]	The study focused on identified cloud computing security issues during data migration to the cloud and presented solutions for resolving potential threats.	√			
[20]	The survey performed a taxonomy to compare key services that are regularly used by cloud applications.	√	√	√	√
[21]	This study focused on the crypto cloud with various Communication, Storage, and Service Level Agreements.		√		√
[22]	The survey focused on data privacy.	√			
[23]	The study highlighted the security requirements for cloud computing.		√		
[24]	The study was classifying types of threats based on service resources in the context of the cloud.	√	√		
[25]	The study reviewed DDoS techniques used in cloud computing.				√
[26]	The study evaluated major attacks targeting the security of Cloud Computing.	√	√	√	√
[27]	The study reviewed technologies that allow for privacy-aware outsourcing of storage and processing of sensitive data to public clouds.	√			
[17]	The study provided security issues and requirements for the cloud, identified threats, and known vulnerabilities.	√	√		√
[30]	The study is more about the security from providers perspectives.	√	√	√	√
This survey	Provides an extensive survey on issues that cloud computing infrastructure faced at its levels (Application, Host, and Network and data level). Presents some existing solutions used to mitigate these issues. Highlights some open challenges that still need to be solved.	√	√	√	√

4. Security Issues in Cloud Computing Infrastructure

Four main levels should be considered when planning for and applying security in cloud infrastructure, which are data level, application level, network level, and the host level [31]. These levels are shown in Figure 6.

According to [31], these levels are described as in the following paragraphs.

Security at the data level refers to providing protection for data at rest and in transit to protect the data from loss or leakage, which significantly impact data security and privacy. Malicious actors could compromise the data exchanged between the systems within the cloud, referred to as data in transit. Sniffing and man-in-the-middle (MITM) are the common attacks against data in transit within cloud ecosystem. In addition, several threats including, but not limited to, data leakage, hijacking, manipulation and eradication can affect the confidentiality, integrity, and availability of the data at rest.

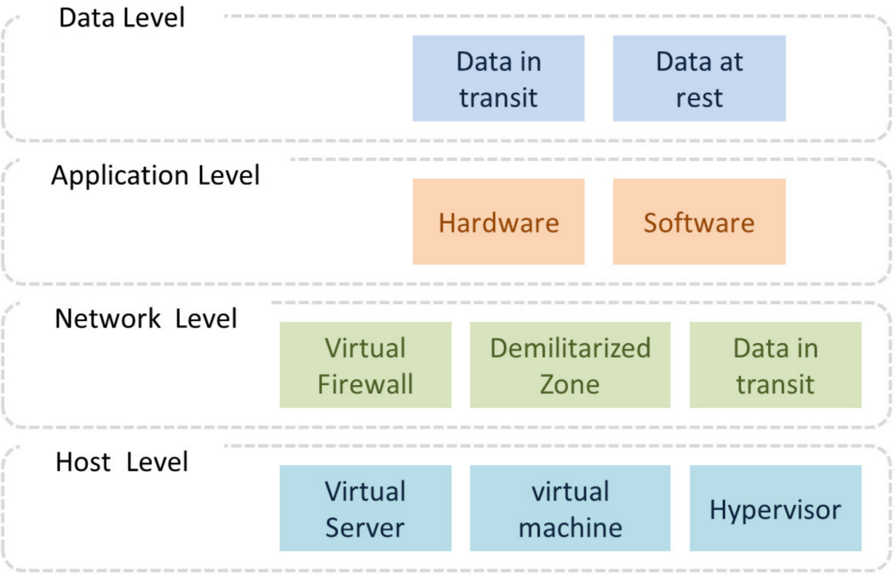

Figure 6. Cloud infrastructure levels.

Application level: Security at this level refers to providing protection for applications when utilizing the hardware and software resources to prevent the attackers to get control over these applications. The most major threats at this level are denial of service (DoS) attacks that affect software applications.

Network level: Security at this level refers to providing protection for the network when using a virtual firewall, demilitarized zone (DMZ), and data in transit. For this purpose, information about different types of firewalls should be monitored, collected, and maintained.

Host level: Security at this level refers to providing security for the host when using a virtual server, hypervisor, and virtual machine. It is important to collect the information about the system log files to know when and where the applications have been logged.

At each level, the main CIA components should be evaluated when protecting cloud infrastructure. Along with the growing popularity of cloud-based systems, the security problems introduced by adapting this technology are increasing. Although cloud computing has many advantages, it is vulnerable to various types of attacks. Attackers are consistently seeking to find weaknesses to attack the infrastructure of cloud computing [32]. The following subsections explore the security issues in the different levels of cloud infrastructure.

4.1. Data-Level Issues

Data breaches, loss, segregation, virtualization, confidentiality, integrity, and availability are the issues faced at this level. Figure 7 depicts these issues and the following subsections discuss them in detail.

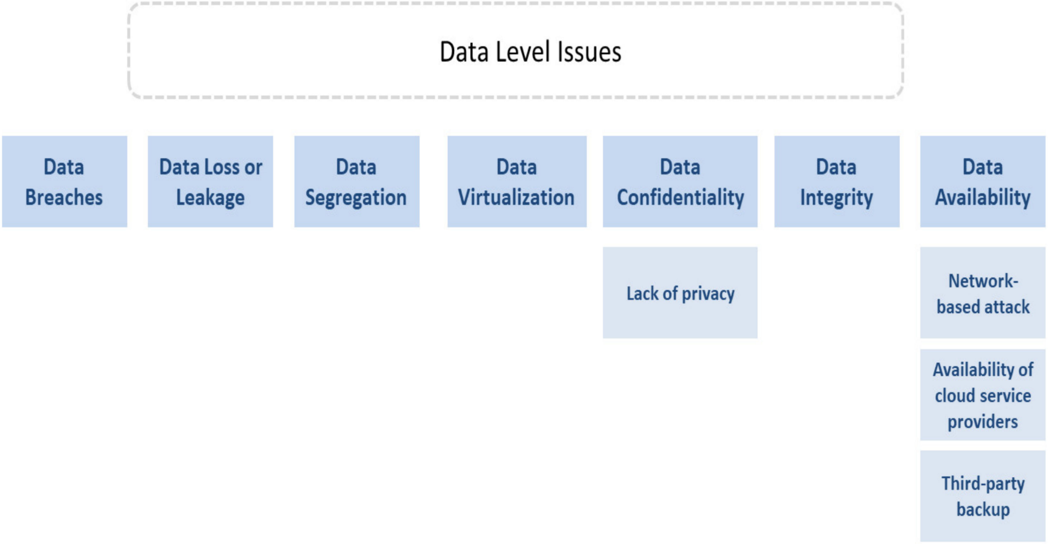

Figure 7. Data Level Issues.

4.1.1. Data Breach Issues

Data breaches are a critical security issue that needs to be focused on in the cloud infrastructure. Because large amounts of data from different users are stored in the cloud, a malicious user can access the cloud in such a way that the entire cloud environment is vulnerable to a high-value attack. Breaches can occur due to various accidental transmission problems [33]. The shared resources in the cloud make it easy for adversaries to target the data in the cloud infrastructure using many types of attacks. These attacks can be classified into several categories, including data loss and data leakage.

4.1.2. Data Loss or Leakage Issues

Data are transferred from data centers to the client's systems and are transmitted from one execution mode to multiple execution mode, which may cause data loss or leakage. Even though data are stored away from the client system, there could be a possibility of data loss or leakage. As a result, data leakage is becoming a critical security issue among the various security issues in the cloud environment [34]. The loss and/or leakage of data may be carried out by internal threat actors such as disgruntled employees, contractors, and other partners. Likewise, external actors could gain access to the cloud infrastructure and disclose, delete, or lock the data they may locate. This could be done with the aid of a wide range of tools and tricks such as malware, identity theft, and password brute force. To protect data in the cloud environment from being leaked, two main types of countermeasures are employed, namely encryption and watermarking. However, encryption cannot protect data at rest if intruders manage to gain access into the cloud using valid credentials. As such, it is imperative to scrutinize cloud access requests and ensure that they come from legitimate users.

4.1.3. Data Segregation Issues

Multi-tenancy is one of the key features of cloud computing. Since multi-tenancy allows multiple users to store data on cloud servers, there is a possibility of data intrusion. Utilizing the shared environment, intruders could gain access using the credentials of an unaware user. Data can also be intruded by injecting a client code or using any application with known vulnerabilities. There is therefore a need for security measures to control the access to shared environments or isolate the data of each user in multi-tenant environments [33].

4.1.4. Data Virtualization Issues

Due to the high mobility and elasticity features of the cloud, VMs along with data can easily be moved from their original location to another. This might lead to loss of the metadata fully or partially, which can cause many service interruptions and an unpleasant experience. For instance, the user might face difficulties in copying or cloning the data, as the movement of sensitive data in the form of metadata causes the loss of these data and the hazard of errors [21].

4.1.5. Data Confidentiality Issues

Often, the confidentiality in a cloud system policy focuses on protecting data during transfers between entities. In addition, it is concerned with data privacy, where customer data must not be disclosed to unauthorized parties at any time. Data are stored on remote servers and can be hosted by single or multi-cloud providers based on the content such as data, videos, etc. This raises several security concerns with regard to the security, compatibility and interoperability between the different cloud service providers. Data confidentiality is one of the essential criteria when data are stored on a remote server. Such confidentiality could be compromised due to the miscoordination between the cloud service providers that co-host the data, which opens one or more vulnerabilities that threat actors can exploit. To maintain confidentiality, understanding and classification of data, users should be aware of the data stored in the cloud and their accessibility [33].

4.1.6. Data Integrity Issues

Integrity issues arise in such an environment due to data being stored remotely and at multiple locations [35]. Such a distributed environment evokes special attention to the integrity when storing and retrieving the data in multiple places, where many errors could occur, such as manipulating, losing, or corrupting these data fragments. Although these issues could occur due to system internal errors, hackers can inflict such damages as well. The system should be so secure that only the legitimate user can access and/or modify the data. In a cloud-based environment, data integrity must be maintained correctly to prevent data loss. In general, data integrity could be avoided by applying several security measures like hashing, salting, timestamping, and digital signatures. The repeatedly used data integrity protection methods provide information about changes in data and checksums to verify the integrity of the data [36].

4.1.7. Data Availability Issues

Data should be available for authorized users at all times. The user must also have control over their data. There are currently three major threats to data availability, which are the network-based attack, the availability of cloud service providers and third-party backup of data collected by cloud service providers. The threat actors could launch massive DoS attacks against the targeted cloud, preventing users from accessing resources on the cloud. Attackers could also erase data on cloud storage or take one or more data storage offline. Therefore, cloud service providers should avoid a single point of failures situation by applying the concept of redundancy on network, service, and data storage levels. Data recovery after an accident, such as a hard disk crash, destruction and natural disasters, should be assured by the cloud provider [36].

4.2. Application-Level Issues

Many issues arise at the application level, as shown in Figure 8. These issues are related to availability, authentication, insecure APIs, malicious insiders, and end user attacks. The following subsections elaborate on these issues.

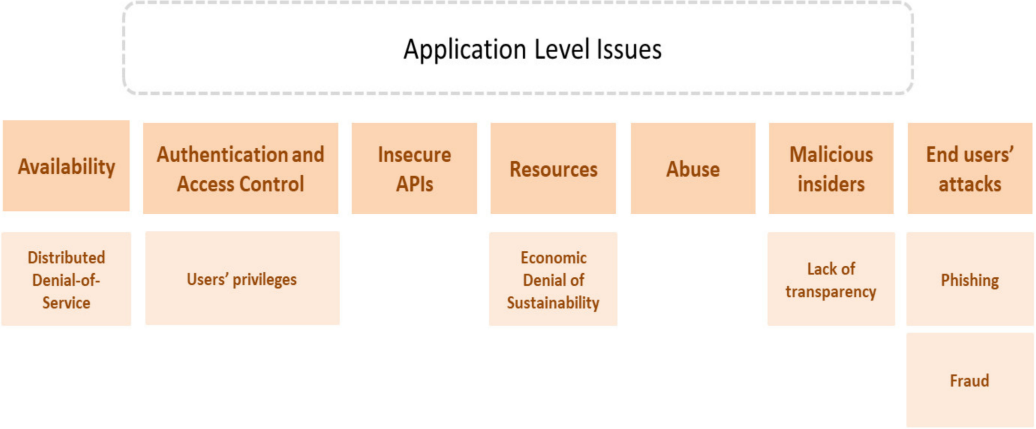

Figure 8. Application-level issues.

4.2.1. Availability Issues

The cloud should be available at all times, and robust to any security threat or user misbehavior. This is a basic, yet difficult, problem in the cloud. Compared to multi-clouds, the issue of availability in a single cloud is very critical. The application availability refers to making it accessible to the user [35]. Distributed denial-of-service attacks (DDoS) are one of the major threats to an application's availability on the cloud. These attacks have become complex and continue to develop rapidly, making it more difficult to identify and tackle them [37]. The major aim for the attacker is to block legal users and take control over resources and services so that the customer will not be able to use the application hosted on the cloud.

4.2.2. Authentication and Access Control Issues

Many issues also came in the context of access control and authentication. These issues come in the form of unauthorized access/use/of the resources on the cloud. In the access control context, the elasticity feature in IaaS introduces several security issues due to the rapid change in the infrastructure configurations, which makes one or more applied access controls outdated. Therefore, an agile and adaptive authentication approach needs to be incorporated into cloud-based applications. There is also a need for mechanisms that enforce a proper configuration and change management [38].

Although the multi-tenancy feature in IaaS facilitates the usage of infrastructure through sharing resources among multiple customers, this causes some issues related to accessing these resources from authenticated, yet unauthorized users. Therefore, proper access controls that solve such conflict need to be in place [38].

In addition, the flexibility of IaaS allows the consumer to configure virtual machines. This could be a security issue, as the misconfiguration of VMs may lead to security violations due to overlooking some security parameters during the creation of the VM. Additionally, there is a need for an approach constructed on role-based access control [38]. In the authentication context, cloud authentication techniques are typically only one party or open access, such that the cloud service provider does not have a platform for multiple user interface authentication, resulting in unauthorized or vulnerable access to the cloud space [39].

4.2.3. Insecure APIs

Cloud APIs are usually used to connect with other systems at all levels of the infrastructure, network, host and application services. These APIs are used for different tasks, such as access and control network and VM infrastructure resources in IaaS, access cloud services (e.g., storage) in PaaS, and link cloud infrastructure to applications in SaaS [40]. However, those APIs, if not secured properly, could be utilized by malicious actors as a platform to carry out many types of attacks against the applications on the cloud. The security of different cloud providers depends upon the security of the APIs. Numerous cloud security problems will result in a poor set of APIs and interfaces. Generally, cloud providers sell their APIs to third parties to provide consumers with services. Nevertheless, weakly secured APIs can be used by hackers to access security keys and sensitive information. Consequently, the encrypted customer data in the cloud can be read using the encryption keys, which violates access control and authentication standards, and compromises data integrity, availability and confidentiality [40].

4.2.4. Resources Issues

A cloud offers computing platforms rich resources where payment is based on the usage of the cloud resources, known as "pay-as-you-use" or utility computing. However, resource-exhaustion attacks like DDoS could consume many resources on the server and cloud infrastructure, which leads to overcharging the customer and/or depleting the quota the user subscribed to. In such instances, the primary aim of the attack is to render cloud computing unsustainable by targeting the cloud adopter's economic resources. Thus, the economic denial of sustainability (EDoS) attack represents a new form of DDoS attack [41].

4.2.5. Abuse of Cloud Computing

IaaS providers provide their customers with unrestricted computing, networking, and storage capacities. These providers sometimes offer a "frictionless" registration process that allows those with a valid credit card to register and start using cloud services. Clients sometimes get limited trial periods free of charge. By exploiting anonymity through these registrations and various templates, spammers have misused malicious software. These kinds of attacks have typically targeted PaaS and IaaS providers. Cloud providers must be concerned about issues such as malicious data hosting, password cracking, key cracking, the building of rainbow tables, the launching of dynamic attack points, CAPTCHA, control, and botnet command solving farms [34].

4.2.6. Malicious Insiders Issues

Malicious insiders pose a threat to customers due to the lack of transparency between cloud providers and customers' procedures to the services. In insider attacks, malicious actors have legitimate access privileges to the resources, which makes it difficult to identify whether what he/she is doing is malicious. This kind of issue normally starts at the very beginning with the hiring process. Sometimes, the visibility of hiring standards and practices for the employees is low. Such a situation often seems to attract attackers who attempt to perform espionage and facilitate organized crime. Malicious insiders cause data breaches, loss, and/or falsification [34].

4.2.7. End Users' Attacks

There are many attacks on cloud users, such as phishing and fraud, that can affect the infrastructure of cloud services. Phishing and fraud are ways to steal a legitimate user's identity, such as credentials and credit card information. Usually, phishing is performed by sending the user an email containing a connection to a fraudulent website that looks like a legitimate one. When the user visits the fraudulent website, the username and password are sent to the attacker, who can use them to attack the cloud. Another type of phishing and fraud is to send the user an email claiming to be from the provider of cloud services and to ask the user to provide his/her credentials for maintenance purposes [42]. Although attacks targeting the end user on the cloud look similar to those on conventional systems, they are not identical, as cloud users can gain access from different platforms, which gives the attacker more options to break into the system.

4.3. Network Level Issues

The issues at this level involve attacks on availability, integrity and confidentiality, as shown in Figure 9.

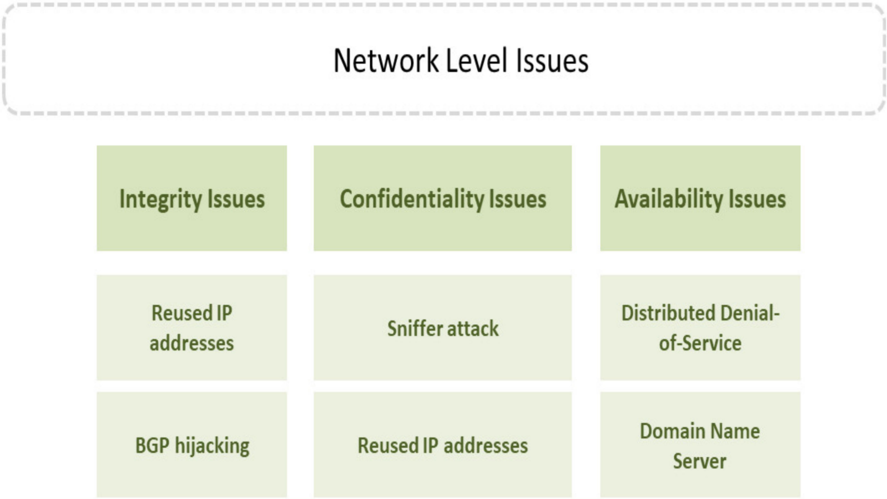

Figure 9. Network level Issues.

4.3.1. Integrity Issues

Integrity refers to the confidence in the protection against changes by unauthorized persons. The issues of integrity came in many contexts in cloud infrastructure [36]. In the context of the network, IP addresses are seized by corrupting the Internet routing tables by BGP hijacking or prefix hijacking. Normally, the border gateway protocol (BGP) is utilized to stabilize the network and transfer the packets from one path route to another route if the original path is down. However, attackers could hijack the BGP and redirect the data to other destinations. BGP hijacking leads to data leakages, and compromises the integrity and sometimes availability [43]. In addition, in the cloud environment, IP addresses are usually reassigned and reused. This occurs when customers change their location. The old "aged" IP can be assigned to other customers. This might lead to increased risk when reusing an existing IP address for a new device/customer happens faster than removing its old assignment from DNS caches [44].

4.3.2. Confidentiality Issues

Issues regarding confidentiality are rising due to the growing number of cloud users working in a multi-tenant environment, where compromising one system could lead to a chain of subsequent compromises in other systems. Sniffing attack is the most prominent issue. This occurs in a cloud environment when unencrypted packets of data are transferred between two entities in the cloud. These packets can, therefore, be captured, leading to the exploitation of confidential information. In a cloud environment, the existence of an entity with a promiscuous mode in the network node highly suggests that data in the node are being monitored by an attacker [44]. In addition, the reused IP addresses lead to the compromising of confidentiality, if not handled properly when reassigned to another user [44].

4.3.3. Availability Issues

Many of the issues come in the context of network availability, such as DDoS and DNS attacks. DDoS floods the customer with useless traffic for an infinite period, rendering resources or services inaccessible. The primary aim is to take control over resources (bandwidth of network or time of CPU) such that they cannot provide services to the legal consumers. The other aim is to hide the attacker's identity by imitating legal web application traffic and creating many agents to launch a DDOS attack [34]. The attacker typically hides their identity by spoofing the victim's IP address portion of a packet header. This makes it very hard to identify the source of an attack. Most providers cannot cover this attack, since they are unable to differentiate between good traffic and bad traffic. A conventional solution has been increasing the number of resources [34]. With regard to the domain name server (DNS), servers play a critical role in cloud infrastructure, given that the failure of DNS will most likely lead to the cloud's lockdown, rendering the data inaccessible. DNS in the cloud infrastructure is exploited to execute large-scale attacks to damage cloud data services. Some common attacks on the DNS infrastructure include DDoS attacks, modified data attacks, corrupted data attacks, man-in-the-middle attacks, and DNS ID spoofing attacks. These attacks compromise server availability [44].

4.4. Host-Level Issues

At the host level, visualization and data storage issues are the main concern, as shown in Figure 10.

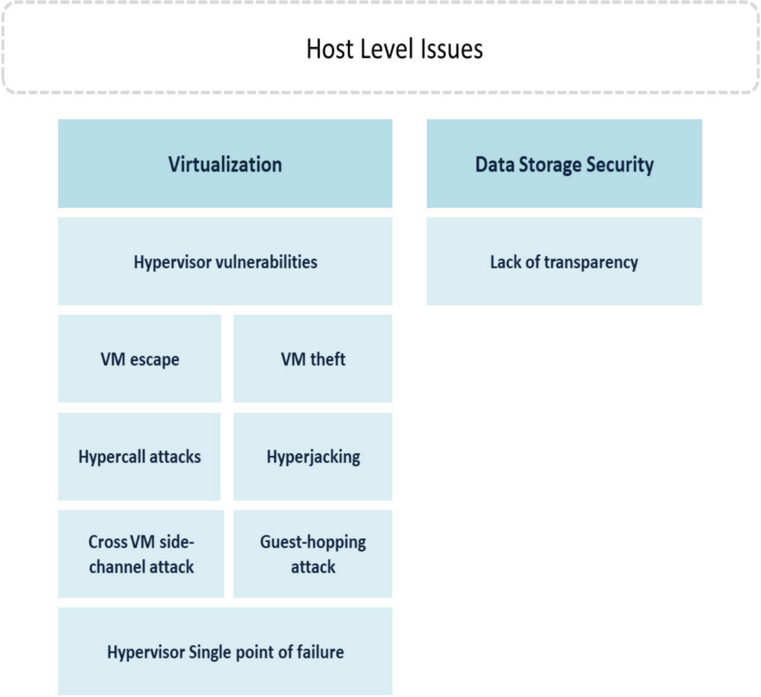

Figure 10. Host Level Issues.

4.4.1. Virtualization Issues

The concept of the cloud is based on virtualization, in which many guest VMs share common physical hardware. Malicious actors can target the virtualization elements, such as the hypervisor and virtual machines [45]. Therefore, securing the hypervisor in cloud environments is necessary, as hackers can use it to compromise all VMs built based on it [46]. Many of the issues raised in the context of virtualization and hypervisor issues [21] can be summarized as follows:

Hypervisor Vulnerabilities

To run multiple guest VMs and applications simultaneously on a single host machine and to provide isolation between the guest VMs, a hypervisor or virtual machine manager (VMM) is generated. While hypervisors are supposed to be vigorous and stable, they are vulnerable to attacks. When attackers take control of the hypervisor, it will be under their full control, and all the VMs and data will be accessible to them. The greater control offered by the bottom layers in the virtual machine is another reason hackers consider the VMM a potential target. Compromising a VMM also allows attackers to access the underlying physical device and applications they host. Many of the well-known attacks (e.g., Hyperjacking, Bluepill, etc.) inject rootkits based on VMs that can mount or change the current rogue hypervisor to take full control of the environment. Since the hypervisor runs underneath the host OS, standard security measures make it difficult to detect these types of attacks [45].

VM Theft

Virtual machine (VM) theft is another virtualization-related attack that can hit cloud environments. For this attack to mount and run, an attacker copies a VM over the network or to a portable storage medium. This could be done by utilizing the migration utility on the hypervisor. Nevertheless, to trigger unauthorized migration of the guest VM to its cloud infrastructure, an intruder may also tamper with the VMM control panel that handles live migration [47]. As such, securing the hypervisor could help in mitigating the VM theft attack.

VM Escape

Virtual machines are intended to support a strong separation between hosts and VMs. However, the operating system's vulnerabilities running within the VM can help attackers to inject malware, which not only can affect the current VM but also bypass the VMM layer into the other VMs on the same hypervisor. This allows the malware to gain access to the host machine and initiate sustainable attacks, utilizing the set of backdoors they open [45].

Hyper Jacking

Hyper jacking is an attack in which, inside a virtual machine (VM) host, a hacker takes control over the hypervisor that generates the virtual environment. This attack aims to target the operating system of the virtual machines. Therefore, the software of the attacker can run, and its existence will be completely hidden from the applications on the VMs [45].

Hyper-Call Attacks

Hyper-call attacks involve an intrusion into the VM using well-defined hyper-call interfaces by an unauthorized guest VM by exploiting vulnerabilities in the hyper-call handler of a VMM. Such attacks could lead to a shift in the functionality of the VMM or a "host crash" when a malicious code with VMM privileges is executed [47].

Guest-Hopping Attacks

Guest-hopping attacks include any failure of separation between shared infrastructures. An attacker tries to access one virtual machine by accessing another virtual machine hosted on the same hardware. The Forensics and VM debugging instruments are one of the potential mitigations of the guest hopping attack to observe any attempts to manipulate VM [42].

Hypervisor Single Point of Failure

The hypervisor technology that regulates the access of VMs to physical resources is the basis of current virtualized environments and is critical for the overall functionality of the system. Therefore, hypervisor failure due to the overuse of hardware or device faults leads to overall system collapse [45]. This is known as single-point-of-failure, which originates from lacking redundant hypervisor and/or underlying hardware. Therefore, a robust cloud environment should implement the high availability approach, in which critical components are redundant. In such a setup, if one component failed, the redundant component takes over the workload. This kind of operation is normally transparent to end users and they do not experience any interruption in the cloud services.

Cross VM Side-Channel Attack

In a side-channel attack, the attacker establishes a hidden channel over shared hardware resources from which he/she collects important information. During this attack, hackers monitor victim's activities and collect information such as cryptographic keys, username, and passwords. Although side-channel attacks have been around for a long time in conventional systems, with the advent of cloud technologies, where the basic concept is to share resources, their effect is growing by several folds [48].

4.4.2. Data Storage Security Issue

Since user data are stored in the server set of the cloud service provider (CSP) that operates concurrently and in a distributed way, the integrity and the confidentiality of the data stored at the CSP must be maintained. This can be achieved by ensuring that CSP employees have restricted access to user data and strict security procedures to ensure that only authorized employees gain control and access to CSP servers. In addition, well-defined data backups and redundant data storage can be used by the CSP to make data recovery possible [42]. However, the transparency between the user and the service provider may play a decisive role in this matter [34], as the customer is aware of the storage sites, the policies followed, as well as the protection methods followed.

Table 3 summarizes the security issues discussed above at every level of the cloud infrastructure. It highlights the threats exhibited at each level and the cloud features affected, in addition to the impact on security measures.

Table 3. Summary of security issues.

Security Issue	Threats	Level Effected	Feature Affected by	Impact on Security	Reference
Availability	DDoS	Application level/Network level	Multi-tenancy and Elasticity	Compromised the availability	[36,38]
	DNS attacks	Network level	Multi-tenancy and Elasticity	Compromised the availability	[34,44]
	Unavailability data	Application level/Host level/Network level/Data level	Multi-tenancy	Compromised the data availability	[37]
Integrity	Data modification	Application level/Host level/Network level/Data level	Multi-tenancy and Elasticity	Change on data that lead to loss of integrity	[36,37]
	Prefix Hijacking	Network level	Multi-tenancy and Elasticity	Affected integrity and availability	[44]
	Reused IP Addressing	Network level	Multi-tenancy and Elasticity	Compromised integrity and confidentiality	[45]
Confidentiality	Lack of data confidentiality	Application level/Host level/Network level/Data level	Flexibility and Multi-tenancy	Impact the data privacy	[44]
	Sniffer Attacks	Network level	Elasticity	Affected confidentiality	[45]
	Reused IP Addressing	Network level	Elasticity	Compromised integrity and confidentiality	[45]
Authentication and Access Control	Sharing resources	Application level	Multi-tenancy	Violate access control standards	[39,40]
	Misconfiguration	Application level	Flexibility	Compromised access control standards	[39,40]
	Unauthorized/ vulnerable access	Application level	Flexibility, Multi-tenancy and Elasticity	Violate authentication and access control standards	[39,40]

Table 3. *Cont.*

Security Issue	Threats	Level Effected	Feature Affected by	Impact on Security	Reference
Virtualization	Hypervisor vulnerabilities	Host level	Multi-tenancy and Elasticity	Can cause damage to the entire system	[46]
	VM theft	Host level/Network level	Flexibility	Effect the network and storage	[48]
	VM escape	Host level	Flexibility	Cause a vulnerability to OS	[46]
	Hyperjacking	Host level	-	Take control over OS	[46]
	Hyper-call	Host level	Elasticity	Shift the functionality of VMM and host crash	[48]
	Guest-hopping attack	Host level	Multi-tenancy	Lead to access VM	[43]
	Hypervisor Single point of failure	Host level	Multi-tenancy	Can cause damage to the entire system	[46]
	Cross VM side-channel attack	Host level	Multi-tenancy	in the valuable information	[48]
	Data virtualization	Application level/Host level/Network level/Data level	Elasticity	Data loss and cause damage to the data	[22]
Insecure API's	Insecure API's	Application level	Flexibility, Multi-tenancy and Elasticity	Violate access control and authentication but also loss of data integrity, availability and confidentiality	[41]
Resources	EDoS	Application level	On-demand services (Pay-as-you use)	Effected the costs of the resources	[42]
Abuse of Cloud Computing	User's abuse	Application level	Multi-tenancy	It can cause malicious data hosting, password cracking, key cracking, the building of rainbow tables, launching of dynamic attack points	[35]
Malicious Insiders	Insider users	Application level	Multi-tenancy	Data Breaches	[35]
End users' attacks	Phishing Fraud	Application level	Multi-tenancy	Steal user's identity	[42]
Data Storage Security	Data Storage Issues (e.g., lack of transparency)	Host level	Multi-tenancy	Data Breaches	[43]
Data Loss or Leakage	Data Loss or Leakage	Application level/Host level/Network level/Data level	Multi-tenancy	loss of data integrity, availability and confidentiality	[35]
Data Segregation	injecting a client code or using any application	Application level/Host level	Multi-tenancy	loss of data integrity, availability and confidentiality	[34]

As shown in Table 4, the most affected cloud feature is multi-tenancy. The reason for this might be related to the interaction between the customers who share the same environment and/or resources. In addition, attackers could carry out utilizing the interface used by customers to interact with the service provider.

In addition, it can be noticed that most security issues affect the application level and data level rather than the network level, but the most serious issues threaten the host level. This fact should be taken seriously, as damage to the host can damage the entire system, including the shared spaces. The following subsections present the proposed solutions in the literature for the issues discussed in this section. The solutions will be discussed based on the levels as well as the issues discussed in the same manner.

5. Related Existing Solutions in Cloud Levels

This section presents solutions proposed in the literature based on the different cloud infrastructure levels. This includes the data, application, network, and host levels. More details about those solutions are discussed in the following subsections.

5.1. Solutions at Data Level

Through the transition from conventional computing models to the Internet-based cloud model, there is a great need for emphasizing data security and privacy. Data loss or data leakage can significantly affect the organization's business and ruin the trust in its brand. A study in [49] investigated the audit in the cloud computing environment. Data auditing involves examining various features that include data confidentiality, integrity, remanence, provenance and lineage. According to the study, there are a range of basic techniques in each of these features that could satisfy the needs of cloud service users for data auditing, except data remanence, which is still an open issue within public cloud services. As concluded, the study found that despite many available techniques to address user auditing issues in the data auditing area, cloud providers have so far focused more on infrastructure security auditing than data auditing.

The authors in [50] focused on the issue of data integrity verification by a third-party auditor for client data that resides on a cloud storage server (CSS). The study suggested a protocol for dynamic data updates using the modified Chameleon Authentication Tree (MCAT). They also demonstrated the security of their optimized auditing protocol by proving that it is resistant to replay, replace, and forge attacks.

A study in [51] proposed a classification technique based on various parameters. The parameters were defined based on different dimensions. It is intended to have security levels based on content type and accessibility. According to the authors, data security can be provided based on the level of protection needed. Depending on the data set classified as dimensions, the corresponding security provisions for storage can be applied.

In [52], the authors proposed a secure data classification-based cloud computing model. The proposed model minimizes the total time necessary to secure data by applying TLS, AES and SHA cryptographic algorithms based on the classified data type. The proposed model has been tested and the results show the reliability and efficient existence of the proposed model.

In [53], the authors proposed a framework for privacy-preserving out-sourced classification in cloud computing (POCC). Using POCC, the evaluator can train a classification model securely over data encrypted with different public keys, that are outsourced to multiple data providers. Based on Gentry's scheme, the authors used a proxy fully homomorphic encryption technique to protect the privacy of sensitive data.

The work in [36] defined the data security modeling design in cloud computing. Data security in all cloud storage layers was discussed. Based on this study, the standard cloud storage uses a three-level cloud data security model that can be expanded to a fourth level responsible for data integrity checks. The paper introduced the design of a four-level data security model in cloud computing that describes each part of cloud data security using Petri nets.

The authors in [54] proposed a framework to protect big data in the cloud computing environment. The Map Reduce framework was used to find the number of users logging into the cloud data center. The proposed framework protects the mapping of different data elements to each provider using the meta cloud data storage interface. While this proposed approach requires a high degree of implementation effort, it offers valuable information for a cloud computing environment that can have a high impact on future systems.

A study in [55] proposed a framework consisting of various techniques and specialized procedures that can protect the data efficiently from the owner to the cloud and then to the user. Data protection strategies include a secure socket layer (SSL) and MAC, which are used to check the integrity of data, to encode the data, and divide it into three sections of the cloud. The division of data into three sections offers additional protection and more accessibility. The proposed method achieves the availability, reliability, and integrity of data travelling through the server owner to the cloud and from the cloud to the customer. In addition, it also offers more flexibility and allows the user to retrieve files from the cloud by searching for encrypted data.

The study in [56] identified problems related to cloud data storage, such as data breaches, data theft, and cloud data unavailability. The study proposed potential solutions to those issues. The proposed solutions addressed issues related to identity management and access control. However, there are many issues related to access control and identity management that are still unsolved, such as weak credentials that can easily be reset, denial of service attack to lock the account for a period of time, weak logging and monitoring capabilities, and XML wrapping attacks on web pages.

The authors in [57] proposed a new technique called match-then-decryption, in which a matching phase is added before the decryption phase. This technique works by computing special components in ciphertexts used to verify whether the private key attribute matches the hidden access policy in ciphertexts without decryption. Formal security analyses and comparisons showed that the suggested solutions simultaneously ensure privacy attributes and increase the efficiency of decryption for outsourced cloud data storage.

In [58], the authors proposed a system to enhance the RSA algorithm by increasing the key size to strengthen the encryption process. The proposed algorithm reduces the time required for encryption and decryption by dividing the file into blocks and enhances the strength of the algorithm by increasing the key size. This power paves the way for users to store data in the cloud efficiently.

The study in [59] used elliptic curve cryptography (ECC) to encrypt data in the cloud environment because the key size used by ECC is very small. Owing to the small key size of the ECC, the computing power is reduced, and the energy consumption is minimized. This study showed that ECC is fast and more effective for data protection in a cloud computing environment and reduces computing power and also improves performance.

The authors in [60] suggested a hybrid algorithm to improve cloud data security using an encryption algorithm. To improve cloud security, this study combined homographic and blowfish encryption algorithms. The blowfish algorithm was used to generate a security key. A symmetric key block was used for both decryption and encryption. Homographic encryption, on the other hand, provides confidentiality of data and prevents storing the information in plain text at any stage.

In [61], the authors proposed a novel lightweight encryption algorithm consisting of combining a symmetric algorithm for encrypting data and an asymmetric one for distributing keys. This combination allows users to benefit from successful asymmetric encryption protection and rapid symmetric encryption performance while maintaining uses' rights to protected and permitted access to data. The findings reveal that the lightweight algorithm's processing time is faster than state-of-the-art cryptographic algorithms.

In the study [8], the authors suggested a hybrid layered approach to protect the data of the user, along with a combination of a lattice-based security technique. A new approach was introduced for responsibilities and roles examination using the lattice model. The AES and RSA algorithms were used to provide sensitive data with more and better protection.

The study in [60] proposed a hybrid algorithm to enhance the security of cloud data using an encryption algorithm. It combined homographic encryption and blowfish encryption to enhance cloud security. However, this hybrid algorithm does not appear to be effective in practice, as the homographic encryption is extremely slow and computationally expensive, to the point that it is not currently practical. In addition to that, the blowfish algorithm does not provide authentication and non-repudiation because more than one person might share the same key. Additionally, there are some drawbacks in this method of decryption, as it takes up more time and bandwidth.

To conclude, the proposed solutions for cloud data protection vary between data auditing, encryption, classification, and secure data modeling. However, these techniques are still not fully mature and face many problems. In Section 6, some open challenges are highlighted, followed by future research recommendations in Section 7.

5.2. Solutions at Application Level

To mitigate risks at the application level, several solutions have been proposed by researchers. For instance, a study in [62] provided a novel "Scale Inside Out" technique that decreases the Resource Utilization Factor to a minimum value during attacks to rapidly absorb the DDoS attack. In addition to other co-located facilities, the recommended solution sacrifices victim service resources and provides certain resources to the prevention service to assess the availability during the attack. According to the study, the experimental evaluation indicates a decrease of up to 95% in total attack downtime of the victim's service in addition to significant improvements in attack detection and reporting time and downtime of co-located facilities.

A contribution in [63] suggested a method to limit the effects of economic denial of service (EDoS) attacks on cloud applications. This method was dependent on the adoption of the service level agreement (SLA) supplemented by an intrusion prevention scheme (IPS).

Another effort in [64] suggested a new method that used an artificial neural network (ANN) along with the genetic algorithm (GA) for EDoS attack detection in the cloud. The classification was carried out using an ANN that classifies the customer of the cloud server and minimizes the EDoS attacks in the cloud environment, while the GA was used to optimize the attributes of each server using appropriate fitness functions.

Researchers in [5] proposed an approach to mitigate EDoS attacks in the SDN-based cloud computing environment. An unsupervised deep learning technique called long short-term memory (LSTM) was used as a multivariate time series anomaly detection model. The main concept was to try to predict the values of a cloud customer's resource use (memory use, CPU load, etc.). The experiments were conducted with different EDoS attack levels and proved that the proposed approach was an effective and innovative solution for SDN-based cloud defense of EDoS attacks according to the authors.

Another study in [37] designed a technique for identifying cloud computing DDoS attacks. This technique employs machine learning algorithms such as support vector machine (SVM), naive Bayes (NB), and random forest (RF) for classification. The study was carried out using Tor Hammer as an attacking tool on a cloud environment, and a new dataset for the intrusion detection technique was developed.

A study in [65] discussed various authentication schemes used in cloud computing and proposed a framework for using passphrase-based multifactor authentication to make cloud resources more secure. The primary comparison of authentication models reinforced the level of security and the disadvantages of corresponding schemes in the cloud computing environment. The passphrase in the proposed scheme ensures secure passwords and provides extra security for the SSH key pair. In [66], the authors proposed an authentication-based AES and MD5 technique for data encryption to protect the data and the login of the users over the cloud at the time of login.

The authors in [67] proposed a novel security model for authentication-supported cloud computing. The model introduced a new idea for a biometric security system based on fingerprint recognition. The proposed method automated the verification process to match human fingerprints, where fingerprints are used to identify the individuals and verify their identity. Users are authenticated based on the fingerprint templates, which must be given based on random numbers generated each time. The experimental results showed that the proposed system outperforms the single-fingerprint authentication system.

The researchers in [68] recently proposed a novel hash-based, multi-factor, secure mutual authentication scheme that includes mathematical hashing properties, certificates, nonce values, traditional user IDs and password mechanisms. The strength of the proposed authentication procedure was evaluated using the GNY belief logic and the Scyther method. The results show that the proposed scheme can prevent the man-in-the-middle, replay and forgery attacks.

In another recent study [69], the Seamless Secure Anonymous Authentication Scheme (S-SAAS) was proposed to establish a secure session for cloud-based mobile edge computing. This proposed protocol used elliptic-curve cryptography, one-way hash function and less expensive operation to provide seamless connectivity. In addition, this proposed protocol applied a new random integer to withstand potential attacks and satisfies important security features.

The authors in [70] recently proposed a novel pairing-free multi-server authentication protocol based on ECC for the MCC environment. The proposed scheme not only offers computational cost-efficiency but also preserves the features of costly pairing schemes, such as the achievement of secure mutual authentication, anonymity and scalability. The strength of the scheme is theoretically illustrated by the formal security model.

The authors in [71] developed various models for information and resource sharing among tenants in an IaaS cloud using the Open Stack platform as a reference. The models encourage a tenant to engage its IT resources with other tenants in a controlled method. Nevertheless, the VMs need to be restricted in network access so that malicious software is incapable of transmitting the information in an uncontrolled manner.

The work in [72] proposed a novel access control framework for security and privacy issues in the cloud environment. The proposed framework was based on dynamic trustworthiness. Access control that is based on dynamic trustworthiness is applied to decrease the possibility to perform unauthorized activities and to make sure that only authorized users can access cloud resources. The result show that the system identifies malicious behavior to avoid any unauthorized access, will enhance the security of cloud computing, and will therefore lead to an increased trust degree of users.

The authors in [73] proposed a hybrid access control framework called iHAC that enables combining the features of type enforcement and role-based access control. The proposed framework enables flexible access control and is unified for IaaS clouds environments. In addition, a VMM-based access control technique was designed to restrict the VM's behaviors to the underlying resources in a fine-grained method. The experimental results show that the iHAC framework helps to make true access control decisions with an acceptable performance overhead.

Another study in [74] proposed a dynamic access control approach to solve the multifarious security breaches that occur in the cloud. This approach tends to secure data in the cloud that should address the interrelationship between the requestor, data that are requested, and the action that will be performed on the data. Furthermore, the study considered the user for granting access control dynamically. The result only presented an initial implementation of the proposed approach.

A recent study in [75] proposed a blockchain-based access control framework called AuthPrivacyChain and privacy protection in clouds. All authorization that is linked to transactions is posted through the user to the blockchain. Moreover, the framework was designed based on an enterprise operation system (EOS) blockchain to access the permission and the information as a further description of blockchain transactions. Additionally, AuthPrivacyChain provides access control, authorization revocation and authorization. The experimental results show that only legal users can access resources, but AuthPrivacyChain cannot prevent attacks from external users.

A study in [76] proposed an approach for cloud identity management with privacy and security improvements based on blockchain. This approach provides a mechanism for authentication and decentralized trust. In the trust model, the cloud service providers (CSPs) do not require pre-configured parameters or rules to establish interactive trust relationships. Therefore, this approach manages trust relationships between the clients and CSPs effectively and ensures secure IaaS for cloud federations. The results show the effectiveness of the proposed identity management blockchain-based approach while improving privacy and security capabilities.

The authors in [77] proposed a novel dynamic trust model for federated identity management (FIM) based on fuzzy cognitive maps. This model aimed at evaluating trustworthiness relationships between unknown entities dynamically and securely which makes FIM more flexible and scalable to be maintained and deployed in the cloud. Furthermore, the proposed model provides a set of trust features that serve as a basis for quantifying and modeling the trust level of unknown entities.

The study in [78] introduced a framework that enables the CSPs to supply the identity and access management (IAM) as a public cloud service, which is also called IAMaaS. This framework aims at ensuring that the collection of identities complies with the cloud. According to the authors, the IAMaaS can work perfectly with an existing on-premise platform in a hybrid manner to promote the capacity of security. In addition, the IAMaaS enables users to define the virtual private area in cloud space to enhance the security and protection of their resources.

The researchers in [79] proposed an identity management system (IDMS) to preserve the security of communication among servers and clients in cloud computing. The proposed system relied on the dual certificate manager (DCM) technique for authorizing and authenticating users to avoid privacy violations. The DCM technique uses token-based terminology for tracking and easy data access, which lead to downsizing the domain of the attacks. Additionally, this technique was commonly applied for the SSL/TLS protocol to protect data transmission.

To conclude, the review of solutions in the literature at the application level revealed that solutions at this level focused on the use of IDS/IPS techniques to mitigate the risks associated with DDoS and EDoS. These techniques have certain limitations, such as ineffectiveness when dealing with complex and unknown patterns of attacks, while the cloud needs techniques that can detect and/or prevent sophisticated attacks. In addition, the existing access control and identity management solutions (e.g., traditional firewall, encryption, and virtualized access control) at this level are not appropriate to promote security, because these solutions have a deficiency in managing the privileges the trust relationships needed to prevent the internal/external attackers. Consequently, the researchers should incorporate advanced techniques such as blockchain.

Moreover, numerous models used various techniques for authentication, but there are many barriers against implementing these techniques, such as the different testing environments and the use of a small amount of data during the verification process. This does not give confidence in the suitability of the models in the cloud computing environment even. Additionally, biometric systems are emerging as one of the best solutions to improve authentication security and privacy. Biometric systems play a key role in government and commercial applications outsourced to the cloud. Therefore, security and privacy are the biggest concerns for users. Unfortunately, most of these techniques are complex, impractical, and time-consuming.

5.3. Solutions at Network Level

In [80], the authors proposed SNORT as an intrusion detection system to defend against DoS and DDoS attacks in cloud computing. The DDoS attack floods the server with a huge number of needless packets and makes it unavailable to legal consumers. The proposed system depends on some written rules to detect and prevent DDoS attacks. Similarly, the authors in [81] proposed an approach to identify and filter a variety of DDoS attacks in cloud environments. This approach is based on the GARCH model and an artificial neural network (ANN). GARCH is used to estimate the value of variances and to figure out any possible anomalies in the real traffic relative to the actual value of variances. The ANN is used to identify the traffic after discarding values that are less than a certain threshold into regular traffic and anomalous traffic.

A recent study in [6] presented a technique for the consumers to encrypt and push the data blocks randomly in the P2P network based on blockchain. There are several data centers and multiple users in a distributed cloud, and this may sometimes pose a problem in file block replica placement. Therefore, the blockchain approach seems to be the perfect technique in terms of file security and network transmission delay.

Another study in [82] proposed a dynamic proof to communication-efficient recovery and supporting public audibility from data corruptions through irretrievability schemes. In this study, the data were divided into two parts: coding operation and data block which are performed for all blocks individually. The proposed approach can be applied to storage to minimize the update impact on the remote data. Any attempt to update will therefore impact only on small codeword symbols. In addition, an efficient data reform strategy is proposed in case of a server breakdown.

The authors in [83] summarized all types of attacks on DNS that exploit the DNS infrastructure. According to the authors, the most used DNS technique is the use of firewalls, which are considered one of the best practices in setting up DNS servers. Furthermore, the dynamic DNS firewall and appropriate signatures protect against whole potential attack surfaces.

The study [84] designed a software-as-a-service (SaaS) model that was called OpenPipe. The OpenPipe model adopted a hybrid control mode that was applied with two hierarchical control levels, in which a software-defined networks (SDN) controller forms the higher level, and the local controllers comprise the lower level. The SDN worked to separate the control plane from the data plane to provide network virtualization and programmability. A lab demo was performed to verify the effectiveness of openPipe.

The study [85] presented several security approaches that were used to prevent unauthorized access to cloud computing environments, such as certificates (e.g., Public Key Infrastructure), a high level of authentication and authorization, and different encryption methods (e.g., symmetric and asymmetric key algorithms).

The authors in [86] proposed a Bayesian network-based weighted attack path modeling technique to model attack paths. They also proposed an optimized algorithm to find the shortest attack path from multiple sources based on key nodes and key edges. Not only does the algorithm find the shortest path, but it also resolves any existing ties between equal weight paths.

A study in [87] proposed a Hypervisor Level Distributed Network Security (HLDNS) framework to be deployed on each cloud server. Each server monitors the network traffic between the VMs and the other components such as the virtual network, the internal network, and the external network for intrusion detection. The study tested the proposed HLDNS framework on a cloud-tested NIT Goa by performing various attacks in real-time using recent intrusion detection datasets such as UNSW-NB15 and CICIDS-2017. The results of the experiments were encouraging.

The authors in [88] focused on detecting the DDoS attack by developing a deep learning classifier. The users' service requests are collected and grouped as log information. Some important features of the log file are selected for classification using the Bhattacharya distance measure to reduce the training time of the classifier. From the simulation results, it was concluded that the proposed TEHO-based DBN classifier yielded improved detection performance.

At this level, more emphasis was given to solve the DoS/DDoS attacks by using IDS/IPS techniques. However, these techniques are not accurate (e.g., generate a false alarm for legal requests), and deal with unique or single attacks only. In addition, these solutions did not deal with IP spoofing, while attackers use this kind of attack with

DoS/DDoS to overload networks. Consequently, they were unable to differentiate between good traffic and bad traffic. In addition, very few efforts have been made to address prefix hijacking attacks, while it is a major problem.

Another important point is that more attention is given to the availability of the network by solving DNS issues using firewalls; however, there are several forms of DNS attacks such as a man-in-the-middle attack, modified data attack, DNS ID spoofing attack, corrupted data attack, and DDOS attack that cannot be solved by using the traditional firewalls and can be overcome by other techniques.

5.4. Solutions at Host Level

The authors in [89] investigated the virtual machines and hypervisor intrusion detection method, VMHIDS, as a technique in the virtualized cloud environment to detect and prevent hypervisor attacks. This method protected both the hypervisor and virtual machines from cloud environment attacks, either internal or external. The continuous hypervisor or VM monitoring with VMHIDS made it possible to analyze real-time events for automated detection and blocking malicious events. VMHIDS monitors and keeps track of each file and process that interacts with the hypervisor. As VMHIDS is placed on both VMs and hypervisors, it is easy to detect new attacks or suspected attacks on hypervisors for faster prevention.

A study in [90] proposed a host-based intrusion detection model that provides security as a service at the host level in the cloud. This model alerts the host to malicious activities inside the system. Furthermore, a KNN classifier has been used to classify the system call traces that allow integration of new training documents. The result showed that the proposed method achieved high detection accuracy.

The authors in [91] developed a prevention model for DDOS attacks over hypervisor environments. This model was based on host-based intrusion detection defense system. In other words, the model was based solely on IDS modeling and then incorporated into the hypervisor environment with IPS. To identify and configure the cloud server, the prevention model uses principal component analysis and linear discriminant analysis with a hybrid, nature-inspired metaheuristic algorithm named Ant Lion optimization for feature selection. An artificial neural network is then used as a classifier. The results indicate that the model was able to detect malicious activities and block the malicious IP by sending it to the blacklist.

Another study in [92] suggested a framework to decrease the co-located VM attack on the same hypervisor. This was done by implementing virtual machine security policies when an illegal transfer or copy of live VMs into a suspicious hypervisor occurs. The preset data traffic rate monitoring between two VMs and the VSwitch node helped to detect VM confusion at a particular time point. The results show that the framework decreases the risk associated with the VM running upon this suspected hypervisor. This framework, however, focused only on the live migration from one hypervisor to another hypervisor of single VMs.

A study in [34] proposed various ways to secure the servers by using IDS, by storing hashed values, as the data in the cloud are naturally plaintext. The study suggested that multiple applications that run on single servers must be separated. Furthermore, the threshold that monitors server load and prevents DOS attacks should be determined. Finally, data replication is necessary to ensure the availability of data and that the server works all of the time.

In [93], the authors proposed an in-and-out-of-the-box virtual machine and hypervisor by using a prevention system and intrusion detection. The goal of this work was to detect vulnerabilities including persistent attacks such as DoS attacks and stealthy self-hiding rootkits. The experiments were conducted on the open-source host that is based on IDS, also known as Open-Source Security Event Correlator (OSSEC). The experimental results show that OSSEC IDS effectively detects rootkits and DoS attacks in both Linux and Windows operating systems.

A study in [94] discussed the virtualization issues in cloud computing infrastructure. According to the study, the major threats for cloud infrastructure are distributed side-channel attacks that can be used to exploit sensitive information from various parts of a distributed system. Furthermore, they sketched an approach for the reduction in side-channel attacks utilizing an autonomic system.

The researchers in [95] suggested a framework that used the VM monitoring script to obtain the status of the VMs to defend the VMs from an attack. As part of the kernel-based virtual machine manager (KVM), a smart virtualization monitoring system was integrated by sending the status of each VM running on a hypervisor. The intelligent device classifies and actively rectifies attack patterns. Via the cloud API, the appropriate action that should be taken will be communicated.

In [7], the authors proposed a Security-aware Virtual Machine Placement Algorithm (SMOOP) based on multi-objective optimization to search for a pare-to-optimal method to reduce cloud's overall security risks. SMOOP assessed cloud security from four perspectives: hypervisor vulnerabilities, networking, co-residence, and VM vulnerabilities. The proposed vulnerability assessment was location-specific and spans multi dimensions. Compared to existing solutions, the experimental findings indicate the efficacy of the proposed method and the enhancement.

A study in [96] evaluated the private cloud infrastructure tools called Ceilometer and Monasca to test the ability of information collected in a short time to detect the resource constraints and determine the effect of resource consumption of host systems. Both tools were analyzed, and the evaluation revealed that the Monasca achieved better performance than Ceilometer.

The authors in [97] implemented signature-based network intrusion detection (NIDS) such as OSSEC as host-based IDS and SNORT for the detection of intrusions at the cloud VM instances and network level. In addition, the study discussed the flow of traffic and monitoring on various occasions. The results show that the proposed systems were able to detect attacks on host VMs and can send alerts to the organization.

A recent study in [98] introduced a new hypervisor-based cloud IDS that utilizes online multivariate statistical change analysis to detect anomalous network behaviors. In the proposed system, the hypervisor benefits from a collection of instances to introduce an instance-oriented new feature mode that exploits the correlated and individual behaviors of instances to enhance the detection capability. The proposed approach was evaluated using a newly collected cloud intrusion dataset that includes a wide diversity of attack vectors.

According to [99], a parameterized scheduling policy focused on minimizing the makespan, combined with an energy-efficiency policy based on the hibernation of every virtual machine whenever possible, could reduce the energy consumption of large-scale data centers without affecting the overall performance of cloud computing systems. In the same work, the authors described a model for reducing energy consumption in cloud computing environments that can reduce the energy consumption of a cloud computing system by up to 45%. The proposed model is divided into two parts: an energy-aware independent batch scheduler and a set of energy-efficiency policies for idle VM hibernation. The experimental results show the good performance of the proposed model.

Furthermore, in [100], the online non-clairvoyant scheduling algorithm Highest Scaled Importance First (HSIF) method was proposed, in which HSIF chooses an active job with the highest scaled importance to minimize the sum of scaled importance-based flow time and energy consumed. The use of HSIF in data centers and battery-based devices reduces power consumption and improves computing capability.

To determine which cloud scheduling solution is more important to select, this paper [101] proposed an energy-efficient task-scheduling algorithm based on best-worst (BWM) and the technique for order preference by similarity to ideal solution (TOPSIS). The experimental results demonstrate that, when compared to its counterparts, the proposed approach can effectively reduce energy consumption. Furthermore, the proposed approach can significantly improve VM utilization, making it suitable for exploring large-scale problems.

In addition, the SCORE tool was defined in this paper [102] as an extension to the Google Omega lightweight simulator, which is devoted to the simulation of energy-efficient monolithic and parallel-scheduling models as well as the execution of heterogeneous, realistic, and synthetic workloads. Empirical tests were used to evaluate the simulator. The experiment results confirm that SCORE is a performant and reliable tool for testing energy efficiency, security, and scheduling strategies in cloud computing environments.

At this level, the majority of solutions employed IDS/IPS models to detecting and preventing hypervisor attacks and identifying malicious activities inside the system. However, the cloud is a large-scale and heterogeneous environment that needs to mitigate the risks of hypervisors in multiple VMs, while some studies, such as [93], focused on mitigating risks on hypervisors in single VMs only. Furthermore, some solutions were customized to specific scenarios, known patterns of attacks, or even specific software [92,94]. To conclude, the proposed solutions should consider some serious attacks such as the distributed side-channel attacks while designing their detection or prevention techniques. These attacks are major threats to cloud infrastructures that can be used to exploit sensitive data from various parts of a distributed system [95]. The host-level techniques are still not fully mature, in which these techniques need to immediately respond, automatically block malicious events, and take appropriate action to prevent attacks from happening.

Table 4 presents a summary of the existing solutions in the literature according to the four levels discussed in the previous subsections.

Table 4. Summary of existing solutions in the literature.

Level Name	Techniques	Limitations	References
Data Level	Data loss or leakage used a technique to secure data are by applying encryption mechanisms like TLS, AES and SHA Classification technique to have security levels for data	The encryption techniques are still not fully mature and face many problems The available technique to classification is consumes resources	[9,37,50–62]
Application Level	IDS/IPS techniques were used to solve DDoS attacks in cloud applications and services	The existing techniques deal with simple DDoS attacks only, while the nature of the cloud needs techniques can prevent and detect the complex attacks and unknown patterns	[6,38,63–80]
	IDS/IPS techniques were used to solve EDoS attacks	The techniques used to solve simple attacks	
	The techniques to solve poor authentication are identity management system (IDMS), and also some authentication based on AES and MD5	Testing environments and use a small amount of data are considered barriers against implementation.The traditional access control and identity management are not suitable to promote security	
Network Level	The existing techniques using a IDS/IPS to solve DoS and DDoS attacks	Some of DDoS/DoS techniques did not deal with IP spoofing where these attacks often use IP spoofing to overload networks; therefore, it is unable to differentiate between good traffic and bad traffic	[7,81–89]
	The techniques of DNS issues vary between dynamic firewalls and IDS	These techniques did not take into consideration some of the serious attacks such as Man in the middle attack, modified data attack, DNS ID spoofing attack, corrupted data attack, . . . etc.	

Table 4. *Cont.*

Level Name	Techniques	Limitations	References
Host Level	The techniques to solve the virtual machines and hypervisor issues are intrusion detection and VM monitoring	These techniques were limited their techniques to specific scenarios, known patterns of attacks or even specific software Techniques need more focus on other types of attacks such as distributed side-channel attacks while designing their detecting or preventing techniques	[8,35,90–102]

6. Open Challenges

While cloud computing has been widely embraced by businesses and industries, cloud computing research is still immature. Many of the current gaps regarding the cloud infrastructure have not been completely addressed, while new challenges continue to arise. The following subsections summarize the most important open challenges that need to be studied further.

Securing Hypervisor

An insecure hypervisor is a serious challenge that threatens cloud computing. It can damage the entire system [21]. Traditional detection/prevention solutions are not efficient enough with the dynamic nature of the cloud. The cloud needs context-aware solutions to differentiate between normal and abnormal behaviors. Additionally, any proposed solution should take immediate action to avoid damaging the cloud infrastructure or disrupting the normal operations.

Third-party Auditing

The popularity and rapid growth of cloud-based information storage services have generated controversy about the integrity of cloud-based data, which can be lost or destroyed because of unavoidable hardware-software failures and/or human-related errors. The third-party auditor should provide expert integrity verification services. During public auditing of cloud information, the content of the private information of the individual client should not be revealed to any public verifier. As a result, a new major issue regarding privacy, and more specifically the leakage of data privacy to third-party auditors, has been being introduced. It remains a difficult research challenge to establish solutions that ensure the integrity of cloud storage security and privacy.

Data Availability

Under security breaches, the system must be able to continue its normal operations. Availability also refers to the data, software and hardware available to approved users based on demand. System availability incorporates the capacity of the framework to carry out operations at all times. Data availability, protection, and data security stand out amongst the most perplexing challenges of the cloud environment up to now.

Data Remanence

Data remanence is the presence of residual data even after deletion, reformatting, or reallocation of it to another person. This is a major threat to the confidentiality of deleted files (passwords, encryption keys, government data, financial or health data, etc.). Data remanence may be discovered by computer forensics and other various techniques. In addition, it is possible to find and recover files that might have been removed from a computer [103]. Cloud providers have not fully addressed data remanence, and this issue is even ignored by some cloud providers, even though it is one of the most critical issues.

Network security

At the network level, the proposed security mechanisms were presented to be defensive in IaaS, such as a dynamic DNS firewall that protects against attack, as mentioned in [83]. However, there are still a lot of attacks that cannot be resolved with a traditional firewall. The DNS attack is an increased risk in cloud computing due to the several attacks that are identified as a consequence of it. In addition, there are few research efforts about reusing IP addresses, which leads to serious data and system breaches from a customer security perspective.

Access control and Identity Management

Due to the obvious cloud-specific characteristics, conventional access control and identity management techniques are not suitable for promoting IaaS security. New technologies such as blockchain and computational intelligence should be used in this regard to provide sufficient security in this new computing environment.

Authentication

Most authentication solutions are time-consuming and complex. Existing studies tested their techniques via simulation with a small amount of data, less complex resources and a smaller number of users. However, the cloud in reality has a huge number of users and other complex features. Therefore, more effort should be given to developing techniques that take into consideration all of these constraints. Moreover, authentication techniques are usually for one party, and the cloud service provider does not have a platform for multiple user interface authentication.

7. Future Recommendations

Based on the open challenges discussed so far, this section recommends some future research directions.

Securing Hypervisor

To distinguish between normal and abnormal behaviors, the cloud requires context-aware solutions to detect new and emerging attack patterns and respond immediately to prevent any possible harm to the cloud infrastructure. This should also take into account the dynamic nature of the cloud environment and the mobility of its customers. Additionally, customer preferences and his/her level of security awareness should be considered when building these solutions.

Third-party Auditing

Some recommendations for developing third-party auditing solutions should consider the following characteristics:

Third-party auditing should be performed without retrieving a copy of the data; therefore, privacy is maintained.

The data should be divided into parts and stored in an encrypted format in the cloud storage, thereby maintaining the confidentiality of the data.

Verifying data integrity at the client's request to check whether the stored data are tampered with and inform the user as such.

Data Availability

How to store data is also key to ensuring data availability. Some techniques can be used to ensure data availability and could be a focus for future research in securing cloud infrastructure as in the following points:

- Data backups must be stored separately or in a distributed network. This means that the user will not lose information permanently if the storage part degrades or fails.
- Update backups periodically, so that the user can restore the most current data versions.
- Data loss prevention (DLP) tools help to minimize data violations and data center physical damage. These tools use cloud-based secure storage from third parties to avoid loss of data. Some DLP tools provide monitoring, blocking of threats, and forensic analysis.
- Object storage uses advanced erasure coding to ensure data availability. Erasure coding blends data with parity data, and then breaks and distributes them throughout the storage environment. This could prevent component failure since users only need a subset of the shared data for data restoration.

Data Remanence

These solutions can be used to remove or minimize the presence of residual data as mentioned below.

- Sterilization, also known as purging, refers to removing confidential information from a storage system to avoid ant recovery by a known method or technique.
- Data encryption is an effective data protection method.

Network security

Some security recommendations for network security can be summarized as follows:

- The internal communication of the cloud must adopt secure communication techniques such as HTTPS, and also the transmission channel must be encrypted by TLS.
- Using anomaly detection solutions for HTTP requests that can effectively prevent any malicious network intrusion behaviors.
- The cloud can use public security services such as web application firewalls (WAF), virtual firewalls, virtual bastion machines, virtual host protection and virtual database audit systems.

Access control and Identity management

The following are some security considerations for access control and identity management that should be considered by future research.

- The cloud must be accessed only by the access key authentication.
- The cloud must apply some security operation management such as (A) situation awareness that sort all assets and business systems in the cloud, (B) safe operation and maintenance that provide unified account management, unified authority management, unified interface management and unified ID authentication.
- Single sign-on (SSO), currently applied in many cloud environments, could be incorporated with blockchain-based self-sovereign identity management approaches. This will give customers more autonomy in keeping and managing their credentials in a unified and more private manner.

Authentication

There is a need for authentication mechanisms that can deal with complex resources, a large number of users, and the heterogeneous nature of the cloud without consuming time. Furthermore, there is a need for authentication techniques for multiple user interface authentication. Blockchain technology could be utilized to design stronger authentication mechanisms.

8. Conclusions

Despite bringing many benefits, the cloud computing paradigm imposes serious concerns in terms of security and privacy, which are considered hurdles in the adoption of the cloud at a very large scale. Customers and organizations in the cloud should be aware of threats, attacks and vulnerabilities, as security awareness is considered the first step to ease the adoption of the cloud. This paper discussed the concerns and challenges in the cloud computing infrastructure at various levels (Application, Network, Host, Data). To deal with these challenges, several existing solutions were introduced to alleviate them. Many existing gaps, however, have not been fully resolved, and new problems continue to appear due to the shared, virtualized, distributed, and public nature of the cloud. Subsequently, this paper focused on various solutions to address security issues at different levels in the cloud infrastructure.

Funding: The APC was funded by Deanship of Scientific Research, Qassim University.

Acknowledgments: The researcher(s) would like to thank the Deanship of Scientific Research, Qassim University for funding the publication of this project.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Elsherbiny, S.; Eldaydamony, E.; Alrahmawy, M.; Reyad, A.E. An extended Intelligent Water Drops algorithm for workflow scheduling in cloud computing environment. *Egypt. Inf. J.* **2018**, *19*, 33–55. [CrossRef]
2. Hanen, J.; Kechaou, Z.; Ben Ayed, M. An enhanced healthcare system in mobile cloud computing environment. *Vietnam J. Comput. Sci.* **2016**, *3*, 267–277. [CrossRef]
3. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing*; Nation-al Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
4. Hatwar, S.V.; Chavan, R. Cloud Computing Security Aspects, Vulnerabilities and Countermeasures. *Int. J. Comput. Appl.* **2015**, *119*, 46–53. [CrossRef]
5. Dinh, P.T.; Park, M. Dynamic Economic-Denial-of-Sustainability (EDoS) Detection in SDN-based Cloud. In Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 20–23 April 2020.
6. Karajeh, H.; Maqableh, M.; Masa'deh, R. Privacy and security issues of cloud computing environment. In Proceedings of the 23rd IBIMA Conference Vision, Valencia, Spain, 13–14 May 2020.
7. Han, J.; Zang, W.; Chen, S.; Yu, M. Reducing Security Risks of Clouds Through Virtual Machine Placement. In Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, Philadelphia, PA, USA, 19–21 July 2017.
8. Saravanan, N.; Umamakeswari, A. Lattice based access control for protecting user data in cloud environments with hybrid security. *Comput. Secur.* **2021**, *100*, 102074. [CrossRef]
9. Vaquero, L.M.; Rodero-Merino, L.; Caceres, J.; Lindner, M. *A Break in the Clouds: Towards a Cloud Definition*; ACM: New York, NY, USA, 2008.
10. Siddiqui, S.; Darbari, M.; Yagyasen, D. A Comprehensive Study of Challenges and Issues in Cloud Computing. In *Soft Computing and Signal Processing*; Springer: Singapore, 2019; pp. 325–344.
11. Marston, S.; Li, Z.; Bandyopadhyay, S.; Ghalsasi, A. Cloud Computing—The Business Perspective. *Decis. Support Syst.* **2011**, *51*, 176–189. [CrossRef]
12. Kuyoro, S.; Ibikunle, F.; Awodele, O. Cloud computing security issues and challenges. *Int. J. Comput. Netw.* **2011**, *3*, 247–255.
13. Alajmi, Q.; Sadiq, A.S.; Kamaludin, A.; A Al-Sharafi, M. Cloud Computing Delivery and Delivery Models: Opportunity and Challenges. *Adv. Sci. Lett.* **2018**, *24*, 4040–4044. [CrossRef]
14. Diaby, T.; Rad, B.B. Cloud Computing: A review of the Concepts and Deployment Models. *Int. J. Inf. Technol. Comput. Sci.* **2017**, *9*, 50–58. [CrossRef]
15. Chauhan, V.K.; Bansal, K.; Alappanavar, P. Exposing cloud computing as a failure. *Int. J. Eng. Sci. Technol.* **2012**, *4*, 1320–1326.
16. Bamiah, M.A.; Brohi, S.N. Exploring the cloud deployment and service delivery models. *Int. J. Res. Rev. Inf. Sci.* **2011**, *1*, 77–80.
17. Tabrizchi, H.; Rafsanjani, M.K. A survey on security challenges in cloud computing: Issues, threats, and solutions. *J. Supercomput.* **2020**, *76*, 9493–9532. [CrossRef]
18. An, Y.Z.; Zaaba, Z.F.; Samsudin, N.F. Reviews on Security Issues and Challenges in Cloud Computing. *IOP Conf. Ser. Mater. Sci. Eng.* **2016**, *160*, 012106. [CrossRef]
19. Faheem, M.; Akram, U.; Khan, I.; Naqeeb, S.; Shahzad, A.; Ullah, A.; Mushtaq, M.F. Cloud Computing Environment and Security Challenges: A Review. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 183–195. [CrossRef]
20. Sikeridis, D.; Papapanagiotou, I.; Rimal, B.P.; Devetsikiotis, M. A Comparative taxonomy and survey of public cloud infrastructure vendors. *arXiv* **2017**, arXiv:1710.01476.
21. Subramanian, N.; Jeyaraj, A. Recent security challenges in cloud computing. *Comput. Electr. Eng.* **2018**, *71*, 28–42. [CrossRef]
22. Kumar, P.R.; Raj, P.H.; Jelciana, P. Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Comput. Sci.* **2018**, *125*, 691–697. [CrossRef]
23. Bokhari, M.U.; Makki, Q.; Tamandani, Y.K. A Survey on Cloud Computing. In *Big Data Analytics*; Advances in Intelligent Systems and Computing; Springer: Singapore, 2018; Volume 654, pp. 149–164.
24. Abdurachman, E.; Gaol, F.L.; Soewito, B. Survey on Threats and Risks in the Cloud Computing Environment. *Procedia Comput. Sci.* **2019**, *161*, 1325–1332. [CrossRef]
25. Dong, S.; Abbas, K.; Jain, R. A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. *IEEE Access* **2019**, *7*, 80813–80828. [CrossRef]
26. Alhenaki, L.; Alwatban, A.; Alamri, B.; Alarifi, N. A Survey on the Security of Cloud Computing. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019.
27. Domingo-Ferrer, J.; Farràs, O.; Ribes-González, J.; Sánchez, D. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. *Comput. Commun.* **2019**, *140*, 38–60. [CrossRef]
28. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Comput. Sci. Rev.* **2019**, *33*, 1–48. [CrossRef]
29. Ibrahim, F.A.M.; Hemayed, E.E. Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review. *Comput. Secur.* **2019**, *82*, 196–226. [CrossRef]
30. Qureshi, A.; Dashti, W.; Jahangeer, A.; Zafar, A. Security Challenges over Cloud Environment from Service Provider Prospective. *Cloud Comput. Data Sci.* **2020**, *1*, 1–48. [CrossRef]
31. Saini, H.; Saini, A. Security Mechanisms at different Levels in Cloud Infrastructure. *Int. J. Comput. Appl.* **2014**, *108*, 1–6. [CrossRef]

32. Inukollu, V.N.; Arsi, S.; Ravuri, S.R. Security Issues Associated with Big Data in Cloud Computing. *Int. J. Netw. Secur. Appl.* **2014**, *6*, 45–56. [CrossRef]
33. Rao, R.V.; Selvamani, K. Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Comput. Sci.* **2015**, *48*, 204–209. [CrossRef]
34. Aich, A.; Sen, A. Study on Cloud Security Risk and Remedy. *Int. J. Grid Distrib. Comput.* **2015**, *8*, 155–166. [CrossRef]
35. Farsi, M.; Ali, M.; Shah, R.A.; Wagan, A.A.; Kharabsheh, R. Cloud computing and data security threats taxonomy: A review. *J. Intell. Fuzzy Syst.* **2020**, *38*, 2517–2527. [CrossRef]
36. Balogh, Z.; Turčáni, M. Modeling of data security in cloud computing. In Proceedings of the 2016 Annual IEEE Systems Conference (SysCon), Orlando, FL, USA, 18–21 April 2016.
37. Wani, A.R.; Rana, Q.P.; Saxena, U.; Pandey, N. Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019.
38. Al Amri, S.M.; Guan, L. Infrastructure as a service: Exploring network access control challenges. In Proceedings of the 2016 SAI Computing Conference (SAI), London, UK, 13–15 July 2016.
39. Sharma, A.; Keshwani, B.; Dadheech, P. Authentication issues and techniques in cloud computing security: A review. In Proceedings of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Jaipur, India, 26–28 February 2019.
40. Kazim, M.; Zhu, S.Y. A survey on top security threats in cloud computing. *Int. J. Adv. Comput. Sci. Appl.* **2015**, *6*. [CrossRef]
41. Al-Haidari, F.; Sqalli, M.; Salah, K. Evaluation of the impact of EDoS attacks against cloud computing services. *Arab. J. Sci. Eng.* **2015**, *40*, 773–785. [CrossRef]
42. Turab, N.M.; Abu Taleb, A.; Masadeh, S.R. Cloud Computing Challenges and Solutions. *Int. J. Comput. Netw. Commun.* **2013**, *5*, 209–216. [CrossRef]
43. Sermpezis, P.; Kotronis, V.; Dainotti, A.; Dimitropoulos, X. A Survey among Network Operators on BGP Prefix Hijacking. *ACM SIGCOMM Comput. Commun. Rev.* **2018**, *48*, 64–69. [CrossRef]
44. Mohiuddin, I.; Almogren, A.; Alrubaian, M.; Al-Qurishi, M. Analysis of network issues and their impact on Cloud Storage. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019.
45. Tank, D.; Aggarwal, A.; Chaubey, N. Virtualization vulnerabilities, security issues, and solutions: A critical study and comparison. *Int. J. Inf. Technol.* **2019**, 1–16. [CrossRef]
46. Krishna, S.R.; Rani, B.P. Virtualization Security Issues and Mitigations in Cloud Computing. In *Proceedings of the First International Conference on Computational Intelligence and Informatics*; Springer: Singapore, 2017; pp. 117–128.
47. Rakotondravony, N.; Taubmann, B.; Mandarawi, W.; Weishäupl, E.; Xu, P.; Kolosnjaji, B.; Protsenko, M.; De Meer, H.; Reiser, H.P. Classifying malware attacks in IaaS cloud environments. *J. Cloud Comput.* **2017**, *6*, 26. [CrossRef]
48. Saxena, S.; Sanyal, G.; Srivastava, S.; Amin, R. Preventing from Cross-VM Side-Channel Attack Using New Replacement Method. *Wirel. Pers. Commun.* **2017**, *97*, 4827–4854. [CrossRef]
49. Rasheed, H. Data and infrastructure security auditing in cloud computing environments. *Int. J. Inf. Manag.* **2014**, *34*, 364–368. [CrossRef]
50. Singh, A.P.; Pasupuleti, S.K. Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing. *Procedia Comput. Sci.* **2016**, *93*, 751–759. [CrossRef]
51. Shaikh, R.; Sasikumar, M. Data Classification for Achieving Security in Cloud Computing. *Procedia Comput. Sci.* **2015**, *45*, 493–498. [CrossRef]
52. Tawalbeh, L.; Darwazeh, N.S.; Al-Qassas, R.S.; AlDosari, F. A Secure Cloud Computing Model based on Data Classification. *Procedia Comput. Sci.* **2015**, *52*, 1153–1158. [CrossRef]
53. Li, P.; Li, J.; Huang, Z.; Gao, C.-Z.; Chen, W.-B.; Chen, K. Privacy-preserving outsourced classification in cloud computing. *Clust. Comput.* **2017**, *21*, 277–286. [CrossRef]
54. Manogaran, G.; Thota, C.; Kumar, M.V. MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing. *Procedia Comput. Sci.* **2016**, *87*, 128–133. [CrossRef]
55. Sood, S.K. A combined approach to ensure data security in cloud computing. *J. Netw. Comput. Appl.* **2012**, *35*, 1831–1838. [CrossRef]
56. Vurukonda, N.; Rao, B.T. A Study on Data Storage Security Issues in Cloud Computing. *Procedia Comput. Sci.* **2016**, *92*, 128–135. [CrossRef]
57. Zhang, Y.; Chen, X.; Li, J.; Wong, D.S.; Li, H.; You, I. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. *Inf. Sci.* **2017**, *379*, 42–61. [CrossRef]
58. Amalarethinam, I.G.; Leena, H. Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud. In Proceedings of the 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, India, 2–4 February 2017; IEEE: Tiruchirappalli, India, 2017; pp. 172–175.
59. Khan, I.A.; Qazi, R. Data Security in Cloud Computing Using Elliptic Curve Cryptography. *Int. J. Comput. Commun. Netw.* **2019**, *1*, 46–52.

60. Sajay, K.R.; Babu, S.S.; Vijayalakshmi, Y. Enhancing the security of cloud data using hybrid encryption algorithm. *J. Ambient. Intell. Hum. Comput.* **2019**, 1–10. [CrossRef]
61. Belguith, S.; Jemai, A.; Attia, R. Enhancing data security in cloud computing using a lightweight cryptographic algorithm. In Proceedings of the Eleventh International Conference on Autonomic and Autonomous Systems, Rome, Italy, 24–29 May 2015.
62. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Rajarajan, M. Scale Inside-Out: Rapid Mitigation of Cloud DDoS Attacks. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 959–973. [CrossRef]
63. Ficco, M.; Rak, M. Economic denial of sustainability mitigation in cloud computing. In *Organizational Innovation and Change*; Springer International Publishing: Cham, Switzerland, 2016; pp. 229–238.
64. Nautiyal, S.; Wadhwa, S. A Comparative Approach to Mitigate Economic Denial of Sustainability (EDoS) in a Cloud Environment. In Proceedings of the 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019.
65. Rehman, F.; Akram, S.; Shah, M.A. The framework for efficient passphrase-based multifactor authentication in cloud computing. In Proceedings of the 2016 22nd International Conference on Automation and Computing (ICAC), Colchester, UK, 7–8 September 2016.
66. Ojha, S.; Rajput, V. AES and MD5 based secure authentication in cloud computing. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017.
67. Rajeswari, P.; Raju, S.V.; Ashour, A.S.; Dey, N. Multi-fingerprint unimodel-based biometric authentication supporting cloud computing. In *Intelligent Techniques in Signal Processing for Multimedia Security*; Springer: Cham, Switzerland, 2017; pp. 469–485.
68. Devipriya, K.; Lingamgunta, S. Multi Factor Two-way Hash-Based Authentication in Cloud Computing. *Int. J. Cloud Appl. Comput.* **2020**, *10*, 56–76. [CrossRef]
69. Deebak, B.; Al-Turjman, F.; Mostarda, L. Seamless secure anonymous authentication for cloud-based mobile edge computing. *Comput. Electr. Eng.* **2020**, *87*, 106782. [CrossRef]
70. Irshad, A.; Chaudhry, S.A.; Alomari, O.A.; Yahya, K.; Kumar, N. A Novel Pairing-Free Lightweight Authentication Protocol for Mobile Cloud Computing Framework. *IEEE Syst. J.* **2021**, *15*, 3664–3672. [CrossRef]
71. Zhang, Y.; Krishnan, R.; Sandhu, R. Secure Information and Resource Sharing in Cloud Infrastructure as a Service. In Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, Scottsdale, AZ, USA, 3 November 2014; pp. 81–90.
72. Banyal, R.K.; Jain, V.K.; Jain, P. Dynamic Trust Based Access Control Framework for Securing Multi-Cloud Environment. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies—ICTCS '14, Udaipur, India, 14–16 November 2014.
73. Zhou, C.; Li, B. iHAC: A Hybrid Access Control Framework for IaaS Clouds. In Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, London, UK, 8–11 December 2014.
74. Auxilia, M.; Raja, K. Dynamic Access Control Model for Cloud Computing. In Proceedings of the 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, 17–19 December 2014.
75. Yang, C.; Tan, L.; Shi, N.; Xu, B.; Cao, Y.; Yu, K. AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. *IEEE Access* **2020**, *8*, 70604–70615. [CrossRef]
76. Bendiab, K.; Kolokotronis, N.; Shiaeles, S.; Boucherkha, S. WiP: A novel blockchain-based trust model for cloud identity management. In Proceedings of the 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Athens, Greece, 12–15 August 2018.
77. Bendiab, G.; Shiaeles, S.; Boucherkha, S.; Ghita, B. FCMDT: A novel fuzzy cognitive maps dynamic trust model for cloud federated identity management. *Comput. Secur.* **2019**, *86*, 270–290. [CrossRef]
78. Sharma, D.H.; Dhote, C.; Potey, M. Identity and Access Management as Security-as-a-Service from Clouds. *Procedia Comput. Sci.* **2016**, *79*, 170–174. [CrossRef]
79. Khajehei, K. Preserving Privacy in Cloud Identity Management Systems Using DCM (Dual Certificate Management). *Int. J. Wirel. Microw. Technol.* **2018**, *8*, 54–65. [CrossRef]
80. Hassan, Z.; Odarchenko, R.; Gnatyuk, S.; Zaman, A.; Shah, M. Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems. In Proceedings of the 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), Kyiv, Ukraine, 16–18 October 2018.
81. Badve, O.P.; Gupta, B.; Yamaguchi, S.; Gou, Z. DDoS detection and filtering technique in cloud environment using GARCH model. In Proceedings of the 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 27–30 October 2015.
82. Jouini, M.; Rabai, L.B.A. A. A security framework for secure cloud computing environments. In *Cloud Security: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2019; pp. 249–263. [CrossRef]
83. Rajendran, B.; Shetty, P. Domain Name System (DNS) Security: Attacks Identification and Protection Methods. In Proceedings of the International Conference on Security and Management (SAM), Las Vegas, NV, USA, 30 July–2 August 2018.
84. Liang, K.; Zhao, L.; Chu, X.; Chen, H.-H. An Integrated Architecture for Software Defined and Virtualized Radio Access Networks with Fog Computing. *IEEE Netw.* **2017**, *31*, 80–87. [CrossRef]
85. Maithili, K.; Vinothkumar, V.; Latha, P. Analyzing the Security Mechanisms to Prevent Unauthorized Access in Cloud and Network Security. *J. Comput. Nanosci.* **2018**, *15*, 2059–2063. [CrossRef]

86. Zimba, A.; Chen, H.; Wang, Z. Bayesian network based weighted APT attack paths modeling in cloud computing. *Future Gener. Comput. Syst.* **2019**, *96*, 525–537. [CrossRef]
87. Patil, R.; Dudeja, H.; Modi, C. Designing an efficient security framework for detecting intrusions in virtual network of cloud computing. *Comput. Secur.* **2019**, *85*, 402–422. [CrossRef]
88. Velliangiri, S.; Karthikeyan, P.; Kumar, V.V. Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *J. Exp. Artif. Intell.* **2021**, 1–20. [CrossRef]
89. Dildar, M.S.; Khan, N.; Bin Abdullah, J.; Khan, A.S. Effective way to defend the hypervisor attacks in cloud computing. In Proceedings of the 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 26–27 March 2017.
90. Deshpande, P.; Sharma, S.C.; Peddoju, S.K.; Junaid, S. HIDS: A host based intrusion detection system for cloud computing environment. *Int. J. Syst. Assur. Eng. Manag.* **2018**, *9*, 567–576. [CrossRef]
91. Jaber, A.N.; Zolkipli, M.F.; Shakir, H.A.; Jassim, M.R. Host based intrusion detection and prevention model against DDoS attack in cloud computing. In Proceedings of the International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Barcelona, Spain, 8–10 November 2017.
92. Ramamoorthy, S.; Rajalakshmi, S. A Preventive Method for Host Level Security in Cloud Infrastructure. In *Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC–16′)*; Springer: Cham, Switzerland, 2016; pp. 3–12.
93. Kumara, A.; Jaidhar, C. Hypervisor and virtual machine dependent Intrusion Detection and Prevention System for virtualized cloud environment. In Proceedings of the 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), Kuala Lumpur, Malaysia, 26–28 May 2015.
94. Bazm, M.-M.; Lacoste, M.; Südholt, M.; Menaud, J.-M. Isolation in cloud computing infrastructures: New security challenges. *Ann. Telecommun.* **2019**, *74*, 197–209. [CrossRef]
95. Deshpande, S.M.; Ainapure, B. An Intelligent Virtual Machine Monitoring System Using KVM for Reliable And Secure Environment in Cloud. In Proceedings of the 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), Pune, India, 2–3 December 2016.
96. Gomez-Rodriguez, M.A.; Sosa-Sosa, V.J.; Gonzalez-Compean, J.L. Assessment of Private Cloud Infrastructure Monitoring Tools. In Proceedings of the 6th International Conference on Data Science, Technology and Applications, Madrid, Spain, 26–28 July 2017.
97. Mahajan, V.; Peddoju, S.K. Deployment of Intrusion Detection System in Cloud: A Performance-Based Study. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, 1–4 August 2017. [CrossRef]
98. Aldribi, A.; Traoré, I.; Moa, B.; Nwamuo, O. Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. *Comput. Secur.* **2020**, *88*, 101646. [CrossRef]
99. Fernández-Cerero, D.; Jakóbik, A.K.; Grzonka, D.; Kołodziej, J.; Fernández-Montes, A. Security supportive energy-aware scheduling and energy policies for cloud environments. *J. Parallel Distrib. Comput.* **2018**, *119*, 191–202. [CrossRef]
100. Singh, P.; Khan, B.; Vidyarthi, A.; Alhelou, H.H.; Siano, P. Energy-Aware Online Non-Clairvoyant Scheduling Using Speed Scaling with Arbitrary Power Function. *Appl. Sci.* **2019**, *9*, 1467. [CrossRef]
101. Khorsand, R.; Ramezanpour, M. An energy-efficient task-scheduling algorithm based on a multi-criteria decision-making method in cloud computing. *Int. J. Commun. Syst.* **2020**, *33*, e4379. [CrossRef]
102. Fernández-Cerero, D.; Fernández-Montes, A.; Jakóbik, A.; Kołodziej, J.; Toro, M. SCORE: Simulator for cloud optimization of resources and energy consumption. *Simul. Model. Pract. Theory* **2018**, *82*, 160–173. [CrossRef]
103. Aissaoui, K.; Idar, H.A.; Belhadaoui, H.; Rifi, M. Survey on data remanence in Cloud Computing environment. In Proceedings of the 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Fez, Morocco, 19–20 April 2017.