symmetry

MDPI

Article

Cyberattacks and Security of Cloud Computing: A Complete Guideline

Muhammad Dawood [1], Shanshan Tu [1], Chuangbai Xiao [1], Hisham Alasmary [2], Muhammad Waqas [3,4,*] and Sadaqat Ur Rehman [5]

[1] Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China; mdaudkhan777@yahoo.com (M.D.); sstu@bjut.edu.cn (S.T.); cbxiao@bjut.edu.cn (C.X.)
[2] Department of Computer Science, King Khalid University, Abha 61421, Saudi Arabia; alasmary@kku.edu.sa
[3] School of Computing and Mathematical Science, Faculty of Engineering and Science, University of Greenwich, London SE10 9LS, UK
[4] School of Engineering, Edith Cowan University, Perth, WA 6027, Australia
[5] School of Computer Science and Engineering, University of Salford, Manchester M5 4BR, UK; s.rehman15@salford.ac.uk
* Correspondence: engr.waqas2079@gmail.com

Abstract: Cloud computing is an innovative technique that offers shared resources for stock cache and server management. Cloud computing saves time and monitoring costs for any organization and turns technological solutions for large-scale systems into server-to-service frameworks. However, just like any other technology, cloud computing opens up many forms of security threats and problems. In this work, we focus on discussing different cloud models and cloud services, respectively. Next, we discuss the security trends in the cloud models. Taking these security trends into account, we move to security problems, including data breaches, data confidentiality, data access controllability, authentication, inadequate diligence, phishing, key exposure, auditing, privacy preservability, and cloud-assisted IoT applications. We then propose security attacks and countermeasures specifically for the different cloud models based on the security trends and problems. In the end, we pinpoint some of the futuristic directions and implications relevant to the security of cloud models. The future directions will help researchers in academia and industry work toward cloud computing security.

Keywords: cloud computing; security threats; security attacks

Citation: Dawood, M.; Tu, S.; Xiao, C.; Alasmary, H.; Waqas, M.; Rehman, S.U. Cyberattacks and Security of Cloud Computing: A Complete Guidelines. *Symmetry* **2023**, *15*, 1981. https://doi.org/10.3390/sym15111981

Academic Editor: Alexander Zaslavski

Received: 13 September 2023
Revised: 30 September 2023
Accepted: 20 October 2023
Published: 26 October 2023

1. Introduction

Cloud computing offers several benefits, including cost reduction, sharing and configuring computing resources, on-demand service, and high flexibility and scalability [1,2]. In addition, cloud computing provides services on the internet that have become widely used technology. The cloud computing model evolved from virtualization technology, distributed computing, utility computing, and other computer technologies to provide availability and scalability features for large enterprise-level applications. It also offers services to virtual machines assigned through a sizable physical resource pool. The five vital features of cloud computing include on-demand self-service, extensive access to the network, resource pooling, high-speed resiliency, and measurable services [3]. These benefits encourage large companies to dump their IT infrastructure into the cloud environment. For reliable services, cloud computing needs to be secured for users' data. Cloud computing faces several typical cloud risks, such as data abuse, malicious insider, insecure interfaces, access points, shared technological problems, loss of data, and hijacking. Therefore, an accurate understanding of cloud security is a fundamental requirement for the successful deployment of cloud computing [4].

Different types of attacks make it difficult for cloud providers and administrators to deploy possible solutions needed by customers [5]. This is because various attacks are

associated with different threats, where the importance of risks varies depending on the security needs of other customers using cloud services. Thus, security administrators will evaluate and implement security mechanisms to meet essential security requirements as service providers. However, the security can be further improved as it is almost impossible to configure a fully secure system in practice [6]. Consequently, it is necessary to find security threats followed by their associated solutions, such as accountability, authentication, and privacy preservation [5,7,8].

This work discusses security problems and issues caused by the unique characteristics of the cloud. Thus, we offer a complete sketch of the diverse issues and proposed solutions to prevent potential attacks. We studied various strategies and mechanisms to explain the security management methods, thereby reducing risks and vulnerabilities and enhancing people's confidence in cloud services. We also provide a complete analysis of security issues, classified security challenges, and countermeasures to address the issues.

2. Threat Reasons in Cloud Computing

Cloud security protects information, software, and resources involved with cloud computing. Many security aspects of cloud environments (public, private, or hybrid) are the same for any organization. Cloud security is a broad arrangement of developments and controls to ensure information and the basis of cloud computing [9]. Many business and research associations are uncomfortable with fully believing in cloud computing to secure their data. Security threats affect both traditional IT and cloud systems. Like any computing environment, cloud security involves adequate protection. Hence, the data and network are safe and can immediately determine if there is anything unusual, and unexpected events can be tracked [10].

Cloud security must reach the mark and be updated at the right time so that no intruder gets any access or causes interruptions [11]. To overcome cloud issues and challenges, cloud providers must take rigorous steps to protect their data and resources by providing reliable and secure services. Cloud providers need to apply segmentation and separation concepts to multitenant architectures. The first thing for building a robust model in the cloud environment is to check the risk related to outsourced data. To achieve this, the data must be sorted by the risks aligned with the data. The security model will then act and prioritize essential data in the organization. Therefore, it is necessary to identify the risks, because they can be used for numerous applications, such as enterprise, services, implementation, social networks, and business tools [12,13]. We investigate the security issues that will simplify cloud-specific attacks' understanding, scaling, and evaluation. We examine some fundamental research on the confrontation of security explications to secure cloud computing. These security explications need to provide hands-on solutions in securing data. Furthermore, some novel security trends are needed in relation to cloud computing.

2.1. Cloud Computing Fundamentals

Cloud computing represents a transformative approach to delivering computing services and resources to end-users over the internet. It is a paradigm shift in how IT infrastructure is managed and utilized. In this model, various hardware and software components collaborate seamlessly to provide a wide array of services. The essence of cloud computing lies in the on-demand accessibility of computing resources, including data storage and processing power, obviating the need for users to manage their dedicated infrastructure. The core concept of cloud computing is the on-demand availability of computing resources. This means that users can access the computing power and data storage they need without the burden of managing their dedicated infrastructure. The benefits of cloud computing are numerous and include cost-efficiency, scalability, improved speed and efficiency, enhanced performance, and robust security measures [3,14]. Cloud computing can be implemented in different settings, such as public, private, or hybrid models. Public cloud providers offer services over the internet to a broad range of clients, while private cloud firms limit their offerings to specific clients or organizations. Hybrid

models combine elements of both public and private cloud deployments. Cloud computing is a versatile approach for distributing valuable information through the internet, and it is typically categorized into three primary service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

2.2. Cloud Security: Safeguarding Data and Resources

In the world of cloud computing, keeping data and resources safe is a top priority. Cloud security is like a shield that protects all the important stuff in the cloud, whether it is data, software, or the technology behind it all. This is crucial, because security concerns are similar whether you are using a public, private, or hybrid cloud system. Organizations, both in the business and research sectors, sometimes hesitate to fully embrace cloud computing for data security reasons. Security threats pose risks to both traditional IT systems and cloud-based systems alike. Therefore, cloud security is essential to ensure adequate protection for data and networks, with the ability to promptly detect and respond to any unexpected or unusual events. Effective cloud security measures must constantly evolve to stay ahead of potential intruders. Timely updates and proactive measures are crucial to preventing unauthorized access or interruptions. To address the challenges and concerns associated with cloud security, cloud providers must implement rigorous measures to protect their data and resources while delivering reliable and secure services. One approach involves the application of segmentation and separation concepts within multitenant cloud architectures. An essential step in building a robust security model within a cloud environment is to assess the risks associated with outsourced data. Data should be categorized based on the level of risk it poses, and a security model should prioritize the protection of critical data within the organization Identifying and understanding these risks is paramount, as they can have broad applications across various domains, including enterprise, service implementation, social networks, and business tools. This understanding of risks serves as a foundation for developing practical security solutions tailored to the unique challenges posed by cloud computing Furthermore, as we delve deeper into this literature review, we will explore specific security issues that simplify our understanding of cloud-specific attacks, scaling security measures, and evaluating their effectiveness. We will also examine ongoing research efforts aimed at enhancing security solutions for cloud computing, as well as emerging security trends relevant to this dynamic and ever-evolving field

2.3. Recent Studies in Cloud Security

Kushala and Shaylaja [15] conducted a survey focused on the contemporary security challenges within MultiCloud Computing (MCC). They address the transition from local to cloud computing, which has brought about security challenges for both clients and service providers. The primary objective of their paper is to provide insights into the core characteristics of Cloud Computing (CC) and MultiCloud Computing (MCC). Additionally, they delve into the security issues associated with these models and propose potential solutions. The researchers specifically address the types of security risks, the security mechanisms employed, and the various cloud deployment models relevant to each risk.

Mondal et al. [16] conducted a comprehensive review of cloud computing security challenges. Their study sheds light on critical concerns in securing cloud computing environments, including trust, authenticity, confidentiality, encryption, key management, multitenancy, data splitting, and virtual machine security. They also proposed potential solutions to mitigate these challenges. Notably, the study emphasized the importance of addressing resource-sharing issues in cloud environments, suggesting this as a priority for future research in the field of cloud security.

Subashini et al. [17] conducted a survey examining security concerns within various service delivery models of cloud computing. They explore issues related to data privacy, data integrity, authentication, authorization, and access control. The authors also examine the risks associated with multitenancy, virtualization, and the potential for unauthorized

data exposure. Additionally, the paper addresses security concerns arising from the geographical distribution of cloud data centers. They also noted the advantages of cloud computing, including swift deployment, pay-as-you-go pricing, cost reduction, flexibility, rapid provisioning, enhanced scalability, improved stability, and hypervisor protection against network-based attacks.

Grusho A et al. [18] discussed various artificial intelligence methods and technologies aimed at enhancing the protection of cloud computing systems. In particular, their research examined the significant security threats within cloud computing environments, which often involve the abusive and malicious utilization of cloud services. The paper highlighted the use of Intrusion Detection Systems (IDPs) as a valuable tool in identifying security policy issues, recording existing threats, and preventing data exchange participants from violating security policies.

In their paper, Liu et al. [19] conduct an extensive survey focusing on the security and privacy challenges within the realm of cloud computing. They also explore potential solutions and outline future research directions in this field. The authors underscore that the adoption of cloud computing has introduced a host of security challenges. These challenges pertain to safeguarding data, applications, and services hosted within cloud environments. Security risks may involve unauthorized access, data breaches, loss of control over data, and compliance with regulatory requirements.

Syed et al. [20] conducted a review focused on cloud storage security risks, practices, and measures. The primary objective of their paper was to examine security concerns and present contemporary implementations aimed at addressing them. The authors identify several security risks associated with cloud storage, including challenges related to data visibility, unprotected storage locations, data breaches, and vulnerabilities in application programming interfaces (APIs). These risks have the potential to lead to significant financial losses and data exposure for individuals and organizations. It offers practical guidance on mitigating risks and implementing effective security measures, making it a valuable resource for organizations and individuals looking to enhance their cloud storage security practices.

Kumari et al. [21] conducted a comprehensive review focusing on security issues and challenges in cloud computing. The study highlighted the increased risk of data breaches in cloud computing systems, attributed to emerging technologies like the Internet of Things (IoT), big data, and smart cities. The study explores privacy and security concerns related to data protection and proposes countermeasures. Furthermore, it emphasizes the importance of future research efforts in developing secure models and addressing fundamental security issues in cloud computing.

Ghaffari et al. [22] conducted a survey that examined cloud security issues using the People, Process, and Technology (PPT) model. The primary aim of the survey was to meticulously identify cybersecurity problems and classify these threats into categories of individuals, processes, and technologies. This categorization was crucial for identifying security solutions that are not only cost-effective but also reliable and feasible. They utilized this approach to systematically categorize the challenges associated with cloud security, offering a structured framework for understanding and addressing security concerns in cloud environments.

Mandal and Khan [23] conducted a study on security threats in cloud computing with a focus on the passive impact of the COVID-19 pandemic. With the global pandemic leading to remote work and online learning, many organizations shifted to cloud computing. However, this rapid adoption without adequate security measures raised significant security concerns. The primary objective of the study was to identify the specific areas contributing to security breaches in cloud environments and to propose general preventive measures. The paper discussed various cyberattacks that posed risks to cloud services and hosts. Additionally, it examined the societal impact of these attacks and discussed potential safeguards. It aimed to raise public awareness about these threats and recommended changes to security policies.

Bhajantri and Mujawar [24] conducted a survey addressing security challenges and issues in cloud computing, along with potential countermeasures. The paper provided a brief overview of security concerns across different levels of cloud computing, including infrastructure, data, and the cloud itself. Additionally, the paper discussed the significance of Identity and Access Control in addressing these security challenges. Furthermore, the paper introduced several countermeasures to mitigate security issues within cloud environments. Notably, it proposed the implementation of a robust access control framework featuring Attribute-based Encryption (ABE) and trust mechanisms. These measures were presented as solutions to enhance security and access control within cloud computing.

Gupta and Kumar [25] conducted a study on security threats in cloud computing. The primary objective of their research was to improve the security issues associated with cloud computing by employing various techniques. Their study encompassed an examination of cloud computing architecture, models, current security threats, and challenges, and it introduced a potential security solution involving two-step fingerprint authentication to mitigate the risks associated with account hijacking in cloud environments.

3. Service Models of Cloud Computing

Cloud computing comprises three primary service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each of these service models caters to the needs of different businesses and offers unique benefits [26].

3.1. Infrastructure as a Service (IaaS)

This service model provides access to fundamental computing resources such as virtual machines, servers, storage, and networking infrastructure. While IaaS offers several advantages, it is not without its challenges. One notable issue is the potential misalignment of security between the cloud infrastructure and the virtual machines hosted within it. This misalignment can lead to security vulnerabilities. For example, both the cloud customer and the cloud provider may have different policies regarding data retention and deletion, which can pose security risks. Additionally, when clients use legacy code to build applications on IaaS platforms, they may inadvertently introduce security vulnerabilities from outdated code.

Security Challenges:

- Securing virtual machine instances and hypervisors.
- Protecting against unauthorized access to IaaS resources.
- Ensuring data security and isolation in a multitenant environment.

3.2. Platform as a Service (PaaS)

PaaS provides software environments for application development and management. The PaaS delivers end-users with software applications. While PaaS streamlines the development process, it also introduces specific security considerations. These include interoperability challenges, potential vulnerabilities in platform components, security-aware authentication and authorization mechanisms, and robust fault tolerance strategies.

Security Challenges:

- Ensuring secure application development and deployment.
- Protecting sensitive data processed by platform services.
- Guarding against vulnerabilities in custom-developed applications.

3.3. Software as a Service (SaaS)

SaaS delivers software applications over the internet, eliminating the need for local installations. Although SaaS offers rapid deployment and accessibility benefits, it raises various security concerns. Authentication and authorization mechanisms, data encryption,

data availability, and network security become paramount in ensuring the security of SaaS applications.

3.3.1. Security Challenges:

- Ensuring data privacy and compliance in shared SaaS environments.
- Protecting against account hijacking and unauthorized access.
- Managing the security of data handled by the SaaS provider.

3.3.2. Cloud Deployment Models

Cloud computing offers various deployment models, including private, public, hybrid, and community clouds. Each deployment approach comes with its unique advantages and challenges [27].

3.3.3. Private Cloud

A private cloud operates exclusively on behalf of a single organization and is not accessible to the general public. This deployment model provides cloud infrastructure dedicated to the private and specific use of the organization or institution. It is utilized solely by members of the same organization, ensuring stringent control and security. Key features of private clouds include reliability, flexibility, data security, and scalability. In a private cloud setup, the organization's network serves as the administrator of the data center, leveraging virtualization and distributed computing to cater to the needs of its members.

3.3.4. Security Challenges:

- Ensuring data privacy and compliance with internal policies and regulations.
- Protecting against insider threats, as access is limited to organizational members.
- Maintaining robust access controls to prevent unauthorized entry.

3.3.5. Public Cloud

The public cloud represents one of the most widely recognized deployment models, offering computing resources and infrastructure over the internet to the general public. Public cloud services are characterized by their large-scale availability and accessibility. These services are typically provided by third-party vendors and can be accessed in two ways: through payment or as free offerings to consumers. In this model, external vendors maintain and manage the physical resources at their data centers. Some well-known public cloud service providers include Amazon EC2, Microsoft Azure, Google App Engine, and Microsoft Azure.

3.3.6. Security Challenges:

- Protecting data in a shared environment with multiple users.
- Ensuring data sovereignty and compliance with regional regulations.
- Guarding against external threats, such as DDoS attacks.

3.3.7. Community Cloud

The community cloud deployment model strikes a balance between public and private clouds. It is designed to serve a group of institutions, organizations, or partnerships with specific and private needs. Community clouds can be hosted either on-premises or off-premises, and the responsibility for building, managing, and operating them may lie with one or more organizations, a third-party provider, or a collaborative consortium. This model is ideal for situations where multiple entities share common security and compliance requirements.

3.3.8. Security Challenges:

- Balancing the unique security requirements of multiple community members.
- Establishing trust among community members.
- Ensuring data separation and access control.

3.3.9. Hybrid Cloud

The hybrid cloud model combines two or more clouds, which may consist of private, public, or community clouds. It maintains a cohesive structure while capitalizing on the strengths of individual cloud types. Hybrid clouds are characterized by their ability to facilitate the seamless movement of data and applications between different cloud environments. This flexibility and adaptability make hybrid clouds an attractive choice for organizations seeking to optimize their cloud resources [28].

3.3.10. Security Challenges:

- Ensuring seamless data and application portability between diverse cloud environments
- Coordinating security measures across different clouds.
- Managing the complexity of multiple security domains.

3.4. Virtualization Issues

Virtualization is a technology that runs multiple virtual machines (VMs) through one physical device, and all these VMs use the hardware of one machine. Virtualization creates a virtual version of the operating system, server, network resources, and storage device. VMs turn the operating systems and storage into virtual platforms that provide multiple machines using only single physical resources to several cloud computing users. Traditional security strategies may not work for virtualization systems, particularly when two VMs share the same physical host [29]. A different customer can use a single physical host in the cloud platform, which increases the importance of isolation. In this case, data must be protected against attacks by another guest in the same physical machine. For instance, a Denial of Service (DoS) attack against a physical host initiated by a VM should be diminished, or it can affect the entire VM in the server. In addition, some of the new forms of malware that target virtualization cannot be stopped by traditional methods such as antivirus software [30].

3.5. Hypervisor

In order to provide controlled access to physical resources, the hypervisor is the software component placed between the host and visitors. For a nonprivileged user entering the guest, this layer should be invisible. However, it cannot be completely hidden. As a result, an attacker can use hypervisor weaknesses to access both the host system and guests.

3.6. Migration and Pivoting

For load balancing or disaster recovery, virtual machines can be transferred among different hosts. Copying the VM image over the network is used to carry out this migration. If the connection is not encrypted, a hacker might be able to eavesdrop on data and execute a man-in-the-middle attack.

Different services hosted by a VM usually allow users to log in. Once the user gains access, the intruder has the option to damage the physical system and exit the virtual machine. The authors of [31] examined inter-VM communication based on Xen for both local and remote environments to create scenario-based hypotheses to identify different communication sequences. The authors' findings suggest that trigger scenarios can be used to extract VM communication sequences. The performance aspect of virtual machines (VMs) shows more consideration than the potential security risks associated with VM connectivity.

In addition, the authors of [32] present a unique method for examining how quickly malware spreads in virtualized cloud systems. To quantify the effects of antimalware software on malware propagation in virtualized environments, the paper proposed the

Susceptible–Protected–Infected (SPI) cloud malware attack model. The suggested model was also analyzed. In order to assess control measures for malware propagation, the authors also analyze the proposed model using the stability theory of differential equations and epidemic modeling. Furthermore, Sharifi et al. [33]. provide a novel architecture called Alamut for reshaping any normal network intrusion detection system (NIDS) to perform in a virtual execution environment based on Xen. The proposed design places basic security implementations for common NIDS security issues, including signature matching; however, security policies and administration modules are preserved in that domain's user space. By separating methods from policies, it is possible to verify network packets directly at the kernel level more effectively without having to use time-consuming contexts.

One of the main issues is that any system can tolerate fault and run properly without any fault leading to system failure. The virtualization and fault tolerance (VFT) technique is proposed, which helps reduce the service time and increase the system's overall availability. Decision-maker and cloud manager modules manage the virtualization process, which caters to load balancing and handling faults. Redundancy and checkpointing are also used to achieve fault tolerance. The proposed scheme differs from the previous one because this fault handler is included in the virtualization module, which can detect and remove temporary software faults and stop unrecoverable faults. The approach in [34] extends the lives of IoT-restricted devices, including new protocols making the development and configuration of IoT innovative applications. An open-source software platform is developed to achieve the goal of utilizing the OpenStack API and leverages a web interface that provides all the functionality typically available in a home gateway through the OpenWRT Linux distribution. Results show that this approach reduces the amount of data transmitted, with benefits in reduced workload, power consumption, and extended device lifetime.

Cloud migration is the process of migrating digital business operations to the cloud. Cloud migration is similar to physical movement. Applications and IT processes are moved from one data center to another, rather than packing and moving physical goods [35,36]. A data security solution and analysis provided for a privacy protection framework during data migration. A secure socket layer (SSL) is installed, and the migration ticket is offered with minimal privileges [37,38]. Prediction-Based Encryption (PBE) is also used for data encryption. The system is used for healthcare and e-commerce systems that can store data on credit card details. An anomaly collaborative detection system called Mixture Localization-based Outliers (MLO) was proposed in [39,40] to discover the outside and inside attacks from cloud systems and their migration process. It uses a Gaussian mixture model for a local external factor function for relevant network data and searching unusual patterns in network traffic data. Several research projects have been carried out on VM migration to reduce energy consumption in data centers, ensuring a high level of service-level agreements (SLAs). However, the service level of the running application can be affected negatively during live VM migration. The author of [41] introduced a new intelligent VM transfer approach called CLANFIC to minimize the number of VM transfers and improve energy consumption, including modified cellular learning automated evolutionary computing (CLA-EC) and neuro-fuzzy [42].

3.7. Scalability and Availability

Scalability means the ability to develop systems and maintain performance. Scalability is the cloud layer's ability to increase software service delivery capacity by expanding the number of software services. A scalable system always supports its effectiveness at a high-level end and increases capacity [43]. In [44], the authors discussed two main topics, i.e., how to provide reliability, safety, and privacy of information and how to deliver scalable and robust cloud behavior under uncertainties and specific constraints, such as budgets, QoS, SLA, energy costs, availability, reliability, safety, and privacy. As more users use cloud technologies to build IT infrastructure, reliability, safety, and privacy become crucial for providers and consumers. Preservation of confidentiality is interpreted as limited

access to information, integrity as the assurance that the data are trustworthy and accurate, and availability as a guarantee of reliable access to the information by authorized people.

The technical metrics of scalability for cloud-based software service address both the quality and scaling of cloud-based software services. The work in [45] focuses on measuring the scalability of cloud-based software services. The proposed technical scalability matrix can be used to design and run cloud-based application services to identify system components that contribute to scalability performance. IoT/M2M/V2V devices connected to the internet are increasing day by day [46,47]. These devices deployed to the cloud are overloaded with significant data traffic. To extend the scalability of IoT/M2M/V2V platforms in the cloud, the authors of [48] proposed utilizing fog computing. Fog provides low latency and also offloads over the congested cloud. The data are migrated to a fog computing architecture to make the whole platform more scalable in the proposed scheme [49].

Availability is essential for many applications, including IoT applications. Services in the cloud system usually have the same availability level, in which fault identification and recovery procedures are unaware of the service features. Existing cloud systems are inefficient in improving availability methods and resources to meet service needs. A high-availability architecture is presented in [50] to address the issue of dynamically customizing the availability method based on service characteristics. Based on OpenStack, the proposed architecture is verified through an implementation system. It achieved the target availability while optimizing resources, unlike existing architectures that use predefined availability methods. The availability model presented in [51] is based on stochastic Petri nets to evaluate two approaches, i.e., hot standby and cold standby. In cold-standby migration, the migration target machine is started just before VM Live migration. The migration target machine operates with the source transfer machine in hot-standby migration. Results show that VM Live migration dramatically improved system availability.

3.7.1. Data Integrity

Integrity is also one of the severe problems in cloud computing. Integrity means that data can be accessed only by those authorized and ensures that data have not been changed. It is also called the process of verifying data. During resource sharing, there is the possibility that data can be misused. Message authentication code and digital signatures are commonly used techniques to provide data integrity [52]. A data-sharing scheme in [53] is proposed for a dynamic user group to achieve user ID tracking and add/delete dynamic group users, called the rights distribution center (RDC). However, it is impossible to determine a specific user when performing the third-party audit to verify data integrity to protect user identity privacy. The integrity audit model defined for shared cloud data is also discussed in [52]. In this scheme, by using blindness technology, the user sends data tags to RDC. Most existing techniques ignore data integrity issues. However, in one recent work, Identity-based Remote Data Integrity Checking (RDIC) is proposed [54] that uses homomorphic variable tags to reduce system complexity.

When we deal with more critical data than usual, they are defined as large and complex data that are too complex to be handled by standard computers, and more space and processing power are required to deal with them. Cloud computing is used to manage big data, which provides space and solves big data problems [55]. For instance, the authors of [56] explained the big data concept and proposed analytical tools, like data science and machine learning, that help in the financial area. The area involves a deeper understanding of ways to reach customers' banking experience. The authors believe that a more accepted attitude toward innovative technologies can pave the way for more applications in the field. Also, the authors of [57] described the design and improvement of the IoT extensive data cloud system for the Industrial Internet of Things (IIoT) analysis, as well as prediction and maintenance [58]. Hence, the authors of [59] proposed a system for cloud computing integrated with IoT as the base case for big data. Hence, a security wall between the internet and cloud server in the proposed solution eliminates security and privacy issues. Despite the security, the data privacy issue is another of the most important issue in cloud

computing, where users' secret data can be stolen due to various software vulnerabilities and hardware attacks. An efficient and secure big data archiving system in cloud computing is proposed in [60]. The authors proposed a leak-resistant encryption scheme that serves as the main ingredient. The proposed method could guarantee user privacy, even if a partial key is leaked in cloud computing.

3.7.2. Cloud Broker

A cloud broker reduces cloud user costs and plays an agent role between cloud users and providers. It offers reserved VM at a lower price to the cloud user. In this regard, the authors of [61] focused on cloud broker configuration and managing VM price to obtain more worth and save user costs. Cloud broker profits are influenced by many factors, including VM purchase, user demand, and sale prices. The authors presented a compositional analysis of all the influencing factors, identifying the optimum configuration of multiple servers and the VM pricing issue, which has been modeled as the problem of profit maximization. However, several cloud service providers participate in providing different services and in the effectiveness of service specifications and defining services. Therefore, the authors of [62] proposed a broker-based cloud computing framework to enable cloud users to specify their service requirements.

Recent attempts have tried to identify the security level of the cloud service with the help of the security SLA. However, security SLAs in their current format are not fully measurable and are challenging to monitor. The quantization and standardization of security SLAs will attract and accelerate the cloud adoption process; customers will gain confidence and benefit from the advantages of cloud computing safety. Hence, the broker-based framework that manages cloud security SLA is proposed in [63]. The author developed a standard, quantitative and measurable form of representation. A selection model is proposed based on computing the adequate trade-off among confidentiality, integrity, and availability in a multiobjective optimization problem.

4. Security Problems

According to a cloud security threat report in 2019 [64], novel cross-cloud attacks are increasing rapidly. In [64], malware attacks are ranked second after data breaches in security threats [65]. The cloud service model provides users with different services and reveals information, which increases cloud computing systems' security issues and risks. In cloud computing, data loss is a fundamental security problem. Hackers from external and internal employees can access the data unintentionally or intentionally. External hackers may use hacking techniques (i.e., hijacking and eavesdropping) to access databases in such environments. Viruses and Trojan horses are also added to a cloud services designed to inflict harm. Therefore, it is necessary to identify possible cloud threats to implement a system with better security mechanisms. The above discussion is summarized in Table 1 to suggest some security problems with their descriptions. Typical attacks are also summarized as Table 2.

Table 1. Security problems.

Category	Description
Auditing	Review and investigating cloud infrastructure
Data confidentiality	Data that are not provided to unauthorized users
Data access controllability	Restrict access to data outsourced to the cloud.
Privacy preservability	Users hide their identity and protect their actions in data and information retrieved from the cloud
Data accountability	Users ensure that others do not unknowingly misuse their data
Network	Involves network attacks such as network availability Denial of Service (DOS)
Access control	Privacy of user information and data storage

Table 2. Security threats and countermeasures.

Area	Threats	Problems	Affected Cloud Services	Solutions
Infrastructure Threats	Data breaches	Unauthorized access or retrieval of data, application, or service	IaaS, SaaS, and PaaS	Encryption of data, proofs of storage, server-aided secure computation
	Cloud service abuse	loss of validation service fraud and more vigorous attacks due to unidentified login	PaaS and IaaS	monitor network status and provide robust registration and authentication
	Hijacking	Illegal control of certain authorized services by unauthorized users. Stolen user account credentials	IaaS, SaaS, and PaaS	Adopt a robust authentication mechanism, security policies, and a secure communication channel
Service threats	Service delivery	loss of control of cloud infrastructure	IaaS, SaaS and PaaS	Offer services that monitor and control cloud infrastructure
	Insecure interface	Improper authorization and incorrect authentication transmission of content	IaaS, SaaS, and PaaS	Transmission of data is encrypted, and there are authentication mechanisms
Platform threats	Malicious insiders	Infiltration of organizational resources, destruction of asset productivity losses, and impact on operations	IaaS, SaaS, and PaaS	Security and management processes that use protocol reports and breach notifications
	Identity theft	An attacker could gain the identity of a valid user to access the usage resources	IaaS, SaaS, and PaaS	Use strong multilayer passwords and authentication mechanisms

4.1. Data Breaches

Data breaches occur when sensitive information is disclosed to an unauthorized party. Various reasons may cause data breaches in cloud environments. In cloud computing, attackers specifically target the provider because of the large amount of stored data in a cloud server. Hence, the damage often surmises the sensitivity of the exposed data. Cloud service providers ensure the protection of customer data. There have been plenty of data breaches in cloud computing history that troubled some reputed companies. Before transferring information to the cloud server, the customer may encrypt their data, and the customer must be careful to protect the encryption key. The data might be lost if the key is lost. However, multiple compliance policies specify how long an organization must keep records of data [66].

4.2. Data Confidentiality

In data confidentiality, the data must not be revealed to unauthorized users. Data processing is maintained in the cloud and managed directly by the administrator [67]. Sensitive data can only access by authorized users, and no other person, including a cloud service provider, should have access to any information about a users' data. Cloud storage services, such as data processing, data computing, and data sharing, take advantage of data owners without revealing data content to a cloud service provider or adversaries [68].

4.3. Data Access Controllability

Access control means restricting the data transferred to the cloud by the data owner. The owner can only authorize legitimate users to access their data, while others can access the data without permission. However, owners can only control access authorization in untrusted cloud environments.

4.4. Authentication

The process of verifying the identity of the user is authentication. An authentication method is required for cloud users supported by the cloud service provider. Cloud service providers offer different authentication techniques depending on integrity and reliability [69,70]. Cloud users need the user authentication process through the cloud service providers [71]. Cloud service providers can choose to provide different authentication mechanisms with diverse security mechanisms at different levels, and the power depends on the reliability and integrity of the mechanism. Besides, authentication procedures must work properly by maintaining data privacy and confidentiality [69].

4.5. Inadequate Diligence

Organizations fully aware of the cloud computing environment and accepting of the cloud computing risks may experience significant business, financial, technical, legal, and compliance risks. For example, an organization that fails to check contracts might be unaware of the provider's responsibilities in the violation or loss of data [69]. In addition, if an organization's development team is unfamiliar with cloud technology, it will have operational and architecture issues because it is deployed to a specific cloud [72]. Finally, due to the risks associated with cloud computing, organizations should conduct adequate research before migrating to cloud computing.

4.6. Phishing

Phishing is accessing personal information from an individual user using the concept of social engineering. This usually happens by putting links to a webpage via email or instant message. These links seem to be correct, but when the internet site is visited, data may be compromised, like account number logins or bank card confirmation and authentication details. The the user us taken to the wrong position [73]. Attackers can quickly access login credentials and credit card information via this scam. Phishing attacks might be divided into two classes, i.e., cloud service abuse and service hijacking.

4.7. Key Exposure

Key exposure is an essential issue in cloud computing which has recently been considered. The key exposure problem is itself unusual in nature. Once the customer's database verification key is released to the cloud to preserve its integrity, the cloud can quickly conceal data breach events and even delete restricted access to client information to conserve storage space. The malicious attacker acquires the client's cloud storage audit key and can hide data loss events by falsifying fake data authenticators [74]. For the same reason, they can even discard the data that clients access to save storage space without being discovered by cloud storage [75]. It can be challenging to find the key direction, because the attacker can immediately stop the intrusion if it attains the client's secret keys. The key exposure may only be recognized if the user determines that they have not generated valid authenticators. The user has to remove the existing public and secret keys and create a new pair of keys [76,77].

4.8. Auditing

An audit reviews and investigates any business aspect and necessary function application. It deals with different models in cloud computing, such as public, private, or hybrid. Because of its complexity, cloud auditing is of far-reaching importance in the cloud environment. This means that the infrastructure must be audited. The audit's primary purpose is to determine whether the administration and management of the organization's information systems meet a series of criteria and requirements provided by an external standard authority [78]. The system framework of auditing consists of cloud users, cloud service providers, and third-party auditors. Audit management pays attention to the specific values of propositions. The future principles and advantages of embracing cloud computing are solutions to any requirement and budget, maximum versatility, efficient use of energy,

excellent performance and agility, openness to emerging technologies, and security. In the broader context of cloud security, the importance of cloud auditing is reflected in the following key aspects.

4.8.1. Quality Assessment and Trust Building

Cloud audits provide customers with valuable quality assessments, helping them decide whether to trust network operators' assurances regarding internal processes. It also assesses the effectiveness of cloud infrastructure service providers' internal monitoring and compliance, which is critical to stakeholders.

4.8.2. Identify Organizational Weaknesses

In addition to technical assessments, cloud audits also reveal organizational management weaknesses in the customer structure and their interactions with cloud services. This comprehensive perspective addresses not only technical aspects but also management and program security aspects.

4.8.3. Audit Report

Upon completion of an audit, the auditor prepares a comprehensive report documenting all identified items. The report usually consists of three parts: the audit purpose, audit protocol, and related common findings. The objective portion of the report meets independent audit standards to ensure compliance with cloud computing best practices and security standards. The cloud computing audits include the following main objectives:

- Provide a quality evaluation to audit customers and their willingness to trust the assurances of the network operator on internal processes.
- Evaluate the effectiveness of internal monitoring and compliance of the cloud infrastructure service provider for stakeholders.
- Describe organizational management weaknesses in the organization of the client and the interface to services.
- The audit report shall be drawn up by the auditors, in which all the identified items must be registered. Three sections need to be completed, including the purpose, the audit protocol, and the related common findings. The objective portion of the applicable specification carries out the independent audit standard requirements to be audited for conformity with cloud computing.

4.9. Privacy Preservability

Users must be aware of their privacy when accessing cloud data or services. Users typically want to hide their identities when using cloud data services. In addition, the users want to protect the retrieved data for their actions. For example, keywords for query results for outsourced data and cloud returns should not be made public. Furthermore, no other party in the cloud should infer the user's access behavior or habits [79].

4.10. Security Threats to Hosted Virtual Machines

Here are the main identified threats affecting hosted virtual machines (VMs), focusing on areas such as software vulnerabilities, data breaches, and unauthorized access to VM instances

1. Software vulnerabilities: Hosted VMs can be vulnerable to software exploits, including application vulnerabilities, operating system vulnerabilities, and unpatched software. Attackers may target these vulnerabilities to gain unauthorized access or disrupt VM functionality.
2. Data breaches: Data stored within VMs are at risk of being breached if proper security measures are not in place. Unauthorized access to VMs can lead to the theft or exposure of sensitive data, compromising confidentiality and compliance requirements.

3. Unauthorized access: Attackers may attempt to gain unauthorized access to VM instances. Once inside, they can potentially compromise the integrity of the VM, disrupt its operations, or use it as a launching point for further attacks within the network.

These threats underscore the importance of robust security measures and ongoing monitoring to protect hosted VMs from potential risks.

5. Attacks in Cloud Computing

This section outlines security threats and potential countermeasures for various cloud-assisted applications.

5.1. Denial of Service (DoS) Attacks

A Denial of Service (DoS) is the most severe attack because of its significant network impact. The main objective of these attacks is to limit users' legal use of network services and resources. Additionally, distributed Denial of Service (DDoS) utilizes multiple mechanisms to initiate a DoS attack on a single victim to make it more challenging to locate the specific attackers [80].

5.2. Jamming Attack

This attack is primarily directed at wireless networks. It blocks communication channels by sending undesirable data or noise signals, damaging the original message's content or preventing it from reaching the target [79]. These attacks can be detected or controlled by various methods and encryption and authentication techniques. Defaults in the prevention process include developing a well-accredited credit system, advanced credit systems, and communication programs.

5.3. Sybil Attack

Sybil attacks are types of attacks in which network criminals use fake identification names to control the effectiveness of cloud computing and convert genuine nodes into compromised nodes. These attackers are capable of disclosing a valid user's personal information. Detecting Sybil attacks in dynamic computing systems, such as cloud computing, is a difficult task because the network topology is not fully connected due to its highly distributed property. A number of logical nodes in an overlay network are under the control of Sybil nodes, allowing them to take over the network when the Sybil attack is successful. Network security has been threatened by Sybil attacks in a variety of ways, and a small number of Sybil nodes can damage the network by isolating benign nodes in membership management. There are malicious users in a multiple identity network in a Sybil attack. As a result, legitimate nodes in the system cannot detect the received information from single or multiple users. Therefore, the central organization carries out the identity-based authentication of users in the network to prevent this attack and ensure one-to-one mapping of node identity. Other countermeasures against Sybil attacks include trusted authentication, testing, permission decay, validation, and authentication.

5.4. Black Hole Attack

Like Sybil attacks, a black hole attack attacks the system based on an attacker's expectations. The networks, such as smart cities, intelligent transportation systems, and electronic health systems, are vulnerable to black hole attacks [81]. In such an attack, the malicious users show how it actively participates in the network routing mechanism. As most traffic is routed through the network, the attacker receives communicated messages from different network nodes. As a result, transmitted messages are not received at their correct destination but are dropped, causing packets loss. The attacks are hazardous to latency-sensitive applications like emergency patient care, disaster recovery, and road safety. Detecting and preventing such attacks requires active route searches and secure passive routing protocols by identifying the correct route and eliminating malicious routing messages [82].

5.5. Wormhole Attack

During this attack, the attacker transmits the routing messages to users, and the node broadcasts the message to its vicinity. Since the packets are encapsulated, the hop count is not diminished by the middle node between attacker nodes. This attack creates a circular route to gather or modify heavy network traffic, routing interruption, traffic tests, or selected data packets. This attack can be made without damaging the network or encryption system. Wormholes can be avoided using dedicated hardware that contains information on flight time, geographical area, or signal position [82].

5.6. Accountability

This can be defined as recognizing actions and activities within the network and identifying the particular individual. Audit trails and logs provide accountability. Accountability is used to perform forensic research and evaluate historical events and associated individuals or procedures. Three layers are defined to facilitate accountability and validation: the system and data and the workflow layers. The service provider has direct access to customers and software in cloud services. This means improper manipulation or client data use will not be detected. On the client side, using a hybrid cloud can increase and control who can access and change client data.

6. Possible Solutions

We must develop a secure cloud environment model and determine the risk associated with outsourcing data. We need to consider all the possible risks of misusing the data. To achieve this, the data must be sorted according to the associated risks [83]. The security model then acts accordingly and prioritizes essential data. The power of cloud computing is limitless, which can be used to deal with different attacks. Service-level agreements (SLAs) are treated as contracts between cloud vendors and users and include all cloud services aspects. Additionally, multitenancy is a hallmark of cloud environments, because using the same resources among users can pose a severe data risk. Therefore, it is essential to isolate resources in the multitenant model by segmentation and to restrict user access for a secure cloud model [84]. Multitenancy is a cloud-based feature environment that brings the concept of sharing when each running instance is available to one or more users. It can share among multiple users in a single cloud. In SaaS, multitenancy means the same service utilized by two or more customers. On the other hand, multitenancy occurs when two or more virtual machines (VMs) belonging to different customers share the same physical machine in IaaS. Multitenancy occurs when the cloud service provider allows resource sharing and virtualization. The overall summary of this section is presented in Tables 3–5.

6.1. Data Transmission

Data are transmitted through the internet and stored in a cloud computing environment. There is always the risk of attack and malicious activities when the cloud provides its services. The attacker tries to access user data without their permission. Sometimes original data are replaced with fake data. For instance, the authors of [85] introduced a data encryption technology for cloud computing, i.e., DNA-based data security (DNABDS). The data owners encrypt the data in the proposed scheme, unlike traditional methods. The authors proposed the deduplication process in another article [86]. The deduplication process is an effective technique that has gained widespread attention in the storage system. Deduplication improves storage utilization, eliminates unnecessary data, and reduces storage costs. Another recent approach is proposed by [87]. In this technique, the authors proposed a safe and adequate access control model for cloud computing environments to share resources and knowledge by using attribute-based encryption (ABE), distributed hash table (DHT) networks, and identity-based timed-release encryption (IDTRE). Initially, the data and resources are encrypted using user attributes, and encrypted data are separated into enclosed ciphertext.

Table 3. Summary of Section 5.

Ref.	Category	Problems	Method	Achievements
[85]	Data transmission	Replacement of original data by fake data	DNA-based data security	1024-bit secret key is generated based on DNA computing, user attributes, and MAC address
[86]	Data transmission	Duplicate data in the cloud storage	Deduplication based on text and multimedia data	Improves storage utilization, eliminates unnecessary data and reduces storage costs
[87]	Data transmission	Resource and knowledge sharing	Attribute-based encryption (ABE), a distributed hash table (DHT), and identity-based timed-release encryption (IDTRE)	Distributed into the DHT network, and encapsulated ciphertexts are stored on the cloud servers
[88]	Two-factor authentication	Fetching, uploading, and manipulation of data	AES-based encryption and decryption	User login details are stored in one database, and encryption/decryption details are stored on a different database
[89]	Two-factor authentication	Offloading mobile applications	Decision-making process to offload the authentication application and virtual smart card	Security, mobile device's residual energy, and energy cost
[90]	Two-factor authentication	Data storage and multiuser collaboration over an infrastructure of untrusted storage servers	Trusted third-party free protocol	Unauthorized parties (attackers) or a small set of colluding servers cannot gain access to the stored data
[91]	Two-factor authentication	Voice-controlled digital banking and online payments	Authentication service protocol with two-factor authentication	Voice assistants to enable financial and commercial operations which require authentication with an increased level of security
[92]	Honeypot	Tracking unusual methods of attack	Kerberos authentication system, VPC (Virtual Private Cloud), VPN (Virtual Private Network), and EFS (Elastic File System)	Seize, recognize, and duplicate the hacker behavior
[93]	Honeypot	Hardware failure, web hosting, and space and memory allocation of data, direct or indirect data loss	Honeypot on third-party cloud vendor servers	Honeypot is implemented in a file-sharing application which is deployed on cloud server
[94]	Changing cloud servers	Data loss control by the data owner	Verifiable data storage and secure data deduplication	To reduce the cost of data management
[95]	Changing cloud servers	Computing power or storage capacity	Qualitative in-depth examination of companies' attitudes towards security	Cost-saving and data processing
[96]	Self-adaptive approach	To detect abnormalities	Active Bundle (AB), a distributed self-protecting entity, wrapped with policy enforcement engine	To grant or limit permissions to their AB peers and provide them with access to anonymized data

Table 4. Summary of Section 5.

Ref.	Category	Problems	Method	Achievements
[97]	Self-adaptive approach	Cyber-resiliency concepts	Continuous trust restoration concept	To consider cyber-resiliency and to incorporate it early in the design process
[98]	Self-adaptive approach	Key exposures	Third-party auditor (TPA)	Auditing procedure with key exposure resistance as transparent as possible for the client
[99]	Self-adaptive approach	Computation overhead for users' data integrity	Third-party medium (TPM) to perform time-consuming operations	Time-efficient decryption
[100]	Self-adaptive approach	Secret key burden	Third-party auditor (TPA)	Reduces the local burden on the client
[101]	Ring signatures	Deduplication problems with data confidentiality	multiple key servers (KSs)	To construct an inter-KS deduplication algorithm, cloud storage service provider can perform deduplication over ciphertexts
[102]	Ring signatures	Data sharing in cloud storage	ID-based public shared data integrity auditing scheme	Secure against an untrusted cloud server and also preserves data privacy against the public verifier
[103]	Ring signatures	Requires the provision for user revocation	CDH-based ring signature and vector commitment	Dynamic data in untrusted cloud servers with provisions for privacy preserving
[104]	Ring signatures	Data sharing	Homomorphic authenticators	To reduce the space used to store such verification information
[105]	Runtime auditing	Cloud storage and access control	ABE-based techniques	Secure ciphertext deduplication scheme based on a classical CP-ABE scheme by eliminating the duplicated secrets and adding additional randomness to ciphertext
[106]	Runtime auditing	Lack of transparency and accountability	Runtime security auditing framework including RBAC, ABAC, SSO, and OpenStack	Reducing the response time to perform the costly operations only once, and efficient runtime verification
[107]	Runtime auditing	User access control	Authentication, authorization, and accounting (AAA)	To secure the lower layer of cloud infrastructure
[108]	Runtime auditing	Computational and storage cost for healthcare data	Ciphertext policy Attribute-based Encryption (CP-ABE)	To reduce computational and storage power and semitrusted third parties, ensuring local computations
[109]	Revocation keys	Execution time or the cost of running the applications	Service placement algorithm	Reduce execution time and running cost of application due to user's mobility
[110]	Revocation keys	Storing and processing of digital records	Shamir's Secret Share (SSS) scheme	Avoid complex mathematical operations and ensure fault tolerance

Table 5. Summary of Section 5.

Ref.	Category	Problems	Method	Achievements
[111]	Revocation keys	To ensure shared data integrity	Public auditing mechanism	To resign blocks during user revocation, a public verifier to audit the integrity of shared data without retrieving the entire data, and ability to support batch auditing
[112]	Revocation keys	To reveal user secrets or confidential data on the cloud	Cloud storage encryption scheme	To ensure user privacy is securely protected
[113]	Revocation keys	Collision resistance of hashing keys	Chameleon hash function	To improve collision resistance of hashing keys
[114]	Revocation keys	Data utility	Distributed servers, secret sharing, FHE, and chameleon hash functions	Long-term privacy-preserving computations for encrypted data and is secure even after a device-key is compromised
[115]	Revocation keys	Cloud server authorization	Privacy-preserving broker-ABE scheme for multiple CCPSs	Reduce computational burden, policy embedding task to the broker, and protect data privacy
[116]	Security model as a service	Tenancy and flexibility	-	To protect cloud infrastructure and provide flexibility to tenants to have additional security functionalities

6.2. Two-Factor Authentication

Application development also provides an interface for cloud services and prevents attacks and other data abuse caused by web browser leaks. These applications understand the user's behavior and take appropriate action if any unauthorized access is detected [88]. Nowadays, hijacking an account is a severe attack, and attackers have repeatedly tried to obtain account credentials for different cloud consumers. Security issues faced by end-users can be minimized by using an authentication mechanism. It is a process in which the provided credentials are compared on a file in a database of authorized users' information on a local operating system or within an authorized server. However, if the credentials match, the process is completed, and the user is granted permission to access.

The two-factor authentication mechanisms are more potent than traditional password authentication [89]. Two-factor solid authentication will form additional security checks to identify real customers and make the cloud environment more secure and reliable [90]. Two-factor authentication is a method that allows users to protect their data using a two-layer security system. This ensures a higher level of data security. In addition, the two-factor authentication prevents the confidentiality of end-users' information and data stored in a cloud from unauthorized access [91].

6.3. Honeypot

Honeypots are set up to locate, gather information, and prevent various attacks. The honeypot mechanism records the data and provides an early warning regarding threats and attacks. Since the honeypots are mostly placed inside the firewall program, they are used to secure the system from intruders from corporate organizations. A honeypot is a trap designed to deceive an intruder by disrupting an information system in an organization [92]. It can be used as early warning and advanced security monitoring tools to minimize the risk of attacks on IT systems and networks. Implementing the honeypot system in the cloud infrastructure will solve the distributed Denial of Service (DDoS) attacks and the abuse of cloud services to the greatest extent [117].

Since honeypots cannot contain a specific intrusion or the virus's spread, they only collect data and isolate the attack pattern. Nevertheless, they are a great way to track programmed behavior and raise the viability of security tools [93]. Honeypots not only

deliberately engage and deceive hackers but also identify malicious activities. The purpose is to analyze, understand, observe, and monitor the attacker's behaviors.

6.4. Changing Cloud Servers

The security solution is based on the two concepts of cloud servers: zero reliable and unchanging servers [94]. The solution uses the concept of unchanged servers as one of the recovery actions. The primary condition is to create a new server with predefined controls, and security policies are better. As a result, the configuration management challenges are minimized, rather than changing the existing server after the threat is detected. The configuration, user access logs, network protocols, and end-point protocols should be continuously analyzed to apply the zero-trust concept of cloud security. Immutable servers can be used in the cloud to take additional steps to block configurations, workloads, applications, and users with minimal privileges and known and accepted usage patterns [95].

6.5. Self-Adaptive Approach

A self-adaptive resilience approach automatically uses live monitoring and a targeted defense approach to identify typical behavior differences. The solution promises to create a unified framework for resilient cloud systems [96]. The authors in [96] proposed cloud-based sector activity screens to monitor service behavior and performance changes to detect abnormalities. The reorganization is based on redistribution involving service performance monitoring and regenerative elements. The proposed model aims to provide a unified framework for flexible and sustainable computing in reliable and unreliable clouds [97].

The work in [98] focused on making the customer's most critical updates as transparent as possible. It proposed a new cloud storage auditing paradigm with verifiable outsourcing of essential updates. In this article, important updates can be safely outsourced to an authorized party, keeping the customer's load on key updates to a minimum. In particular, they used the external auditor in many existing public auditing designs [99]. Glare technology with homomorphic characteristics forms an encryption algorithm that encrypts the key by a third-party auditor [99]. It formalizes the security model of the cloud storage control protocol by outsourcing verifiable key updates and demonstrates the specific implementation of a security protocol that describes consistent performance [100].

6.6. Ring Signatures

Ring signatures are another technique that can validate the metadata to monitor shared data's correctness. The mechanism verifies the signer's identity with each block of data transmitted and kept private by the public auditor, efficiently verifying the integrity of shared data without recovering the entire file. This mechanism can also perform multiple monitoring tasks simultaneously, rather than reviewing them one at a time. A tool for privacy uses ring signatures for creating homomorphic authenticators in Oruta [102,103]. Consequently, a public expert can find the integrity of shared data without retrieving the entire data. However, each block's signatory identity in shared data is kept private by the public auditor. Nevertheless, homomorphic authenticators can be further expanded to batch monitoring that can simultaneously perform multiple monitoring tasks and improve the efficiency of numerous monitoring tasks [104].

6.7. Runtime Auditing

In [105], the authors proposed a security auditing runtime framework for the cloud focused on user levels, such as shared access control and authentication [106]. The runtime security auditing framework is widely used for a cloud management system. The core concept of reducing response time to a practical level is to perform an invasive treatment [107]. The authors in [105] focus on ciphertext deduplication under Attribute-based Encryption (ABE). This fundamental observation stems from ABE numeral texts' structure and the possible agreements between different access structures. It also shows how to design a secure digit text deduplication scheme based on a classic ciphertext policy Attribute-based

Encryption (CP-ABE) system by adjusting construction with a recursive algorithm. CP-ABE can eliminate the duplicated secrets and add additional randomness to some certain digital text [108]. The authors in [105] also provided a detailed analysis of the proposed arrangements on efficiency and safety. To improve the proposed system's performance, they also developed a prototype. They conducted extensive experiments, which showed that their digital text reduplication schedule could reduce the storage cost to 80%. They also provided a detailed analysis showing that the resulting schedule is safe if the original CP-ABE scheme's safety is guaranteed.

6.8. Revocation Keys

The cloud can resign blocks with a revocation user using a revocation key. This can significantly increase user failure efficiency and reduce computing and communication resources [109,110]. The authors propose semisecure protocols and actively violate data integrity for attacker. However, this can inform the general data inaccuracy evaluators to maintain their data reputation and services. The cloud storage encryption scheme presented in [112] enables cloud storage providers to create compelling fake user secrets to protect users' privacy. Since the needy cannot know whether the secrets obtained are real, they build a cryptographic scheme that can be denied through a multidimensional space [118]. It can only obtain the original data if the dimensions are configured correctly. The text is encrypted into the desired counterfeit data in the fake configuration. The information that defines the aspects is kept secret and utilizes multidimensional bilinear groups to build multifaceted spaces. A chameleon hash function can also be used to persuade both true and false messages [113–115].

6.9. Security Model as a Service

The authors in [116] suggested a security architecture that enables user authentication as a service model. Authentication as a service model also provides primary security to cloud infrastructure, giving customers the flexibility to control virtual machines. Security is required from the supplier to ensure that malicious tenants do not attack the cloud infrastructure or host malware. Each tenant must have safety features to provide standard operating guarantees. In comparison, other tenants require additional security services from their cloud providers to meet their needs and protect them from other malicious tenants. The security features may require tenants to disclose information about their services and applications, leading to concerns about tenant privacy. This allows the tenants to deal with disputes between privacy issues and the security management of cloud providers. Hence, the model's feature is to compromise security and privacy.

7. Countermeasures for Threats in Cloud Computing

Cloud computing has become integral to modern businesses and organizations. However, with its widespread adoption, concerns about security have also grown. Researchers and organizations have proposed various recommendations, countermeasures, and best practices to enhance the security of cloud environments [119]. This section outlines key countermeasures that address specific security threats in cloud computing.

7.1. Protecting against Data Breaches and System Vulnerability

Cloud computing's shared resources demand stringent security measures. The repercussions of data misuse can have far-reaching effects on organizations, eroding trust and business integrity

7.1.1. Multifactor Authentication (MFA)

Implementing MFA significantly enhances security. It introduces multiple layers of authentication beyond traditional passwords, raising the bar for potential attackers. MFA fortifies cloud environments against unauthorized access.

7.1.2. Encryption

Robust encryption techniques are crucial for protecting data at rest and in transit. Encryption ensures the confidentiality and integrity of sensitive data within the cloud environment.

7.1.3. Routine Vulnerability Scanning

To identify and address potential vulnerabilities, regular vulnerability scans should be conducted. Swift remediation of identified device threats is essential to maintain cloud security.

7.2. Secure Interfaces and APIs

Ensuring the security of cloud applications requires meticulous attention to detail. Robust measures for secure interfaces and APIs include the following.

7.2.1. Source Code Review

In-depth security code reviews involve scrutinizing application source code to verify the presence and proper functionality of security checks. This process guarantees that security measures are consistently invoked across various code sections.

7.2.2. Entrance Testing

Rigorous entrance testing helps identify vulnerabilities and weaknesses in security barriers. Successful testing is instrumental in strengthening cloud security, ensuring that the system is resilient against potential threats.

7.3. Credential and Access Management

Effective credential and access management are imperative for both cloud service consumers and operators. Multifactor authentication mechanisms, including smart cards, One-Time Passwords (OTP), and mobile authentication, play a pivotal role in preventing unauthorized access.

Enhanced Security against Password Theft

These mechanisms create substantial challenges for attackers attempting to exploit stolen passwords, particularly in lateral movement attacks.

7.4. Account Hijacking and Denial of Service (DoS)

Identifying and mitigating threats such as account hijacking and DoS attacks are paramount for organizations.

7.4.1. Prohibition of Credential Sharing

Strict policies should be in place to prohibit users and services from sharing account credentials, reducing the risk of account hijacking.

7.4.2. Two-Factor Authentication (2FA)

Implementing 2FA adds an extra layer of security, making it significantly more difficult for attackers to compromise accounts.

7.4.3. Bandwidth Expansion

While expensive, investing in ample bandwidth makes it challenging for attackers to execute DoS attacks, as it increases the volume of traffic required to saturate the network.

7.4.4. Intrusion Prevention Systems (IPS) and Firewalls

Modern intrusion prevention systems and firewalls offer advanced DoS protection technologies, including signature detection and connection verification techniques, limiting the success of DoS attacks.

7.5. Identity and Access Management (IAM)

Identity and Access Management (IAM) is foundational to cloud security, ensuring that only authorized individuals gain access to resources when needed. IAM comprises identity management, authentication, and authorization.

7.5.1. Identity Management

Robust identity management involves enforcing strong password policies, including regular password resets and expiration periods. These measures reduce the risk associated with prolonged password use.

7.5.2. Authentication

Effective authentication verifies users' identities during login. Multifactor authentication (MFA), which incorporates hard or soft tokens and biometrics, adds an extra layer of security to thwart unauthorized access attempts.

7.5.3. Authorization

Authorization grants users permission to use specific resources. Authentication is a prerequisite for authorization, ensuring that only authenticated users are allowed access.

7.6. Digital Signatures and Message Digests

To guarantee the integrity, authenticity, and nonrepudiation of data exchanged over the cloud, several cryptographic mechanisms are employed.

7.6.1. Message Digests

Message digests, created using well-known hash functions such as MD5 or SHA, encrypt messages to safeguard data integrity during transmission.

7.6.2. Digital Signatures

Digital signatures, based on asymmetric cryptography, provide robust authentication. Combining Single Sign-On (SSO) with Lightweight Direct Access Protocol enhances authentication strength. Additionally, various other methods are proposed for digital signatures, offering anonymity and traceability, addressing issues like free riders of Software as a Service (SaaS) and proof of data possession.

7.7. Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are indispensable for identifying anomalies by analyzing network traffic patterns and activities within cloud environments. Different types of IDS are deployed at various levels.

7.7.1. Network-Based IDS

Analyzes network packets using signature or anomaly-based techniques to detect malicious activities, including Denial of Service (DoS) attacks and port scanning.

7.7.2. Host-Based IDS

Monitors and analyzes the host's file system, kernel, and behavior for changes. It also reviews system logs against access control policies to detect intrusions. Distributed IDS Utilizes multiple IDSs across a large network to identify anomalies based on traffic patterns.

7.7.3. Hypervisor-Based IDS

Operates at the hypervisor level, analyzing and detecting anomalies in communication between Virtual Machines (VMs), the hypervisor, and the virtual network.

7.8. Security Measures for Data Storage

Data are the lifeblood of any organization, demanding stringent security measures to protect against cyberthreats.

7.8.1. Data Classification

Categorize data based on sensitivity and enforce strict access controls to restrict unauthorized access.

7.8.2. Data Encryption

Encrypt stored data to ensure both confidentiality and integrity. Transparency: Maintain transparency between cloud providers and clients regarding data storage. This includes specifying backup locations, backup frequency, and data availability.

7.8.3. Data Sanitization

Implement data sanitization practices to remove all traces of sensitive data before disposing of or reusing assets, reducing the risk of data breaches.

7.9. Network Security Measures

The Cloud Security Alliance (CSA) recommends robust network security measures to safeguard data in transit.

7.9.1. Firewalls

Protect external interfaces with firewalls, permitting only the required ports to remain open.

7.9.2. Intrusion Detection and Prevention Systems (IDS/IPS)

Deploy updated IDS/IPS systems to analyze traffic flow across the virtual network, detecting and mitigating potential threats.

7.9.3. Penetration Testing

Validate network security through penetration testing, packet analysis, session management, and take appropriate security measures when anomalies or deviations are observed. These comprehensive countermeasures provide a multidimensional approach to enhancing cloud security. By implementing these recommendations and addressing specific security risks associated with data breaches, such as system vulnerabilities, credential and access management, insecure interfaces, and account hijacking, cloud environments can be fortified against a wide range of threats. This comprehensive security strategy ensures data integrity, confidentiality, and accessibility while minimizing vulnerabilities.

8. Future Directions

The field of cloud computing security continues to evolve, and while significant progress has been made, numerous open issues and future research directions persist [64]. Addressing these concerns and advancing security measures is vital to fostering trust and confidence among cloud users [120]. In this section, we delve into the key open issues and propose future directions for research in cloud security [121,122].

8.1. Safeguarding Cloud Infrastructure

Securing cloud infrastructure is of paramount importance, requiring protection against both known and unknown attacks across all its components. Nevertheless, establishing a robust and secure cloud infrastructure still presents unresolved challenges. Security concerns span various domains, including cloud communications, network security, data protection, applications, and web services, which initially emerged with the advent of cloud computing. Security issues have evolved with the proliferation of cloud tenancy,

virtualization, and shared resources. Here, we explore potential research avenues and emerging technologies that could impact the security of cloud infrastructure

8.2. Ensuring Data Privacy and Security

Data privacy remains a pressing concern in cloud computing, with data often stored in encrypted form. However, not all operations are performed on encrypted data, leaving certain attack vectors. Many operations require plaintext data during computation, which can be vulnerable to attacks [123]. To address these challenges, research should consider innovative solutions and emerging technologies.

8.3. Multitenancy Efficiency

Multitenancy is a fundamental characteristic of cloud computing, enabling resource sharing among multiple clients [124]. While this improves resource utilization, it also poses unique security challenges. Distributed Denial of Service (DDoS) attacks targeting multitenancy environments can disrupt services, affecting multiple tenants. Researchers must explore ways to optimize multitenancy while fortifying defenses against DDoS attacks and resource underutilization.

8.4. Fog Computing for Improved IoT Security

Fog computing, an emerging paradigm, brings computing resources closer to IoT devices, reducing latency and enhancing processing capabilities. However, as fog computing gains traction, security concerns must be adequately addressed. Research efforts should prioritize minimizing data loss, safeguarding data transported by IoT devices, and preserving data integrity and confidentiality within fog computing environments.

8.5. Homomorphic Encryption

Homomorphic encryption has the potential to revolutionize data privacy in cloud computing. It allows operations to be performed on encrypted data without decryption, preserving the confidentiality of sensitive information. Future research should focus on enhancing the efficiency and scalability of homomorphic encryption schemes for practical cloud applications.

8.6. Leveraging Machine Learning Techniques

Machine learning techniques are increasingly employed in security platforms to elevate threat detection capabilities. Exploring advanced applications of machine learning can significantly impact the security landscape of cloud computing.

8.7. Deduplication in Cloud-to-Cloud Backups

Efficient data deduplication mechanisms for cloud-to-cloud backups are essential to minimize storage costs and optimize data transfer. Research should focus on developing deduplication techniques that align with the unique requirements of cloud-to-cloud backup scenarios.

8.8. Insider Threat Detection

Identifying normal users from malicious insiders remains a formidable challenge in cloud security. Although machine learning and artificial intelligence have been employed to address this issue, the lack of standardized solutions hinders widespread adoption. Future research should strive for seamless integration of insider threat detection solutions, enabling organizations to rapidly deploy and effectively manage security measures against insider threats. as cloud computing continues to evolve, addressing these open issues and pursuing these future research directions is essential to bolstering cloud security. Collaboration among researchers, industry professionals, and policymakers is imperative to develop innovative solutions that mitigate emerging threats and ensure the confidentiality, integrity, and availability of cloud resources and data. Strengthening cloud security is not

only vital for organizations but also for maintaining trust in the cloud computing paradigm as a whole.

9. Implications of Cloud Deployment Models on Security

Cloud computing encompasses diverse deployment models, each carrying unique security implications. In this exploration, we uncover the specific security considerations associated with private, public, and hybrid cloud models.

9.1. Private Clouds

Private clouds provide cloud services with scalable resources and virtual applications that organizations can access as if they were part of an internal network. However, the billing structure for private clouds is typically subscription-based, with minimal consideration for individual usage. This model often results in cost considerations and operational security risks. Organizations wield significant influence over the design and implementation of security techniques, making security challenges multifaceted. These challenges include issues related to poor management, suboptimal implementation, technical requirements, and management constraints. Furthermore, cost and return on investment considerations play a pivotal role, leading to a nuanced approach to security implementation and emphasizing risk assessment. As a result, security allocation in private clouds may not be absolute. Here are additional implications to consider in private cloud environments.

9.1.1. Operational Security

Ensuring operational security in private clouds is paramount. Organizations must implement robust security measures to safeguard sensitive data and applications.

9.1.2. Customized Security

Organizations have significant control over the design and implementation of security techniques in private clouds. This customization allows tailoring security measures to specific needs and challenges.

9.1.3. Management Complexity

Managing security in a private cloud environment can be complex, with challenges arising from poor management, suboptimal implementation of security controls, and technical requirements.

9.1.4. Resource Constraints

Organizations may face resource constraints, both in terms of budget and skilled personnel, which can impact the effectiveness of security measures.

9.1.5. Cost vs. Security

Private cloud deployments often involve a delicate balance between cost and security. Organizations must assess the return on investment (ROI) of security implementations and allocate resources accordingly.

9.1.6. Risk Assessment

Security in private clouds requires a nuanced approach, emphasizing thorough risk assessment to identify vulnerabilities and prioritize security efforts.

9.1.7. Flexibility in Compliance

Private clouds offer flexibility in meeting compliance requirements, allowing organizations to align security policies with industry regulations and internal standards.

9.2. Public Clouds

Public clouds offer resources dynamically through the internet or portals, with costs usually based on consumption and pay-as-you-go pricing models. Due to the multitenancy nature of public clouds, security risks are inherently higher, stemming from the presence of numerous users and their transactional activities. Cloud service providers often implement multitiered security systems to counter these risks. The one-off implementation and multipurpose architecture of public clouds theoretically lead to a high-security standards while substantially reducing the costs associated with security. However, the absence of dedicated resources, as resources are shared among multiple users, poses significant security challenges. Organizations must navigate various external impacts, including compliance with legislation and data protection regulations, which become added responsibilities in a public cloud environment.

9.2.1. Shared Resources

Public clouds are multitenant environments where multiple organizations share the same infrastructure. This shared nature raises concerns about data isolation and the potential for data leakage. Limited Control Users have limited control over the underlying infrastructure and security measures, as these are managed by the cloud service provider (CSP).

9.2.2. Compliance Challenges

Meeting industry-specific compliance requirements may be challenging, as public cloud providers must cater to a broad range of customers.

9.3. Security Measures

9.3.1. Access Control

Implement robust access control mechanisms to ensure that only authorized users can access your resources.

9.3.2. Data Encryption

Encrypt data both in transit and at rest to protect it from unauthorized access.

9.3.3. Vendor Security

Evaluate the CSP's security practices and certifications to ensure they meet your organization's requirements.

9.3.4. Regular Auditing

Continuously monitor and audit configurations and permissions to prevent misconfigurations and unauthorized access.

9.4. Hybrid Clouds

A hybrid cloud is a combination of a private cloud connected to external cloud providers in a well-designed manner. It offers scalability and flexibility to cloud users, making it relatively straightforward to implement [125]. However, the hybrid cloud model introduces complexities in billing and management. It enables the proactive creation of security measures tailored to counter assessed threats, vulnerabilities, and risks. Proactive security measures can be cost-effective and precisely targeted. Cloud providers and vendors can develop mitigation and management strategies based on their threat analysis. While specifics may vary, some best practices for enhancing security in cloud deployments include the following.

9.4.1. Data Segmentation

Hybrid clouds involve the movement of data and applications between on-premises and public cloud environments. Properly segmenting and classifying data based on sensitivity is crucial to maintain security during transitions.

9.4.2. Interoperability Challenges

Integrating and ensuring compatibility between different cloud platforms can be complex. Inadequate interoperability measures can lead to security gaps or operational issues.

9.4.3. Data Transfer Security

Data transfer between on-premises and cloud environments, known as "data in transit", must be encrypted and secure to prevent interception or tampering during transit.

9.4.4. Identity and Access Management (IAM)

Managing user identities and access rights across hybrid environments requires robust IAM solutions. Implementing consistent access policies can be challenging but is essential.

9.4.5. Logging and Monitoring

Hybrid clouds generate extensive logs and monitoring data across various platforms. Aggregating, analyzing, and responding to security events and incidents from these diverse sources demands advanced monitoring tools and strategies.

9.4.6. Compliance Complexity

Meeting compliance requirements in hybrid environments can be intricate, as regulations may vary for on-premises and cloud-hosted data. Careful mapping of compliance controls and practices is essential.

9.4.7. Resource Management

Optimizing resource allocation and utilization across hybrid environments is complex. Security measures must adapt to resource scaling and shifting between on-premises and cloud infrastructure. Here are some security measures to counteract the implications mentioned above.

9.4.8. End-to-End Encryption

Given the potential geographic dispersal of data in cloud environments, data should be encrypted from end to end to ensure their confidentiality and integrity.

9.4.9. Monitoring for Malicious Activity

Implementing end-to-end encryption can introduce new risks, as encrypted data cannot be easily inspected by firewalls or intrusion detection systems. Consequently, it is essential to employ robust monitoring and countermeasures to mitigate malware risks. User Validation Cloud vendors should take adequate measures to authenticate and validate users accessing critical cloud features. Securing Interfaces and Access Points Protect vital interfaces and access points with robust security measures, including firewalls, intrusion detection systems, and access controls. Regularly update and patch these security components. Mitigating Internal Threats Implement comprehensive internal security protocols and monitoring mechanisms to safeguard against insider threats. Regularly audit and review employee access and activities.

9.4.10. Securing Shared Resources

In multitenant environments, cloud providers should employ strong isolation mechanisms to secure shared resources. Utilize monitoring tools to ensure the integrity and security of the entire cloud infrastructure.

These security measures, when effectively implemented, can help organizations navigate the challenges posed by cloud deployment models while maintaining the confidentiality, integrity, and availability of their data and operations.

10. Conclusions

Cloud computing has the following advantages: fast management, cost-effective performance, large-capacity memory, and the benefits of quick access to end devices at any time and everywhere. However, many security issues are hindering the adoption of cloud computing. Therefore, there is an ardent need for security solutions to tackle diverse security threats in cloud computing. For this purpose, we provide a complete overview of the security issues and threats in diverse cloud models, i.e., public, community, private, and hybrid cloud computing. Next, we explored the core aspects of cloud computing and suggested several techniques and countermeasures to address security problems in different cloud domains. After discussing security threats, attacks, and countermeasures, we presented future directions of study. This will help researchers in academia and industry find novel techniques to tackle the security threats in different cloud models.

Author Contributions: M.D.: conceptualization, methodology, idea, writing—original draft preparation, writing—review and editing. S.T.: conceptualization, methodology, idea, writing—original draft preparation, writing—review and editing, visualization, supervision, funding acquisition. C.X.: conceptualization, methodology, idea, writing—original draft preparation, writing—review and editing, visualization, supervision, funding acquisition. H.A.: writing—review and editing, visualization, validation, supervision, funding acquisition. M.W.: writing—original draft preparation, writing–review and editing, visualization, supervision, funding acquisition, formal analysis, investigation. S.U.R.: writing—original draft preparation, writing–review and editing, visualization, supervision, funding acquisition, formal analysis, investigation. All authors have read and agreed to the published version of the manuscript.

Funding: This work is partly supported by the Beijing Natural Science Foundation (No. 4212015). The authors also extend their appreciation to King Khalid University for funding this work through Large Group Project under grant number RGP.2/312/44.

Data Availability Statement: No data is available.

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

References

1. Tu, S.; Waqas, M.; Rehman, S.U.; Aamir, M.; Chang, C.C. Security in Fog Computing: A Novel Technique to Tackle an Impersonation Attack. *IEEE Access* **2018**, *6*, 74993–75001. [CrossRef]
2. Qiu, H.; Noura, H.; Qiu, M.; Ming, Z.; Memmi, G. A user-centric data protection method for cloud storage based on invertible DWT. *IEEE Trans. Cloud Comput.* **2019**, *9*, 1293–1304. [CrossRef]
3. Li, Z.; Yang, Z.; Xie, S. Computing resource trading for edge-cloud-assisted Internet of Things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3661–3669. [CrossRef]
4. Fan, X.; Yao, J.; Cao, N. Research on Cloud Computing Security Problems and Protection Countermeasures. In Proceedings of the International Symposium on Cyberspace Safety and Security, Guangzhou, China, 1–3 December 2019; pp. 542–551.
5. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Comput. Sci. Rev.* **2019**, *33*, 1–48. [CrossRef]
6. Huss, M.; Waqas, M.; Ding, A.Y.; Li, Y.; Ott, J. Security and Privacy in Device-to-Device (D2D) Communication: A Review. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1054–1079. [CrossRef]
7. Fazal, H.; Memon, I.; Khatri, T.K.; Muhammad, G.; Ali, Q. A survey on cloud computing, security Challenges, architecture, applications & solutions. *Univ. Sindh J. Inf. Commun. Technol.* **2020**, *4*, 24–30.
8. Tu, S.; Waqas, M.; Rehman, S.U.; Mir, T.; Abbas, G.; Abbas, Z.H.; Halim, Z.; Ahmad, I. Reinforcement Learning Assisted Impersonation Attack Detection in Device-to-Device Communications. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1474–1479. [CrossRef]
9. Kumar, R.; Goyal, R. Assurance of Data Security and Privacy in the Cloud: A Three-Dimensional Perspective. *Softw. Qual. Prof.* **2019**, *21*, 7–26.
10. Tu, S.; Waqas, M.; Meng, Y.; Rehman, S.U.; Ahmad, I.; Koubaa, A.; Halim, Z.; Hanif, M.; Chang, C.C.; Shi, C. Mobile fog computing security: A user-oriented smart attack defense strategy based on DQL. *Comput. Commun.* **2020**, *160*, 790–798. [CrossRef]
11. Shen, J.; Gui, Z.; Ji, S.; Shen, J.; Tan, H.; Tang, Y. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *J. Netw. Comput. Appl.* **2018**, *106*, 117–123. [CrossRef]

12. Ahmed, M.; Li, Y.; Waqas, M.; Sheraz, M.; Jin, D.; Han, Z. A Survey on Socially Aware Device-to-Device Communications. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2169–2197. [CrossRef]
13. Mani, A.C.; Malviya, A.K. Security Challenges in Cloud Computing Networks. *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE),* Sultanpur, India, 8–9 February 2019.
14. Waqas, M.; Niu, Y.; Li, Y.; Ahmed, M.; Jin, D.; Chen, S.; Han, Z. A Comprehensive Survey on Mobility-Aware D2D Communications: Principles, Practice and Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1863–1886. [CrossRef]
15. Kushala, M.V.; Shylaja, B.S. Recent Trends on Security Issues in Multi-Cloud Computing: A Survey. In Proceedings of the 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 10–12 September 2020; pp. 777–781.
16. Mondal, A.; Paul, S.; Goswami, R.T.; Nath, S. Cloud computing security issues & challenges: A Review. In Proceedings of the 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 22–24 January 2020; pp. 1–5.
17. Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1–11. [CrossRef]
18. Grusho, A.A.; Zabezhailo, M.I.; Zatsarinnyi, A.A.; Piskovskii, V.O. On some artificial intelligence methods and technologies for cloud-computing protection. *Autom. Doc. Math. Linguist.* **2017**, *51*, 62–74. [CrossRef]
19. Liu, Y.; Sun, Y.L.; Ryoo, J.; Vasilakos, A.V. *A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions*; Korean Institute of Information Scientists and Engineers (KIISE): Seoul, Republic of Korea, 2015.
20. Syed, A.; Purushotham, K.; Shidaganti, G. Cloud storage security risks, practices and measures: A review. In Proceedings of the 2020 IEEE International Conference for Innovation in Technology (INOCON), Bangluru, India, 6–8 November 2020; pp. 1–4.
21. Kumari, C.; Singh, G.; Singh, G.; Batth, R.S. Security issues and challenges in cloud computing: A mirror review. In Proceedings of the 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 11–12 December 2019; pp. 701–706.
22. Ghaffari, F.; Gharaee, H.; Arabsorkhi, A. Cloud security issues based on people, process and technology model: A survey. In Proceedings of the 2019 5th International Conference on web research (ICWR), Tehran, Iran, 24–25 April 2019; pp. 196–202.
23. Mandal, S.; Khan, D.A. A Study of security threats in cloud: Passive impact of COVID-19 pandemic. In Proceedings of the 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 10–12 September 2020; pp. 837–842.
24. Bhajantri, L.B.; Mujawar, T. A survey of cloud computing security challenges, issues and their countermeasures. In Proceedings of the 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 12–14 December 2019; pp. 376–380.
25. Nafea, R.A.; Almaiah, M.A. Cyber security threats in cloud: Literature review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 779–786.
26. Butt, U.A.; Amin, R.; Mehmood, M.; Aldabbas, H.; Alharbi, M.T.; Albaqami, N. Cloud security threats and solutions: A survey. *Wirel. Pers. Commun.* **2023**, *128*, 387–413. [CrossRef]
27. Shamshirband, S.; Fathi, M.; Chronopoulos, A.T.; Montieri, A.; Palumbo, F.; Pescapè, A. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *J. Inf. Secur. Appl.* **2020**, *55*, 102582. [CrossRef]
28. Alotaibi, A.F. A comprehensive survey on security threats and countermeasures of cloud computing environment. *Turk. J. Comput. Math. Educ. (TURCOMAT)* **2021**, *12*, 1978–1990.
29. Basu, S.; Bardhan, A.; Gupta, K.; Saha, P.; Pal, M.; Bose, M.; Basu, K.; Chaudhury, S.; Sarkar, P. Cloud computing security challenges & solutions—A survey. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 347–356.
30. Nagesh, O.; Kumar, T.; Venkateswararao, V. A Survey on Security Aspects of Server Virtualization in Cloud Computing. *Int. J. Electr. Comput. Eng.* **2017**, *7*, 1326–1336. [CrossRef]
31. RahimiZadeh, K.; AnaLoui, M.; Kabiri, P.; Javadi, B. Performance modeling and analysis of virtualized multi-tier applications under dynamic workloads. *J. Netw. Comput. Appl.* **2015**, *56*, 166–187. [CrossRef]
32. Abazari, F.; Analoui, M.; Takabi, H. Effect of anti-malware software on infectious nodes in cloud environment. *Comput. Secur.* **2016**, *58*, 139–148. [CrossRef]
33. Sharifi, M.; Salimi, H.; Asadi, E. Alamut: A high-performance network intrusion detection system in support of virtualized environments. *Secur. Commun. Netw.* **2013**, *6*, 1310–1318. [CrossRef]
34. Atzori, L.; Bellido, J.L.; Bolla, R.; Genovese, G.; Iera, A.; Jara, A.; Lombardo, C.; Morabito, G. SDN & NFV contribution to IoT objects virtualization. *Comput. Netw.* **2019**, *149*, 200–212.
35. Goyal, K.; Jain, V.; Verma, P. An analysis on virtual machine migration issues and challenges in cloud computing. *Int. J. Comput. Appl.* **2018**, *975*, 8887.
36. Ahmed, M.; Litchfield, A.T. Taxonomy for identification of security issues in cloud computing environments. *J. Comput. Inf. Syst.* **2018**, *58*, 79–88. [CrossRef]
37. 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]
38. Jabeen, T.; Ashraf, H.; Khatoon, A.; Band, S.S.; Mosavi, A. A lightweight genetic based algorithm for data security in wireless body area networks. *IEEE Access* **2020**, *8*, 183460–183469. [CrossRef]

39. AlKadi, O.; Moustafa, N.; Turnbull, B.; Choo, K.K.R. Mixture localization-based outliers models for securing data migration in cloud centers. *IEEE Access* **2019**, *7*, 114607–114618. [CrossRef]
40. Haider, S.; Abbas, Z.H.; Abbas, G.; Waqas, M.; Tu, S.; Zhao, W. A Novel Cross-Layer V2V Architecture for Direction-Aware Cooperative Collision Avoidance. *Electronics* **2020**, *9*, 1112. [CrossRef]
41. Moghaddam, M.J.; Esmaeilzadeh, A.; Ghavipour, M.; Zadeh, A.K. Minimizing virtual machine migration probability in cloud computing environments. *Clust. Comput.* **2020**, *23*, 3029–3038. [CrossRef]
42. Tu, S.; Liu, M.; Waqas, M.; ur Rehman, S.; Zhu, R.; Liu, L. FHC-PCIA: A Physical Cell Identification Allocation Method Based on Fuzzy Hierarchical Clustering for Heterogeneous Cellular Network. *IEEE Access* **2018**, *6*, 46976–46987. [CrossRef]
43. Joshi, N.; Shah, S. A comprehensive survey of services provided by prevalent cloud computing environments. In *Smart Intelligent Computing and Applications*; Springer: Singapore, 2019; pp. 413–424.
44. Tchernykh, A.; Schwiegelsohn, U.; Talbi, E.-g.; Babenko, M. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *J. Comput. Sci.* **2019**, *36*, 100581. [CrossRef]
45. Ahmad, A.A.S.; Andras, P. Measuring the scalability of cloud-based software services. In Proceedings of the 2018 IEEE World Congress on Services (SERVICES), San Francisco, CA, USA, 2–7 July 2018; pp. 5–6.
46. Ullah, S.; Abbas, G.; Abbas, Z.H.; Waqas, M.; Ahmed, M. RBO-EM: Reduced Broadcast Overhead Scheme for Emergency Message Dissemination in VANETs. *IEEE Access* **2020**, *8*, 175205–175219. [CrossRef]
47. Waqas, M.; Tu, S.; Rehman, S.U.; Halim, Z.; Anwar, S.; Abbas, G.; Abbas, Z.H.; Rehman, O.U. Authentication of Vehicles and Road Side Units in Intelligent Transportation System. *CMC-Comput. Mater. Contin.* **2020**, *64*, 359–371. [CrossRef]
48. Tseng, C.L.; Lin, F.J. Extending scalability of IoT/M2M platforms with fog computing. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 825–830.
49. Zeng, M.; Li, Y.; Zhang, K.; Waqas, M.; Jin, D. Incentive Mechanism Design for Computation Offloading in Heterogeneous Fog Computing: A Contract-Based Approach. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
50. Yang, H.; Kim, Y. Design and implementation of high-availability architecture for IoT-cloud services. *Sensors* **2019**, *19*, 3276. [CrossRef] [PubMed]
51. Torquato, M.; Umesh, I.; Maciel, P. Models for availability and power consumption evaluation of a private cloud with VMM rejuvenation enabled by VM Live Migration. *J. Supercomput.* **2018**, *74*, 4817–4841. [CrossRef]
52. Zafar, F.; Khan, A.; Malik, S.U.R.; Ahmed, M.; Anjum, A.; Khan, M.I.; Javed, N.; Alam, M.; Jamil, F. A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. *Comput. Secur.* **2017**, *65*, 29–49. [CrossRef]
53. Yan, Y.X.; Wu, L.; Xu, W.Y.; Wang, H.; Liu, Z.M. Integrity audit of shared cloud data with identity tracking. *Secur. Commun. Netw.* **2019**, *2019*, 1354346. [CrossRef]
54. Li, J.; Yan, H.; Zhang, Y. Identity-based privacy preserving remote data integrity checking for cloud storage. *IEEE Syst. J.* **2020**, *15*, 577–585. [CrossRef]
55. Badshah, A.; Jalal, A.; Farooq, U.; Rehman, G.U.; Band, S.S.; Iwendi, C. Service Level Agreement Monitoring as a Service: An Independent Monitoring Service for Service Level Agreements in Clouds. *Big Data* **2022**, *11*, 339–354. [CrossRef]
56. Huttunen, J.; Jauhiainen, J.; Lehti, L.; Nylund, A.; Martikainen, M.; Lehner, O. Big data, cloud computing and data science applications in finance and accounting. *ACRN J. Financ. Risk Perspect.* **2019**, *8*, 16–30.
57. Truong, H.L. Integrated analytics for IIoT predictive maintenance using IoT big data cloud systems. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, USA, 21–23 October 2018; pp. 109–118.
58. Waqas, M.; Niu, Y.; Ahmed, M.; Li, Y.; Jin, D.; Han, Z. Mobility-Aware Fog Computing in Dynamic Environments: Understandings and Implementation. *IEEE Access* **2019**, *7*, 38867–38879. [CrossRef]
59. Stergiou, C.; Psannis, K.E.; Gupta, B.B.; Ishibashi, Y. Security, privacy & efficiency of sustainable cloud computing for big data & IoT. *Sustain. Comput. Inform. Syst.* **2018**, *19*, 174–184.
60. Zhang, Y.; Yang, M.; Zheng, D.; Lang, P.; Wu, A.; Chen, C. Efficient and secure big data storage system with leakage resilience in cloud computing. *Soft Comput.* **2018**, *22*, 7763–7772. [CrossRef]
61. Mei, J.; Li, K.; Tong, Z.; Li, Q.; Li, K. Profit maximization for cloud brokers in cloud computing. *IEEE Trans. Parallel Distrib. Syst.* **2018**, *30*, 190–203. [CrossRef]
62. Nagarajan, R.; Thirunavukarasu, R.; Shanmugam, S. A cloud broker framework for infrastructure service discovery using semantic network. *Int. J. Intell. Eng. Syst.* **2018**, *11*, 11–19. [CrossRef]
63. Halabi, T.; Bellaiche, M. A broker-based framework for standardization and management of Cloud Security-SLAs. *Comput. Secur.* **2018**, *75*, 59–71. [CrossRef]
64. Kanagaraju, P.; Nallusamy, R. Registry service selection based secured Internet of Things with imperative control for industrial applications. *Clust. Comput.* **2019**, *22*, 12507–12519. [CrossRef]
65. Ramachandra, G.; Iftikhar, M.; Khan, F.A. A comprehensive survey on security in cloud computing. *Procedia Comput. Sci.* **2017**, *110*, 465–472. [CrossRef]
66. Ahmed, M.; Shi, H.; Chen, X.; Li, Y.; Waqas, M.; Jin, D. Socially Aware Secrecy-Ensured Resource Allocation in D2D Underlay Communication: An Overlapping Coalitional Game Scheme. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 4118–4133. [CrossRef]

67. Majumdar, S.; Jarraya, Y.; Madi, T.; Alimohammadifar, A.; Pourzandi, M.; Wang, L.; Debbabi, M. Proactive verification of security compliance for clouds through pre-computation: Application to OpenStack. In Proceedings of the European Symposium on Research in Computer Security, Heraklion, Greece, 26–30 September 2016; pp. 47–66.
68. Tu, S.; Waqas, M.; Rehman, S.U.; Mir, T.; Halim, Z.; Ahmad, I. Social phenomena and fog computing networks: A novel perspective for future networks. *IEEE Trans. Comput. Soc. Syst.* **2021**, *9*, 32–44. [CrossRef]
69. Kalaiprasath, R.; Elankavi, R.; Udayakumar, D.R. Cloud security and compliance—A semantic approach in end to end security. *Int. J. Mech. Eng. Technol.* **2017**, *8*, 987–994. [CrossRef]
70. Tanveer, M.; Abbas, G.; Abbas, Z.H.; Waqas, M.; Muhammad, F.; Kim, S. S6AE: Securing 6LoWPAN Using Authenticated Encryption Scheme. *Sensors* **2020**, *20*, 2707. [CrossRef] [PubMed]
71. Singh, C.; Singh, D. A 3-Level Multifactor Authentication Scheme for Cloud Computing. *Int. J. Comput. Eng. Technol.* **2019**, *10*, 184–195. [CrossRef]
72. Casola, V.; Benedictis, A.D.; Rak, M.; Villano, U.; Rios, E.; Rego, A.; Capone, G. Model-based deployment of secure multi-cloud applications. *Int. J. Grid Util. Comput.* **2019**, *10*, 639–653. [CrossRef]
73. Bhushan, K.; Gupta, B.B. Distributed Denial of Service (DDoS) attack mitigation in software-defined network (SDN) - based cloud computing environment. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 1985–1997. [CrossRef]
74. Zhang, X.; Wang, H.; Xu, C. Identity-based key-exposure resilient cloud storage public auditing scheme from lattices. *Inf. Sci.* **2019**, *472*, 223–234. [CrossRef]
75. Wan, J.; Waqas, M.; Tu, S.; Hussain, S.M.; Shah, A.; Rehman, S.U.; Hanif, M. An efficient impersonation attack detection method in fog computing. *CMC Comput. Mater. Contin.* **2021**, *68*, 267–281. [CrossRef]
76. Waqas, M.; Ahmed, M.; Yong, L.; Jin, D.; Chen, S. Social-Aware Secret Key Generation for Secure Device-to-Device Communication via Trusted and Non-Trusted Relays. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 3918–3930. [CrossRef]
77. Waqas, M.; Ahmed, M.; Zhang, J.; Li, Y. Confidential Information Ensurance through Physical Layer Security in Device-to-Device Communication. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–7.
78. Archana, B.; Chandrashekar, A.; Bangi, A.G.; Sanjana, B.; Akram, S. Survey on usable and secure two-factor authentication. In Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017; pp. 842–846.
79. Waqas, M.; Tu, S.; Halim, Z.; Rehman, S.U.; Abbas, G.; Abbas, Z.H. The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. *Artif. Intell. Rev.* **2022**, *55*, 5215–5261. [CrossRef]
80. Nadeem, M.; Arshad, A.; Riaz, S.; Band, S.S.; Mosavi, A. Intercept the Cloud Network From Brute Force and DDoS Attacks via Intrusion Detection and Prevention System. *IEEE Access* **2021**, *9*, 152300–152309. [CrossRef]
81. Safdar Malik, T.; Siddiqui, M.N.; Mateen, M.; Malik, K.R.; Sun, S.; Wen, J. Comparison of Blackhole and Wormhole Attacks in Cloud MANET Enabled IoT for Agricultural Field Monitoring. *Secur. Commun. Netw.* **2022**, *2022*, 4943218. [CrossRef]
82. Dwivedi, R.K.; Saran, M.; Kumar, R. A survey on security over sensor-cloud. In Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 10–11 January 2019; pp. 31–37.
83. Halim, Z.; Sulaiman, M.; Waqas, M.; Aydın, D. Deep neural network-based identification of driving risk utilizing driver dependent vehicle driving features: A scheme for critical infrastructure protection. *J. Ambient. Intell. Humaniz. Comput.* **2023**, *14*, 11747–11765. [CrossRef]
84. Tu, S.; Huang, X.; Huang, Y.; Waqas, M.; Rehman, S.U. SSLSS: Semi-Supervised Learning-Based Steganalysis Scheme for Instant Voice Communication Network. *IEEE Access* **2018**, *6*, 66153–66164. [CrossRef]
85. Namasudra, S.; Devi, D.; Kadry, S.; Sundarasekar, R.; Shanthini, A. Towards DNA based data security in the cloud computing environment. *Comput. Commun.* **2020**, *151*, 539–547. [CrossRef]
86. Kaur, R.; Chana, I.; Bhattacharya, J. Data deduplication techniques for efficient cloud storage management: A systematic review. *J. Supercomput.* **2018**, *74*, 2035–2085. [CrossRef]
87. Namasudra, S. An improved Attribute-based Encryption technique towards the data security in cloud computing. *Concurr. Comput. Pract. Exp.* **2019**, *31*, 4364. [CrossRef]
88. Kumar, S.; Jafri, S.A.A.; Nigam, N.; Gupta, N.; Gupta, G.; Singh, S.K. A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *748*, 012026. [CrossRef]
89. Derhab, A.; Belaoued, M.; Guerroumi, M.; Khan, F.A. Two-Factor Mutual Authentication Offloading for Mobile Cloud Computing. *IEEE Access* **2020**, *8*, 28956–28969. [CrossRef]
90. Esiner, E.; Datta, A. Two-factor authentication for trusted third party free dispersed storage. *Future Gener. Comput. Syst.* **2019**, *90*, 291–306. [CrossRef]
91. Vassilev, V.; Phipps, A.; Lane, M.; Mohamed, K.; Naciscionis, A. Two-factor authentication for voice assistance in digital banking using public cloud services. In Proceedings of the 2020 10th International Conference on Cloud Computing, Data Science Engineering (Confluence), Noida, India, 29–31 January 2020; pp. 404–409.
92. Saxena, M.A.; Ubnare, G.; Dubey, A. Virtual Public Cloud Model in Honeypot for Data Security: A New Technique. In Proceedings of the 2019 5th International Conference on Computing and Artificial Intelligence, Bali, Indonesia, 19–22 April 2019; pp. 66–71.

93. Negi, P.S.; Garg, A.; Lal, R. Intrusion detection and prevention using honeypot network for cloud security. In Proceedings of the 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 29–31 January 2020; pp. 129–132.
94. Wang, J.; Chen, X. Efficient and secure storage for outsourced data: A survey. *Data Sci. Eng.* **2016**, *1*, 178–188. [CrossRef]
95. Pape, S.; Stankovic, J. An Insight into Decisive Factors in Cloud Provider Selection with a Focus on Security. In *Computer Security*; Springer: Cham, Switzerland, 2019; pp. 287–306.
96. Mani, G.; Ulybyshev, D.A.; Bhargava, B.K.; Kobes, J.; Goyal, P. Autonomous Aggregate Data Analytics in Untrusted Cloud. In Proceedings of the 2018 IEEE First International Conference on Artificial Intelligence and Knowledge Engineering AIKE, Laguna Hills, CA, USA, 26–28 September 2018; pp. 138–141.
97. Norman, S.; Chase, J.; Goodwin, D.; Freeman, B.; Boyle, V.; Eckman, R. A condensed approach to the cyber resilient design space. *Insight* **2016**, *19*, 43–46. [CrossRef]
98. Yu, J.; Ren, K.; Wang, C. Enabling cloud storage auditing with verifiable outsourcing of key updates. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1362–1375. [CrossRef]
99. Shen, W.; Yu, J.; Xia, H.; Zhang, H.; Lu, X.; Hao, R. Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium. *J. Netw. Comput. Appl.* **2017**, *82*, 56–64. [CrossRef]
100. Vijayakumar, K.; Suchitra, S.; Shri, P.S. A secured cloud storage auditing with empirical outsourcing of key updates. *Int. J. Reason.-Based Intell. Syst.* **2019**, *11*, 109–114. [CrossRef]
101. Shin, Y.; Koo, D.; Yun, J.; Hur, J. Decentralized server-aided encryption for secure deduplication in cloud storage. *IEEE Trans. Serv. Comput.* **2017**, *13*, 1021–1033. [CrossRef]
102. Rabaninejad, R.; Sedaghat, S.M.; Attari, M.A.; Aref, M.R. An ID-Based Privacy-Preserving Integrity Verification of Shared Data Over Untrusted Cloud. In Proceedings of the 2020 25th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Iran, 1–2 January 2020; pp. 1–6.
103. Thokchom, S.; Saikia, D.K. Privacy preserving integrity checking of shared dynamic cloud data with user revocation. *J. Inf. Secur. Appl.* **2020**, *50*, 102427. [CrossRef]
104. Wang, B.; Li, B.; Li, H. Knox: Privacy-preserving auditing for shared data with large groups in the cloud. In Proceedings of the International Conference on Applied Cryptography and Network Security, Singapore, 26–29 June 2012; pp. 507–525.
105. Tang, H.; Cui, Y.; Guan, C.; Wu, J.; Weng, J.; Ren, K. Enabling ciphertext deduplication for secure cloud storage and access control. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–3 June 2016; pp. 59–70.
106. Majumdar, S.; Madi, T.; Wang, Y.; Jarraya, Y.; Pourzandi, M.; Wang, L.; Debbabi, M. User-level runtime security auditing for the cloud. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 1185–1199. [CrossRef]
107. Mercl, L.; Sobeslav, V.; Mikulecky, P.; Macinka, M. Infrastructure Authentication, Authorization and Accounting Solutions for an OpenStack Platform. In Proceedings of the International Conference on Mobile Web and Intelligent Information Systems, Istanbul, Turkey, 26–28 August 2019; pp. 123–135.
108. Wang, S.; Wang, H.; Li, J.; Wang, H.; Chaudhry, J.; Alazab, M.; Song, H. A Fast CP-ABE System for Cyber-Physical Security and Privacy in Mobile Healthcare Network. *IEEE Trans. Ind. Appl.* **2020**, *56*, 4467–4477. [CrossRef]
109. Badri, H.; Bahreini, T.; Grosu, D.; Yang, K. Multi-stage stochastic programming for service placement in edge computing systems: Poster. In Proceedings of the Second ACM/IEEE Symposium on Edge Computing, San Jose, CA, USA, 12–14 October 2017; pp. 1–2.
110. Marwan, M.; AlShahwan, F.; Sifou, F.; Kartit, A.; Ouahmane, H. Improving the Security of Cloud-based Medical Image Storage. *Eng. Lett.* **2019**, *27*, 175–193.
111. Wang, B.; Li, B.; Li, H. Panda: Public auditing for shared data with efficient user revocation in the cloud. *IEEE Trans. Serv. Comput.* **2013**, *8*, 92–106. [CrossRef]
112. Chi, P.W.; Lei, C.L. Audit-free cloud Storage via deniable Attribute-based Encryption. *IEEE Trans. Cloud Comput.* **2015**, *6*, 414–427. [CrossRef]
113. Khalili, M.; Dakhilalian, M.; Susilo, W. Efficient chameleon hash functions in the enhanced collision resistant model. *Inf. Sci.* **2020**, *510*, 155–164. [CrossRef]
114. Ramesh, S.; Govindarasu, M. An efficient framework for privacy-preserving computations on encrypted IoT data. *IEEE Internet Things J.* **2020**, *7*, 8700–8708. [CrossRef]
115. Chi, P.W.; Wang, M.H. Privacy-Preserving Broker-ABE Scheme for Multiple Cloud-Assisted Cyber Physical Systems. *Sensors* **2019**, *19*, 5463. [CrossRef] [PubMed]
116. Varadharajan, V.; Tupakula, U. Security as a service model for cloud environment. *IEEE Trans. Netw. Serv. Manag.* **2014**, *11*, 60–75. [CrossRef]
117. Tu, S.; Yu, H.; Badshah, A.; Waqas, M.; Halim, Z.; Ahmad, I. Secure Internet of Vehicles (IoV) with Decentralized Consensus Blockchain Mechanism. *IEEE Trans. Veh. Technol.* **2023**, *72*, 11227–11236. [CrossRef]
118. Glory, H.A.; Anusha, S.; Revathy, P.; Sandhya, G. Audit-Free Cloud Storage Via Randomized Key Protocol. *Int. J. Contemp. Res. Comput. Sci. Technol.* **2016**, *2*, 585-587.
119. Tubaishat, A. Security in Cloud Computing: State-of-the-Art, Key Features, Challenges, and Opportunities. In Proceedings of the 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, 23–25 February 2019; pp. 311–315.

120. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2018**, *78*, 680–698. [CrossRef]
121. Alarifi, A.S. Information Privacy in the Cloud: Actual and Expectation. In Proceedings of the RSEP Conferences, Madrid, Spain, 10–12 September 2019; p. 51.
122. Sgandurra, D.; Lupu, E. Evolution of attacks, threat models, and solutions for virtualized systems. *ACM Comput. Surv. (CSUR)* **2016**, *48*, 1–38. [CrossRef]
123. 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]
124. Subramanian, N.; Jeyaraj, A. Recent security challenges in cloud computing. *Comput. Electr. Eng.* **2018**, *71*, 28–42. [CrossRef]
125. Tian, H.; Chen, Z.; Chang, C.C.; Huang, Y.; Wang, T.; Huang, Z.; Cai, Y.; Chen, Y. Public audit for operation behavior logs with error locating in cloud storage. *Soft Comput.* **2019**, *23*, 3779–3792. [CrossRef]