electronics

MDPI

Article

Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey

Waqas Ahmad [1], Aamir Rasool [2], Abdul Rehman Javed [1], Thar Baker [3,*] and Zunera Jalil [1]

[1] Department of Cyber Security, Air University, Islamabad 44000, Pakistan; waqaskhattak99@gmail.com (W.A.); abdulrehman.cs@au.edu.pk (A.R.J.); Zunera.jalil@mail.au.edu.pk (Z.J.)
[2] Institute of Avionics and Aeronautics, Air University, PAF Complex, E-9, Islamabad 44000, Pakistan; aamir.rasool.au@gmail.com
[3] Department of Computer Science, College of Computing and Informatics, University of Sharjah, Sharjah P.O. Box 27272, United Arab Emirates
* Correspondence: tshamsa@sharjah.ac.ae

Abstract: Cloud computing provides the flexible architecture where data and resources are dispersed at various locations and are accessible from various industrial environments. Cloud computing has changed the using, storing, and sharing of resources such as data, services, and applications for industrial applications. During the last decade, industries have rapidly switched to cloud computing for having more comprehensive access, reduced cost, and increased performance. In addition, significant improvement has been observed in the internet of things (IoT) with the integration of cloud computing. However, this rapid transition into the cloud raised various security issues and concerns. Traditional security solutions are not directly applicable and sometimes ineffective for cloud-based systems. Cloud platforms' challenges and security concerns have been addressed during the last three years, despite the successive use and proliferation of multifaceted cyber weapons. The rapid evolution of deep learning (DL) in the artificial intelligence (AI) domain has brought many benefits that can be utilized to address industrial security issues in the cloud. The findings of the proposed research include the following: we present a comprehensive survey of enabling cloud-based IoT architecture, services, configurations, and security models; the classification of cloud security concerns in IoT into four major categories (data, network and service, applications, and people-related security issues), which are discussed in detail; we identify and inspect the latest advancements in cloud-based IoT attacks; we identify, discuss, and analyze significant security issues in each category and present the limitations from a general, artificial intelligence and deep learning perspective; we provide the technological challenges identified in the literature and then identify significant research gaps in the IoT-based cloud infrastructure to highlight future research directions to blend cybersecurity in cloud.

Keywords: cloud computing; IoT security; cybersecurity; cloud configuration; deep learning; machine learning; attacks; attack prevention; platform as a service (PaaS); infrastructure as a service (IaaS); software as a service (SaaS); development as a service (DaaS); forensic as a service (FaaS)

Citation: Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics* **2022**, *11*, 16. https://doi.org/10.3390/electronics11010016

Academic Editors: Carsten Maple, Matthew Bradbury and Munam Ali Shah

Received: 28 October 2021
Accepted: 18 December 2021
Published: 22 December 2021

1. Introduction

An internet of things (IoT)-based cloud infrastructure is an extensive network that includes several IoT-supported applications and devices. The infrastructure includes servers and storage, underlying infrastructure, real-time processing, and operations. An IoT-based cloud infrastructure also includes standards and services essential for securing, managing, and connecting different IoT applications and devices. Figure 1 depicts the typical IoT architecture, and Figure 2 provides the overview of IoT-based cloud attack model. The emergence of the cloud has been seen in the recent decade, and its variants are still rising in the new decade [1–3]. We see IoT taking the lead among these variants, the internet of things (IoT). In contrast, others, such as service architectures, distributed cloud

environments, data center operations, and management areas, follow it in recent trends [4]. In a recent article published by Gartner [5], cloud computing is included in the top ten strategic technology trends for 2020, with the cloud service market forecasted to grow by 17% in 2020.

Figure 1. Typical IoT architecture.

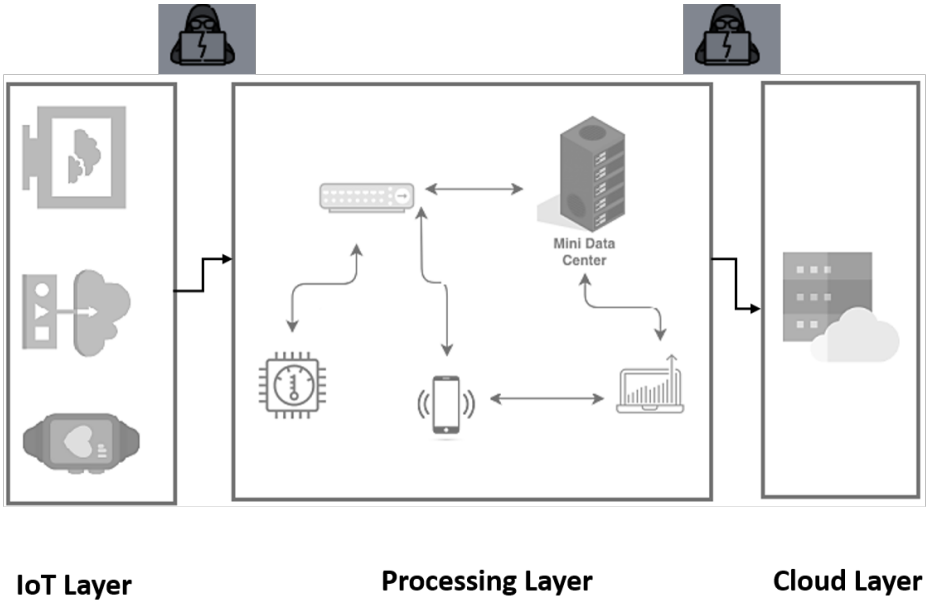

Figure 2. IoT-based cloud attack model.

The term cloud computing was used in the 1990s for the first time as reported in [6] where it referred to the platforms for distributed computing. For example, Elastic Compute Cloud (EC2) was created by Amazon in 2006 [7]. Similarly, the beta version of Google App Engine was released by Google in 2008 [8]. For deployment of hybrid and private clouds in 2008, NASA launched the first open-source software called OpenNebula [9]. Microsoft released Microsoft Azure in 2008 [10], and in 2010, OpenStack was launched, which was an open-source cloud-software initiative [11]. In 2011, IBM came up with the IBM smart cloud framework. Following that, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) were offered by the first Oracle Cloud in 2012. This journey is still persistent now, with more improvements emerging on the horizon of the internet world. The timeline of cloud computing history is shown in Figure 3.

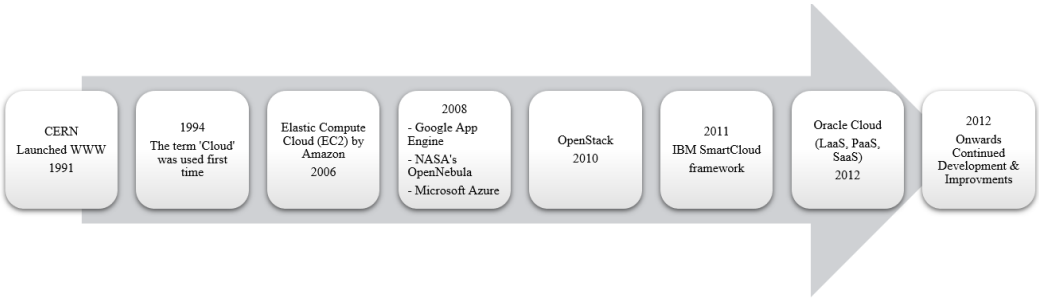

Figure 3. Cloud computing history.

Five key characteristics of cloud computing are identified by the National Institute of Standards and Technology (NIST) [12]. They are (1) measured service, (2) resource pooling, (3) rapid expansion, (4) network access, and (5) on-demand self-service. In addition, four deployment models and three service models are listed to deliver cloud services while working together. Cloud computing mainly aims to provide computing services, such as servers, storage, databases, networking, software, analytics, and intelligence, on the internet. Users can receive the type and amount of services as per their needs. Traditional IT services have shifted to the cloud due to cost effectiveness, convenience, and flexibility in work, along with quick data storage and access. With cloud computing, industries are not required to buy expensive hardware and software to set up physical on-site data centers. Cloud technologies automate industries by storing their software systems and services on remote servers. Most industries now adopt this trend and now increasing with every passing year [13].

Cloud computing provides scalability and regular updates on software and hardware for a vast number of industrial applications [14–16]. In addition, the cloud enables the user to make efficient utilization of network resources and provides a range of security solutions. With these advantages, it is evident that the prospect of cloud computing has great potential. Cloud computing and underlying technologies provide many potential opportunities for industries, and it can open up a wide range of applications, solutions, services, platforms, and more in the future. Large datasets and training algorithms can be ingested by using DL cloud computing. Its application can also allow DL models to achieve efficiency on a scale at a low cost, using the processing power of GPU.

The success of any cloud-based solution is heavily reliant on providing the best experience to cloud administrators, software developers, and end-users. There are specific barriers to the adoption of clouds, such as complexity, compliance, security, reliance, privacy, control, and cost [17]. Security in cloud computing is considered a crucial barrier since data and applications may reside at multiple layers depending on the chosen cloud service model. This uncertainty led researchers to consider security as the number one concern with cloud computing [18]. Gartner [19] mentioned four trends impacting cloud adoption in January 2020, where distributed multi-cloud scenarios are more commonly used. Handling associated security and privacy issues are one of them.

Cloud offers the distribution of heterogeneous data and resources along with virtual environments. In a traditional software infrastructure of businesses, a user can only use the resources available to them (i.e., storage space, computation capabilities, and hardware), whereas in cloud computing, a user can enjoy unlimited storage space and more server resources when required. Traditional approaches for user identification, authentication, access management are not adaptable for the cloud in their current form. External data storage, less user control, integrated models, and architectures are significant areas of security concern. The most significant concern for security and privacy in cloud-based systems is protecting data. If this is compromised, then the private information of each user will be at risk, resulting in an increasing number of cybercrimes affecting individuals, organizations, and states.

Crypto-jacking, denial of service, accounts theft, and data breaches are common threats. As reported in Forbes [20], Skybox Security released a Vulnerability and Threat Trends Report in mid-2019, with the key finding as a rapid increase in the number of vulnerabilities in cloud containers (a replacement of traditional VMs architecture). Compared to the traditional architecture of storage, data are more susceptible to attacks in the cloud. This is because cloud providers only secure the cloud platform, not the customer data. As per the Oracle and KPMG Cloud Threat Report 2019, 82% of cloud users have experienced security events [21]. Thus, it has become essential to ensure security and privacy over the cloud.

Security is considered the most important factor to make cloud computing a success story [22]. The location of data was identified as a security concern in 2011 [23]. Data security concerns were discussed [24,25]. Trust is another factor that researchers focused on since it is directly linked with the legitimacy of cloud service providers. The provision of the trust model and then trust management were key concerns. Inherent security issues in cloud computing result in the trust being the most significant factor for cloud computing [26]. The attacks faced by traditional systems on data are equally applicable and faced in cloud-based systems. The security of the virtual machine was discussed and was highlighted to be significant for the security of cloud computing and integrity of data in it [27].

Ref. [28] presents a review of the past five years research articles worked on the applications of consumer-oriented IoT cloud for the understanding of smart IoT cloud systems. The author presented a novel model for the IoT cloud and conducted a security analysis of the IoT cloud system. Ref. [29] presents a framework for the analysis of the privacy and security issues in social networks based on cloud systems. For different cyber-attacks in cloud systems from a technical viewpoint, [30] examines both under-explored and common security threats related to the cloud system.

A threefold analysis on the issues in cloud computing was reported in [31]. This threefold study analyzed the existing challenges of security surrounding cloud computing. In addition, the research proposed implications for the adoption of cloud computing in light of these challenges. Furthermore, authors in [32] presented another detailed survey of a security issue by presenting a comparative analysis of the threats being encountered by cloud platforms as well as comparing various intrusion detection and prevention techniques being used. Furthermore, for a real-time cloud-based environment, [33] discussed the real-life implementation of techniques of query processing over encrypted data in a high throughput cloud-based environment. Finally, [34] in 2016, proposed multi-dimensional mean failure cost (M2FC), which was identified as a quantitative security risk assessment model against the security problems discussed by these researchers. They also proposed appropriate countermeasures to solve identified security problems.

Authors in [35] discussed security-related challenges in cloud computing, the internet of things and discussed accountability in the cloud. Authors in [36] looked at the factors affecting cloud computing acceptance, attacks, and proposed solutions for strengthening privacy and security in cloud-based environments. Authors in [37] presented a detailed survey on the work related to cloud security issues, vulnerabilities, threats, and attacks and proposed an arrangement for their classification. Authors in [38] identified privacy schemes in IoT-based cloud-based systems to protect data more vigorously. Finally, authors in [39] presented a review of the critical security issues in IoT-based cloud computing and cloud infrastructures.

1.1. Methodology

The proposed research survey is conducted based on existing research studies. We build a proper paper selection strategy mechanism. Based on the following screening mechanism, we select papers from different sources.

1. For the proposed survey, we collect IoT-based cloud computing papers from the timeline of 2015–2021.
2. Research studies not published in English are excluded.

3. The research studies not relevant to the IoT-based cloud computing survey scope are excluded.
4. The main focus during paper selection is IoT-based cloud security and privacy.
5. The research papers published on the same idea are eliminated to remove redundancy.
6. We focus on the papers that performed experiments on the IoT-based cloud infrastructure.

1.2. Quality Analysis Criteria

The selected research studies for the proposed survey are passed through several quality analysis criteria to ensure efficiency. For the survey, we select 100+ research studies from different sources. With the help of the following quality analysis criteria, the selected papers are cross-checked.

1. Does the selected research contribute to the proposed survey?
2. Does the selected research belong to the survey scope? Does the selected research follow appropriate research standards?
3. Does the selected research results are cleared?
4. Does the author use appropriate techniques and features?
5. Does the selected research objectives are clearly stated?
6. Does the selected research focus on IoT-based cloud security?
7. Does the selected research perform any experiments related to IoT-based cloud?
8. Does the selected research share experiments details?

1.3. Contributions

Several researchers previously explored and highlighted privacy and security issues involving IoT cloud computing. However, existing surveys [40–42] present security issues in general or have focused on studies based on only a few factors. The following are the main contributions of this paper:

1. The research presents a consolidated survey on IoT cloud architecture, services, configurations, and security models. Additionally, we classify IoT cloud security concerns into four major categories: data, network and service, applications, and people-related security issues.
2. The research identifies and inspects the latest advancements and trends in IoT cloud-based attacks.
3. The research identifies, discusses, and analyzes significant security issues in each group and identifies the general limitations of AI, specifically DL.
4. Furthermore, the research discusses technological challenges identified in the literature and the future directions at the intersection of cybersecurity and cloud.

1.4. Paper Structure

The rest of the paper follows the following structure. Section 2 provides the background about cloud architectures, cloud types, and SPI model. Section 3 provides a detailed overview of relevant work to security issues in cloud computing in the past. Section 4 provides the cloud configuration. Section 5 provides detail about cloud-based attacks. Section 6 presents details about security issues. Next, Section 7 presents challenges and limitations in cloud computing. Future work is presented in Section 8. Finally, the last Section 9 concludes our discussion about highlighted security issues. Table 1 presents the list of notations used in this research paper.

Table 1. List of Notation.

Abbreviation	Description
AI	Artificial Intelligence
AES	Advanced Encryption Standard
APIs	Application Programming interfaces
CBC-MAC	Cipher Block Chaining Message Authentication Code
CIA	Confidentiality, Integrity and Availability
DDoS	Distributed Denial of Service
DSA	Digital Signature Algorithm
DaaS	Development as a Service
DL	Deep Learning
ECDSA	Elliptic Curve Digital Signature Algorithm
EC2	Elastic Compute Cloud
FaaS	Forensic as a Service
GDPR	General Data Protection Regulation
HMAC	Hash-based Message Authentication Code
IoT	Internet of Things
IDPS	Intrusion Detection Prevention System
IaaS	Infrastructure as a Service
KPMG	Klynveld Peat Marwick Goerdeler
LDAP	Lightweight Directory Access Protocol
ML	Machine Learning
NIST	National Institute of Standards and Technology
NCC-SRA	NIST Cloud Computing Security Reference Architecture
PaaS	Platform as a Service
PKI	Public Key Infrastructure
QoS	Quality of Service
SAAS	Software as a Service
SLR	Systematic Literature Review
SLA	Service Level Agreement
SSL	Secure Socket Layer
SDLC	Software Development Life Cycle
TTP	Trusted Third Party
VM	Virtual Machine

2. Background

Cloud computing, along with IoT, has emerged as the most popular technology in recent years [43]. With the current trends, the pace of expansion in digital technologies is anticipated to be exponential, where the integration of these two technologies can promise efficient management of resources. This section provides a brief overview of existing cloud architectures, cloud types, deployment models, and associated attacks before getting into security issues and challenges.

In the modern era of IoT-based cloud computing, a new type of DDoS has emerged; the attack is known as economic denial of sustainability (EDoS) [44]. EDoS could be defined as increased wear of flexible packaging, taking the server-shared measurement service as

an example (something cloud server). EDoS attacks can be carried out by remote sensing robots reloading target cloud service with a hidden vulnerability detector request. This way, cloud services will be available to students with scalable personalization. To get a customer account, follow the pay-as-you-go principle. Then, charge for these erroneous orders by forcing the customers to accept cloud services. These shortcomings will have the most terrible impact. This will lead to the loss of cloud computing customers, such as the customer preferring to choose the cheaper and more efficient method and supporting business from the headquarters and data center instead of sending unrealistic requests to the cloud [45].

2.1. Cloud Architectures and Deployment

Cloud architecture comprises different cloud components, such as data centers, software features, services, and applications, organized in an optimum way to solve small- and large-scale business problems. Cloud architecture aims to provide end-users with high bandwidth, uninterrupted access to their data and applications, on-demand network with adaptability and security [46–50]. Cloud architecture usually lays down the components and the interactions amid those components. A few key components of generic cloud architecture are as follows: (1) data and resources available with the client, (2) data and resources available on the cloud, (3) software components and services, and (4) middleware.

The purpose and environment of the cloud can be determined based on its deployment model. The deployment model comprises different cloud types, namely public and private, hybrid and multi-cloud (shown in Figure 4):

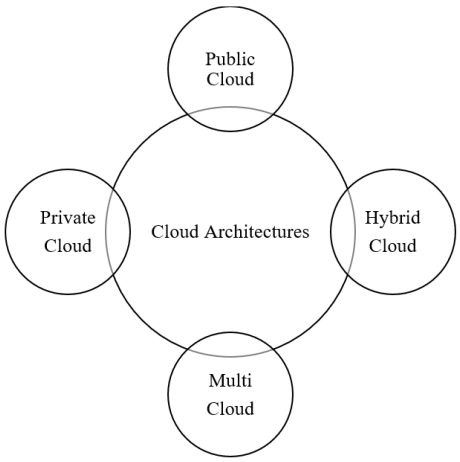

Figure 4. Types of cloud architectures.

Figure 5 also illustrates a three-dimensional approach of NCC-SRA for data collection, aggregation and data classification with respect to cloud type.

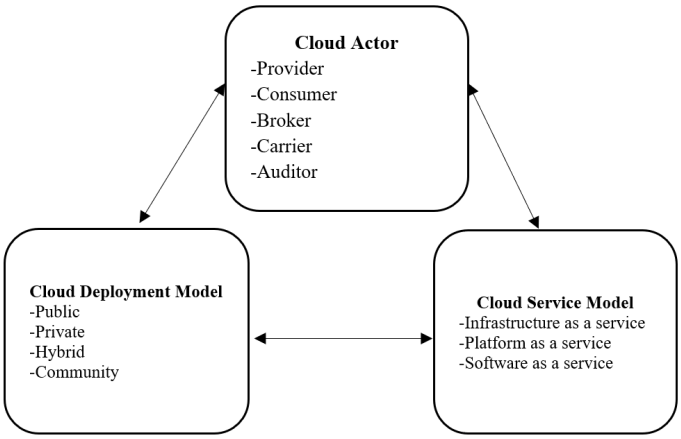

Figure 5. Three-dimensional approach of NCC-SRA from NIST Cloud Computing Security Reference Architecture [51].

2.1.1. Public Cloud

Different organizations own and operate a public cloud in this type of cloud. Many thousands of individuals and organizations (many thousands) use these resources, infrastructures, and networks simultaneously. Google, Amazon, and Microsoft are some of the renowned public cloud providers. In this type of cloud, resource allocation, ownership detection, shared access management, and cloud data security from attacks are key concerns. The advantages of utilizing public clouds are reliability, location independence, utility-style costing, cost effectiveness, high scalability, and flexibility. Disadvantages of using the public cloud are minor customization, and low-security [52].

2.1.2. Private Cloud

This kind of cloud is typically owned by a sole organization and is more specifically designed as per the needs of that organization. Private cloud storage allows organizations to control their data better (maybe susceptible to regulatory compliance requirements). It can be managed and hosted internally or by a third party. This data can also be medical records, trade secrets, or other classified information. The same organization owns and operates the infrastructure. In private cloud solutions, the organization either controls or uses the infrastructure, or the cloud service/infrastructure provider provides them with the necessary service. Security is critical in private cloud, as compared to other cloud environments [53]. User and vendor identification and handling security-related risks are easier than in a public cloud. The advantages of utilizing a private cloud are greater security, more privacy, and greater control, cost, and energy efficiency. Disadvantages of using private cloud include inflexible pricing and less scalability due to limited resources [52].

2.1.3. Hybrid Cloud

One or more external clouds accompanies a private cloud-connected in the hybrid cloud model. In this way, multiple cloud environments, having workload portability and management, are bound together and managed centrally. For example, an organization can keep confidential data in the private cloud and data with general classification at the public cloud and manage security between the two. Hybrid cloud security is considered more reliable than the public cloud's security. The advantages of using a hybrid cloud are flexibility, scalability, security, and cost efficiency. Disadvantages of hybrid clouds include security compliance and networking issues [52].

2.1.4. Multi Cloud

This model has a system with more than one cloud. Clouds may be public or private, and they may not necessarily be linked together. In literature, this is referred to as a community cloud as well. The advantages of utilizing a multi-cloud are better security

than public cloud and resource sharing. Disadvantages include less security than private cloud and the requirement of governing policies for administration [52].

Each of the clouds' architectures, as mentioned above, has its pros and cons. The choice of model depends on the user and organization requirements related to storage, availability, efficiency, and security. The private cloud, for example, offers comprehensive control over the user experience, availability, and better security, whereas the public cloud is less secure and more prone to cyberattacks.

2.2. Cloud Services

Cloud computing facilitates users with various representations of service delivery, called PaaS, IaaS, SaaS, DaaS, and FaaS.

2.2.1. Software as a Service (SaaS)

In the SaaS model, the user is provided access to software and databases. Users can obtain information from applications [54]. This model renders applications in the cloud through a network, and the consumers do not need to install applications on their local computers [55]. The cloud provider installs, hosts, and runs software on the cloud, and access is provided to the user through the cloud client. This leads to multiple users getting served by a single service instance. The CSP operates the hosted application, which manages and warrants up-to-date running of the system [56]. Google Applications, Microsoft Office 365, Dropbox, and Trade card are a few examples of SaaS. Load balancing, multi-tenancy, and scalability are key advantages of SaaS.

2.2.2. Platform as a Service (PaaS)

In PaaS, the user is provided with application platforms and databases as a service. It combines the operating system and application servers, such as the LAMP platform (Linux, Apache, MySQL, and PHP), Google App Engine, Microsoft Azure. The PaaS model makes applications more effective and mainly emphasizes data protection. The cloud provider provides a platform that allows users to develop, run, and manage applications without the complexity of building and sustaining the infrastructure. By allowing the application–hosting environment, the users do not require any command over the underlying infrastructure that includes network, storage, and processing [57]. As a result, users experience reduced control and fewer operational features in this model.

2.2.3. Infrastructure as a Service (IaaS)

If the user is presented with online services to access, process, store, transfer, and execute their applications and data over the cloud, IaaS offers computing capabilities and storage as uniform services across the network. Computing resources are granted in the form of virtual machines (VMs), and storage resources are provided in two ways: block storage and object storage [58]. The user does not require the control or management of the underlying cloud infrastructure to practice control over OS, storage, and applications deployed; sometimes, there is restricted control on a few network components.

2.2.4. Development as a Service (DaaS)

In the DaaS model, a web-based community shared development tool is shared with multiple users. This is similar to experiencing a development tool on a local machine in a traditional model. This is a recent trend in the software development community.

2.2.5. Forensics as a Service (FaaS)

Cloud forensics has significant advantages over traditional digital forensics in terms of large (petabytes) storage for accumulating valuable forensic data and resources for high computation capability [59,60]. The FaaS model is explicitly designed to support forensic investigators when analyzing a large volume of data centrally where data are physically inaccessible or at an unknown physical location. Investigators continuously harvest data

and keep sending them to a centralized system. As a result, investigators can analyze a small subset of traces from huge stacks.

2.3. Information Disclosure

Some malicious activities can leak information to unauthorized users. Out of many ways to leak such information, VM configuration stealing can be identified as one [61,62]; it scans for open ports to discover services and their associated vulnerabilities [63]. Internal as well as external disclosure can happen in the cloud.

- An internal disclosure is the inadvertent making of private information public by an administrator or employee, which would lead to such disclosure. Lack of care and shredding or insufficient understanding of the sensitivity of information may result in such disclosures. The internal attacks can jeopardize certain users and allow absolute control over them [64].
- An external disclosure is the one which would target to acquire the provider's system-specific information. For example, it may include the backup files, temporary files, patch levels, version numbers, and software distribution. For preventing such attacks where the risk of information disclosure is there, third-party authentication and encryption methods are often used [64].

3. Related Work

Cloud computing has emerged during the last years at a rapid pace. As a result, several studies have addressed security threats, vulnerabilities, issues, challenges, and countermeasures. The related work security issues in cloud computing is covered in this section.

The authors in [65] discussed structures of cloud computing, security threats, issues, and solutions for them. The study also highlighted current deployment models, cloud services, and cloud architecture frameworks while discussing the assisting technologies. The findings of this study were used to identify open research directions in the cloud security domain, whereas in [41] the authors highlighted the importance of data security in cloud computing and discussed the cons of data leakages or breaches in cloud computing. Notwithstanding, [41] did not discuss how critical data are leaked and breached from cloud computing and also how the data leakage issues are solved.

The authors in [66] examined cloud computing architectures, service models, deployment models, cloud components, and security issues of the cloud but did not discuss the solution available in the literature for the identified security issues. The authors identified cloud security issues arising from data movement in the cloud. They argued about the effectiveness of the lightweight directory access protocol (LDAP), public key infrastructure (PKI), and the task of a trusted third party (TTP) as security solutions for guaranteeing availability, authenticity, confidentiality, and integrity of data during communications. Authors in [67] provided a qualitative analysis of all vulnerabilities and associated threats in each service model. They also proposed countermeasures to enhance security in cloud computing. In [67], the authors main focus is on the vulnerabilities and associated threats raised from the vulnerabilities. The authors did not discuss future research directions and current challenges raised due to the identified vulnerabilities and threats.

In [68], the authors identified a gap in the literature concerning the security issues' mapping to their corresponding solutions and identified the need for a common framework for generalizing the idea while conducting a detailed analysis of specific needs. The authors also discussed the open problems and future research directions. Authors in [69] performed a systematic literature review for identifying the relevant research done so far on resource scheduling and security in the cloud. In [69], the authors categorized different threats and their possible available solutions in the literature.

The authors in [70] highlighted various security challenges of cloud computing, types of cloud, and several service models of cloud computing. In [70] the author proposed some critical cloud challenges and future research directions based on the literature. Authors

in [71] focused on the identification of security issues in cloud computing that is a concern for both cloud service providers and users. They addressed cloud security by recognizing security requirements and proposing solutions to reduce these potential threats. Finally, the authors in [72] identified the importance of relevant security issues knowledge related to processes, people, and technology. They divided cloud security issues into three categories: processes, people, and technology. They also divided threats in these areas to managers and security divisions to solve the security problems.

DL claims triumph in many areas in cloud computing, such as biomedical data analysis, speech, and image recognition [73–76]. Data can be transformed into more abstract expressions and higher levels using DL. DL architectures are set up as multi-layer neural networks. Suppose the data are already in high dimension. In that case, data may be transformed into low quality by training various neural networks (NN) with a thin central layer to rebuild high dimension data input [77]. It was proposed that improved classification or data visualization can be achieved by the enhanced intrinsic characterization of the data from these characteristics. By using detailed data, functions can be split into simple functions that help understand formations. An exceptional feature of learning abilities was identified in the artificial neural network's multiple layers by [78]. These authors also identified the layer-by-layer "pretraining" procedure as optimization of weights in nonlinear auto-encoders as a method for overcoming the problem.

Authors in [79] discussed data security challenges with the perspective of a developing country, i.e., Nepal, in 2019. The study identified the challenges faced by developing countries, such as confidentiality, charging model, breaches, segregation, access, integrity, security, storage, data center operation, service level agreement, charging model, costing model, and locality. The findings of this research reported storage, virtualization, and networks as main security concerns. Authors in [80] analyzed the public cloud security protection method based on the security threat of public cloud and proposed security protection methods.

The researchers studied security issues in cloud computing from a different perspective. The rapidly evolving nature of clouds in today's world requires prompt identification of security issues and challenges. Some survey papers have identified issues according to the cloud architecture, whereas others have classified security issues based on people, processes, and technology. Some focused only on data security and privacy or have discussed security issues in general. There is a requirement to highlight and address emerging security issues in the cloud computing domain. Table 2 summarizes the details of similar surveys and papers published in the past about security issues in cloud computing.

Table 2. Summary of related work.

Year	Survey	Focus	Key Features and Limitations
2016	M. A. Khan et al. [32]	Security threats and their countermeasure	• Presented security threats and their countermeasure from the perspective of cloud security issues. • Categorized and analyzed the security issues and their solution. •Provide a comparison of several threats and attacks faced by cloud infrastructure. •Author does not provide any IoT-based framework for countermeasure identified attacks and threats in the IoT environment.
2016	Singh et al. [65]	Cloud security issues and their solution	• Discussed different cloud environment features, cloud threats, cloud security issues, and solutions. • Discussed important topics associated with the cloud, such as deployment model, services, technologies, architecture and framework, attacks and threats, and cloud security concepts. • Presented open research issues in cloud security. • Author does not provide any future research challenges associated with IoT-based cloud computing.

Table 2. *Cont.*

Year	Survey	Focus	Key Features and Limitations
2017	Mushtaq et al. [66]	Cloud design and deployment	• Cloud computing design included cloud components, deployment models, cloud security, and explored cloud service models. • Identified practical security challenges and potential threats. • Introduced the TTP to ensure security characteristics. • Did not present future research directions and challenges in IoT-based cloud computing.
2018	Basu et al. [68]	Cloud models and security	• Discussed different cloud properties and models from security perspectives. • Discussed cloud security issues and requirements in detail and proposed a novel methodology to countermeasure them. • Discussed cloud security issues and did not focus on future research directions from IoT-based cloud.
2019	Sheikh et al. [69]	Cloud situation categorization	• Provided systematic literature review to help the reader find relevant research articles on the associated topic. • Categorized literature into groups depends on the current situation to identify future research gaps. • Author did not discuss any IoT-based cloud framework and model and nor discussed cloud-related research challenges.
2019	Khandelwal et al. [70]	Cloud security issues and solution	• Created a list of cloud computing architecture that identifies security issues and finds solutions for the identified issues in cloud computing. • Lacks in proposing a methodology, current challenges, and future research directions.
2019	Ghaffari et al. [72]	Cloud security challenges	• Identified cyber security challenges and address the identified challenges to find feasible, efficient, and cost-effective security solutions. • Discussed cloud security issues but lacks future research directions.
2021	This survey	IoT cloud security issues, solution and categorization	• Presents a comprehensive survey of enabling cloud-based IoT architecture, services, configurations, and security models. • Classification of cloud security concerns in IoT into four major categories: data, network and service, applications, and people-related security issues, which are discussed in detail. • Identifies and inspects the latest advancements in cloud-based IoT attacks. • Identify, discuss and analyze significant security issues in each category and present limitations from general, artificial intelligence, and deep learning perspective. • Provides technological challenges identified in the literature and then identifies significant research gaps in IoT-based cloud infrastructure and highlights future research directions to blend cybersecurity in cloud.

4. Cloud Configuration

The cloud is configured to provide services to consumers by using a secure medium to ensure delivery and connection. According to NIST, the configuration process can be divided into five different responsibilities people perform at different positions. In Table 3, the configuration of the cloud is shown, and the entities with their responsibilities are described [81,82]. All the resources of the cloud company are used to satisfy the demands of consumers. The people at the five positions in Table 3 take part in duties such as transactions in cloud computing, which is the main reason cloud also focuses on threats and risk-assessment of cloud consumers and cloud providers.

Table 3. Responsibilities of different positions associated with cloud services.

No.	Position	Responsibilities
1	Cloud Consumer	Maintain relationship with entity and enable them to utilize cloud services.
2	Cloud Provider	Enable services to all consumers that are eligible.
3	Cloud Auditor	Assessment of services provided by cloud, performance of systems and security.
4	Cloud Broker	Manage the use, performance and delivery of service.
5	Cloud Carrier	Provide connection and transport cloud services.

4.1. Cloud Consumer

The word cloud consumer refers to a category of people who obtain services from cloud providers. The cloud consumer may be given many services from which he/she selects the suitable service and closes a contract. For closing a contract, the cloud consumer signs a service level agreement (SLA) with the cloud provider and then checks the technical performance of the service.

4.2. Cloud Provider

The word cloud provider refers to another category that offers services to cloud consumers and close deals on behalf of cloud organization. In SaaS, the services provided by cloud providers are deployment, maintenance, and updates of applications and software. On the other hand, in PaaS, the infrastructure and the environment components, such as the database, leading software, or any required component, are provided by the cloud software. The cloud provider obtains the physical computing resources, such as storage, server, networks, and hosting infrastructure.

4.3. Cloud Auditor

The cloud auditor is a group of people who can check the cloud services and inspect them independently for any exceptions. The auditing group inspects the standards by checking objective evidence items, and the cloud auditor also checks the privacy impacts, security controls, and performance of all the processes associated with the cloud.

4.4. Cloud Broker

The cloud broker is utilized for managing performance, usage, and cloud service delivery. Cloud consumers use cloud brokers to receive cloud services instead of contacting cloud providers directly.

4.5. Cloud Carrier

The cloud carrier creates a connection between the cloud provider and the cloud consumer. The cloud services are delivered to the consumer over the network by utilizing this connection. Furthermore, the cloud carrier is also responsible for maintaining a secure connection.

5. IoT-Based Cloud Attacks

Security over the cloud is mainly considered the responsibility of cloud providers. However, in recent years, more and more organizations have been shifting their businesses, data, and application over the cloud [83]. As a result, cyber-attackers have also changed their focus and now find cloud services a more lucrative target [84]. Figure 6 shows an illustration of the cloud components, attacks, and vulnerabilities that can be analyzed to exploit new weaknesses in the cloud system. Security risks in cloud computing are the most pressing worry when investing in cloud services. It is because the user's information is saved and processed by a third-party vendor without the user's knowledge. Every day,

the user hears about faulty authentication, compromised credentials, account hacking, data breaches, and other issues. Cloud computing in IoT is used to store IoT data and is utilized as a part of a cooperation. A cloud is a centralized server with computer resources that may be accessed at any time. Cloud computing is a convenient way to transport huge data packages created by the internet of things. In the traditional internet, the connection is made through physical links between web pages, but now, the combination of data is required for situation detection in the IoT. Table 4 presents the characteristics of IoT-based cloud attacks.

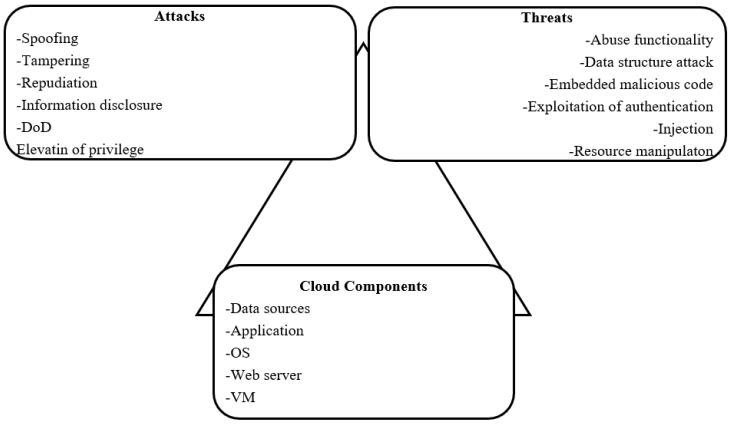

Figure 6. Attacks, threads, and components on cloud.

Table 4. Summary and characteristics of IoT-based cloud attacks.

Attacks and Threads	Description
Information Breaches	Security breaches and the use of protected data
Information Loss	Data loss as a result of poor handling
Service or Account Hijacking	Attacks on the system aimed at stealing information
Applications and API attacks	Attacks to expose software interfaces or APIs
Denial of service (DOS)	Attack on machine or network that make inaccessible to user
Malicious Insider	Any insider can utilize the system for malicious purposes
Abuse and nefarious use of cloud services	Using cloud services for nefarious purposes or misuse of cloud services
Insufficient diligence	Risk due to insufficient and shortage of cloud knowledge
Shared technology	Due to shared resources, there have been several attacks.

This section provides some of the most powerful IoT-based cloud attacks. Their prevention techniques on the cloud experienced in the last few years are given as follows:

5.1. Account Hijacking

This is a kind of attack in which the cloud account of an individual or organization is stolen or hijacked by an intruder. The attacker uses this stolen account information to perform another attack later, or sometimes the individual or organization is the main target. An attacker may conduct malicious or unauthorized activity later by performing impersonation that leads to business and sensitive personal information leaks and causes damage to reputation [85]. A graphical depiction of this attack is shown in Figure 7. Businesses and many organizations may take easy, effective actions to keep their data safe

in the cloud. Some of the simplest solutions to protect from cloud account hijacking are as follows:

- Verify your service provider to see if workers who have physical access to the server have been subjected to background checks.
- Have a reliable authentication strategy for cloud app clients.
- Disable the IP addresses from which cloud apps can be accessed. Several cloud application enables users to specify IP ranges, enabling them to utilize the company network or VPN to reach the app.

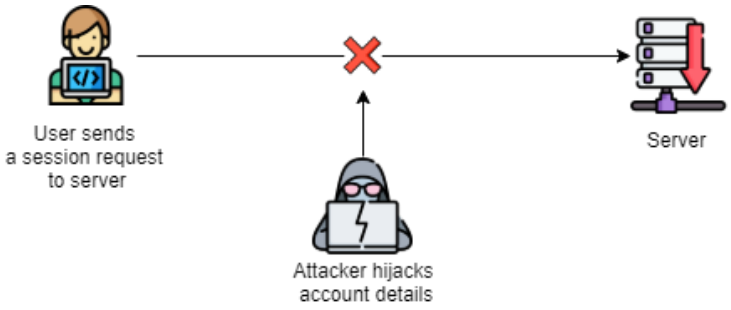

Figure 7. Graphical Representation of an account hijacking attack [85].

5.2. Denial of Service Attacks

Denial of service attacks on IoT systems are the most prevalent and easiest to implement. This kind of attack on the cloud can be pretty detrimental, as in this attack, the attacker makes the services, applications, or data inaccessible to the intended user [86]. The attacker performs this attack by flooding a targeted machine or application, or service with lots of requests until regular traffic becomes challenging to process, resulting in denial-of-service to other requesters. A graphical representation of the denial of service attack is represented in Figure 8. The main incentive behind this kind of attack is to drive the cloud service owner to raise the elasticity levels to handle the increased traffic and utilize more virtual resources to serve the request and ensure the quality of service (QoS), thus making it irresponsible ultimately. Furthermore, denial of service may act as an instigator and be used as a smokescreen to conceal the malicious activities circumventing the firewall of the cloud, and thus, can expand quickly to cause more damage instead of affecting one device [87]. DoS attacks are carried out to prevent users from gaining access to IoT, cloud networks, and other computer services. A denial of service (DoS) attack in IoT attempts to bring a system or network to a halt, rendering it unreachable to its intended users. DoS attacks are not easier to detect and avoid, but we highlight some methods to prevent DoS attacks:

Prevent spoofing: Check whether traffic has a source IP address that matches the list of addresses for the site of origin, and apply filters to prevent spoofing of dial-up connections.
Limit broadcasting: Attackers frequently make requests to all devices connected to the network, magnifying the attack. Attacks can be disrupted by limiting or shutting off broadcast forwarding whenever possible. When feasible, users can also turn off the echo and charge services.
Streamline incident response: When DoS attacks are identified, improving the incident response can assist the security team in responding quickly.
Protect endpoints: Check that these endpoints have been patched to address any known vulnerabilities. EDR agents should be deployed on all endpoints capable of running them.
Dial in firewalls: Whenever feasible, make sure the firewalls restrict entry and exit traffic across the perimeter.

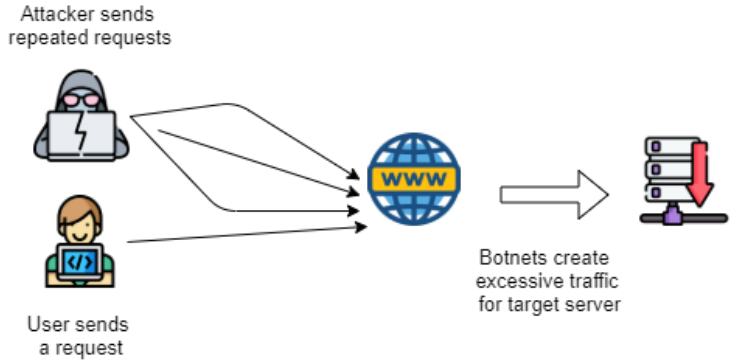

Figure 8. Graphical representation of a denial of service attack [87].

5.3. Phishing Attacks

Phishing attacks against cloud service providers lure users by sharing a document or picture with the victims and making them log in with their account information to access it. In this kind of attack, the attackers send phishing emails to collect individual or corporate account credentials and access their classified data to gain a position to perform the attack and evade their detection [88,89]. A graphical representation of this attack is depicted in Figure 9. Two types of phishing attacks can occur in a cloud computing environment. The first is hijacking the accounts by using conventional social designing techniques, and the second is abusive behavior in which the attacker utilizes some cloud services to host a phishing attack site [90]. So, how may phishing be avoided, and how might a cloud solution assist? To prevent the IoT device from phishing attacks, users need to take these steps.

- Be wary of each email or website.
- Before clicking on a link, verify it.
- Do not send any personal and business information by mail.
- Finally, reveal any suspicious activity to people in control of email and websites.

It is feasible to see how a cloud solution can help from this list. By limiting access to harmful files and screening incoming email, a cloud-based email system, for example, can discover and aid in defanging malware. It can also offer the two-way communication required to warn the user and others about phishing efforts. The information received also aids in tuning the software's response and improving phishing defense.

Figure 9. Graphical representation of a phishing attack [90].

5.4. Malware Injection Attacks

In a malware injection attack, the attacker tries injecting malicious applications and services into the cloud [91]. The attacker uses different methods to perform this attack, keeping in the view of the cloud model. First, the attacker produces its own malicious service application module or a virtual machine instance and attempts to supplement it to the cloud. Then, the attackers make an effort to make it a valid instance, then redirect the demands of the valid user to the malicious service application, and execute the malicious code [92]. A visual representation of the malware injection attack is shown in Figure 10. The attacker attempted to operate on the cloud platform, access user data, and resources, and manipulate data. Because cloud computing is extensively used and appreciated worldwide, IoT relies on it for data and resource storage. Mirai Malware is one such attack that infects the IoT devices, using their factory default login information.

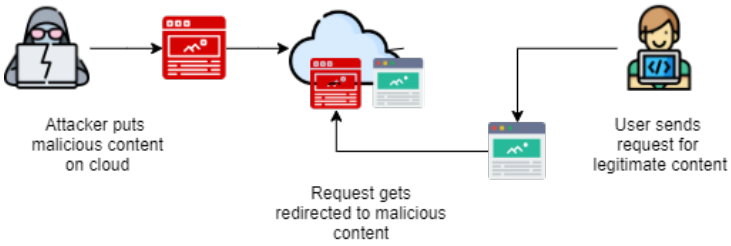

Figure 10. Graphical representation of a malware injection attack [92].

5.5. Port Scanning Attacks

In this kind of attack, open ports can be discovered by the attackers, which can cause an attack on the services running on the same ports [93]. This type of attack may result in a loss of confidentiality and integrity in the cloud [93,94]. A graphical representation of the port scanning attack is represented in Figure 11. The ability to prevent a port scan attack is dependent on having adequate, up-to-date threat information that is in sync with the growing threat landscape. Businesses also require robust security software, port scanning tools, and security alerts to monitor ports and avoid harmful actors from accessing their network. IP scanning, Nmap, and Netcat are all useful tools. Some of the defense mechanisms include the following:

A strong firewall: Unauthorized access to a company's private network can be prevented by using a firewall. It manages ports and their visibility, as well as recognizing when a port scan is underway and shuts it off.

TCP wrappers: Administrators can use these to grant or prohibit access to servers based on the IP address and domain names.

Uncover network holes: A port scanner can be used by businesses to check whether other ports are open unnecessarily. They must perform frequent system audits to identify any weak points or vulnerabilities that an attacker might exploit.

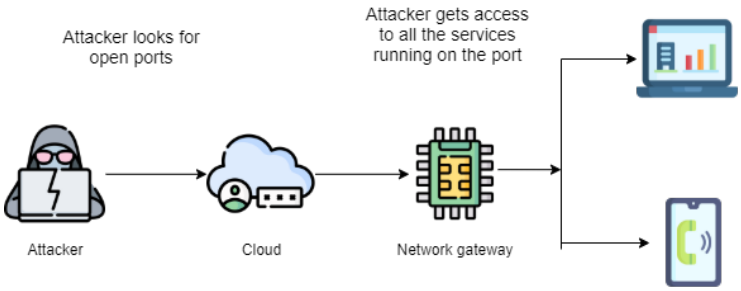

Figure 11. Graphical representation of a port scanning attack [93].

5.6. Man-in-the-Middle Attacks

Two parties are relied upon secretly by an attacker in a man-in-the-middle attack. Here, eavesdropping on the data can help the attacker modify the message. In addition, message relays can also be altered by the attacker [95]. This type of attack intends to obtain sensitive information being yielded, and then the attack can occur during an ongoing communication if the channel of communication is also compromised [96]. A graphical representation of this attack is depicted in Figure 12. Detecting man-in-the-middle attacks can be challenging depending on the vulnerability point employed, current IT security architecture, and users' understanding of possible IT security dangers—in this instance, prevention is far superior to treatment. Using a robust encryption mechanism between the client and the server is the best strategy to avoid a man-in-the-middle attack. The connection can be created only when the server authenticates a client's request by submitting and validating a digital certificate. When manufacturing IoT devices and releasing them to the market, IoT makers should keep identification and authentication in mind. Because a man-in-the-middle assault is all

about providing false information and posing as a device to another device or user, users need to have a mechanism to confirm that devices and people are whom they say they are when they interact. Furthermore, users need to take care of the following to prevent man-in-the-middle attacks:

- Implement virtual private networks (VPNs);
- Using HTTPS, the user can ensure that sensitive online transactions/logins are safe;
- Create separate Wi-Fi networks;
- Use SSL/TLS encryption to secure email;
- Install an intrusion detection system (IDS).

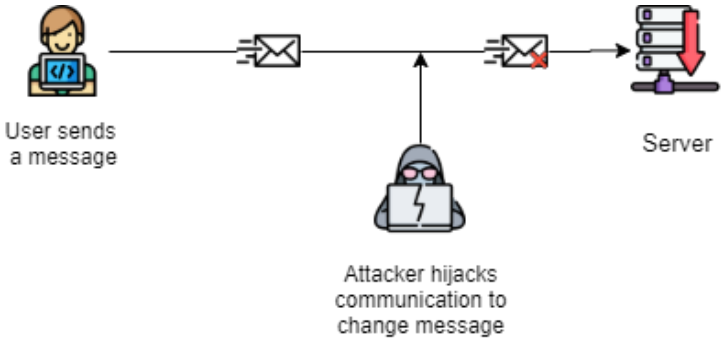

Figure 12. Graphical representation of a man-in-the-middle attack [96].

5.7. Botnet Attacks

In this type of attack against the cloud, a network of infected machines collectively controlled by cybercriminals performs malicious activities [97]. Botnets spread by working through a list of IP addresses and vigorously scanning the machines or network devices with vulnerabilities. Botnets pose a severe threat to user networks, businesses, and customers [98]. Botnets exploit the power of today's intelligent cloud computing platform and can use the user's network to perform malicious activities—distributed denial of service (DDoS), spamming, data stealing, and phishing attacks. In addition, a bot master can use cloud services to build botnets. Cloud-based botnets, also called bot-cloud, can be online in minutes and perform its task without interruptions. Attackers use botnets to launch attacks that are difficult to prevent or even detect [99], which makes it one of the most damaging attacks for the victim. A graphical representation of the botnet attack is shown in Figure 13. With several botnets on the cloud nowadays, prevention is critical, but that is not simple. Botnets are constantly changing in order to exploit vulnerabilities and security shortcomings. As a result, each botnet might be vastly different from another. Botnet operators are fully aware that the more IP addresses and devices they use in their attacks, the more difficult it is for bot defense solutions to reliably screen out bad requests for access to websites and APIs while simultaneously providing access to legitimate requests from customers or partners. Botnet assaults require advanced detection skills to identify and prevent them. Some of them are as follows:

- Keep the software up to date;
- Closely monitor the network;
- Keep track of unsuccessful login attempts.

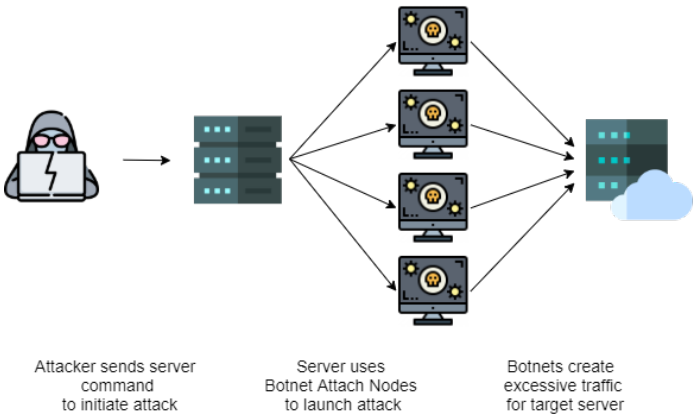

Figure 13. Graphical representation of a botnet attack [99].

5.8. VM Rollback Attacks

In this form of attack, a malicious hypervisor executes VM from its previous old snapshot without the user's knowledge [90]. Rolling back can disable security measures or patches taken in new versions. Furthermore, an attacker may use a brute-force technique to find the login password of a virtual machine, even if the guest operating system has a restriction on the number of failed trials [100]. A visual representation of a VM rollback attack is shown in Figure 14. In the IaaS platform, it is hard to differentiate between a normal suspend-resume and migration operation.

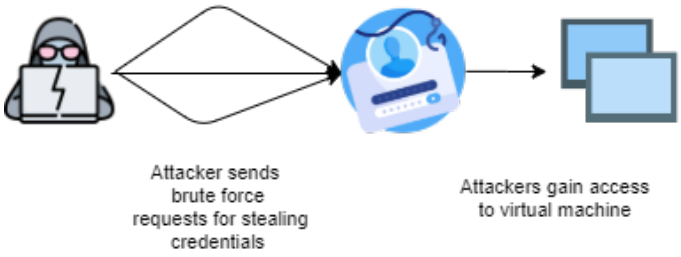

Figure 14. Graphical representation of a virtual machine rollback attack [100].

5.9. Crypto-Jacking Attack

This form of attack targets enterprise cloud environments that have a higher computational capacity [101]. By performing this attack, cybercriminals are interested in stealing computational resources from users' devices to mine or steal cryptocurrencies from digital wallets. Thus, cybercriminals drain off the money they make or steal into their private digital wallet by using these hijacked processors. In addition, these hijacked processors result in reduced CPU performance and sometimes increased electricity usage for processing. A graphical representation of a crypto-jacking attack is shown in Figure 15.

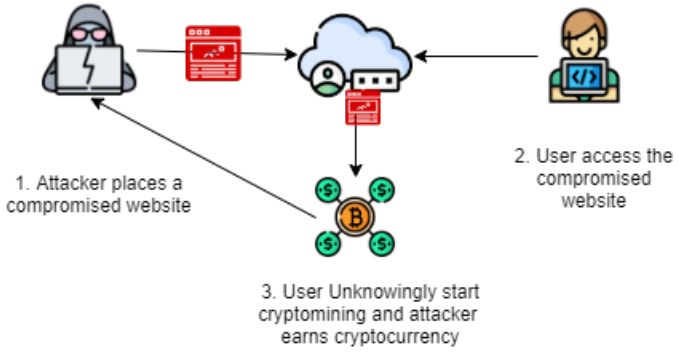

Figure 15. Graphical representation of a crypto-jacking attack [101].

5.10. Security Service

Table 5 shows some services that are used to protect our data concerning security perspective and a suitable example for a specific type of security. The security types are confidentiality, integrity, availability, authentication, and non-repudiation [102].

Table 5. Security type with respect to mechanism, with example.

Security Type	Mechanism	Example
Confidentiality	Secure Socket Layer (SSL) and Encryption	Advanced Encryption Standard (AES), RSA, Digital Signature Algorithm (DSA)
Integrity	Hash function, signature/authentication code	SHA-256,MD5, HMAC.
Availability	Intrusion Detection Prevention System (IDPS), Firewall	SNORT, Suricata.
Authentication	Endorsing certificate, SSL, Digital signature	Hash-based Message Authentication Code (HMAC), Elliptic Curve Digital Signature Algorithm (ECDSA), Cipher Block Chaining Message Authentication Code (CBC-MAC).
Non-repudiation	Public/Private block chain, notary	Email tracking.

6. Security Issues

This section identifies and discourses major cloud security issues and challenges. A security issue in the cloud is defined as something bad that can happen to digital assets residing over the cloud. These assets can be data, software, infrastructure, client trust, organization repute [103]. This paper place security issues in the following four categories: (1) data security issues, (2) network and services security issues, (3) applications security issues, and (4) people-related security issues. This categorization is made keeping in view the latest trends of attacks on cloud computing systems. A brief description of each category is presented in Table 6 and a summary in Figure 16.

Table 6. Categorization of security issues in cloud computing.

No.	Category	Description
C1	Data Security issues	Includes data security issues related to data storage, location, backup, integrity, access, and breaches.
C2	Network and Services related security issues	This category comprises security issues related to networks and services such as Service /Account hijacking, insider threats, virtualization, and multitenancy issues.
C3	Applications security issues	includes issues related to cloud-based applications such as malware injections, malicious insiders development life cycle, and UI issues.
C4	people-related security issues	Issues involving people such as trust management issues, compliance issues, human resource, and legal issues are included in this category.

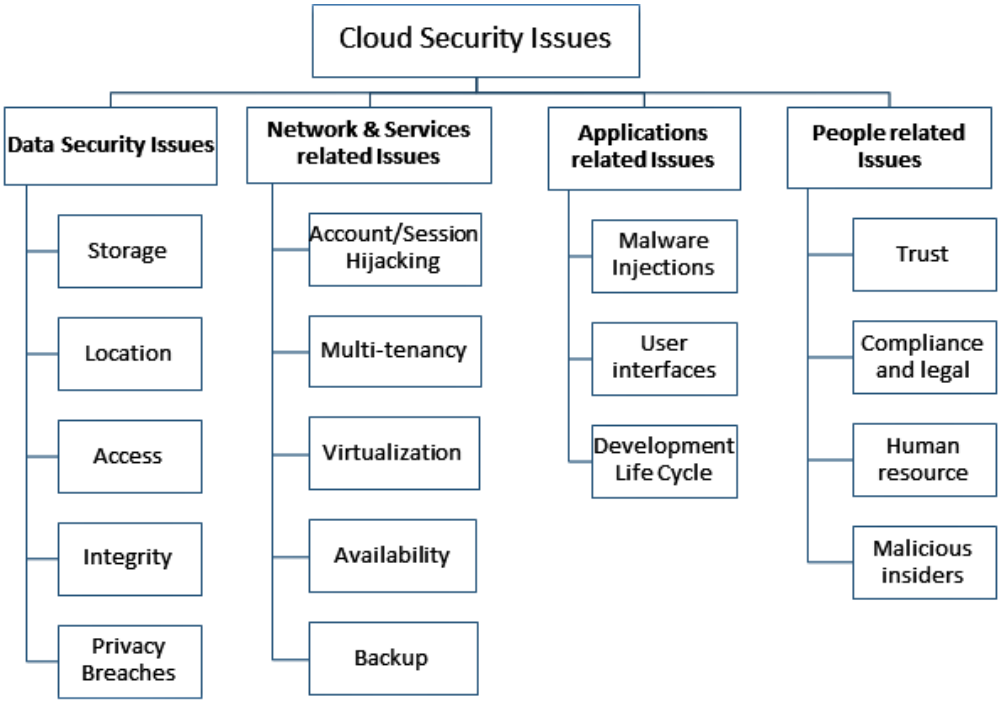

Figure 16. Summary of security issues in each category.

The security issues of each category are discussed in further detail in the following sub-sections.

6.1. C1-Data Security Issues

Data security issues are included in the top ten predicted cloud security challenges in 2020 by several reports and articles [104–106].

The data of enterprises and users include private personal information. For storing, collecting, and using users' information, enterprises are bound by the general data protection regulation" (GDPR) regulations to acquire these users' consent. In addition, data backup, recovery indicators, data confidentiality, and data integrity were highlighted in cybersecurity classified protection 2.0 issued by China in 2019. Cloud computing is a unique data-sharing method that uses user data to be located at different places during processing and shared with stakeholders when and if needed. Therefore, data security over the cloud is a significant question for SaaS, PaaS, and IaaS users. Data security aims to limit data access only to those authenticated successfully, and to let authentic users access, transmit, or modify only the data they are entitled to while ensuring that unauthorized resources cannot be requested by anyone.

6.1.1. Storage

Cloud computing models do not offer control over the data stored by data centers of the cloud service provider in most cases [107]. Though some level of control is given over the virtual machines, loss of control exists for the data storage. Attackers can tamper with the data after command and control are lost by a user as he/she uploads the data into the cloud [108]. In addition, cloud service providers can copy, manipulate, or modify user data without user knowledge. This results in many security issues related to storage. Encryption is used to provide better control over data, but it is not sufficient and has its associated cons.

6.1.2. Location

Data are dispersed at different physical locations and in different formats in cloud computing. Identifying the location of each data item is difficult. In addition, each geographical location has its laws and legal guidelines for data handling, which need to be

followed. Customers or users sometimes may be required to know their data /information vicinity, and cloud service providers may be bound to disclose this information. Irrelevant applications may be saved in the cloud when a user uses a public cloud. The cloud supplier may also counterfeit the data at various areas crosswise over nations to maintain high accessibility. Hence, there is room for exploitation as users give up control over data, and concerns are likely to emerge in the absence of sufficient information about the cloud environment [31]. This is another security issue in cloud-based systems.

6.1.3. Access

While keeping users' data on the cloud, it is vital to keep track of user identity and activities to avoid unauthorized access to services and stored data. Access controls ensure that the confidentiality of data is preserved. As the data owners and data are at different locations and platforms, it is challenging to manage access and identity controls in cloud computing. Organizations cannot rely only on their authentication and authorization controls in cloud-based environments. The cloud resources are dynamic and they shrink and grow as per the needs of cloud users. IP addresses of service providers are continuously changed when services start or restart in different costing models. Multiple key management mechanisms and encryption techniques are utilized to guarantee the limitation of data sharing with legitimate users only [109]. A cloud should have a fast identity management system to log for joining and leaving users over the cloud resources. Numerous concerns exist in identity management and access control; for instance, the problem of weak credentials may lead to a leisurely rest, weak logging and monitoring, account locked during DDoS attack, inefficient tenant segmentation, and poor identity management.

6.1.4. Integrity

Integrity means checking data for correction. In cloud-based systems, the purpose is to ensure the data storage is in complete form, and it is correct and precise flows in the database over the service. The data should be attributable to the user(s) or system(s) that generated it. The data should always be retrievable when needed and with time stamps. The data also need to be consistent and complete. Data integrity issues are intensified in cloud computing environments, as users hardly manage where their data are saved, who can access them, and in which way [110]. In cloud-based systems, multiple organizations share the application or platform, and users working on the same job can share information with any other unauthorized user who shares the application or platform in the cloud. This leads to a violation of integrity.

6.1.5. Privacy Breaches

Data privacy is an inherent challenge in cloud computing, as unencrypted data are stored on a machine owned and run by someone other than the actual data owner. Any data breach on the cloud may uncover an organization's sensitive data to the users of other organizations sharing the same storage. Due to multi-tenancy, customers using different applications on virtual machines could share an identical database [111], and an event of comprising will impact others along with the intended one. "When, how, and to what extent" are three essential aspects that need to be considered while investigating data privacy events; when were the data disclosed, how did they get exposed, and how much? To ensure privacy, it must apply laws, procedures, and processes to protect personally identifiable information [112]. If any cloud user visits sensitive data, they are not authorized to access it, and the cloud service provider should immediately identify it as a violation of privacy. Privacy issues vary depending on cloud models and scenarios.

6.2. C2-Network and Services Related Security Issues

This category comprises security issues related to networks and services, such as account or session hijacking, virtualization, and multi-tenancy and availability issues.

6.2.1. Account or Session Hijacking

Cloud users can access their data and service through cloud-based systems. User credentials can be hijacked, or sessions can be hijacked as well. Attackers use passwords to access cloud service resources and sometimes modify these credentials and account data. The unauthorized user with a password can access the customer's data and may steal, alter, delete or sell it to third-party individuals or organizations for malicious purposes. As a result, company integrity and prestige can be ruined, and private data can be falsified or leaked, resulting in costs for businesses or consumers. For companies in industries, such as healthcare, legal implications are also possible if clients' classified data are disclosed during hijacking incidents of the cloud account [113]. Keeping credentials safe, using two-factor authentication, and monitoring operations can help avoid these issues to some extent.

6.2.2. Multi-Tenancy

Multi-tenancy in cloud computing means multiple users of a cloud vendor use the same computational resources, be they software, hardware, service, network resource, or data. Cloud users do share resources, but their data are kept separately. In a multi-tenant architecture, multiple users share the same infrastructure, be it IaaS, PaaS, SaaS, containers, or serverless computing, but at the same time keep their data separate and secure. For example, customer data can be kept at the same physical site. The concept of coexistence and sharing resources of different occupants that are unknown to each other facilitate all the security risks [114]. However, multi-tenancy can be exploited in the form of colocation or co-tenancy attacks in which an attacker gains access to neighboring VMs or applications. Additionally, multiple data volumes are reserved for various tasks in multi-tenant architectures, which leaves a vulnerability for information leakage.

6.2.3. Virtualization

Cloud computing uses virtualization technology to utilize resources efficiently. Cloud users can also acquire resources on a pay-per-use business model. They choose resources, such as processors, RAM, bandwidth, or OS, according to their needs and pay only for acquired services and resources. Virtualization technology permits several security harms in the system and lets many new security threats evolve. Virtualized environments are unprotected from all types of attacks for different infrastructures, but security is an essential challenge, as virtualization provides more entrance points and interconnection density [115]. Customer data could be intercepted, the operation of VM may get modified, and malware can delete or obfuscate user data, thus attacking the CIA triad of security. In addition, VM-based rootkit attacks can infect both client and server machines in the cloud.

6.2.4. Availability

The availability of cloud systems is crucial. Cloud service providers should make sure that the service is conveyed on demand. Most organizations require cloud-based services because of the critical services they provide; any service interruption can lead to loss and subsequently, loss of consumer confidence. Attacks, such as denial of service, can cause non-availability, where all the available resources are utilized by the attacker and make them unavailable to others, resulting in a denial of service and slow access to them. In addition, customers who used the cloud service and were influenced by the botnet affect other providers' availability. Cloud interruptions, misuse of cloud resources, hardware faults, under-provisioned bandwidth can be the reasons for non-availability [46,48].

6.2.5. Backup

Keeping data backup is a critical task, as it is essential to store and uphold its security orders for facilitating recovery in case of any accidental or intentional disaster. There needs to be a guarantee that all the information is consistently backed up to encourage quick recovery on account of disasters occurring [116]. Regular backups of stored data need to be

made to ensure data availability by keeping it aligned with security guidelines to avoid malicious activities, such as unauthorized access, and tampering [46,48].

6.3. C3-Application Related Security Issues

Cloud applications can also become targets of attackers. Some of the issues faced by cloud applications are mentioned as follows:

6.3.1. Malware Injections

Cloud configurations for multi-user support need to be done with care since this attack has become a significant security challenge in cloud systems. Improper cloud configurations result in data leakages and malware infections, which can damage the whole cloud computing environment of the organization and cloud service provider. Malware injections are performed by embedded code execution in cloud services which may operate as SaaS in cloud servers. In some cases, such an injection is hidden for a lengthy time, which formulates a grave concern in the cloud environment [117]. This malware then multiplies with ease of execution and spreads in cloud environments. This is another serious security issue that needs to be tackled. Hyper-call attack, distributed denial of service (DDoS), hyper-jacking, VM escape, prime, and probe are some widespread malware attacks [118]. Malware residing on VMs, cloud malware syncing, and metamorphic engines are other security concerns that require attention.

6.3.2. User Interfaces

The applications that a user runs on the cloud environment allow users to customize their cloud experience and pose a severe security threat to the entire cloud architecture. Even many container-based platforms do not manage security out of the box. Application programming interfaces (APIs), also known as user interfaces, enable programmers to build their programs and integrate with the cloud. This interface is meant to provide access to the cloud services but can be misused since some APIs give access to the cloud customer's system, which may have vulnerabilities. Having up-to-date patches installed for software services is vital. The client may have been hacked unknowingly and might be unaware of what information was compromised.

6.3.3. Development Life Cycle

Any preventive measure taken against attack may have multiple firewalls, up-to-date anti-virus solutions, logging, monitoring of ports and events, encryption, or any other security measure, which will not work if the software itself is weak. The software application development in the cloud is more multifaceted than traditional application development. The development life cycle of software codes for the cloud introduces security loopholes, and frequent changes may reduce security and increase the development life speed. The requirements, design, development, and testing of cloud applications require us to differ from the traditional techniques used in the SDLC [119] and take a proactive approach against vulnerabilities, malicious attacks and target cloud platforms; in particular, PaaS applications need more attention. Wrong software development life cycle (SDLC), too much reliance on programmers, unsafe reverse engineering procedures, and the identification of problems after release or deployment are security issues of the development life cycle.

6.4. C4-People Related Security Issues

In general, people are considered the weakest link in security. However, in a cloud-based system, people inside and outside the organization are involved, resulting in more people-related security issues. Some significant issues are trust, human resources, compliance and legal requirements, and other issues arising from malicious insiders.

6.4.1. Customer Trust

In cloud environments, customer applications, data, and infrastructures are not located in a single place and are coped with by a second/third party. This results in increased trust issues on the part of customers compared to traditional systems. Configurations of the underlying SaaS, PaaS, or IaaS infrastructure and their security management are considered responsibilities of the cloud provider. When a user replies for the security of crucial data on a third party, a lack of trust is experienced, and questions arise, from the minutest security incident to the most prevalent security depiction. In a survey by [120] in 2015, almost 74% of responders said they do not trust that the cloud can provide security for their data. Trust management for cloud-to-cloud interactions, cloud system openness, fate sharing, data locality, audit techniques, and perimeter security are issues in this trust domain that need to be addressed.

6.4.2. Compliance and Legality

Compliance can be a huge security issue if handled carelessly. Cloud compliance is about complying with the laws and regulations that apply to using the cloud, storing and transferring data to and from the cloud, maintaining cloud architecture. Compliance is a complicated and somewhat complex subject in cloud computing environments mainly because security and privacy laws and regulations differ from region to region [121]. A cloud provider and user should be aware of laws and standards to manage data on the cloud. Compliance is about confirming proper controls over who has access to cloud assets, their level of access, and how it is upheld. This is achieved through auditing. The relative immaturity of the public cloud environment makes audits very challenging. Public cloud providers do not ensure primarily that compliance requirements are met. Legal problems, incorrect resource usage, and governance are other concerns in this category.

6.4.3. Human Resource

The security of human resource systems being hosted over the cloud and protecting necessary credentials and data of employees from getting sniffed and misused is a pinnacle concern. Many cloud service providers present cloud HR solutions as SaaS. Its broad-spectrum and ease in hiring make organizations choose this option and shift their payroll management, recruitment, task management over the cloud. An attack on these services causes serious harm to the organizations in terms of finance and reputation.

6.4.4. Malicious Insiders

Cloud-based systems are more prone to social engineering and phishing attacks than traditional systems. Once a malicious user gains access to login information or other confidential data, he/she can easily log into a system, as it is remotely accessible from the cloud [29]. Attack from within the organization or team can be catastrophic. Similar to unauthorized access, access by authorized users to harm the cloud environment is incredibly dangerous. A malicious insider can be a former or existing employee or any other stakeholder. Malicious outsiders who have sway or control over an insider may compel an otherwise innocuous insider to help launch an attack [122]. They can obtain customer accounts, financial, and other sensitive data. Insider attacks are hard to detect and prevent, as they would be considered routine access, and no alarm would be generated. Only after attacks cause harm can logging applications be used to track back to the attacker. The lack of cloud standards, mismanagement of internal access points, and lack of monitoring result in this security issue in most organizations.

Cloud computing security reference architecture is made with the help of NIST cloud computing reference architecture. The updated NIST Cloud Computing Security Reference Architecture from [51] can be seen in Figure 17.

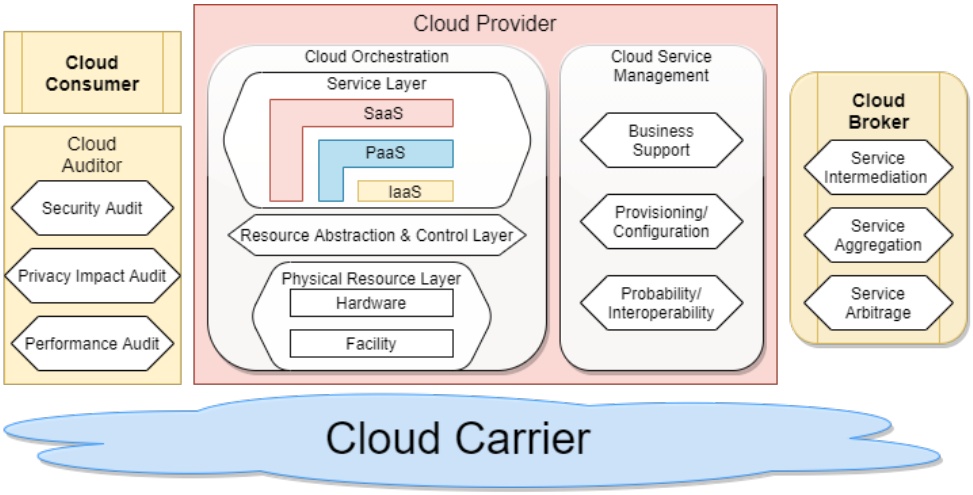

Figure 17. NIST's updated cloud computing reference architecture [51].

7. Challenges and Limitations in Cloud Computing

Cloud computing has enabled organizations to benefit from advanced cloud infrastructures with increased efficiency, improved work throughput, and reduced cost. In the current era, with advancements in 5G, reliable internet, smart mobile devices, IoT infrastructures, and intelligent AI-based data analytics platforms, there is a need to reevaluate how traditional cloud infrastructures are managed and address associated security issues [123,124]. With cloud-based systems, provisioning IT resources requires little knowledge of the underlying infrastructure. Thus, the cloud configuration requires little effort and knowledge for an organization. However, at the same time, with little knowledge of a specific cloud and the heterogeneous nature of the cloud, a user can end up with an infrastructure vulnerable to numerous cybersecurity issues, and this may result in data breaches, denial of service, session hijacking, and other similar attacks.

7.1. Confidentiality, Integrity and Availability (CIA)

The significant challenges of cloud computing include the maintenance of availability, integrity, and confidentiality. Data collected from IoT devices have to be protected from unauthorized access. This can result in the modification, addition, copy, or deletion of data. In addition, ensuring confidentiality is essential before uploading the data to the cloud servers when the communication of data has to be made through any insecure media [125,126].

7.2. Aspect of Application Security

Software application security serves as a significant challenge and critical point of vulnerability in information security. There may be various types of vulnerabilities associated with the different frameworks and platforms of applications [127,128]. A significant area of challenges constitutes application security aspect vulnerabilities in cloud computing. In relevance to this, it is worth it because millions of programming lines are behind the development of applications that are written in different languages by various programmers, bringing diversity to the list of vulnerabilities associated with them. In cloud computing, the developers may just be responsible for applying in the cloud. However, the security aspects of the entire application network and programming leave no loose ends. Operating systems may also prove to be vital in playing their role for the information security in the cloud [129].

7.3. COVID-19 or Similar Situation Challenges

COVID-19 has emerged as an infectious disease in recent years, transmitted mainly through air droplets. The generation of these droplets causes the spread of disease by the

coughing, breathing, and sneezing of infected individuals. Besides the external challenges on the cloud consumer end, employees have also faced many complex challenges. These are drastic times, and urgent actions have been taken, such as working from home to ensure the safety of employees. Unfortunately, the remote working model adopted by many industries has forced the excessive use of cloud resources. The safety concerns concerning COVID-19 have minimized the spread of infection, and the remote working policy is gradually ending. However, this will be a challenge for the cloud computing industry if a similar situation arises shortly.

7.4. Limited Computation Resources

In recent years, organizations have usually been unaware of where, how, and how much data and workload reside on cloud-based systems. It has become vital to rely on cloud service providers for these issues. Variable workloads demand that the service capacity be accommodated to demand to evade service performance debasement (in the event of an increase in demand) or service over-sizing (in the event of a decrease in demand) [130]. Network monitoring and logging were much easier on systems, IoT data, and networks physically connected and located together, and forensic investigation revealed more details [131,132]. However, cloud service providers charge for mirroring, resulting in additional costs, as it requires additional bandwidth. It is challenging for a cloud service provider to meet the requirements of all cloud users with no additional cost.

The traffic consuming nodes' energy is generated by exploiting a compromised node when a resource depletion attack occurs. The energy of these nodes is exhausted by making efforts to disable the network. Hence, the attack is held at the routing protocol layer. Computing resources, such as those in the cloud, are susceptible to such attacks, where these abilities along with memory and network bandwidth are exhausted on purpose [133]. The scalability of the cloud to manage the workload makes the cloud vulnerable to such attacks, where the resources are subjected to depletion when the attack is launched. Examples of such attacks may include exploiting application communication flaws and volume-based flooding protocol exploitation.

7.5. Security Issue Classification

Cloud computing has had some security issues since its inception. Still, with the emerging technology and cloud architectures, some new security issues, such as virtualization, multi-tenancy, and varying cyber-attacks, require the researcher's attention. Information assets exist at different locations and forms in a cloud computing environment. Therefore, it is necessary to classify information assets and handle security issues according to the associated classification level. This would result in ensuring security with reduced cost and effort. The classification of information when multiple users and organizations share it is challenging since, for one organization, a piece of information might be of more value than the other.

With multifaceted modern cloud infrastructures, security organizations face data duplication issues, identification of threats on time, reduced control over data access, and the need for regulatory compliance. Furthermore, to realize all-inclusive cloud security, protection against unidentified cyber-attacks and identified attacks must be given to the cloud infrastructure and data in it, athwart all cloud components, which is a pretty challenging task.

Cloud service providers face challenges to ensure that controls are in place to avoid data loss or manipulation. A data breach/data hacking incident is manageable, data and applications are kept securely, interfaces are secured, data are retrieved only by authorized users, and are available when needed. Cloud service providers need to keep controls in place to tackle these issues. Besides this, the botnet's timely detection of eavesdropping malware is essential. These mats remain undetected over a cloud for longer than traditional systems and can cause serious harm. Improper intrusion detection systems with traffic monitoring may also result in data breaches that need to be tackled [134,135]. Another

challenge to cloud computing is to handle insider threats. This is an open research problem. Risks and ambiguity inherent in current cloud architectures and models require more innovative solutions from cloud services providers. Contracts between clients and providers should precisely address these security issues.

7.6. Limitations concerning Deep Learning/AI

Cloud computing services are available online and are not located in a single place, and anyone can gain access with the proper credentials. The online enterprise data availability over the cloud makes it a lucrative target for many attackers attempting to study the systems, catch vulnerabilities in those systems, and exploit them for their advantage. The intersection of cybersecurity, AI and using data and resources provided by the cloud has made it extremely important to detect cyber-attacks and security issues in the cloud before they cause any significant harm. AI and DL make machines learn to perform tasks based on previous experiences and provide a higher level of intelligence to identify and detect cyber-attacks. Unfortunately, many organizations are not yet aware of the imposed threats to their cloud and the need to invest in prevention against emerging cyber-attacks.

7.7. Obsolete Laws

Organizations and cloud service providers rely on laws and standards which sometimes are inapplicable and obsolete. Instead of relying on laws of the former era, new laws must be shaped to accommodate the growing changes and uncertainties of cloud computing and the widespread internet use in general. All stakeholders in cloud-based systems must recognize the intrinsic risks involved with cloud computing and steps taken on the user side to mitigate these risks. Cloud application development teams need adequate and need-based security training, often neglected by software development organizations. Insecure APIs, misconfigured cloud storage, and poor access management are some more security issues, and they pose challenges for researchers to find feasible and cost-effective solutions. Following cloud security standards is essential for organizations to prevent reputation and monetary losses.

7.8. Security Policy Issues

The preventive measures taken to prevent attacks are the standards called security policies. In the cloud, it is expected that the working environment is secured by the security policies or standards without affecting the reliability and performance [136,137]. In addition, a set of various service-level agreements (SLAs), antecedent trust, and client management issues are involved with these security policies, and some regulatory authorities regulate them.

8. Future Directions

This research work presents additional security and privacy issues associated with cloud systems in the IoT world. In the future, researchers may work on the following areas of cloud computing systems: Security Issues: Researchers may focus on more security issues in the current cloud systems and provide different logical control techniques for the improvement of cloud security; study the most recent cloud security models and present their analysis; review existing security issues and challenges regarding cloud computing, such as authenticity, encryption, multi-tenancy, security of virtual machines, and how to reduce these issues; and resource sharing in the cloud computing infrastructures.

Data Storage and Processing: With technological advancements, such as smart cities, IoT, and 5G internet, the role of cloud systems will increase in terms of data storing and processing [138]. The cloud infrastructure and data must be protected from different attacks to accomplish inclusive cloud system security.

Secure and Reliable Cloud Environment: Still, several issues need to be solved for a secure and reliable cloud environment. These security issues include network, application, communication, web services, and data privacy.

Cloud as a Service: Most of the developing manufacturing companies are already using cloud services, and in the future, cloud services will be the priority of manufacturing companies.

Blockchain for Cloud Data Security: Security problems, such as shared pool resources, virtualization, and multi-tenancy, are emerging cloud security issues—several techniques were introduced by researchers to secure cloud logs. To enhance the data storing methods in the cloud and data security, blockchain technology with decentralized cloud storage is effective, and this technique protects the store data from modification and deleting.

Blockchain based Cloud Log Security: A new research direction is called securing cloud logs using blockchain. The proposed architecture provides security to cloud logs using blockchain technology, making cloud systems unbreachable, increasing users' trust in a cloud environment.

Authentication Mechanism: The authentication mechanism of cloud databases using blockchain is another future direction in the cloud environment. Blockchain technology will make it difficult for an insider to change user login credentials. Using distributed ledger-based authentication techniques, insiders cannot access user login credentials.

Federated Learning for Cloud: A new machine learning technique called federated learning trains different algorithms on multiple decentralized servers using local data without sharing. The main challenge in the cloud environment is the communication cost between clients and the cloud server because of limited bandwidth. Highly well-organized federated learning techniques can be used in cloud computing for achieving strong privacy.

Privacy Issues in Cloud: Achieving strong privacy increases user trust in cloud computing. To increase the algorithm training efficiency, advanced optimization strategies can be used. These techniques will be efficient against extreme collusion and honest but curious servers. Using federated learning, researchers and developers can solve different challenges associated with cloud computing, including expensive communication, privacy concern, statistical heterogeneity, and systems heterogeneity.

9. Conclusions

The embracing of cloud technology has become a game changer for industries, organizations, and hackers during the last decade. The advent of modern cloud architectures and high-speed internet with emerging innovations brought security threats for cloud computing. This shift to cloud technology contributed to an organization's flexibility and scalability to remain innovative and competitive in the ever-changing industrial environment. Still, concurrently, it made their data less secure and vulnerable to attacks for several reasons. This paper discussed cloud architectures, deployment models, and common attacks. We then placed security issues in the cloud in four categories and discussed the associated issues in each. We also deliberated various challenges in cloud computing that need to be addressed soon. These challenges also include the limitations that have risen in the AI and DL domain concerning cloud computing.

Author Contributions: This research specifies the following individual contributions: conceptualization, A.R.J. and W.A.; data curation, W.A.; formal analysis, A.R.J.; funding acquisition, A.R.; investigation, A.R.J.; methodology, A.R.J.; project administration, T.B. and A.R.; resources, Z.J. and A.R.; software, A.R.J.; supervision, T.B., A.R.J., and T.B.; validation, W.A., and Z.J.; visualization, W.A. and T.B.; writing—review and editing, A.R. and Z.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Mohiyuddin, A.; Javed, A.R.; Chakraborty, C.; Rizwan, M.; Shabbir, M.; Nebhen, J. Secure Cloud Storage for Medical IoT Data using Adaptive Neuro-Fuzzy Inference System. *Int. J. Fuzzy Syst.* **2021**, 1–13. [CrossRef]
2. Karam, Y.; Baker, T.; Taleb-Bendiab, A. Security support for intention driven elastic cloud computing. In Proceedings of the 2012 Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation, Malta, Malta, 14–16 November 2012; pp. 67–73.
3. Abid, R.; Iwendi, C.; Javed, A.R.; Rizwan, M.; Jalil, Z.; Anajemba, J.H.; Biamba, C. An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. *Pers. Ubiquitous Comput.* **2021**, 1–14. [CrossRef]
4. Ikram, A.A.; Javed, A.R.; Rizwan, M.; Abid, R.; Crichigno, J.; Srivastava, G. Mobile Cloud Computing Framework for Securing Data. In Proceedings of the 2021 44th International Conference on Telecommunications and Signal Processing (TSP), Brno, Czech Republic, 26–28 July 2021; pp. 309–315.
5. Gartner-Top-10-Strategic-Technology-Trends-for-2020. Available online: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/ (accessed on 8 August 2020).
6. Regalado, A. Who Coined Cloud Computing? *MIT Technology Review*, 31 October 2011. Available online: https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/ (accessed on 8 August 2020).
7. Amazon Web Services, Inc. Announcing Amazon Elastic Compute Cloud (Amazon EC2)—Beta. 2006. Available online: https://aws.amazon.com/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2---beta/ (accessed on 8 August 2020).
8. Googleappengine.blogspot.com. Introducing Google App Engine + Our New Blog. 2008. Available online: https://googleappengine.blogspot.com/2008/04/introducing-google-app-engine-our-new.html (accessed on 8 August 2020).
9. Larsson, L.; Henriksson, D.; Elmroth, E. Scheduling and monitoring of internally structured services in cloud federations. In Proceedings of the 2011 IEEE Symposium on Computers and Communications (ISCC), Kerkyra, Greece, 28 June–1 July 2011; pp. 173–178.
10. Hauger, D.; Microsoft Blog Editor—Microsoft News Center Staff. Windows Azure General Availability. *The Official Microsoft Blog*, 1 February 2020. Available online: https://blogs.microsoft.com/blog/2010/02/01/windows-azure-general-availability/ (accessed on 8 August 2020).
11. dzone.com. Apache CloudStack vs. OpenStack: Which Is the Best? DZone Cloud. 2016. Available online: https://dzone.com/articles/apache-cloudstack-vs-openstack-which-is-the-best (accessed on 8 August 2020).
12. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing*; Special Publication (NIST SP) Series; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
13. Ghobaei-Arani, M.; Souri, A.; Baker, T.; Hussien, A. ControCity: An autonomous approach for controlling elasticity using buffer Management in Cloud Computing Environment. *IEEE Access* **2019**, *7*, 106912–106924. [CrossRef]
14. Shabbir, M.; Shabbir, A.; Iwendi, C.; Javed, A.R.; Rizwan, M.; Herencsar, N.; Lin, J.C.W. Enhancing security of health information using modular encryption standard in mobile cloud computing. *IEEE Access* **2021**, *9*, 8820–8834. [CrossRef]
15. Baker, T.; Mackay, M.; Randles, M.; Taleb-Bendiab, A. Intention-oriented programming support for runtime adaptive autonomic cloud-based applications. *Comput. Electr. Eng.* **2013**, *39*, 2400–2412. [CrossRef]
16. Al-Khafajiy, M.; Baker, T.; Asim, M.; Guo, Z.; Ranjan, R.; Longo, A.; Puthal, D.; Taylor, M. COMITMENT: A fog computing trust management approach. *J. Parallel Distrib. Comput.* **2020**, *137*, 1–16. [CrossRef]
17. Xia, T.; Washizaki, H.; Fukazawa, Y.; Kaiya, H.; Ogata, S.; Fernandez, E.B.; Kato, T.; Kanuka, H.; Okubo, T.; Yoshioka, N.; et al. CSPM: Metamodel for Handling Security and Privacy Knowledge in Cloud Service Development. *Int. J. Syst. Softw. Secur. Prot. (IJSSSP)* **2021**, *12*, 68–85. [CrossRef]
18. Mather, T.; Kumaraswamy, S.; Latif, S. *Cloud Security and Privacy*; OReilly Media Inc.: Sebastopol, CA, USA, 2009.
19. 4 Trends Impacting Cloud Adoption in 2020. Available online: https://www.gartner.com/smarterwithgartner/4-trends-impacting-cloud-adoption-in-2020/ (accessed on 8 August 2020).
20. Su, J. Why Cloud Computing Cyber Security Risks Are On The Rise: Report. *Forbes*, 25 July 2019. Available online: https://www.forbes.com/sites/jeanbaptiste/2019/07/25/why-cloud-computing-cyber-security-risks-are-on-the-rise-report/#13a36bfc5621. (accessed on 8 August 2020).
21. Mishra, P.; Negi, A.; Pilli, E.; Joshi, R. VMProtector: Malign Process Detection for Protecting Virtual Machines in Cloud Environment. In *Third International Conference on Advances in Computing and Data Sciences, ICACDS 2019, Ghaziabad, India, April 12–13, 2019, Revised Selected Papers, Part I*; Springer: Singapore, 2019; pp. 360–369.
22. Khorshed, M.T.; Ali, A.S.; Wasimi, S.A. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Gener. Comput. Syst.* **2012**, *28*, 833–851. [CrossRef]
23. Teneyuca, D. Internet cloud security: The illusion of inclusion. *Inf. Secur. Tech. Rep.* **2011**, *16*, 102–107. [CrossRef]
24. Ismail, N. Cursing the cloud (or) controlling the cloud? *Comput. Law Secur. Rev.* **2011**, *27*, 250–257. [CrossRef]
25. King, N.J.; Raja, V. Protecting the privacy and security of sensitive customer data in the cloud. *Comput. Law Secur. Rev.* **2012**, *28*, 308–319. [CrossRef]
26. Ryan, P.; Falvey, S. Trust in the clouds. *Comput. Law Secur. Rev.* **2012**, *28*, 513–521. [CrossRef]
27. Rai, R.; Sahoo, G.; Mehfuz, S. Securing software as a service model of cloud computing: Issues and solutions. *arXiv* **2013**, arXiv:1309.2426.

28. Chen, F.; Luo, D.; Xiang, T.; Chen, P.; Fan, J.; Truong, H.L. IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-oriented Applications. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36. [CrossRef]
29. Rao, P.M.; Saraswathi, P. Evolving cloud security technologies for social networks. In *Security in IoT Social Networks*; Elsevier: Amsterdam, The Netherlands, 2021; pp. 179–203.
30. Montasari, R.; Daneshkhah, A.; Jahankhani, H.; Hosseinian-Far, A. Cloud Computing Security: Hardware-Based Attacks and Countermeasures. In *Digital Forensic Investigation of Internet of Things (IoT) Devices*; Springer: Cham, Switzerland, 2021; pp. 155–167.
31. Puthal, D.; Sahoo, B.P.; Mishra, S.; Swain, S. Cloud computing features, issues, and challenges: A big picture. In Proceedings of the 2015 International Conference on Computational Intelligence and Networks, Odisha, India, 12–13 January 2015; pp. 116–123.
32. Khan, M.A. A survey of security issues for cloud computing. *J. Netw. Comput. Appl.* **2016**, *71*, 11–29. [CrossRef]
33. Shahzad, F.; Iqbal, W.; Bokhari, F.S. On the use of CryptDB for securing Electronic Health data in the cloud: A performance study. In Proceedings of the 2015 17th International Conference on E-health Networking, Application Services (HealthCom), Boston, MA, USA, 14–17 October 2015; pp. 120–125. [CrossRef]
34. Jouini, M.; Rabai, L.B.A. A security framework for secure cloud computing environments. In *Cloud security: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2019; pp. 249–263.
35. Rong, C.; Nguyen, S.T.; Jaatun, M.G. Beyond lightning: A survey on security challenges in cloud computing. *Comput. Electr. Eng.* **2013**, *39*, 47–54. [CrossRef]
36. Modi, C.; Patel, D.; Borisaniya, B.; Patel, A.; Rajarajan, M. A survey on security issues and solutions at dif ferent layers of Cloud computing. *J. Supercomput.* **2013**, *63*, 561–592. [CrossRef]
37. Fernandes, D.A.; Soares, L.F.; Gomes, J.V.; Freire, M.M.; Inácio, P.R. Security issues in cloud environments: A survey. *Int. J. Inf. Secur.* **2014**, *13*, 113–170. [CrossRef]
38. Jain, R.; Madan, S.; Garg, B. Privacy sustainability scheme in cloud environment. *CSI Trans. ICT* **2016**, *4*, 123–128. [CrossRef]
39. Shahzad, A.; Hussain, M. Security issues and challenges of mobile cloud computing. *Int. J. Grid Distrib. Comput.* **2013**, *6*, 37–50. [CrossRef]
40. Sgandurra, D.; Lupu, E. Evolution of attacks, threat models, and solutions for virtualized systems. *ACM Comput. Surv. (CSUR)* **2016**, *48*, 1–38. [CrossRef]
41. 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]
42. Tabrizchi, H.; Rafsanjani, M.K. A survey on security challenges in cloud computing: Issues, threats, and solutions. *J. Supercomput.* **2020**, *76*, 9493–9532. [CrossRef]
43. Anuradha, M.; Jayasankar, T.; Prakash, N.; Sikkandar, M.Y.; Hemalakshmi, G.; Bharatiraja, C.; Britto, A.S.F. IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocess. Microsyst.* **2021**, *80*, 103301. [CrossRef]
44. Monge, M.A.S.; Vidal, J.M.; Pérez, G.M. Detection of economic denial of sustainability (EDoS) threats in self-organizing networks. *Comput. Commun.* **2019**, *145*, 284–308. [CrossRef]
45. Sotelo Monge, M.A.; Maestre Vidal, J. Conceptualization and cases of study on cyber operations against the sustainability of the tactical edge. *arXiv* **2021**, arXiv:2101.08676.
46. RM, S.P.; Bhattacharya, S.; Maddikunta, P.K.R.; Somayaji, S.R.K.; Lakshmanna, K.; Kaluri, R.; Hussien, A.; Gadekallu, T.R. Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything. *J. Parallel Distrib. Comput.* **2020**, *142*, 16–26.
47. Ahamad, R.Z.; Javed, A.R.; Mehmood, S.; Khan, M.Z.; Noorwali, A.; Rizwan, M. Interference Mitigation in D2D Communication Underlying Cellular Networks: Towards Green Energy. *CMC-Comput. Mater. Contin.* **2021**, *68*, 45–58. [CrossRef]
48. Reddy, G.T.; Sudheer, K.; Rajesh, K.; Lakshmanna, K. Employing data mining on highly secured private clouds for implementing a security-asa-service framework. *J. Theor. Appl. Inf. Technol* **2014**, *59*, 317–326.
49. Naeem, A.; Javed, A.R.; Rizwan, M.; Abbas, S.; Lin, J.C.W.; Gadekallu, T.R. DARE-SEP: A hybrid approach of distance aware residual energy-efficient SEP for WSN. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 611–621. [CrossRef]
50. Javed, A.R.; Abid, R.; Aslam, B.; Khalid, H.A.; Khan, M.Z.; Alhazmi, O.H.; Rizwan, M. Green5g: Enhancing capacity and coverage in device-to-device communication. *Comput. Mater. Continua* **2021**, *67*, 1933–1950. [CrossRef]
51. NIST Cloud Computing Security Reference Architecture. Available online: https://csrc.nist.gov/publications/detail/sp/500-299/draft (accessed on: 8 August 2020).
52. Rani, B.K.; Rani, B.P.; Babu, A.V. Cloud computing and inter-clouds–types, topologies and research issues. *Procedia Comput. Sci.* **2015**, *50*, 24–29. [CrossRef]
53. Diaby, T.; Rad, B.B. Cloud computing: A review of the concepts and deployment models. *Int. J. Inf. Technol. Comput. Sci.* **2017**, *9*, 50–58. [CrossRef]
54. Shaikh, A.H.; Meshram, B. Security issues in cloud computing. In *Intelligent Computing and Networking*; Springer: Singapore, 2021; pp. 63–77.
55. Bahrami, M.; Singhal, M. The role of cloud computing architecture in big data. In *Information Granularity, Big Data, and Computational Intelligence*; Springer: Cham, Switzerland, 2015; pp. 275–295.

56. Odun-Ayo, I.; Ananya, M.; Agono, F.; Goddy-Worlu, R. Cloud computing architecture: A critical analysis. In *Proceedings of the 2018* 18th International Conference on Computational Science and Applications (ICCSA), Melbourne, Australia, 2–5 July 2018; pp. 1–7.
57. Piraghaj, S.F.; Dastjerdi, A.V.; Calheiros, R.N.; Buyya, R. A survey and taxonomy of energy efficient resource management techniques in platform as a service cloud. In *Handbook of Research on End-to-End Cloud Computing Architecture Design*; IGI Global: Hershey, PA, USA, 2017; pp. 410–454.
58. Huang, W.; Ganjali, A.; Kim, B.H.; Oh, S.; Lie, D. The state of public infrastructure-as-a-service cloud security. *ACM Comput. Surv. (CSUR)* **2015**, *47*, 1–31. [CrossRef]
59. Nanda, S.; Hansen, R.A. Forensics as a service: Three-tier architecture for cloud based forensic analysis. In Proceedings of the 2016 15th International Symposium on Parallel and Distributed Computing (ISPDC), Fuzhou, China, 8–10 July 2016; pp. 178–183.
60. Iqbal, F.; Batool, R.; Fung, B.C.; Aleem, S.; Abbasi, A.; Javed, A.R. Toward Tweet-Mining Framework for Extracting Terrorist Attack-Related Information and Reporting. *IEEE Access* **2021**, *9*, 115535–115547. [CrossRef]
61. Tan, Y.; Wu, F.; Wu, Q.; Liao, X. Resource stealing: A resource multiplexing method for mix workloads in cloud system. *J. Supercomput.* **2019**, *75*, 33–49. [CrossRef]
62. Hong, J.B.; Nhlabatsi, A.; Kim, D.S.; Hussein, A.; Fetais, N.; Khan, K.M. Systematic identification of threats in the cloud: A survey. *Comput. Netw.* **2019**, *150*, 46–69. [CrossRef]
63. Haber, M.J.; Hibbert, B. Penetration Testing. In *Asset Attack Vectors*; Apress: Berkeley, CA, USA, 2018; pp. 93–98.
64. Lin, H.; Xu, L.; Huang, X.; Wu, W.; Huang, Y. A trustworthy access control model for mobile cloud computing based on reputation and mechanism design. *Ad Hoc Netw.* **2015**, *35*, 51–64. [CrossRef]
65. Singh, A.; Chatterjee, K. Cloud security issues and challenges: A survey. *J. Netw. Comput. Appl.* **2017**, *79*, 88–115. [CrossRef]
66. Mushtaq, M.F.; Akram, U.; Khan, I.; Khan, S.N.; Shahzad, A.; Ullah, A. Cloud computing environment and security challenges: A review. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 183–195.
67. Singh, A. Security concerns and countermeasures in cloud computing: A qualitative analysis. *Int. J. Inf. Technol.* **2019**, *11*, 683–690.
68. 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.
69. Sheikh, A.; Munro, M.; Budgen, D. Systematic Literature Review (SLR) of resource scheduling and security in cloud computing. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*. [CrossRef]
70. An, Y.; Zaaba, Z.; Samsudin, N. Reviews on security issues and challenges in cloud computing. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2016; Volume 160, p. 012106.
71. Wani, A.R.; Rana, Q.; Pandey, N. Analysis and countermeasures for security and privacy issues in cloud computing. In *System Performance and Management Analytics*; Springer: Singapore, 2019; pp. 47–54.
72. 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.
73. Chan, T.H.; Jia, K.; Gao, S.; Lu, J.; Zeng, Z.; Ma, Y. PCANet: A simple deep learning baseline for image classification? *IEEE Trans. Image Process.* **2015**, *24*, 5017–5032. [CrossRef]
74. Graves, A.; Mohamed, A.r.; Hinton, G. Speech recognition with deep recurrent neural networks. In Proceedings of the 2013 IEEE international conference on acoustics, speech and signal processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 6645–6649.
75. Hinton, G.; Deng, L.; Yu, D.; Dahl, G.E.; Mohamed, A.R.; Jaitly, N.; Senior, A.; Vanhoucke, V.; Nguyen, P.; Sainath, T.N.; et al. Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups. *IEEE Signal Process. Mag.* **2012**, *29*, 82–97. [CrossRef]
76. Liang, M.; Li, Z.; Chen, T.; Zeng, J. Integrative data analysis of multi-platform cancer data with a multimodal deep learning approach. *IEEE/ACM Trans. Comput. Biol. Bioinform.* **2014**, *12*, 928–937. [CrossRef]
77. Li, P.; Li, J.; Huang, Z.; Li, T.; Gao, C.Z.; Yiu, S.M.; Chen, K. Multi-key privacy-preserving deep learning in cloud computing. *Future Gener. Comput. Syst.* **2017**, *74*, 76–85. [CrossRef]
78. Hinton, G.E.; Salakhutdinov, R.R. Reducing the dimensionality of data with neural networks. *Science* **2006**, *313*, 504–507. [CrossRef]
79. Giri, S.; Shakya, S. Cloud Computing and Data Security Challenges: A Nepal Case. *Int. J. Eng. Trends Technol.* **2019**, *67*, 146–150.
80. Wu, W.; Zhang, Q.; Wang, Y. Public Cloud Security Protection Research. In Proceedings of the 2019 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Dalian, China, 20–22 September 2019; pp. 1–4.
81. Ramachandra, G.; Iftikhar, M.; Khan, F.A. A comprehensive survey on security in cloud computing. *Procedia Comput. Sci.* **2017**, *110*, 465–472. [CrossRef]
82. Sunyaev, A. Cloud Computing. In *Internet Computing*; Springer: Cham, Switzerland, 2020; pp. 195–236.
83. Javed, A.R.; Usman, M.; Rehman, S.U.; Khan, M.U.; Haghighi, M.S. Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4291–4300. [CrossRef]
84. Ahmed, W.; Rasool, A.; Javed, A.R.; Kumar, N.; Gadekallu, T.R.; Jalil, Z.; Kryvinska, N. Security in Next Generation Mobile Payment Systems: A Comprehensive Survey. *IEEE Access* **2021**, *9*, 115932–115950. [CrossRef]

85. Riaz, S.; Khan, A.H.; Haroon, M.; Latif, S.; Bhatti, S. Big Data Security and Privacy: Current Challenges and Future Research perspective in Cloud Environment. In Proceedings of the 2020 International Conference on Information Management and Technology (ICIMTech), Bandung, Indonesia, 13–14 August 2020; pp. 977–982.
86. Iwendi, C.; Rehman, S.U.; Javed, A.R.; Khan, S.; Srivastava, G. Sustainable Security for the Internet of Things Using Artificial Intelligence Architectures. *ACM Trans. Internet Technol. (TOIT)* **2021**, *21*, 1–22. [CrossRef]
87. Harkut, D.G. Introductory Chapter: Cloud Computing Security Challenges. In *Cloud Computing Security-Concepts and Practice*; IntechOpen: London, UK, 2020.
88. Basit, A.; Zafar, M.; Liu, X.; Javed, A.R.; Jalil, Z.; Kifayat, K. A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommun. Syst.* **2021**, *76*, 139–154. [CrossRef] [PubMed]
89. Basit, A.; Zafar, M.; Javed, A.R.; Jalil, Z. A novel ensemble machine learning method to detect phishing attack. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–5.
90. Pothuganti, S. Overview on Security Issues in Cloud Computing. *Int. J. Innov. Res. Comput. Commun. Eng.* **2020**, *10*, 4064–4068.
91. Afzal, S.; Asim, M.; Javed, A.R.; Beg, M.O.; Baker, T. URLdeepDetect: A Deep Learning Approach for Detecting Malicious URLs Using Semantic Vector Models. *J. Netw. Syst. Manag.* **2021**, *29*, 1–27. [CrossRef]
92. Chouhan, P.; Singh, R. Security attacks on cloud computing with possible solution. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2016**, *6*, 92–96.
93. Kene, S.G.; Theng, D.P. A review on intrusion detection techniques for cloud computing and security challenges. In Proceedings of the 2015 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 26–27 February 2015; pp. 227–232.
94. Chiba, Z.; Abghour, N.; Moussaid, K.; El Omri, A.; Rida, M. A survey of intrusion detection systems for cloud computing environment. In Proceedings of the 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 22–24 September, 2016; pp. 1–13.
95. Logesswari, S.; Jayanthi, S.; KalaiSelvi, D.; Muthusundari, S.; Aswin, V. A study on cloud computing challenges and its mitigations. *Mater. Today Proc.* **2020**. [CrossRef]
96. Singh, A.; Shrivastava, D.M. Overview of attacks on cloud computing. *Int. J. Eng. Innov. Technol. (IJEIT)* **2012**, *1*, 321–323.
97. Muhammad, A.; Asad, M.; Javed, A.R. Robust early stage botnet detection using machine learning. In Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 20–21 October 2020; pp. 1–6.
98. Rehman Javed, A.; Jalil, Z.; Atif Moqurrab, S.; Abbas, S.; Liu, X. Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles. *Trans. Emerg. Telecommun. Technol.* **2020**, e4088. [CrossRef]
99. Bakr, A.; El-Aziz, A.; Hefny, H.A. A Survey on Mitigation Techniques against DDoS Attacks on Cloud Computing Architecture. *Int. J. Adv. Sci. Technol.* **2019**, *28*, 187–200.
100. Alhenaki, L.; Alwatban, A.; Alamri, B.; Alarifi, N. A survey on the security of cloud computing. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–7.
101. Sigler, K. Crypto-jacking: How cyber-criminals are exploiting the crypto-currency boom. *Comput. Fraud. Secur.* **2018**, *2018*, 12–14. [CrossRef]
102. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2018**, *78*, 680–698. [CrossRef]
103. Iwendi, C.; Jalil, Z.; Javed, A.R.; Reddy, T.; Kaluri, R.; Srivastava, G.; Jo, O. Keysplitwatermark: Zero watermarking algorithm for software protection against cyber-attacks. *IEEE Access* **2020**, *8*, 72650–72660. [CrossRef]
104. Chaudhary, A. Cloud Security Challenges in 2020. *Cloud Security Alliance*, 18 February 2020. Available online: https://cloudsecurityalliance.org/blog/2020/02/18/cloud-security-challenges-in-2020/ (accessed on 8 August 2020).
105. Isc2.org. 2020 Cloud Security Report. 2020. Available online: https://www.isc2.org/resource-center/reports/2020-cloud-security-report (accessed on 8 August 2020).
106. Cybersecurity Insiders. 2020 Cloud Security Report—Cybersecurity Insiders. 2020. Available online: https://www.cybersecurity-insiders.com/portfolio/cloud-security-report-prospectus/. (accessed on 8 August 2020).
107. Abbasi, A.; Javed, A.R.; Chakraborty, C.; Nebhen, J.; Zehra, W.; Jalil, Z. ElStream: An Ensemble Learning Approach for Concept Drift Detection in Dynamic Social Big Data Stream Learning. *IEEE Access* **2021**, *9*, 66408–66419. [CrossRef]
108. Pujari, V.; Patil, R.; Palkar, R. A Study of Data Storage Security Issues in Cloud Computing. In Proceedings of the National Seminar on "Trends in Geography, Commerce, IT And Sustainable Development", Khed, India, 29 February 2020.
109. Rao, R.V.; Selvamani, K. Data security challenges and its solutions in cloud computing. *Procedia Comput. Sci.* **2015**, *48*, 204–209. [CrossRef]
110. Gaetani, E.; Aniello, L.; Baldoni, R.; Lombardi, F.; Margheri, A.; Sassone, V. Blockchain-based database to ensure data integrity in cloud computing environments. In Proceedings of the Italian Conference on Cybersecurity, Venice, Italy, 17–20 January 2017.
111. Chen, D.; Zhao, H. Data security and privacy protection issues in cloud computing. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Volume 1, pp. 647–651.
112. Ahmed, W.; Shahzad, F.; Javed, A.R.; Iqbal, F.; Ali, L. WhatsApp Network Forensics: Discovering the IP Addresses of Suspects. In Proceedings of the 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 19–21 April 2021; pp. 1–7. [CrossRef]

113. Christina, A.A. Proactive measures on account hijacking in cloud computing network. *Asian J. Comput. Sci. Technol.* **2015**, *4*, 31–34.
114. Mishra, A.; Mathur, R.; Jain, S.; Rathore, J.S. Cloud computing security. *Int. J. Recent Innov. Trends Comput. Commun.* **2013**, *1*, 36–39.
115. Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. *J. Internet Serv. Appl.* **2013**, *4*, 5. [CrossRef]
116. Thabita, F.; Alhomdyc, S.; Al-Ahdalc, A.H.; Jagtapa, S. Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with their Alleviating Techniques. *J. Inf. Comput. Sci.* **2020**, *12*, 35–57.
117. 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]
118. Tripwire Guest Authors. Malware in the Cloud: What You Need to Know. *Tripwire: The State of Security*, 25 September 2018. Available online: https://www.tripwire.com/state-of-security/security-data-protection/cloud/malware-cloud/ (accessed on 8 August 2020).
119. Kashfi, H. Software engineering challenges in cloud environment: Software development lifecycle perspective. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2017**, *2*, 251–256.
120. Horvath, A.S.; Agrawal, R. Trust in cloud computing. In Proceedings of the SoutheastCon 2015, Fort Lauderdale, FL, USA, 9–12 April 2015; pp. 1–8.
121. Awodele, O.; Adebayo, A.; Tayo, O. Security and Privacy Issues in Cloud Computing. *Commun. Appl. Electron.* **2017**, *7*, 14–17.
122. Duncan, A.J.; Creese, S.; Goldsmith, M. Insider attacks in cloud computing. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 857–862.
123. Javed, A.R.; Beg, M.O.; Asim, M.; Baker, T.; Al-Bayatti, A.H. Alphalogger: Detecting motion-based side-channel attack using smartphone keystrokes. *J. Ambient. Intell. Humaniz. Comput.* **2020**, 1–14. [CrossRef]
124. Javed, A.R.; Rehman, S.U.; Khan, M.U.; Alazab, M.; Khan, H.U. Betalogger: Smartphone Sensor-based Side-channel Attack Detection and Text Inference Using Language Modeling and Dense MultiLayer Neural Network. *Trans. Asian -Low-Resour. Lang. Inf. Process.* **2021**, *20*, 1–17. [CrossRef]
125. Islam, M.A.; Vrbsky, S.V. Transaction management with tree-based consistency in cloud databases. *Int. J. Cloud Comput.* **2017**, *6*, 58–78. [CrossRef]
126. Tang, J.; Cui, Y.; Li, Q.; Ren, K.; Liu, J.; Buyya, R. Ensuring security and privacy preservation for cloud data services. *ACM Comput. Surv. (CSUR)* **2016**, *49*, 1–39. [CrossRef]
127. Sehgal, N.K.; Bhatt, P.C. Cloud Workload Characterization. In *Cloud Computing*; Springer: Cham, Switzerland, 2018.
128. Xuan, S.; Yang, W.; Dong, H.; Zhang, J. Performance evaluation model for application layer firewalls. *PLoS ONE* **2016**, *11*, e0167280. [CrossRef] [PubMed]
129. Shin, S.; Song, Y.; Lee, T.; Lee, S.; Chung, J.; Porras, P.; Yegneswaran, V.; Noh, J.; Kang, B.B. Rosemary: A robust, secure, and high-performance network operating system. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 78–89.
130. Moreno-Vozmediano, R.; Montero, R.S.; Llorente, I.M. Key challenges in cloud computing: Enabling the future internet of services. *IEEE Internet Comput.* **2012**, *17*, 18–25. [CrossRef]
131. Hina, M.; Ali, M.; Javed, A.R.; Ghabban, F.; Khan, L.A.; Jalil, Z. SeFACED: Semantic-Based Forensic Analysis and Classification of E-Mail Data Using Deep Learning. *IEEE Access* **2021**, *9*, 98398–98411. [CrossRef]
132. Javed, A.R.; Jalil, Z. Byte-level object identification for forensic investigation of digital images. In Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 20–21 October 2020; pp. 1–4.
133. Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. *J. Netw. Comput. Appl.* **2016**, *67*, 147–165. [CrossRef]
134. Mittal, M.; Iwendi, C.; Khan, S.; Rehman Javed, A. Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e3997. [CrossRef]
135. Rehman, A.; Rehman, S.U.; Khan, M.; Alazab, M.; Reddy, T. CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1456–1466.
136. Ahmed, M.; Litchfield, A.T. Taxonomy for identification of security issues in cloud computing environments. *J. Comput. Inf. Syst.* **2018**, *58*, 79–88. [CrossRef]
137. Alzahrani, A.; Alalwan, N.; Sarrab, M. Mobile cloud computing: Advantage, disadvantage and open challenge. In Proceedings of the 7th Euro American Conference on Telematics and Information Systems, Valparaiso, Chile, 2–4 April 2014; pp. 1–4.
138. Shahzad, F.; Javed, A.R.; Zikria, Y.B.; Rehman, S.u.; Jalil, Z. Future Smart Cities: Requirements, Emerging Technologies, Applications, Challenges, and Future Aspects. *TechRxiv* **2021**. [CrossRef]