ISSN: 0974-6471, Vol. 15, No. (1-2-3) 2022, Pg. 27-52

Oriental Journal of Computer Science and Technology

www.computerscijournal.org

A Comprehensive Survey of IoT- Based Cloud Computing Cyber Security

SHIPRA YADAV

Lincoln University Malaysia.

Abstract

The flexible architecture offered by cloud computing allows for the dispersion of resources and data over numerous places, making it possible to access them from a variety of industrial settings. The use, storage, and sharing of resources such as data, services, and industrial applications have all changed as a result of cloud computing. In the past ten years, companies have quickly shifted to cloud computing in order to benefit from increased performance, lower costs, and more extensive access. Additionally, the internet of things (IoT) has significantly improved when cloud computing was incorporated. However, this quick shift to the cloud brought up a number of security concerns and challenges. Traditional security measures don't immediately apply to cloud-based systems and are occasionally inadequate. Despite the widespread use and proliferation of various cyber weapons, cloud platform issues and security concerns have been addressed over the last three years.Deep learning's (DL) quick development in the field of artificial intelligence (AI) has produced a number of advantages that can be used to cloud-based industrial security concerns. The following are some of the research's findings, We provide a detailed evaluation of the structure, services, configurations, and security fashions that enable cloud-primarily based IoT. We additionally classify cloud protection dangers in IoT into four foremost areas (records, network and carrier, programs, and gadgets). We discuss the technological issues raised in the literature before identifying key research gaps. In each class, describe the boundaries using a popular, artificial intelligence, and in-depth studying attitude. and security concerns relating to individuals), which are fully covered, we find and analyze the most recent cloud-primarily based IoT attack innovations, we identify, talk, and verify key safety challenges show the regulations from a standard, synthetic intelligence, and deep learning perspective in every class angle, we first present the technological difficulties identified in the literature before identifyingIoT-based cloud infrastructure has significant research gaps which should be highlighted for future research orientations. Cloud computing and cyber security.

Article History
Received: 09 July 2022
Accepted: 01 November 2022

Keywords
Cloud Configuration;
Cyber Security;
Cloud Computing;
Deep Gaining Knowledge;
Forensic as a Service;
Gadget Studying (Faas);
Improvement as a Carrier (Daas);
Infrastructure as a Service (Iaas);
IoT Safety;
Platform as a Provider (Paas),
Software Program as a Service (Saas).

CONTACT Shipra Yadav ✉ shiprayadav621@gmail.com Lincoln University Malaysia.

Doi: http://dx.doi.org/10.13005/ojcst15.010203.04

Introduction

A large community of IoT-enabled devices and applications makes up a web of factors (IoT)-based cloud structure. Servers, garage, underpinning infrastructure, actual-time processing, and operations are all blanketed within the infrastructure. IoT-primarily based cloud architecture also includes the requirements and services required for safeguarding, managing, and connecting various IoT packages and devices. The traditional IoT architectureis shown in Figure 1, and the IoT-based cloud attack model is shown in Figure 2. The recent decade witnessed the advent of the cloud, and the next decade is seeing the rise of its varieties.[1-3] We observe that among these variations, IoT, or the internet of things, is leading (IoT). Others, however, like service architectures and distributed cloudrecent trends follow it in habitats, data centre operations, and management domains.[4] According to a recent Gartner article, cloud computing is one of the top ten strategic technological trends for 2020.[5] with the market for cloud services likely to increase by 17% during that year.

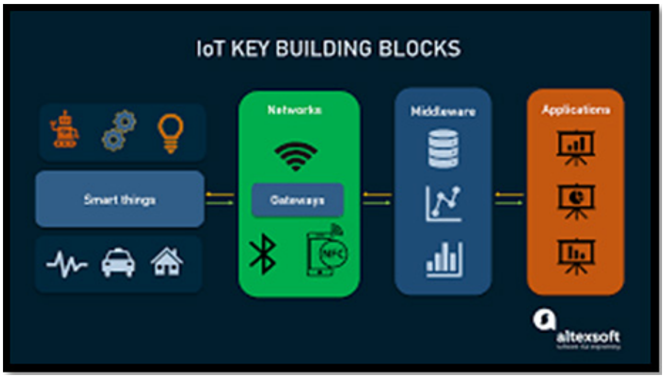


Fig. 1: Typical IOT Architecture

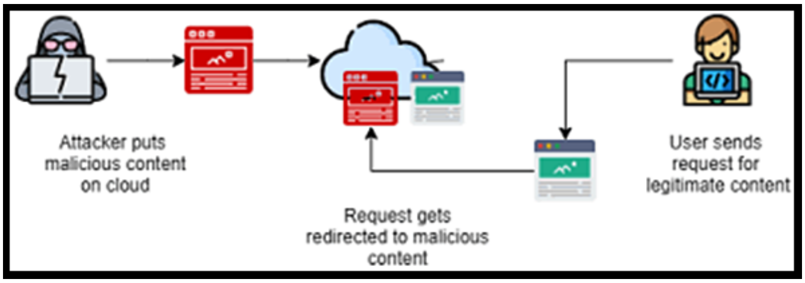

Attacker puts malicious content on cloud
Request gets redirected to malicious content
User sends request for legitimate content

Fig. 2: IOT Based Cloud Attack Model

According to.[6] the phrase "cloud computing" was originally used to describe platforms for distributed computing in the 1990s. As an instance, Amazon delivered Elastic Compute Cloud (EC2) in 2006.[7] Just like something like this, Google launched the beta model of Google App Engine in 2008.[8] NASA released the primary aspect of open-source software, named Open Nebula, for the deployment of hybrid and personal clouds in 2008.[9] In 2008, Microsoft released Microsoft Azure,[10] and in 2010, its open-source cloud computing venture Open Stack was introduced.[11] IBM developed the IBM smart cloud framework in 2011. After then, the first Oracle Cloud started offering software as a service (SaaS), platforms as a service (PaaS), and infrastructure as a service (IaaS) in 2012. More developments in the digital world are on the horizon, therefore this adventure is still ongoing. Figure 3 displays the history of cloud computing.

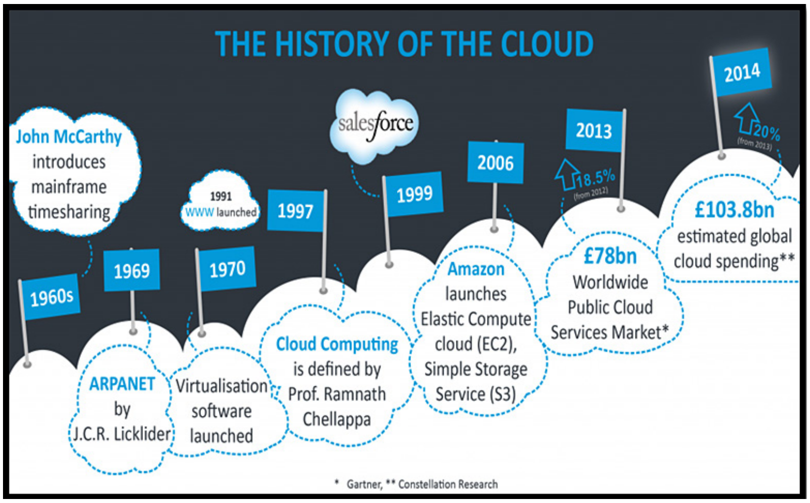

THE HISTORY OF THE CLOUD
John McCarthy introduces mainframe timesharing
1960s
1969
ARPANET by J.C.R. Licklider
1970
Virtualisation software launched
1991 WWW launched
1997
Cloud Computing is defined by Prof. Ramnath Chellappa
salesforce
1999
2006
Amazon launches Elastic Compute cloud (EC2), Simple Storage Service (S3)
2013
18.5% (from 2012)
£78bn Worldwide Public Cloud Services Market*
2014
20% (from 2013)
£103.8bn estimated global cloud spending**
* Gartner, ** Constellation Research

Fig. 3: Cloud computing history

The countrywide Institute of requirements and era (NIST) has highlighted 5 fundamental elements of cloud computing.[12] One is measured service, two is resource pooling, three is quick growth, four is network access, and five is on-demand self-service. Three service types and four deployment models are also described in order to simultaneously provide cloud services. The fundamental goal of cloud computing is to provide online computing services such as servers, storage, databases, networking, software, analytics, and intelligence. Customers can also pick the type and quantity of offerings that excellent healthy their need. Due to the cloud's speedy data storage and access, cost effectiveness, convenience, and flexibility, traditional IT services have migrated there. Organizations no longer have to spend a million on expensive equipment and software to set up on-site data centers thanks to cloud computing. By the use of remote servers to host software and services, cloud technologies automate various sectors. The majority of sectors are currently following this trend, which is growing with each passing year.[13] For a wide range of industrial applications, traditional Cloud computing offers scalability and frequent software and hardware updates.[14–16] Additionally, the cloud offers a variety of security options and allows for effective network resource utilization. With these benefits, it is clear that cloud computing has a lot of promise. An extensive range of destiny opportunities for industries are offered via cloud computing and its supporting technologies, which also have the ability to open up some of packages, solutions, offerings, structures, and other things. Via using DL cloud computing, massive datasets and education algorithms can be consumed. With the aid of utilizing the GPU's processing capability, it could additionally assist DL fashions attain efficiency on a big scale at an inexpensive value.

The success of any cloud-based solution strongly depends on giving cloud directors, software program developers, and cease users the greatest viable enjoy. The adoption of clouds is constrained through unique factors such complexity, compliance, security, dependency, privateness, manage, and value.[17] considering the fact that records and packages might also live at many layers depending at the cloud carrier architecture adopted, security can be seen as a critical barrier in cloud computing. Because of this uncertainty, security has now been identified as the top cloud computing risk.[18] Gartner identified four key issues that could influence cloud adoption in January 2020 as distributed multi-cloud scenarios become more common.[19] Considered one of them is coping with related safety and privacy problems. In conjunction with digital environments, cloud carrier enables for the distribution of heterogeneous statistics and sources. In contrast to the limited storage space, computation power, and hardware that users have access to in traditional software infrastructure for enterprises, users of cloud computing have access to infinite storage space and virtual servers resources as needed. Conventional methods for user identification, authentication, and access management cannot be adapted for the cloud in their current state.Significant security concerns include integrated models, architectures, less user control, and external data storage, User vulnerability will lead to an increase in cybercrimes affecting the people, businesses, and authorities.

Crypto-jacking, denial of service attacks, account theft, and data breaches are all common threats. according to Forbes,[20] Skybox security published a Vulnerability and chance developments document within the center of 2019, with a wide spread upward push within the number of vulnerabilities in cloud bins as the report's fundamental locating (a replacement of conventional VMs architecture). Data on the cloud are more vulnerable to threats than they are in traditional storage architecture. This is so that just the cloud platform, not the client data, is secured by cloud providers.[82] percent of cloud users have encountered security events, consistent with the Oracle and KPMG Cloud risk record 2019.[1] Therefore, it has become crucial to guarantee cloud security and privacy.

The most crucial element for cloud computing to succeed is security, according to research.[12] In 2011,[12] the placement of data was noted as a security problem. Concerns about data security were raised.[14,15] Another element that researchers concentrated on was trust because it is closely related to the reliability of cloud service providers. The provision of the trust version and subsequent agreement with management were critical. Because cloud computing has inherent security difficulties, trust is ultimately the most important consideration.[16] The same data assaults that affect traditional systems also affect cloud-based services. It was noted that the security of the virtual machine was crucial for the integrity of the data stored there and the security of cloud computing.[17]

In order to understand smart IoT cloud systems, references.[18] provides a survey of research articles from the previous five years that focused on consumer-oriented IoT cloud applications. The author conducted a security analysis of the IoT cloud gadget and presented a novel IoT cloud paradigm. Reference presents a paradigm for analyzing privacy and security challenges in social networks built on cloud platforms.[19] From a technological perspective,[30] explores both well-known and less-examined security risks associated with cloud systems for various hacks.

As reported on a triangulated study of the cloud computing difficulties. This three-part study examined the security issues that currently surround cloud computing.[11] In light of these challenges, the study also suggested implications for cloud computing adoption.moreover, writers in[12] supplied every other thorough exam of a safety trouble by using comparing the dangers that cloud systems face in addition to the numerous intrusion detection and prevention methods that are currently in use. moreover,[13] examined the usefulness of query processing algorithms over encrypted data in a high throughput cloud-based device for a real-time context. The multi-dimensional imply failure cost (M2FC), which turned into identified as a quantitative safety danger evaluation version in opposition to the security issues raised with the aid of those researchers, turned into proposed by[14] in 2016. They also counseled appropriate measures to clear up the diagnosed security problems.

The net of factors, cloud computing protection challenges, and cloud accountability troubles were all covered by using the authors of.[15] The authors of reviewed the factors influencing cloud computing adoption, cyber attacks, and suggested remedies for improving privacy and security in cloud-based systems.[16] The authors of[17] provided a thorough overview of the research on cloud security challenges, vulnerabilities, threats, and attacks, as well as a classification system for them. In order to more effectively protect data, authors in[18] recognized privateness techniques in IoT-based totally cloud-based structures. Ultimately, writers in[19] furnished a top level view of the most important protection issues in cloud computing and cloud infrastructures primarily based at the internet of factors.

Methodology

Based on previous research investigations, the proposed research survey is carried out. We create a good method for paper selection. We choose papers from various sources based on the following screening process.

- For the suggested survey, we collect IoT-based cloud computing publications from 2015 to 2021.
- Studies that have not been published in English are not included.2022, 11, 16 5 of 34 Electronics
- Research which can be irrelevant to the scope of the IoT-primarily based cloud computing survey is eliminated.
- IoT-based cloud safety and privateness are the important thing topics of debate at the same time as choosing papers.
- To reduce duplication, the research publications that have been published on the same concept are removed.
- We concentrate on the studies that carried out tests on cloud infrastructure based on the Internet of Things.

Quality Analysis Criteria

To ensure effectiveness, the research studies chosen for the planned survey are subjected to a number of quality analysis criteria. We choose more than 100 research studies from various sources for the survey. The chosen papers are cross-checked using the quality analysis criteria listed below.

- Do the chosen studies supplement the advised survey?
- Does the chosen research fall within the scope of the survey? Performs the chosen studies. Adhere to the proper standards?
- Are the findings of the chosen research conclusive?
- Does the author employ the right methods and features?
- Are the chosen research objectives spelled out in detail?
- Is IoT-primarily based cloud safety the principle emphasis of the selected studies?
- Does the chosen research conduct any IoT-based cloud-related experiments?

Contributions

Researchers have previously investigated and drawn interest to privateness and protection issues with IoT cloud computing. But cutting-edge studies[10-12] both talk safety challenges generally or have focused on research primarily based on a small number of parameters. The primary contributions of this observe are as follows

- A complete survey of IoT cloud structure, services, configurations, and safety models is included within the research. We similarly classes IoT cloud protection risks into four fundamental companies: facts, network and provider, apps, and security concerns relating to human beings.
- Recent developments and trends in IoT cloud-based threats are identified and examined by the research.

Paper Structure

The majority of the essay is organized as follows. Background information on cloud designs, cloud kinds, and the SPI model is provided in Section 2. A thorough overview of prior work that has addressed security challenges in cloud computing is provided in Section 3. The cloud configuration is presented in Section 4. Information on cloud-based assaults is detailed in Section 5. Details on security-related issues is provided in Section 6. The challenges and restrictions of cloud computing are then discussed in Section 7. Section 8 presents future work. Finally, Section 9 brings our study of the highlighted security vulnerabilities to a close.

Background

Cloud computing and the Internet of Things have recently been the most popular technologies.[43] Current trends predict that the rate of development of digital technologies will be exponential, and the combination of these two technologies can result in efficient resource management. Before moving on to security concerns and problems, this element offers a quick advent of the various cloud designs, cloud kinds, deployment fashions, and related attacks. A new aspect of DDoS assault termed as financial denial of sustainability (EDoS) has evolved in the contemporary IoT-based cloud computing generation.[14] EDoS is defined as the expanded use of flexible packaging, using the server-shared dimension service as an example Electronics 2022, eleven, sixteen 7 of 34. (Something cloud server). Remote sensing robots that reload the target cloud service with a covert vulnerability detector request can conduct EDoS attacks. Students will have access to cloud services in this manner with scalable customization. A client account can be obtained by adhering to the pay-as-you-go concept. After that, demand that the clients accept cloud services in order to charge them for these incorrect orders. The worst consequences will result from these flaws. This will result in the loss of cloud computing clients, as they will opt for the less expensive and more effective option and support their operations from their corporate offices and data centers rather than making irrational demands to the cloud[15]

Cloud Architectures and Deployment

To address both small- and huge-scale commercial enterprise troubles, cloud architecture consists of numerous cloud components, including statistics centers, software program functions, offerings, and programs, organized optimally. The purpose of cloud structure is to provide quit customers excessive bandwidth, reliable get right of entry to their records and packages, and an on-call for network this is relaxed and adaptable.[6–10] The components and interactions between those components are typically laid out in cloud architecture. The following are a few crucial elements of generic cloud architecture records and resources on-hand on the purchaser, records and assets in the cloud, software additives and offerings, and middleware are indexed in that order. The cloud's features and surroundings can be diagnosed primarily based on its deployment model. Figure 4 represent the deployment model.

Figure 5 represents the NCC-SRA method for data series; aggregation, and data category with cloud recognition.

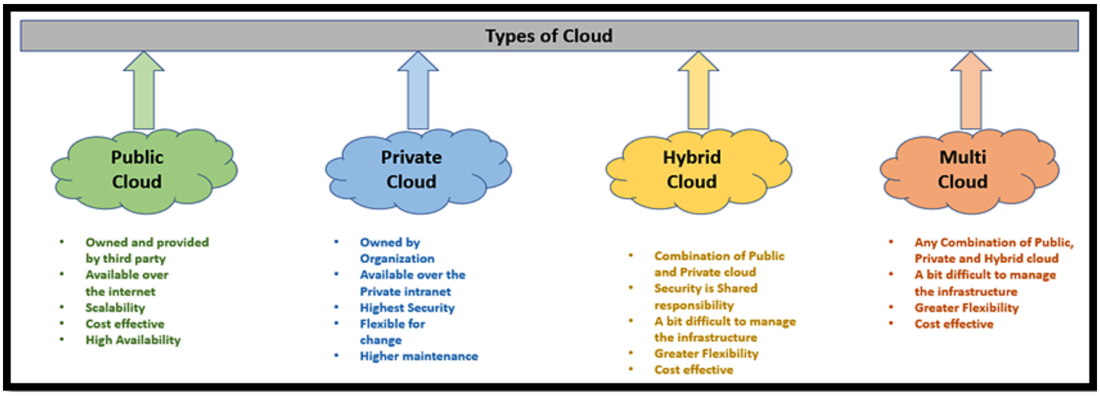

Types of Cloud
Public Cloud
Private Cloud
Hybrid Cloud
Multi Cloud
• Owned and provided by third party
• Available over the internet
• Scalability
• Cost effective
• High Availability
• Owned by Organization
• Available over the Private intranet
• Highest Security
• Flexible for change
• Higher maintenance
• Combination of Public and Private cloud
• Security is Shared responsibility
• A bit difficult to manage the infrastructure
• Greater Flexibility
• Cost effective
• Any Combination of Public, Private and Hybrid cloud
• A bit difficult to manage the infrastructure
• Greater Flexibility
• Cost effective

Fig. 4: Types of cloud architectures

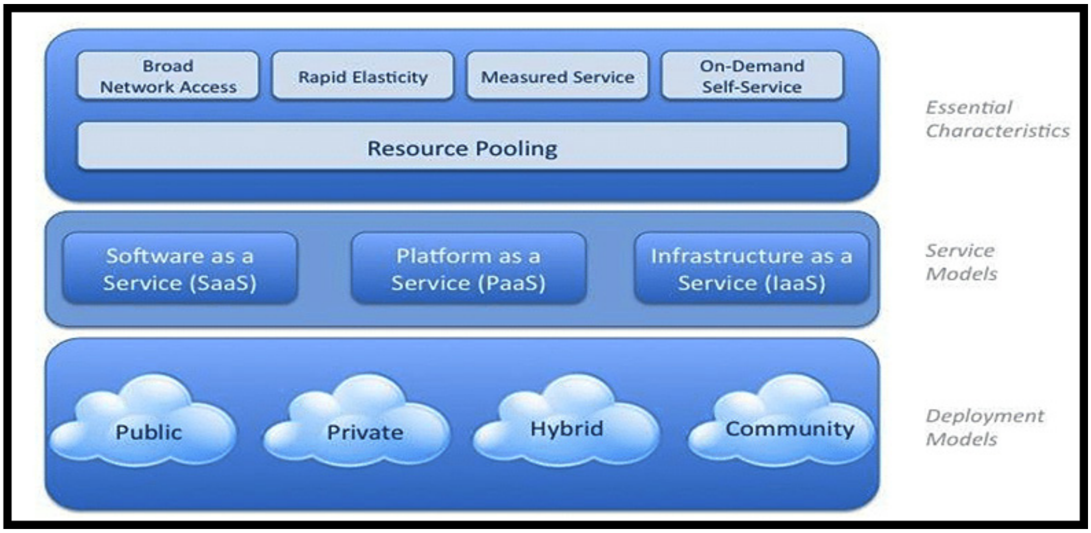


Fig. 5: Cloud Computing NIST Cloud Computing safety Reference structures.[15]

Service Models

By the type of service model it provides, cloud computing can be divided into one of three categories. Infrastructure as a Service (IaaS) (IaaS) IaaS capacity is raw storage space, processing power, or network resources that the customer can use to run and execute any operating system, application, or software of their choice.

Public Cloud

In this kind of cloud, there are public clouds owned and run by various organizations. These resources, infrastructures, and networks are used concurrently by thousands of individuals and organizations. A number of the public cloud providers consist of Google, Amazon, and Microsoft. On this type of cloud, useful resource allocation, possession detection, shared access control, and cloud data security from attacks are critical issues. Reliability, geographical independence, software-fashion costing, price effectiveness, extremely good scalability, and versatility are benefits of using public clouds. Low safety and limited customization are drawbacks of the use of the general public cloud.[12]

Private Cloud

This type of cloud is frequently managed by a single commercial enterprise and is more specifically designed to meet those requirements. Private cloud garage permits businesses to have better data control (perhaps susceptible to regulatory compliance necessities). Either a third party or internal staff can administer and host it. These details may also include trade secrets, medical records, or other sensitive information. The infrastructure is owned and run by the same company. The infrastructure in private cloud solutions is either managed or used by the organization, or it is supplied by the cloud service or infrastructure provider. In contrast to other cloud systems, private cloud security is crucial.[13] It is easier to identify users and vendors, as well as manage security concerns, than it is in a public cloud. Utilizing a private cloud has the benefits of increased security, privacy, control, affordability, and energy efficiency. Private cloud usage has drawbacks including rigid pricing and reduced scalability because of few resources.[12]

Hybrid Cloud

In the hybrid cloud approach, a private cloud is connected to one or more external clouds. Multiple cloud environments with manageable and portable workloads are connected and managed centrally in this way. For instance, a company can manage security between private and public clouds while keeping sensitive data in the former and generic data in the latter. The security of the hybrid cloud is thought to be more trustworthy than that of the public cloud. Utilizing a hybrid cloud has the benefits of flexibility, scalability, security, and cost effectiveness. Networking difficulties and security compliance are drawbacks of hybrid clouds.[12]

Multi Cloud

This model includes a system with many clouds. Clouds can be private or public, and they are now not usually connected. That is frequently known as a network cloud in literature. The blessings of the usage of a multi-cloud system consist of resource pooling and higher protection than a public cloud Electronics 2022, 11, 16 9 of 34. The disadvantages of public cloud include lower security than private cloud and the need for management policies to be controlled.[12] As was already mentioned, cloud architecture has advantages and disadvantages. The model used will depend on how much storage, availability, efficiency, and security are needed by the user and the organization.

Cloud Services

Software as a Services (SaaS)

The SaaS model gives users access to databases and software. Applications allow users to get information.[14] Customers do not need to install software on their local PCs due to the fact this version renders apps inside the cloud across a network.[15] The cloud provider installs, hosts, and operates software on the cloud, and the user gains access via the cloud customer. As a result, a single service instance can serve many users. The hosted application is run by the CSP, who also oversees and guarantees the system's uptime.[16] Some examples of SaaS include Google Applications, Microsoft Office 365, Drop box, and Trade Card. Three of SaaS's main benefits are scalability, multi-tenancy, and load balancing.

Platform as a Service (PaaS)

Databases and alertness platforms are made to be had to users as a service under PaaS. It combines running device and alertness servers, such as Google App Engine, Microsoft Azure, and the LAMP platform (Linux, Apache, MySQL, and Hypertext Preprocessor). The PaaS approach improves application efficiency and places a strong emphasis on data security. The cloud service provider offers a platform that lets users create, run, and administer applications without having to worry about the difficulties of setting up and maintaining the infrastructure. By allowing the application-hosting environment to control the network, storage, and processing infrastructure, users lose control of the network, storage, and processing infrastructure.[17] Users of this paradigm consequently feel less in control and have access to fewer operational features.

Infrastructure as a Service (IaaS)

IaaS offers computational energy and garage as standardized community offerings if the customer is given online offerings to get admission to, procedure, store, transmit, and execute their programs and facts through the cloud. Virtual machines (VMs) are used to grant computing resources, and block storage and object storage are used to grant storage resources.[18] To workout manipulate over the deployed OS, storage, and programs, the consumer does not always want to exercise manipulate or management over the underlying cloud infrastructure; every now and then, there is limited control over a small range of network additives.

Construction as a Service (DaaS)

An internet-primarily based community shared improvement tool is shared by using several users consistent with the DaaS idea. This is comparable to using a development tool locally on a computer in a conventional paradigm. In the world of software development, this is a recent trend.

Forensic consulting (FaaS)

In terms of large (petabytes) storage for collecting useful forensic statistics and sources for high computational power, cloud forensics significantly outperforms traditional digital forensics.[9,10] The FaaS architecture is specifically made to assist forensic investigators in centrally evaluating a significant volume of data that is physically unreachable or located at an unknown physical location. Electronics 2022, 11, 16 10 of 34 Investigators continuously collect data and transfer it to a centralized system. Investigators are able to examine a tiny group of traces from enormous stacks as a result,

Information Sharing

Unauthorized users may receive information as a result of some nefarious activity. One method of leaking such information is through VM configuration theft,[11,12] which searches for open ports to find services and the vulnerabilities connected to them.[13] In the cloud, both internal and external disclosure is possible.

- An internal disclosure is when a manager or employee accidentally makes private information public, which would result in such a revelation. Insufficient awareness of the sensitivity of information or a lack of care in shredding could lead tosuch admissions. Internal attacks may put some users in danger and allow total in charge of them.[14]

- An outside disclosure is one which seeks to accumulate the gadget-specific facts of the provider information.For instance, it could comprise temporary files, backup files,Version numbers, patch levels, and software distribution. In order to stop such attacks where there is a possibility of information leakage, third-party authentication and the usage of encryption techniques is common.[16]

Additional Work

The use of cloud computing has grown significantly in recent years. Several studies have therefore addressed protection threats, vulnerabilities, troubles, problems, and countermeasures. This section covers the associated cloud computing work security issues.

The writers of[15] explored cloud computing topologies, security concerns, problems, and solutions. While discussing the supporting technologies, the study additionally addressed contemporary deployment fashions, cloud offerings, and cloud architectural frameworks.

While in[11] the authors emphasized the significance of information safety in cloud computing and defined the drawbacks of information leaks or breaches in cloud computing, the findings of this look at have been utilized to discover open research guidelines within the cloud safety area.Nevertheless,[14] omitted to address the issue of data leaking and how it is resolved, as well as how important data are compromised and leaked via cloud computing.[16] Examined cloud computing architectures, carrier models, deployment models, and cloud components, and safety challenges; however they did no longer examine the literature's hints for resolving the issues.The authors identified data transfer in the cloud-related security risks. They disagreed at the deserves of using public key infrastructure (PKI), the lightweight directory get admission to protocol (LDAP), and the position of a depended on third party (TTP) as safety features to ensure the supply, authenticity, confidentiality, and integrity of facts in the course of connections. The authors of[17] conducted a qualitative exam of each carrier model's vulnerabilities and associated threats. They also suggested defenses to boost cloud computing security. The authors' main emphasis in[8] is on the vulnerabilities and related dangers that are raised by the flaws. The authors avoided addressing existing issues brought up by the identified vulnerabilities and dangers as well as potential future research directions.

The authors of[18] mentioned a vacuum within the literature regarding the mapping of protection challenges to their corresponding answers and the requirement for a fashionable framework for generalizing the idea even as carrying out an intensive evaluation of particular needs. The authors also talked about unresolved issues and potential future research areas. Resource scheduling and cloud security were the subjects of a thorough literature study conducted by the authors of[19] in order to identify the pertinent work completed to date. The writers of identified several risks and any potential literature-based solutions.[9-12]

DL asserts success in a variety of cloud computing domains, including speech, picture, and biomedical data processing.[13–16] DL architectures are configured as multilayer neural networks, and they are capable of transforming data into more abstract expressions and higher levels. Assume the data are high dimension already. Then, high dimension data input can be rebuilt using different neural networks (NNs) trained with a shallow core layer, resulting in low quality data.[7] It was suggested that by improving the inherent characterization of the data from these features, better categorization or data visualization may be accomplished. Functions can be broken down into simpler functions to better understand formations by using specific data. The various layers of the artificial neural network were found to contain an unusual characteristic of learning capacities by.[18] These authors also suggested layer-by-layer "pertaining" and weight tuning in nonlinear auto-encoders as solutions to the problem.

In[19], authors explored data security issues from the viewpoint of Nepal, a developing nation, in 2019. The study outlined the difficulties that developing nations confront, which includes confidentiality, charging models, breaches, segregation, access, integrity, security, storage, records centre operation, billing models, costing models, and proximity. The key security problems identified by this research's conclusions were storage, virtualization, and networks. Based on the security hazard provided via public clouds and cautioned protection techniques, authors in[10] tested the public cloud security safety technique.

It is necessary to draw attention to and deal with new security concerns in the cloud computing industry. The information from related surveys and studies about security concerns in cloud computing that were previously published is summarized in Table 1.

Configuring the Cloud

The cloud is set up to offer services to customers while utilizing a secure connection and delivery method. NIST claims that the configuration process can be broken down into five distinct tasks that are carried out by individuals in various positions. Table 2 displays the cloud's configuration and lists the organizations and their respective roles.[11,12] The cloud corporation uses all of its resources to meet customer demands. The five jobs in table three are stuffed with the aid of individuals who take part in duties like cloud computing transactions, that's why the cloud also concentrates on risks and danger-assessment of cloud purchasers and cloud carriers.

Table 1: Summary of Additional work.

Year	Survey	Focus	Key Feature and Limitation
2017	Mushtaq *et al.*[16]	Cloud design and deployment	• Cloud computing design included cloud components, deployment models cloud security, and explored cloud service Models.
2018	Basu *et al.*[17]	Cloud models and security	• Discussed different cloud properties and models from security Perspectives.
2019	Sheikh *et al.*[18]	Cloud situation categorization	• Provided systematic literature review to help the reader find Relevant research articles on the associated topic.
2019	Khandelwal *et al.*[19]	Cloud security issues and solution	• Created a list of cloud computing architecture that identifies security issues and finds solutions.
2019	Ghaffari *et al.*[20]	Cloud security challenges	• Identified cyber security challenges and solutions
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.

Table 2: 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.

Cloud Consumer

A group of people who use cloud providers' services are referred to as cloud consumers. The cloud user may be presented with a variety of services from which to choose the best one and enter into a contract. To complete the settlement, the cloud customer bureaucracy enters into a service stage agreement (SLA) with the cloud issuer, and then they examine the service's technical overall performance.

Provider of Clouds

A special organization that provides offerings to cloud customers and closes deals on behalf of cloud companies is known as a "cloud issuer."

In SaaS, cloud service providers offer services for the deployment, upkeep, and updates of software and applications. On the other side, with PaaS, the cloud software program offers the infrastructure and surroundings components, consisting of the database, pinnacle software program, or other vital factor. The bodily laptop assets, which include storage, servers, networks, and web hosting infrastructure, are acquired through the cloud issuer.

Cloud Inspector

A team of specialists known as the cloud auditor can independently check cloud services for any anomalies. The auditing institution inspects the requirements via inspecting tangible portions of evidence, and the cloud auditor additionally examinesthe privacy impacts, security measures, and efficiency of all cloud-related procedures.

The Cloud Broker

The management of performance, consumption, and the provision of cloud services is handled by the cloud broker. In preference to contacting cloud providers at once, cloud clients utilize cloud brokers to attain cloud offerings.

Cloud Carrier

Among the cloud issuer and the cloud client, the cloud provider establishes a connection. Making use of this connection, the cloud offerings are provided to the user across the community. The cloud company is also in charge of retaining a comfy connection.

Cloud-Based IoT Attacks

Cloud service providers are often thought to be in charge of cloud security. However, more and more enterprises, data, and applications are being moved to the cloud in recent years.[13] Cyber attackers' priorities have altered as a result, and they now consider cloud services to be a more profitable target.[14] Figure 6 provides a representation of the cloud system's components, attacks, and vulnerabilities that can be examined to identify new points of weakness. Security threats in cloud computing are the most serious concern when investing in cloud services. This is due to the fact that a third-party provider stores and processes the user's information without the user's knowledge. Every day, users are made aware of issues such as weak authentication, stolen credentials, account hacking, data breaches, and so on. IoT cloud computing is used as part of a collaboration to store IoT data. A cloud is a centralized server that houses accessible computer resources at all times. The internet of things has produced massive data packages, which can be easily sent using cloud computing. Unlike the IoT, where scenario detection depends on the combination of data, the old internet connects users by using physical linkages between web sites. The characteristics of IoT-based cloud attacks are shown in Table 3.

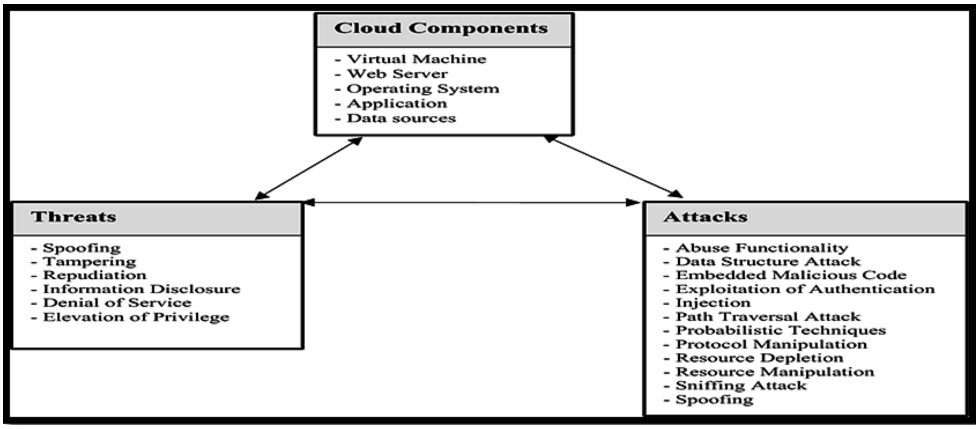


Fig. 6: Attacks, threads, and components on cloud.

Table 3: 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.

Hijacking an Account

This is a type of attack when a hacker steals or commandeers the cloud account of a person or business. Sometimes the main objective is the person or business, and other times the attacker utilizes the stolen account information to carry out a subsequent attack. A later impersonation by the attacker could result in the leakage of confidential corporate information and sensitive individual data as well as reputational harm.[15] Figure 7 illustrates this attack in visual form. Businesses and numerous organizations can safeguard their data by adopting simple measures. Within a cloud. The subsequent are a number of the only techniques to prevent cloud account hijacking.

- Check along with your provider company to affirm that personnel who've direct access to the server have undergone historical past exams.
- Have a solid authentication plan in place for cloud app users.
- Block access to cloud apps from specific IP addresses. Many cloud applications allow users to select IP ranges from which to connect to the service via a VPN or their workplace network.

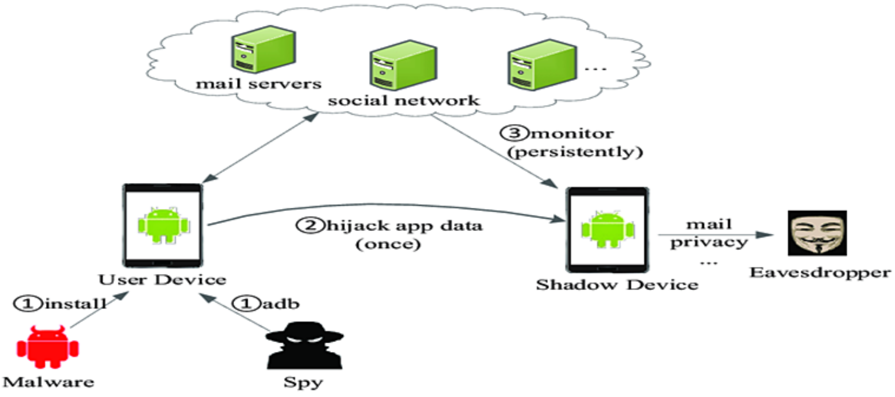


Fig. 7: Graphical Representation of an account hijacking attack [15].

Attacks on a Denial of Service

The most frequent and straightforward attacks on IoT systems are denial of service assaults. This type of cloud attack can be quite harmful because it prevents the intended user from accessing the services, applications, or data.[16] to be able to deprive different requesters of provider, the attacker bombards the focused machine, application, or service with numerous requests until ordinary site visitors becomes tough to deal with. It ultimately will become irresponsible for the cloud service proprietor to boost the elasticity tiers to control the rising visitors and use extra digital resources to fulfill the request and preserve the nice of carrier (QoS). Additionally, denial of service can operate as a catalyst and a smokescreen to hide malicious actions that get past the cloud firewall, which means that it can swiftly spread to destroy multiple devices rather than just one.[17] DoS attacks are used to prevent customers from accessing cloud networks, IoT, and other computer services. A denial of service (DoS) attack in the Internet of Things (IoT) aims to bring a system or network to a halt and make it unavailable to its intended users. Although DoS attacks are difficult to detect and avoid, we outline several approaches.

Prevent Spoofing

Use filters to stop spoofing of dial-up connections and make sure that the source IP cope with of the traffic fits the list of addresses for the website online of starting place. Limit broadcasting: By sending requests to every device on the network, attackers usually escalate their attack. By restricting or turning off broadcast forwarding whenever possible, attacks can be stopped. Users can also disable the echo and charging services when it's practical.

Streamline Incident Response

By streamlining incident response, the security team will be better able to react rapidly when DoS threats are discovered.Safeguard endpoints Verify that any known vulnerabilities have been fixed on these endpoints. All endpoints with the ability to run EDR agents should have them installed. Firewalls should be activated, Whenever possible, make sure the firewalls limit traffic entering and leaving the perimeter.

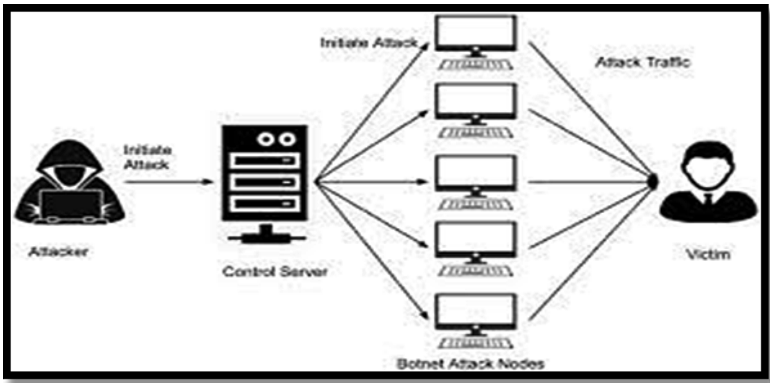


Fig. 8: Graphical representation of a denial of service attack [17].

Attacks by Phishers

Phishing attempts against cloud service providers entice clients by sending them a file or image and requiring them to log in with their account information in order for you to access it.in this type of assault, the perpetrators ship phishing emailsto get login information for personal or corporate accounts and access to sensitive information in order to set up the attack and avoid being discovered.[18,19] Figure 9 shows a graphic picture of this assault. A cloud computing system is susceptible to two different kinds of phishing assaults. The first involves taking control of the accounts via customary social engineering approaches, and the second involves abusive behavior in which the attacker hosts a phishing attack website using some cloud services.[20]

How can phishing be stopped, and how might a cloud help? Provide a solution? Users must follow these steps to guard against phishing attempts on the IoT device.

Steps.

- Be careful when using any emails or websites.
- Double-check a link before clicking on it.
- Avoid mailing any private or business information.
- Finally, alert website and email administrators to any questionable activity.

From this list, it is possible to see how a cloud solution might be useful. By limiting access to dangerous files and filtering incoming correspondence, a cloud-based email system, for example, can detect and assist in the defanging of malware. It can also provide the two-way communication required to warn the user and others about phishing attempts. The information gathered aids in the enhancement of the software's

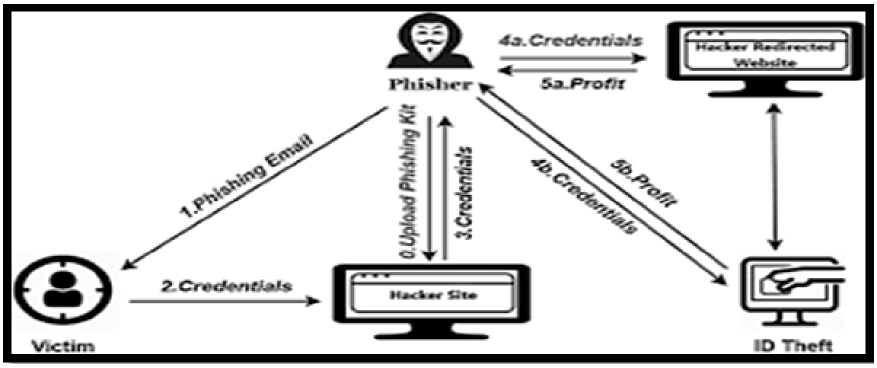


Fig. 9: Graphical representation of a phishing attack.[10]

Attacks Utilizing Malware Injection

Malicious programmes and services are attempted to be injected into the cloud during a malware injection attack.[11] With the cloud idea in thoughts, the attacker executes this assault the usage of a spread of strategies. The attacker starts offevolved by way of creating a malicious service utility module or virtual gadget example on its own, then attempts to feature it to the cloud.

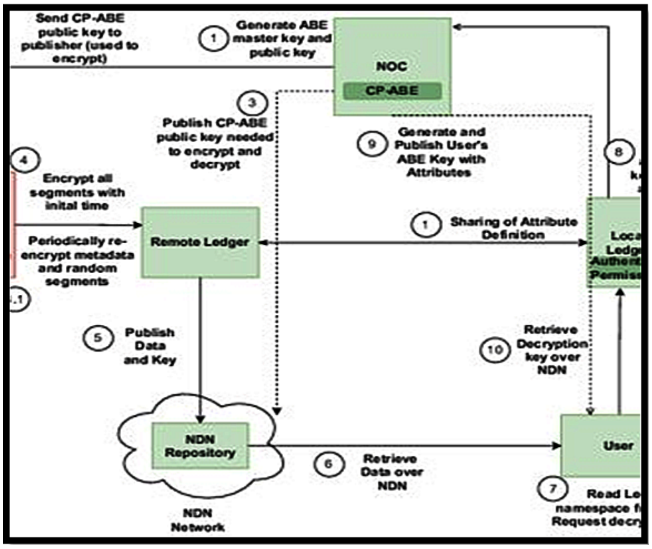

Send CP-ABE public key to publisher (used to encrypt)
1
Generate ABE master key and public key
NOC
CP-ABE
3
Publish CP-ABE public key needed to encrypt and decrypt
9
Generate and Publish User's ABE Key with Attributes
8
4
Encrypt all segments with inital time
Periodically re-encrypt metadata and random segments
.1
Remote Ledger
1
Sharing of Attribute Definition
Loca
Ledg
Authent
Permiss
5
Publish Data and Key
10
Retrieve Decryption key over NDN
NDN Repository
6
Retrieve Data over NDN
User
7
Read Le
namespace f
Request decr
NDN Network

Fig. 10: Graphical representation of a malware injection attack.[12]

Attacks Using Port Scanning

In this type of assault, attackers may find open ports and utilize them to launch an attack on services using those ports.[13] The confidentiality and integrity of the cloud may be compromised as a result of this kind of attack[12,14] Figure 11 suggests a picture representation of the port scanning assault. Having enough, current danger statistics that is in sync with the evolving danger panorama is vital for stopping a port test assault. To display ports and prevent malicious actors from getting into their community, corporations also need dependable security software program, port scanning gear, and protection indicators.Tools like Net cat, Nmap, and IP scanning are all helpful. Following are some of the defense mechanisms:

A Strong Firewall

The use of a firewall effectively prevents unauthorised access to a company's private network. It manages ports, determines their visibility, and detects when a port needs to be changed. While a scan is running, it is turned off.TCP wrappers the use of them, directors can allow or deny get rights of entry to servers based totally at the domain names and IP addresses. Discover community vulnerabilities: Businesses may use a port scanner to determine whether other ports are being left open for no apparent reason. They must perform regular system audits to identify any vulnerabilities or gaps that a malicious threat could exploit.

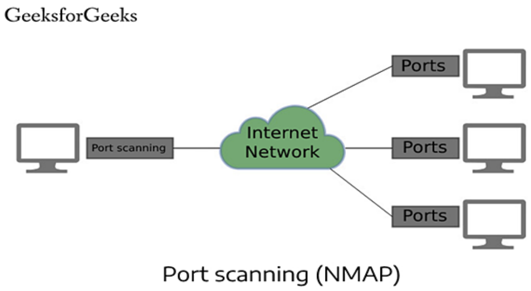


Fig. 11: Graphical representation of a port scanning attack.[13]

Man-in-the-Middle Attacks

In a person-in-the-middle attack, an attacker secretly is based on parties. In this case, listening in at the information can help the attacker in converting the message. Additionally, the attacker may change message relays.[15] If the communication channel is additionally infiltrated, this type of attack can happen during an ongoing conversation in order to get sensitive information being yielded.[16] Figure 12 shows a graphic representation of this assault. Depending on the vulnerability point used, the present IT protection architecture, and customers' attention of capability IT safety dangers, detecting guy-in-the-middle attacks might be hard, in this case, prevention is vastly superior to treatment.The most effective method of preventing a man-in-the-middle attack is to use a strong encryption technique between the client and the server. The connection cannot be established until the server sends and examines a digital certificate to authenticate the client's request.

While designing and marketing IoT devices, identification and authentication should be taken into account. on account that a man-in-the-middle assault revolves round delivering false facts and posing as a device to every other tool or user, users need a mechanism to affirm that the devices and those they connect to are who they claim to be. To further protect themselves from man-in-the-middle attacks, users should take the following steps: Use virtual private networks (VPNs).

- Use HTTPS to ensure the security of critical online transactions and logins,
- Create unique Wi-Fi networks,
- Encrypt emails using SSL/TLS,
- Construct a mechanism for detecting intrusions (IDS).

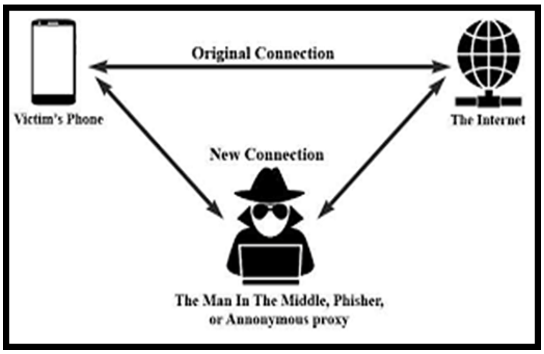


Fig. 12: Graphical representation of a man-in-the-middle attack.[16]

Botnet Attacks

A network of infected computers under the collective management of hackers carries out destructive actions in this kind of attack on the cloud.[17] Botnet spread by way of vigorously scanning the computer systems or network devices for weaknesses while going through a listing of IP addresses. User networks, companies, and customers are all seriously at risk from Botnet.[18] Botnets can use a user's community to carry out harmful actions such as distributed denial of service (DDoS), spamming, data theft, and phishing attacks. They take advantage of today's sophisticated cloud computing platform. A bot master can also create Botnet using cloud services. Cloud-based Botnet, also known as bot-cloud, may get online quickly and continue to work uninterruptedly. Attackers launch challenging to stop or even notice attacks using Botnet.[19] which makes it one of the attacks that causes the victim the most harm. Figure 13 displays a graphic representation of the Botnet attack. Nowadays, there are many Botnet on the cloud, making prevention essential yet challenging. In order to take advantage of security flaws and vulnerabilities, Botnet are continually evolving. As a result, every Botnet may differ greatly from one another. Botnet operators are well aware of how difficult it is for bot defence solutions to reliably display screen out malicious requests for access to websites and APIs while also granting access to legitimate requests from clients or partners the greater IP addresses and devices they use in their attacks. Advanced detection skills are needed to recognize and stop Botnet attacks. The following are a few of them.

- Update the software,
- Carefully watch the network,
- Keep a record of failed login attempts.

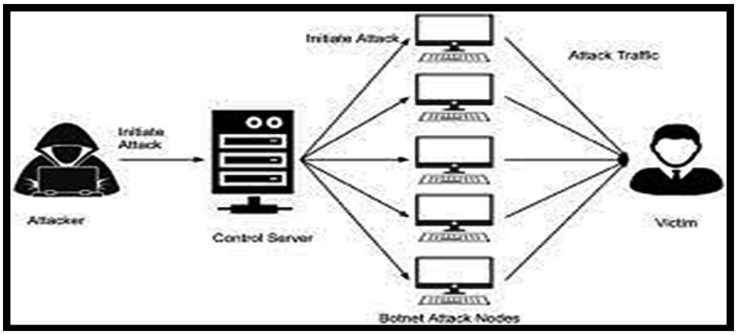


Fig. 13: Graphical representation of a Botnet attack.[19]

Table 4: 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

Security Service

In Table 5, many services utilized to safeguard our data are included together with an appropriate illustration of each sort of protection. The different security types are non-repudiation, authentication, confidentiality, integrity, and availability.[10]

Security Concerns

Major cloud security risks and challenges are identified and discussed in this section. Something terrible that could happen to digital assets stored in the cloud is referred to as a security issue in the cloud. Data, software, infrastructure, client trust, and organizational reputation are some examples of these assets.[13] This study divides security concerns into the following four groups (1) data security concerns, (2) network and service security concerns, (3) application security concerns, and (4) security concerns involving people. This classification was created with the most recent trends in assaults on cloud computing platforms in mind. Table 6 provides a quick summary of each category, while Figure 16 provides a summary.

Table 5: 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 a pplications 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

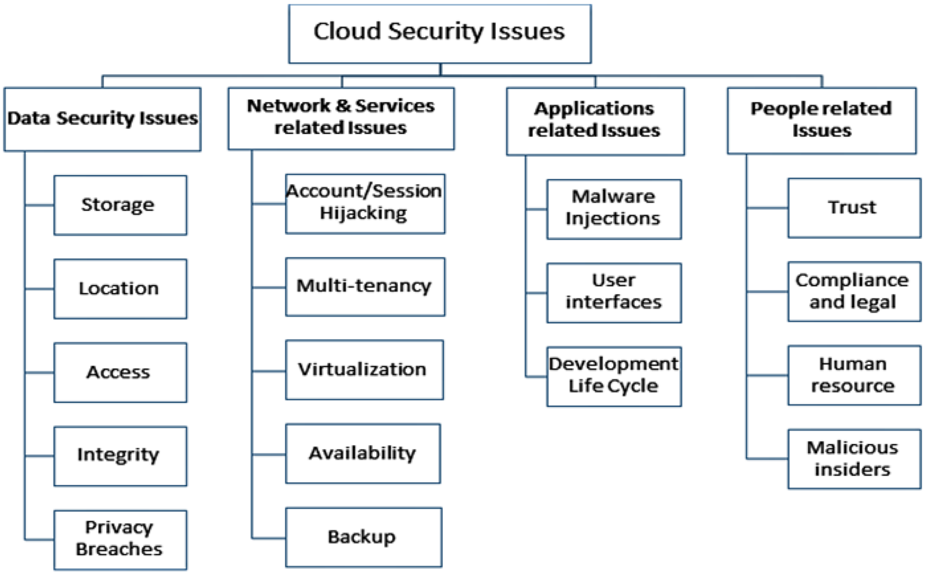


Fig. 16: Summary of security issues in each category.

C1 Issues with Data Security

Numerous papers and articles[14–16] list data security concerns as one of the top ten cloud security threats for 2020. Private personal information is included in both user and company data. Companies have to acquire users' settlement earlier than retaining, collecting, or making use of their non-public facts according with the general statistics safety law (GDPR) policies. The 2019 Chinese release of cyber security classified protection 2.0 also addressed data backup, recovery indications, data secrecy, and data integrity.Utilizing user data that is stored at many locations during processing and shared with stakeholders as and when necessary, cloud computing is a special form of data sharing. Therefore, SaaS, PaaS, and IaaS consumers have serious concerns about data security in the cloud. Data security strives to prevent anyone from requesting unauthorized resources and to restrict access to data to those who have properly authenticated. It also allows legitimate users to view, transfer, or modify just the data that they are authorized to it concerns are among the top ten anticipated cloud security threats.

Storage

Most of the time, cloud computing models don't give users access to the data kept in the cloud service provider's data centers.[17] Despite having a control over the digital machines, there's a loss of manage over the statistics garage. Attackers may modify the facts after a user loses command and control even as importing it to the cloud.[18] Furthermore, cloud service providers can copy, manipulate, or modify user data without the user's knowledge. This causes a slew of storage-related security issues. Encryption is used to give users more control over their data, but it is insufficient and has drawbacks.

Location

In cloud computing, data are scattered across several geographical locations and in various formats. It is challenging to pinpoint the exact location of each data point. Additionally, there are laws and regulations for data handling specific to each geographical area that must be adhered to. The area in their data or statistics can also every now and then be required of customers or users, and cloud service carriers may be pressured to present this information.When a user uses a public cloud, useless programmes could be saved there. At order to maintain high accessibility, the cloud provider may additionally forge the data in several locations across different countries. As users relinquish control over their data, there is therefore possibility for exploitation, and worries are likely to arise in the absence of proper information.

Access

To prevent unauthorized access to services and stored data, it is essential to monitor user identification and activity while preserving user data in the cloud. Access controls guarantee that data confidentiality is maintained. Because data owners and data are spread across multiple platforms and locations, it is difficult to manage access and identity controls in cloud computing. Organizations cannot rely solely on their authentication and permission procedures in cloud-based systems. The resources in the cloud are flexible and change size in response to user demands. When services begin or are restarted in various costing models, service providers' IP addresses are continuously altered. To provide security, a variety of key management systems and encryption methods are used.A quick identity management system should be included in a cloud to track people joining and leaving its resources. There are many problems with identification control and get entry to manage; as an instance, the issue of vulnerable credentials may result in a leisurely rest, insufficient logging and tracking, money owed being locked for the duration of DDoS attacks, useless tenant segmentation, and bad identity control.[19]

Integrity

Integrity entails correcting errors in data. The goal of cloud-based systems is to guarantee that the data is stored in entire form and that it accurately and precisely flows into the database through the service. The user(s) or system(s) that created the data should be identified. Data should always have time stamps and be retrievable as needed.

Additionally, the data must be accurate and comprehensive. Data integrity issues are exacerbated in cloud computing environments because users have no control over where their data is saved, who can access it, and how.[11]

Privacy Breaches

Considering unencrypted records are stored on a pc that is owned and operated by a person other than the real information owner, records privateness is an difficulty that includes cloud computing. Any cloud statistics breach may want to make sensitive information accessible to customers of other firms that share the identical garage. due to multi-tenancy, purchasers the use of diverse apps on virtual machines may additionally share the same database,[11-14] and an incident of compromise may have an effect on all users in addition to the one for which it was intended. When examining data privacy incidents, "when, how, and to what extent" are three crucial factors that must be taken into account.[12] When, how, and how much of the released data were made public.

It must implement laws, policies, and procedures to secure personally identifiable information in order to maintain privacy.[11] Any cloud user who accesses sensitive data is not permitted to do so, and the cloud service provider must report the violation as soon as possible. Various privacy concerns arise depending on cloud architectures and settings.

Network and Service Security Issues Associated

This class includes community and carrier-related security issues like account or consultation stealing, virtualization, and issues with multi-tenancy and availability.

Hijacking Account or session

Cloud users can access their data and services via cloud-based technologies. Sessions, as well as user credentials, can be hijacked. Passwords are used by attackers to gain access to cloud service resources, and these credentials and account information are occasionally changed.

An unauthorised person with a password can access the consumer's data, which they can then sell, change, or steal for their own malicious purposes.

Private information may be fabricated or leaked as a result, harming the reputation and integrity of the firm and costing customers or businesses money. If consumers' confidential data is exposed during account hijacking situations, legal repercussions for businesses in sectors like healthcare are also conceivable.[13] These problems can be prevented to some extent by safeguarding credentials, utilizing two-factor authentication, and closely watching operations.

Multi-tenancy

A couple of customers of a cloud supplier can share the equal computational assets, which include software, hardware, offerings, community resources, and statistics, through multi-tenancy in cloud computing. Users of the cloud do share assets, however their records is saved aside. a couple of users can percentage the identical infrastructure, consisting of IaaS, PaaS, SaaS, packing containers, or server less computing, in a multitenant architecture while still keeping their data private and secure. Customer data, for instance, can be stored on the same physical site. All security threats are facilitated by the idea of coexistence and resource sharing between different residents who are strangers to one another.[14] However, collocation or co-tenancy attacks that provide an attacker access to nearby VMs or apps are one way that multi-tenancy might be exploited. Additionally, multi-tenant systems provide a vulnerability for information leakage because multiple data volumes are set aside for different purposes action

Virtualization

Virtualization technologyis used in cloud computing to efficaciously appoint resources. Customers of the cloud can also purchase resources using a pay-consistent with-use pricing scheme. They select the resources they need, like as CPUs, RAM, bandwidth, or operating systems, and only pay for the goods and services they actually use. The system can suffer from multiple security flaws and numerous new security threats can emerge thanks to virtualization technologies. Since virtualization increases the density of connections and the number of entry points, it leaves environments vulnerable to all forms of attacks for various infrastructures.[15]

Availability

Cloud system availability is essential. The delivery of the service should be on demand, according to cloud service providers. Because of the critical services that most businesses provide, any carrier interruption can result in loss and, as a result, a loss of patron trust. Assaults like denial of carrier attacks can result in non-availability, wherein all of the resources are used by the attacker and made unavailable to others, inflicting a denial of carrier and gradual get admission to them. Additionally, users of the cloud service who were persuaded by the Botnet have an impact on the accessibility of other providers. Cloud outages, improper use of cloud resources, hardware issues, and insufficient bandwidth allocation are possible causes of unavailability.[16,18]

Backup

Monitoring data backups is important because it's important to keep track of them and adhere to their security directives to make recovery easier in the event of an unintentional or intentional disaster. To facilitate speedy recovery in the event of calamities, it must be ensured that all the data is regularly backed up.[16] To assure data availability and make it compliant with security standards to prevent malicious actions like unauthorized access and modification, regular backups of stored data must be made.[16,18]

Issues with Application Security

Attackers may decide to target cloud apps. The following list includes some of the problems that cloud applications encounter:

Malware Injection

On account that this attack has grown to be a vast safety problem in cloud systems, cloud configurations for multi-user guide want to be made with caution.Malware infections and data leaks caused by improper cloud setups can harm both the organization's and cloud service provider's entire cloud computing ecosystem. Malware injections are completed by executing embedded code in cloud services that may be offered as SaaS on cloud servers.When an injection like this remains concealed for a long period, it creates a serious problem in the cloud environment.[17] Then, due to its simplicity of execution, this virus multiplies and spreads in cloud environments. Another critical safety difficulty that calls for attention is this one. Some commonplace malware assaults consist of the hyper-name assault, allotted denial of carrier (DDoS), hyper-jacking, VM escape, high, and probe.[18] Other security issues that need to be addressed include malware that lives on virtual machines (VMs), cloud malware synchronizing, and metamorphic engines.

User Interfaces

Users can customize their cloud experience by running applications in the cloud, but doing so poses a serious security risk to the cloud architecture as a whole.

Even many container-based platforms lack out-of-the-box security management. User interfaces, also known as programming interfaces (APIs), enable developers to create and integrate application forms with the cloud. This interface's purpose is to allow users access to cloud services, but because certain of its APIs grant users access to potentially vulnerable cloud customers' systems, it may also be used improperly. Software services must have the most recent patches installed. The client might not be aware that they were hacked and what information was exposed.

Development Life Cycle

Any security measure used to thwart an attack, whether it's multiple firewalls, modern anti-virus software, logging, port and activity tracking, encryption, or some other security level, could be rendered ineffective if the software is insecure in the first place.In comparison to traditional application development, cloud software development is more complex. The technique of creating software program codes for the cloud provides protection gaps, and common updates might also weaken safety even as accelerating improvement. Cloud application requirements, design, development, and testing need for us to depart from the conventional methods employed in the SDLC[19] and adopt a preventative strategy for vulnerabilities, malicious attacks, and target cloud platforms; PaaS apps in particular require additional attention. Protection problems of the development life cycle consist of the usage of the wrong software program improvement existence cycle (SDLC), relying too closely on programmers, the use of risky reverse engineering strategies, and finding issues after a product has been launched or deployed.

Issues with Security Regarding People

People are typically seen as the weakest link in security. However, since both internal and external parties are involved in cloud-based systems, there are more security risks involving individuals. Trust, human resources, compliance and regulatory requirements, as well as other problems brought on by nefarious insiders, are some of the important difficulties.

Customer Trust

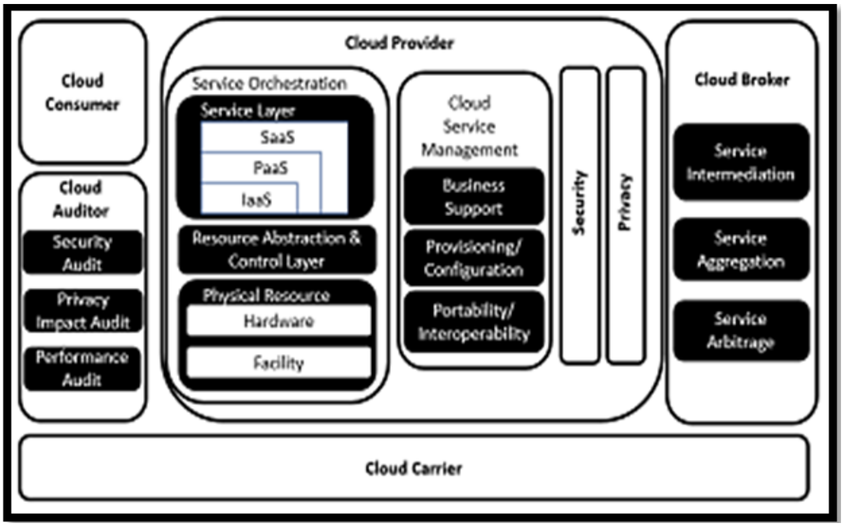
In cloud settings, consumer programs, facts, and infrastructures are controlled by a second or third party and not saved in a single area. Compared to conventional systems, this causes clients to have more trust concerns. The cloud provider is thought to be in charge of configuring the underlying SaaS, PaaS, or IaaS infrastructure and managing its security. When a user expresses concern about the security of sensitive information with a third party, a lack of confidence is felt and questions are raised about everything from the most minor security event to the most common security representation. In a study conducted by[12] in 2015, nearly 74 percent of participants stated they lacked confidence in the cloud's ability to protect their data. Problems that need to be solved in this accept as true with location include agreement management for cloud-to-cloud interactions, cloud machine openness, fate sharing, data locality, audit methodologies, and perimeter security.

Legality and Compliance

Compliance, if poorly managed, can pose a serious security risk. Compliance with legal guidelines and rules is critical when using the cloud, storing and transferring records to and from the cloud, and dealing with cloud architecture.Because security and privacy rules and regulations vary from one place to another, compliance in cloud computing environments is a challenging and fairly difficult topic.[11] To control statistics on the cloud, a cloud issuer and consumer need to be aware about relevant policies and guidelines. Compliance includes confirming suitable safeguards for who has get right of entry to cloud belongings, how a great deal get entry to they have got, and how that get entry to is maintained. Through auditing, this is accomplished. Audits are exceedingly difficult because of how young the public cloud infrastructure is. Providers of public clouds do not prioritize ensuring that compliance standards are satisfied. Other issues in this category include governance, resource mismanagement, and legal issues.

Human Resource

The safety of cloud-hosted human resource systems, as well as safeguarding employee information and essential credentials from being compromised, is of utmost importance. Cloud HR solutions are frequently offered by cloud service providers as SaaS. Companies choose this desire and their payroll management, recruitment, and task control to the cloud due to its broad scope and ease of hiring. While these services are under attack, the organisations' finances and reputation suffer greatly.



Fig, 17: NIST's updated cloud computing reference architecture.[11]

Malicious Insider

Cloud-based systems are more vulnerable to social engineering and phishing attacks than traditional systems.Because a system is remotely accessible from the cloud, a malicious person can easily get in once they have access to login credentials or other sensitive information.[19] An internal attack on the group or team might be disastrous. Access by authorized users to damage the cloud environment is extremely harmful, much as unauthorized access. A malevolent insider could be a stockholder, a former or current employee, etc. An otherwise innocent insider may be forced to assist in the initiation of an assault by malicious outsiders who have influence or control over them.[20] They can collect financial information, client accounts, and other private information. Insider assaults are challenging to identify and stop since they would be mistaken for ordinary access, which would not raise an alarm. Applications for logging data can only be utilized to identify an attacker after an attack has already caused damage. The most of enterprises' security problems are due to a lack of cloud standards, poor management of internal access points, and insufficient monitoring.

The cloud computing security reference architecture is based on the NIST cloud computing reference architecture. Figure 17 displays the revised NIST Cloud Computing Security Reference Architecture from .[11]

Limitations and Challenges in Cloud

Computing Organizations may now take advantage of cutting-edge cloud infrastructures with better productivity, lower costs, and improved efficiency thanks to cloud computing. There's a want to check how conventional cloud infrastructures are maintained and remedy associated security demanding situations within the contemporary day due to upgrades in 5G, reliable net, smart cellular gadgets, IoT infrastructures, and smart AI-based information analytics systems.[13,14] Provisioning IT resources with cloud-based platforms necessitates little understanding of the underlying architecture. As a result, a company needs little time and expertise to configure the cloud. but, because of the heterogeneous nature of the cloud and the user's constrained know-how of a specific cloud, they will turn out to be with an infrastructure this is at risk of numerous cyber protection problems, this could result in data breaches, denial of service, session hijacking, and other issues.

Confidentiality, Integrity and Availability (CIA)

The upkeep of availability, integrity, and secrecy are among the major difficulties with cloud computing. IoT devices' data collection must be shielded againstunauthorized entry this might lead to the alteration, addition, copy, or removal ofdata. Before uploading the data to the server, it is also crucial to ensure confidentiality.Cloud servers when data transmission must occur through any insecuremedia.[15,16]

Application Security and its Aspects

A major obstacle and key area of vulnerability in information security is software application security. The various frameworks and application platforms may each have a different set of vulnerabilities.[17,18] Vulnerabilities in the application security element of cloud computing represent a substantial area of concerns. In relation to this, it is worthwhile since the creation of programmes written in a variety of languages by numerous programmers involved millions of lines of code, varying the list of vulnerabilities associated with them Developers may only be in charge of cloud applications in cloud computing. However, the programming and security features cover every part of the application network.[19]

COVID 19

In recent years, COVID-19 has become a contagious illness that is primarily spread by air droplets. By way of infected people's coughing, inhaling, and sneezing, these droplets are produced, which then leads to the spread of disease. Employees have encountered other difficult problems in addition to the exterior difficulties faced by cloud consumers. As a result of the dire circumstances, quick decisions have been made, like allowing staff to work from home. Unfortunately, the widespread adoption of the remote working style has necessitated an undue reliance on cloud resources. The policy of remote working is being phased out.

However, if a situation similar to this one occurs soon, it will be difficult for the cloud computing sector.

Limited Computation Resources

Agencies typically don't know in which, how, or how lots records and workload are stored on cloud-based totally structures in current years. Counting on cloud provider carriers for those problems has emerged as crucial. A good way to keep away from provider overall performance degradation (in the case of an boom in call for) or provider over sizing (within the event of a drop in call for), Variable workloads necessitate adjusting service capability to demand.[13] Physically linked and situated systems, IoT data, and networks made network monitoring and logging much easier, and forensic investigation produced more information.[11,12] However, because mirroring uses more bandwidth, cloud service providers charge for it, raising the cost. Meeting all of the demands of a cloud service provider is difficult.When a resource depletion attack happens, the energy used by the traffic-consuming nodes is produced by taking use of a compromised node. These nodes lose energy while attempting to take down the network. The attack is therefore contained at the routing protocol layer.

These form of attacks, in which those abilities, collectively with reminiscence and community bandwidth, are purposefully depleted, are able to affecting computing resources, including the ones inside the cloud.[13] Because the cloud can scale to handle the workload, it is susceptible to attacks like these where the resources are depleted as soon as the attack is begun. Such attacks include exploitation of application communication flaws and volume-based flooding protocol exploitation.

Classification and Security Issue

Since its debut, cloud computing has experienced some security problems. The researcher must still pay attention to some new security risks related to virtualization, multi-tenancy, and various cyber-attacks as a result of evolving technologies and cloud architectures. In a cloud computing context, information assets can be found in a variety of places and formats. As a result, it's essential to categories information assets and manages security concerns in accordance with the corresponding level of classification. As a result, security might be maintained for less money and work. When numerous users and organizations share information, it might be difficult to categories data since one company may value one piece of information more than another.

Modern cloud infrastructures have several facets, which present challenges for security organizations in terms of data duplication, timely threat detection, limited control over data access, and the requirement for regulatory compliance. Additionally, protecting the cloud infrastructure and the data within it from known and unknown cyber attacks across all cloud components is necessary to achieve comprehensive cloud security, which is a difficult challenge.

It may be difficult for cloud service providers to ensure that safeguards against data loss or tampering are in place. Records and applications are stored securely, interfaces are secured, facts is retrieved only by authorized users, and statistics is available when required, making a data breach or data hacking crisis manageable. Controls must be in place for cloud service providers to address these problems. In addition, it is critical that eavesdropping malware is promptly detected by the Botnet. These mats are harder to discover over a cloud than conventional gadgets and are able to doing widespread damage. Records breaches resulting from improper intrusion detection structures with traffic monitoring may want to be addressed.[14,15] The handling of insider threats in cloud computing is another difficulty. An unsolved research issue. Because of the risks and ambiguity in current cloud designs and models, cloud service providers must come up with more creative solutions. Contracts between clients and suppliers should specifically address these security concerns.

AI and deep learning limitations

Cloud computing services are accessible to anyone with the right credentials online and are not restricted to a single location. Due to the ease of access to online company data via the cloud, it's a popular goal for attackers looking to research the structures, become aware of flaws, and take gain of those weaknesses. It’s far vital to become aware of cyber attacks and safety vulnerabilities within the cloud before they create any noticeable damage due to the convergence of cyber protection, AI, and utilizing data and resources given by the cloud.AI and DL give computers the ability to learn from their previous performance of jobs and offer a greater level of intelligence to recognize and detect cyber-attacks.

Unfortunately, a lot of businesses are still unaware of the risks presented to their cloud and the necessity of investing in defense against new cyber attacks.

Ineffective Laws

Companies and cloud provider companies rely on rules and requirements which might be every so often out-of-date and inapplicable. In order to account for the expanding changes and uncertainties brought on by cloud computing and the broad usage of the internet in general, new rules must be drafted rather than depending on those from the past. All parties involved in cloud-based systems must be aware of the inherent dangers associated with cloud computing and the measures taken by users to reduce these risks.Teams building cloud applications must receive comprehensive and need-based security training, something that software development enterprises frequently overlook.

More security vulnerabilities, such as insecure APIs, improperly configured cloud storage, and subpar access control, make it difficult for researchers to come up with workable and affordable solutions. Organizations must adhere to cloud security requirements to avoid damage to their reputation and financial losses.

Issues with Security Policy

The guidelines known as security policies are the preventative steps implemented to prevent attacks. It is anticipated that in the cloud, the working environment will be protected by security rules or policies without degrading its dependability or performance.[16,17] These protection guidelines also entail some of specific provider-stage agreements (SLAs), antecedent believe, and purchaser management difficulties, and a few regulatory our bodies govern them.

Future Direction

This research effort addresses additional security and privacy concerns related to cloud systems in the IoT. Future cloud computing gadget research might also consciousness on the following regions, safety concerns the maximum latest cloud security models may be studied and their analysis offered. Researchers may also examine contemporary security issues and challenging situations in cloud computing, such as authenticity, encryption, multi-tenancy, digital machine safety, and how to mitigate these issues. Researchers should be aware of resource sharing in cloud computing infrastructure.

Data Processing: As a result of technological breakthroughs like smart cities, the Internet of Things, and 5G internet, cloud systems will play a larger role in data processing.[18] To achieve comprehensive cloud system security, the cloud infrastructure and data must be safeguarded against various threats.

Secure and Reliable Cloud Environment, In order to create a secure and reliable cloud environment, a number of problems still need to be resolved. Network, software, conversation, net offerings, and data privacy vulnerabilities are among these security concerns.Cloud as a Service The majority of manufacturing businesses in emerging markets now use cloud services, and manufacturing businesses will prioritize cloud services in the future.

Block chain for Secure Cloud Data Emerging cloud security difficulties includeshared pool sources, virtualization, and multi-tenancy, teachers have advanced some of tactics to safeguard cloud logs. Block chain technology with decentralized cloud storage is useful in enhancing cloud data storing methods and data security, and this method safeguards the store data from change and deletion.

Block chain-based Cloud Log Security. Securing cloud logs using block chain is a brand-new area of study. The suggested architecture uses block chain technology to secure cloud logs, making cloud systems impenetrable and boosting users' confidence in a cloud environment.

Authentication Method

Another potential future development in the cloud environment is the block chain-based authentication mechanism for cloud databases. It will be tough for an insider to adjust person login credentials way to block chain era. Insiders are not able to get admission to consumer login credentials when the use of dispensed ledger-based authentication techniques.

Federated Learning for the Cloud

Federated learning is a novel machine learning technique that trains various algorithms on numerous decentralized servers using only local data. Due to bandwidth restrictions, the primary issue in a cloud system is the cost of communication between clients and the cloud server. For attaining robust privacy in cloud computing, federated learning techniques with a high level of organization can be applied.

Cloud Privacy Concerns

Strong privacy protection boosts users' confidence in cloud computing. Advanced optimization techniques can be utilized to improve the effectiveness of algorithm training. These methods will work well against severe collusion and trustworthy but inquisitive servers. Researchers and developers can address a variety of issues related to cloud computing via federated learning, including high communication costs, privacy concerns, statistical heterogeneity, and system heterogeneity.

Conclusion

In the past ten years, adopting cloud technology has changed the game for businesses, organizations, and hackers. Modern cloud architectures, fast internet, and new developments have all created security risks for cloud computing.

The adoption of cloud computing improved an employer's adaptability and scalability, permitting it to stay and competitive inside the ever evolving industrial surroundings. However, it simultaneously rendered their statistics much less relaxed and attackable for some of motives.

The deployment models, cloud architectures, and typical assaults were covered in this article. After that, we divided cloud security concerns into four groups and talked about the problems in each. We also discussed a number of cloud computing concerns that require immediate attention. These difficulties also include the cloud computing-related restrictions that have emerged in the AI and DL fields.

Acknowledgement

The author would like to thank, Lincoln University Malaysia. for their guidance and support to complete this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Conflict of Interest

The authors do not have any conflict of interest.

References

1. Rizwan, M., Shabbir, M., Nebhen, J., Javed, A.R., Chakraborty, C., Mohiyuddin, A. Using an Adaptive Neuro-Fuzzy Inference System, secure cloud storage is provided for medical IoT data. *Int. J. Fuzzy Syst*. 2021, 1–13
2. Taleb-Bendiab, A., Baker, T., and Karam, Y. Support for intention-driven elastic cloud computing in terms of security. The Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation was held in Malta, Malta, from November 14–16, 2012; proceedings are available online.
3. Rizwan, M., Jalil, Z., Anajemba, J.H., and Biamba; Abid, R.; Iwendi, C.; Javed, A.R. a homomorphic CRT-RSA technique that has been optimised for speed and security. *Ubiquitous Computing* 2021, 1–14. Pers.
4. Mobile Cloud Computing Framework for Securing Data by Ikram, A.A., Javed, A.R., Rizwan, M., Abid, R., Crichigno, J., and Srivastava, G. Brno, Czech Republic, 26–28 July 2021; Proceedings of the 2021 44th International Conference on Telecommunications and Signal Processing (TSP); pp. 309–315
5. The Top 10 Strategic Technology Trends for 2020 from Gartner. The top 10 strategic technology trends for 2020 are accessible online at https://www.gartner.com/smarterwithgartner/. (viewed on August 8, 2020). Who First Coined Cloud Computing?
6. Regalado ,A. 2011-10-31, MIT Technology Review. Online at: https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing (viewed on August 8, 2020).
7. Announcing Amazon Elastic Compute Cloud (Amazon EC2)—Beta. 2006. AmazonWeb Services, Inc. Announcing Amazon Elastic Compute Cloud and Amazon EC2 Beta

is available online at https://aws.amazon.com/about-aws/whats-new/2006/08/24/ (viewed on August 8, 2020).

8. Blogspot.com for Google App Engine. Welcome to Our New Blog + Google App Engine. 2008. https://googleappengine.blogspot.com/2008/04/introducing-google-app-engine-our-new.html (viewed on August 8, 2020).
9. Elmroth, E., D. Henriksson, and L. Larsson scheduling and observing of services that are internally organised in cloud federations. The 2011 IEEE Symposium on Computers and Communications (ISCC), held in Kerkyra, Greece, from June 28 to July 1, was published in the proceedings at pages 173–178.
10. Hauger, D.; Microsoft News Center Staff; Editor of the Microsoft Blog. Windows Azure is now generally accessible. Microsoft's official blog, February 1, 2020. The following link is available online: http://blogs.microsoft.com/blog/2010/02/01/windows-azure-general-availability(viewed on August 8, 2020).
11. Dzone.com is Which Is Better: Open Stack vs. Apache Cloud Stack? Cloud DZone. 2016. Online at: https://dzone.com/articles/apache-cloudstack-vs-openstack-which-is-the-best (accessed on 8 August 2020).
12. The National Institute of Standards and Technology, Gaithersburg, Maryland, USA, Special Publication (NIST SP) Series, The NIST Definition of Cloud Computing, P. Mell and T. Grance, 2011.
13. Baker, T., Ghobaei-Arani, M., Souri, A., and Hussien ControCity: An autonomous method for managing buffers in a cloud computing environment to control elasticity. 2019 IEEE Access 7, 106912–106924
14. M. Shabbir, A. Shabbir, C. Iwendi, M. Rizwan, N. Herencsar, and J. C. W. Lin. improving the security of health information utilising mobile cloud computing's modular encryption standard. 8820–8834 IEEE Access 2021, 9.
15. Taleb-Bendiab, A., Mackay, M., Randles, T. Support for runtime adaptive autonomic cloud-based applications through intention-oriented programming. 2013, 39, 2400–2412, Comput. Electr. Eng. [CrossRef]
16. M. Al-Khafajiy; T. Baker; M. Asim; Z. Guo; R. Ranjan; A. Longo; D. Puthal; and M. Taylor A fog computing approach to trust management. 2020, 137, J. Parallel Distributed Computing.
17. Xia, T., Washikaki, H., Fukazawa, Y., Kaiya, H., Ogata, S., Fernandez, E.B., Kato, T., Kanuka, H., Okubo, T., Yoshioka, N., *et al* CSPM stands for Cloud Service Product Metamodel for Handling Security and Privacy Knowledge. Int. J. Syst. Softw. Secur. Prot. (IJSSSP) 2021, 12, 68-85. [CrossRef]
18. Cloud Security and Privacy, by Mather, Kumaraswamy, and Latif; published 2009; Sebastopol, California, USA: OReilly Media Inc.
19. Four Trends Affecting Cloud Adoption by 2020. Online at: https://www.gartner.com/smarterwithgartner/4-trendsimpacting-cloud-adoption-in-2020/ (found at 8 August 2020). Why Cloud Computing Cyber Security Risks Are Growing: Report
20. Su. J Why Cloud Computing Cyber Security Risks Are Growing: Report, 2019 July 25 Forbes. You can access it online at 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).