Vol. 03, No. 02, pp. 47 –57 (2022)
ISSN: 2708-0757

JOURNAL OF APPLIED SCIENCE AND TECHNOLOGY TRENDS

www.jastt.org

A Survey on Cloud Security: Concepts, Types, Limitations, and Challenges

Marya Ayoub Omer[1*], Abdulmajeed Adil Yazdeen[1], Hayfaa Subhi Malallah[1], Lozan Mohammed Abdulrahman[1]

[1]*ITM Dept., Technical College of Administration, Duhok Polytechnic University, Duhok, Iraq, (mariaayob997@gmail.com abdulmajeed.adil@dpu.edu.krd, hayfaa.subhi@dpu.edu.krd, lozan.abdulrahman@dpu.edu.krd)*

**Corresponding Author mariaayob997@gmail.com*

Abstract

Given the world's current situation with the COVID-19 pandemic, several businesses have recently encouraged remote working from home. A variety of benefits are provided by cloud computing, including simplified IT and management, secure Internet-based remote access from practically anywhere, and cost savings. As a result, more people use the cloud, but there are also increasing cyber-attacks on cloud networks. However, several companies and organizations, who do not know the security threats that Cloud systems pose, are still worried about using the cloud. Reports previously released by researchers from academia, business, and standard organizations proposed solutions to these problems. This paper examines state-of-the-art papers on topics, challenges to requirements, and identified security system vulnerabilities. In addition, we will review the different components and the security and privacy concerns of current cloud computing systems. Finally, we present a variety of security threats targeting and addressing cloud storage services. In particular, we raise awareness on security issues that cloud organizations including cloud service providers, data owners and cloud users face and address them.

Keywords—Cloud computing, Security, Data security, cloud services limitation, SaaS, PaaS, IaaS.

Received: October 05, 2022 / Accepted: December 27, 2022 / Online: December 29, 2022

I. INTRODUCTION

The exponential rise of global data sets has posed a dilemma for the information technology sector. The white book Data-Age 2025 published by International Data Corporation forecasts that the world's data universe will more than triple from 33 zettabytes in 2018 to 175 zettabytes by the year 2025. In the next years, it is anticipated that the market for cloud computing would expand at a rapid rate. One solution to the challenges caused by the increase of data is cloud storage, which makes use of a network that is connected to several data centers in order to combine multiple storage devices into a single storage pool. Cloud storage enables users to store data, exchange it with other users, and access it at any time and from any place by using a computer that is linked to a network, most often the Internet [1].

When referring to a technique of storing and accessing data through the Internet rather than on a local server, the phrase "cloud computing" is used.

Customers stand to gain a number of exciting benefits as a result of the company owners' decision to move their operations into the cloud. These benefits include scalability, resilience, high performance, on-demand, and a Pay-Per-Use service model. However, when services are outsourced to other parties, there is an increased risk of data breaches, data loss, and service denial.

A number of well-known cloud storage alternatives, including OpenStack Swift, Ceph, Dropbox, Google Drive, and Microsoft OneDrive, have been put into us. As a direct consequence of this, the most important issue facing the cloud computing business in the present day is one of data security. Customers rely on CSPs to protect the information they provide, the services they provide, and the availability of those services, as well as to demonstrate that they comply with all applicable security standards [2].

Evaluating the security of a CSP is a difficult process because of the intangible nature of the component. Since of this, the process of adopting cloud computing is sped up because customers are better able to make informed judgments based on reliable and consistent information about the security of the services they are contemplating using. This in turn speeds up the adoption process. A Security Service Level Agreement (also known as a Security SLA) is currently being drafted by security service providers and their customers in order to control the nature of their relationship with regard to the management of security [3]. Within this document, the

doi:10.38094/jastt301137

rights of each party are safeguarded, and each party is required to collaborate with the other parties in order to avoid security breaches and the accompanying financial and technical penalties. As a result of the notion of cloud computing, cloud service providers (CSPs) are confronted with a myriad of challenges, some of the most significant of which include output guarantee, resource restrictions, disaster recovery planning, regional workload distribution, and regulatory considerations. As a potential solution to these issues, the idea of a cloud federation was conceived as a possible solution. It makes it possible for a CSP to keep complete control and visibility over the processing of a portion of the requests made by its users while delegating those requests to third-party service providers [4].

The remainder of this paper is structured as follows: section II discussed types of cloud. In section III, the concept of the cloud services model is outlined. Section IV depicts cloud service model limitations. Cloud security issues and challenges are presented in section V Section VI presents the literature review. Section VII presented discussion and comparison, and section VIII concludes the paper.

II. CLOUD TYPES

- Private Cloud: it is restricted and open to a small community of people and organizations. This cloud model provides more protection and resource management.
- Public Cloud: every subscriber is allowed to access the cloud via public cloud internet connectivity. The public or organizations therefore manage public cloud resources. This cloud type contains little control of resources and less privacy [5, 6] .
- Community Cloud: this type of cloud shares more than two cloud-like organizations. A third party or company manages it. It offers services to large users compared to the private cloud, providing more protection than the public cloud [7].
- Hybrid Cloud: Companies that use a hybrid cloud model make use of both private and public cloud resources. A company uses private cloud resources for routine operations but uses public cloud resources for scalability and cost-effectiveness [8].

There is a distinction between cloud computing service models, which is illustrated in Table 1.

TABLE 1: Comparison of Cloud Computing Service Model [5].

Model	Scope	Managed by	Security Level	Advantages	Disadvantages
Public Model	Public and private sectors	Providers of cloud services	Low	Scalability and reliability with on-demand resources Easy to use	Can be unreliable Less secure
Private Model	Single organization	Single organization	High	Organization-specific Customizable	More costly Requires IT expertise
Community Model	Organizations with common strategies and reservations about protection	Many organizations or cloud service providers	High	Flexible and Scalable	costly than the public cloud
Hybrid Model	Public and organization	Public and organization	Medium	Flexible infrastructure Cost controls Faster speeds	Potential challenges in application and data integration

III. CLOUD SERVICES MODEL

Cloud services fall into three categories as shown in Figure 1:

a) Software as a Service (SaaS): This model provides cloud customers with a variety of applications for a variety of operations. Web Browsers are used by users to access the applications. They just charge based on the number of times a program, such as Microsoft Word, Notepad, or Paint, is used. Google, ZOHO, Intuit, and Salesforce.com are all examples of SaaS providers [9].

b) Platform as a Service (PaaS): This model Platform-like Operating System provides services to users. Users create their own frameworks and work with an Integrated Development Environment (IDE) that includes a compiler, editor, and other tools. PaaS providers include Google Apps, Force.com, and Bungee Connect [10].

c) Infrastructure as a Service (IaaS): This model provides cloud users with infrastructures such as storage, networks, and servers as a service. Consumers use these programs based on their own requirements, paying only for what they use. The user manages the operating system and the program's deployment but does not manage or track the cloud environment. IaaS services include Amazon Elastic Compute Cloud (EC2) and EMC Atmos [11].

Fig 1. Cloud services [12].

IV. CLOUD SERVICE MODEL LIMITATIONS

A. *Limitations in SaaS*

Data localization and data integrity are two significant limits that may have an effect on the adoption of software as a service (SaaS) applications. The majority of the time, the customer is unaware of the location at which the service provider maintains its data or the measures that must be taken to protect it from unwanted modifications. The lack of trust that exists between cloud customers and cloud providers is one of the most significant issues that arises with software as a service [13].

In order to protect sensitive student information, the IT department of the university may decide to host the SaaS application on a dedicated server or to make use of the infrastructure services offered by reputable third-party vendors such as Google, Amazon, and others. Both of these options are available to the university. These criteria explain why the majority of the high schools that participated in our study choose to use private clouds rather than public or hybrid ones (Figure 2).

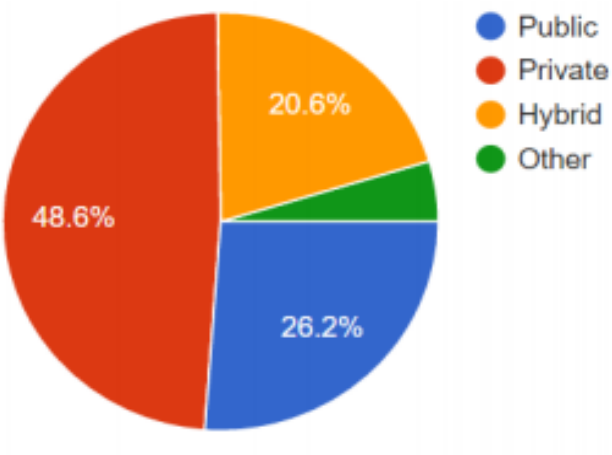

Fig 2: Surveyed Institutions' Use Of Cloud Models [14].

B. *Limitations in PaaS*

Software developers working for educational institutions may be able to develop and move SaaS applications to the cloud in a more expedient manner by using a platform known as PaaS. Nevertheless, working with PaaS services might provide developers with a number of obstacles to overcome. To begin, increasing capability makes it simpler for developers to integrate and manage cloud-based apps provided by other parties. Users of PaaS have yet another significant challenge in the form of being constrained to certain programming paradigms or tiers of service providers. Before being moved to a new PaaS environment, these models and services need to undergo a comprehensive redesign. This is necessary since they are highly dependent on their current setting. Users are unable to switch networks since they are restricted to the one they are currently using. On top of the platform, developers may build and maintain their apps, but they have no clue about the security that the platform's service provider has permitted below the platform [15].

C. *Limitations in IaaS*

IaaS provides its customers with a higher level of security-related agency as compared to the previous two service categories. When selecting a source, the reliability of the information that the source provides is the single most important consideration to make. In the model of infrastructure as a service (IaaS), security is shared responsibility between service providers and end users. Because of the supplier's obligation, stringent safeguards have to be taken to secure both the physical and the digital surroundings. On the other hand, it is the responsibility of the cloud client to guarantee the safety of their own data, applications, and operating system. The model known as Infrastructure as a Service places a significant emphasis on virtualization. In a scenario that makes use of virtualization, the possibility of a cross-tenant attack exists whenever several tenants use the same physical infrastructure. In this scenario, an attacker must first get root access in order to access the cloud accounts of the majority of tenants [16] .

V. CLOUD SECURITY ISSUES AND CHALLENGES

The use of cloud computing has made some tasks simpler to do, but it has also raised new safety issues. As a result of the fact that various types of data are dispersed throughout the network and stored in a variety of cloud services, there are probably a great many distinct vulnerabilities that may be taken advantage of by bad actors. The five various ways in which a cloud environment could be safe are shown for us in Figure 3 : in terms of security rules, data security, user-oriented security, network security, and application security [17].

A. *Security policies*

The goal of security policies is to lay out the procedures that should be followed in order to protect a system from being compromised in some way. The implementation of these

standards will hopefully result in a cloud workspace that can be relied upon and is safe. It is possible for a variety of circumstances, such as regulatory authorities, service level agreements (SLAs), client management challenges, and established trust, to have an effect on security policies [18] .

- Service-level agreement (SLA)

In each of these client-service provider interactions, the Service Level Agreement (SLA) is applicable. SLAs are necessary for suppliers that wish to keep their customers' expectations in control and are required to meet those expectations. Service providers, on the other hand, are often shielded from liability under the provisions of service level agreements in the event of errors or results that are below par (SLAs) [19]. Another factor that should be considered when assessing the quality of a service is the use of service level agreements, or SLAs. On the other hand, SLA is unable to guarantee assurance for a specific method. To restate, the SLA does not promise outstanding service and cannot enhance the quality of delivery that is below standard. The SLA includes a statement of concerns as well as a list of resources that are considered to be within its jurisdiction. In addition to this, it specifies the duties that the service provider must fulfill as well as the responsibilities that the customer must fulfill. The Service Level Agreement (SLA) [20] details the measures for performance, availability, usage, and reaction time.

- Antecedent trust

Establishing mutual trust is one of the most important first steps in any business collaboration. As a direct consequence of this, cloud computing is still having trouble overcoming these challenges [21].

B. User-oriented security

Because of the complexity of utilizing cloud storage, it is necessary to have strong security that is user-oriented in order to safeguard data and resources. Cloud service providers monitoring user-submitted data while it is being stored and processed is a huge security risk. The capacity to identify, verify, authorize, and deal with access concerns are all included in this aspect of security's capabilities [22].

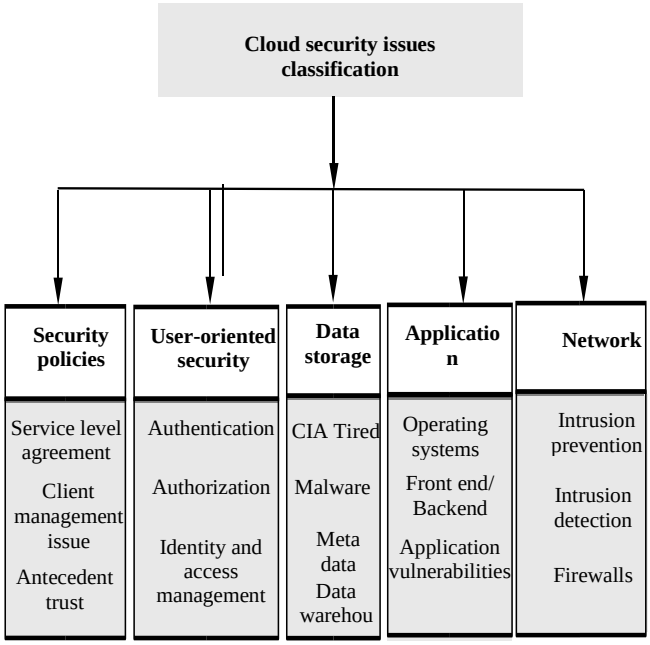

Fig 3. Different types of cloud security issues [18]

- Authentication

With cloud computing, organizations are able to store a greater volume of data at a lower cost. For this reason, the news that service providers are permitted to adopt creative ways of customer verification comes as a welcome relief. Depending on their needs, machines may either conduct complete or partial authentication. In the context of cloud computing, a fundamental authentication method will not let you to access data from a variety of cloud service providers. Access for privileged users may be granted even if doing so carries some inherent danger. Nevertheless, this problem may be solved by using any one of a number of other authentication processes. It is common for users to be granted dedicate access authority when they provide information only they are aware of, such as a card number or a password they have created themselves. The following are the two primary classifications that these techniques belong to: The two most important types of security verification are known as physical authentication and digital authentication [20].

- Authorization

The component of information security known as "authorization" is responsible for deciding whether or not to comply with a user's request to get access to a certain resource. An administrator of the system functions as a liaison between the users of the system and the system itself [5] ageed. Because the cloud is a distributed computing environment, a single client may make use of services offered by a number of distinct providers, each of which may use a security approach that is slightly unlike to the others. For instance, when the user has given authorization to the program, the application may then be available from the outside world. In this context, one may make use of either access management rules or access delegate

credentials. Authorized users are the only ones who are able to manage and make use of available services and resources [21].

One of the advantages of a centralized access system is that it protects sensitive data while also eliminating a number of management and security processes. Another advantage is that it saves time. The MAC, DAC, RBAC, and ABAC are only a few examples of several kinds of authorization systems [23].

- Identity and access management

Identity and access management, which is a policy-based framework for controlling digital identity inside an organization, is one of the most well-supported approaches to identify identity management capabilities. This is because identity and access management is a framework. Identity access management systems are required to take all necessary steps in order to ensure the security of user credentials during storage and recording, as well as to prevent unauthorized access to this information.

Manage the access that users have to the corporate database and make adjustments as required. The identity and access management system acts as a directory that is accessible throughout the whole organization and takes into consideration the many different categories of users that the firm has. Nevertheless, as of just this moment, neither productivity nor income are being negatively impacted by the identity and access control system. As a direct consequence of this, it is very difficult to get financial support for these endeavors. The current state of identity and access management in the business world, on the other hand, poses a risk to both corporate compliance and overall security [24].

C. Data storage

The data associated with the logical pool is stored in a digital archive that is hosted in the cloud. The information is physically kept on a large number of servers, each of which is operated and maintained by a distinct web hosting provider. As more and more people use the internet and many other connected devices, there is an increasing need for distributed computing systems to store data in a manner that is both safe and accessible. Concerns over storage, availability, confidentiality, the CIA, and other sorts of security have surfaced as a direct consequence of difficulties with data management. It is the responsibility of the cloud service provider to ensure that the data are always accessible [25].

- CIA tired in data security

When it comes to cloud computing, the three most pressing concerns are accessibility, honesty, and privacy. (CIA) The ACID property should be adhered to by any and all data that is kept in the cloud in order to provide both privacy and transparency. Cloud service providers recognize that high availability is beneficial not just to them but also to the customers they serve [5]. The dependability of a service may be jeopardized by a variety of factors, including hardware failures, software defects, and aggressive attacks from the outside. OneDrive, the cloud storage service offered by Microsoft, does not provide any type of encryption for the private data stored by its customers, in contrast to both Dropbox and Google Drive [26].

- Metadata

A collection of files constitutes metadata in its most basic form. The use of cloud computing has increased in popularity, which has resulted in a considerable expansion of the significance and complexity of metadata. Metadata now stores sensitive data. What was done, where it was done, the flee style, the data format, and other types of information are examples of the sorts of information that may be found in metadata. Metadata may also include information on the format of the data. Cybercriminals are able to access the information that is saved in metadata, which has a tremendous deal of value. On the other hand, corporations make use of metadata data to extract more monetary value from their already-existing data. In addition, given that metadata might include confidential and private information, it is of the utmost importance to protect metadata using appropriate encryption technology. Unfortunately, only records of massages may be encrypted; this means that any information about touches will still be exposed. The use of Virtual Private Networks (VPNs) makes it simple to prevent unauthorized access to the type of sensitive data that is being discussed here [5].

D. Application security

Vulnerabilities in application security are one of the most significant challenges posed by cloud computing in terms of data protection. Before developing any software applications, there are a number of security considerations associated with the creation of cloud apps and networking that need to be taken into consideration. The trust mechanism is of the utmost importance when it comes to the provision of web-based business services that are secure. OWASP's core area of focus is the security of back-end components of web applications [27].

Mobile apps have long been one of the most popular ways to interact with the Internet, but web application vulnerability security has had many drawbacks. Hackers do, in reality, use endpoint-sent-traffic to inject malicious executable codes. It's referred to as code injection. Malicious code can also be used in cross-site scripting. Scripts are differentiated. Web apps are vulnerable to threshold, exception, and password programming. Configuration or incomplete changes are often the result of management issues. Make special programming languages more difficult. Protecting web applications also adds to the complexity of other issues, such as Internet security. OSs are also crucial in application cloud protection, application program, and related OS. Indeed, as a computer program, the operating system is responsible for managing and monitoring all resources (hard drives, memory, screens, and so on) that are used to run and exchange multiple applications at the same time [28].

E. Network

Since cloud computing is basically network-based, serious security concerns arose. The key parallels between network security and cloud security are emerging data protection, network security, and the information security sub-area. Many real-world security problems confront networks. Using data and cloud technology protections and services, network administrators will need to follow acceptable security policies [29].

Unfortunately, connectivity problems including denial of service (DoS), distributed denial of service (DDoS), flooding attacks, and network protocol vulnerabilities emerged. The easiest way to prevent attacks is to use firewalls. End-users, servers, and cyberspace routers are also subject to data security audits in the cloud. Traditional firewalls are equivalent to firewalls-as-a-service. Since the service is hosted in the cloud, it is available on any network [30].

FWaaS is a good choice for any security network enterprise because it is less expensive, more powerful, and more flexible than traditional firewalls. Firewalls aren't ideal for preventing cloud service attacks, but they do help to limit vulnerabilities and divisions. Simply put, a firewall can prevent backdoor Trojans from entering, but it cannot eliminate viruses, worms, or malware. A firewall must communicate; a firewall only examines packet headers when malicious network access is detected and logged; protocol sorting, protected address, destination address, and secure port policy are all things that a firewall must consider. IDS seeks to gather valuable data for future safety assessments in addition to avoiding attacks. IPS stands for "unnecessary network access." IPS helps to prevent intrusion or ransomware in addition to detecting and tracking risks. Finally, keep in mind the broader sense of network security. Additional articles [31].

VI. LITERATURES REVIEW

Authors of [21] reveal some cloud benefits in the education sector and highlight certain cloud disadvantages. Services, as well as security issues When using cloud technologies, companies face many challenges. Any educational institutions conducted the survey. Investigating stakeholders' cloud security viewpoints Vulnerabilities and overcoming methods, the author proposed as a starting point. When using the cloud, stop all potential security risks. Computing in high-school institutions. Reviews by the author the conclusions and discusses them. Via a survey conducted at several universities that switched to cloud computing Collecting this material. The methodology is used to identify stakeholders' views on cloud security vulnerabilities and tactics to overcome them at colleges and Students of universities, faculty members Students and IT workers filled out the questionnaire. It is approximately 64% of universities were found cloud-based. Just 36% are cloud service providers, however. Even a supplier Looking at the responses to the questionnaire, we noticed something. That several respondents are uninitiated when it comes to privacy risks to their cloud or protection measures in place Avoid at any expense. This means responsibility on those responsible for cloud computing. Stakeholders are not updated on computing security issues related to their cloud computing.

Researchers of [27] suggested The multi-workflow QoS Controlled Scheduling approach fulfills the various QoS goals of the client, such as execution time, cost, and ongoing work planning. They focus only on cost or time, or both in unchanged quality and accessibility. This number meets various service quality, such as time, costs, and consistency and transparency. This proposed diagram satisfies various service quality aspects, including time, cost, accuracy, and transparency. As a result, planning is performed in one target for the basic QoS specifications of a client.

Paper [32] covered cloud computing and mobile cloud computing, combining cloud computing with IoT, and how cloud convergence supports mobile apps. Integrating cloud computing for mobile devices and IoT leads to many vulnerabilities in encryption and security compromises. The authors concentrated primarily on mobile cloud IoT integration security issues and numerous factors affecting mobile cloud IoT security's normal functioning. The various security issues in this field and the various factors affecting security in this area were also discussed, and how they can be managed to provide IoT-enabled service for efficient and natural mobile cloud computing. And grouped security problems into three types: architectural, infrastructural, privacy, and compliance issues. Some preventive measures suggested by various mobile cloud computing researchers based on different mobile cloud computing areas were also discussed.

Work in [33] established key architectural elements of SDCC. The key motivation is achieving agreement within the research community and promoting the SDE concept in cloud environments. Many suppliers actively create SDCC products and specifications. This will benefit ultra-large service providers (e.g., Google, Yahoo, and Amazon). SDCC concepts promote innovation in many fields including physical hardware, network management and legacy networks, and technology bridging elements. Authors strongly believe that SDCC will continue to see huge growth in the near future, bringing new levels of versatility to cloud network programming and management.

Paper [34] concentrated on realizing the security and forensic problems of the MK Smart project, concentrating on the challenges of securing such massive amounts of data on a datahub and focusing on the best way to forensically investigate large complex data such as data stored on Datahub. Authors looked at MK Smart's issues. As this project relies heavily on data (Big Data), countermeasures are important for data protection and cyber-attacks (Forensics). MK Datahub is stable with Arcserve UDP implementation and has reliable backup and recovery solution. MK Smart Project also works on digital forensics. Big data forensics remains a challenge for the discipline of digital forensics, but data system like Hadoop supported data acquisition through its layers, making it easy to define and specify data on the data hub.

The work of [35] went through the service specifics in-depth and looked at their contacts to see what service information they were referring to. LDA2 and word2 can help

to balance accuracy and speed in this situation. The results are applicable in the real world. Transfer learning (i.e. training and testing) word representations has been shown to improve the LDA algorithm's performance. This is especially true in cold climates and when using other approaches to create cutting-edge models. Personal recommendations are made based on the users' own results; Similar domain-based transfer learning will be implemented in the Cloud to further reduce data scarcity. We also know that when used in this setting, it is efficient.

Some virtualization issues related to cloud computing technology isolation were investigated in [36]. Distributed side-channel attacks, including modern multi-domain architectures, are a major cloud infrastructure concern, according to the researchers. The first DSCA classification to take advantage of isolation violations was introduced: DSCAs are coordinated attacks that use multiple local SCAs to infiltrate sensitive data from various parts of a distributed system. Finally, they proposed a plan for preventing side-channel attacks, which included using an autonomous mechanism to execute a moving defensive strategy, among other things. They are primarily concerned with the design and implementation of integrated cloud infrastructure for an autonomous mitigation platform for a variety of SCA groups.

Scholars of [19] proposed a model for cloud federation creation that considers CSP security levels. They begin by constructing a collection of parameters that quantitatively define the Security-SLA in the cloud using the Goal-Question-Metric (GQM) process, and then using it to compare the security levels of CSPs and existing federations to a given Security-SLA baseline, taking into account CSP customers' security satisfaction. The Cloud Federation's creation phase is then modeled after a hedonic alliance game focused on CSP security and reputation. They propose a federation-building algorithm that enables CSPs to enter a federation while mitigating security losses and avoiding federations that are unstable. Experiments show that our model helps existing federations maintain higher standards of safety while reducing the frequency and severity of Security-SLA violations.

The various characteristics of the Transportation Systems Internet, security and privacy systems were discussed in [37]. Explore how to combine AI and defense and cloud-based transport systems were presented. Finally, he explained how to connect AI, Protection, and Things Internet. 'It's just begun to detect the depths of the Internet of Things they understand various types of attacks and formulate ML techniques to fight them. Also, consider how best to handle the attacks on the ML techniques needed for IoT device development. Finally, we must decide to shift the analytics firms to the stable cloud.

Academics of [26] created a cloud flow optimization application and performed an optimization Grey Relational Approach (GREY). The resulting solution is a GRSA architecture that efficiently uses requested flow type and current network conditions to route flows through cloud data center networks, ensuring optimal service levels. An experimental GRSA study showed it provides better balanced loads, uses less energy from the grid, and decreases the average transmission delay compared to ECMP. This work aims to optimize QoS cloud storage by guiding high-priority flows to predict high-priority transmissions. Before collecting tracks from a Ceph storage, authors defined three key types of traffic flows: low, medium, and high volume. Next, find the best solution based on diversity and network latency parameters for these flows. A GRA-based flow scheduling tool was then used to solve the routing path optimization problem covering both aggregation and edge switches. They trace in a realistic setting. Authors performed several experiments to demonstrate that GRSA can provide sufficient capacity while avoiding high-critical delays in busy conditions. But we want GRSA in a large cloud.

Using Honeypot, the authors showed a new way to handle malicious users [26]. Honeypot may be used by organizations to monitor alleged rogue members. Emulating the attacker will easily understand the victim's actions. Additional precautions are required as with each passing day, risks are greater. Honeypots enhance detection and surveillance capabilities as they build on more technologies. They use cloud storage to be stable, fast, and affordable. With all this tremendous industry growth, this innovation's protection is at risk. Traffic diversion can be achieved in different ways, but one of the most effective is using honeypots. The method showed promising results in protective systems evolution. Given the many legal problems that can occur when installing Honeypot, a file-sharing application is placed on a third-party server.

Scholars of [38] proposed architecture for a collaborative security system focuses on risk recognition and analysis during the collaborative platform's life cycle. the protection system is a dynamic, active security system. A "1+3" security framework collaboration network is proposed by the authors. In the framework, they build on the details of the defense model construction scheme. It provides new theoretical support for collaborative research in security technology.

RDFI methods for overcoming challenges were proposed. RDFI uses chaos engineering concepts to secure the cloud, executing, monitoring, analyzing, and scheduling security-based injection campaigns across feedback loops [39]. The fault models in the knowledge base are focused on reliable baselines, cloud security best practices, and input from iterative fault injection campaigns. These findings aid in the detection of flaws while also ensuring that security attributes are adequately tested (integrity, confidentiality and availability). Furthermore, through exchanging security knowledge with security systems, RDFI facilitates risk detection and security hardening. We developed and implemented RDFI techniques as a software tool, including various chaos engineering algorithms: CloudStrike. CloudStrike performed several technology tests on Amazon Web Services and Google Cloud Platform, two big cloud infrastructure providers. With rising attack rates, performance improves linearly over time. In addition, the efficacy of CloudStrike security information was demonstrated by using vulnerability analysis discovered by security fault injection to harden cloud resource security. As a result, we believe our methods are appropriate for addressing current cloud security concerns.

Researchers of [40] employed the new paradigm for cloud computing requirements that incorporates four components, including data security, risk assessment, law enforcement,

industry, and innovations to produce a dataset that scientists can work with in Local governments benefit from attending to their present and legacy IT system's ability to be interconnected. promoting internal protection also enhances the system's controls and firewalls Both government and cloud service providers have expressed their support for shared responsibility The discovery of how important regulations are to cloud protection also highlights the greater need for enforcement in local settings. For good measure, the business and security specifications mention that governments should know about data recovery, and encryption must also. studies study and learn about cloud protection requirements in local governments We are making progress in the areas of cloud protection, but there are still major organizational, human, and legal challenges to work around as well.

AuthPrivacyChain, a blockchain-based privacy management framework, was proposed in [41]. They use the blockchain node account address as a form of identification while also redefining cloud data access control authorization, which is encrypted and stored in the blockchain. After that, AuthPrivacyChain creates protocols for access control, authorization, and revocation. They have used Enterprise Operating System (EOS) to implement AuthPrivacyChain, and the results show that AuthPrivacyChain is capable of not only stopping hackers and administrators from accessing resources illegally, but also of protecting privacy.

Biometrics-based two-factor authentication and a hybrid encryption algorithm are implemented [42]. The efficiency of this architecture is determined in Various tests on the internet network include data uploading and downloading. The Frag Secure Module encrypts the data, and then authentication is checked and matched against the fingerprint. As this cloud architecture is implemented, the findings show that fake and real users can be distinguished 100% of the time.

Authors of [29] addressed the issues that arise when data is inaccessible. There was a lot of discussion about interoperability, but in a few key cases, an open standard was proposed. The authors focus on major cloud computing threats including denial of service attacks, VM-level attacks, and DDoS-related service interruption attacks.

Research [43] proposed a cloud computing and healthcare cloud computing method. They would strengthen the authors' healthcare architecture; cloud infrastructure has the ability to significantly reduce healthcare costs while also allowing countries to improve their overall health. Cloud protection issues, including healthcare, have also been addressed. They've also discussed and suggested ways to improve cloud security.

Study [44] colleagues to enhance protection, the multi pein security scheme was proposed, which provides more security than any single-layer scheme currently in use. The algorithm, in particular, ensures that only pre-authorized users have access to cloud data and that downloading and uploading files is faster and more reliable.

CSBAuditor, a novel cloud security application proposed by [44] , can track device changes and incidents. The entities can be linked together using the state transformation and reconciler pattern CSBA, which employs a specific mechanism for computing vulnerability severity scores (GCP) to target various platforms with varying outcomes (GCP). CSBAuditor has a performance rate of over 98 percent in detecting problems. Furthermore, the production cost is adequate.

With service cost and multi-cloud risk perspectives, the web service composition problem is formulated as a bi-objective optimization problem [45]. This is unmistakably an NP-hard issue. To solve the combinatorial problem, the authors devise a bi-objective time-varying particle swarm optimization (BOTV-PSO) algorithm. To achieve a reasonable balance of exploration and extraction, the parameters are changed based on the amount of time elapsed. To demonstrate the effectiveness of the proposed algorithm, the authors identified several scenarios and compared its performance to that of a multi-objective GA-based (MOGA) optimizer, a single objective genetic algorithm (SOGA) that only optimizes the cost function and ignores CSR, and a multi-objective simulated annealing algorithm. According to the experimental results, the proposed BOTV-PSO outperformed other approaches in terms of convergence, diversity, fitness, performance, and even scalability.

VII. DISCUSSION AND COMPARISON

Depending on the reviewed research in the literature review section, a summarized comparison has extracted as shown in Table II. Hence, the following points can be highlighted:

- The majority of research has focused on or is aimed at enhancing security, ensuring optimal service levels. protecting data in the cloud, and ensuring optimal service levels. They want something that is safe, fast, and affordable.
- Machine learning has used to Best manage attacks on IoT devices that required ML techniques.
- focus only on cost or time, or both in quality and accessibility Focus on mobile cloud IoT security problems and various factors affecting mobile IoT security [5].
- Most of the researchers proposed methods for avoiding security threats as much as possible.
- Based on an enterprise operation system (EOS), the address the issue of leaked data by hackers or cloud internal managers blockchain-based access control framework with privacy protection called AuthPrivacyChain implemented AuthPrivacyChain hacks and admins can be prevented, along with privacy being safeguarded.
- Suggested a different way of using Honeypot to treat malicious users. Monitor potential rogue representatives more comfortably using the Honeypot Technique in organizations. The acts of the perpetrator can clearly be understood.

TABLE I: LITERATURE REVIEW OF VARIOUS RESEARCH WORKS IN CLOUD SECURITY

Authors	Achieved Objectives	Depended Method	Implemented Field	Advantages
[21]	Investigate stakeholders' cloud protection	method for avoiding security threats as much as possible.	educational institutions.	discover some cloud benefits and highlight key cloud disadvantages.
[27]	focus only on cost or time, or both in quality and accessibility	Suggested The QoS multi-workflow scheduling solution	QoS requirements	Carries out the multiple QoS priorities of the client, such as implementation time, cost and ongoing job preparation.
[32]	Focus on mobile cloud IoT security problems and various factors affecting mobile IoT security.	Integrating IoT cloud computing, mobile cloud infrastructure, and IoT	Integrating mobile cloud networks and IoT	Addressed the preventive steps suggested by mobile cloud researchers in different mobile cloud computing areas
[33]	link the research community and encourage SDE in cloud environments.	identified the SDCC's fundamental architectural elements	SDCC values promote change in large organizations	Adding new levels of cloud network programming and management flexibility.
[34]	Concentrated on knowing MK Smart's security and forensic issues	UDP implementation, and MK Datahub	MK Smart Project is also working on digital forensics	secure and has a reliable backup and recovery solution
[35]	the accuracy of recommendation will be improved with the growth of individual data	used to examine the service descriptions and perform LDA on both the text and location data	applied in various fields	provide personalized services based on the users' historical data
[36]	Develop and deploy autonomous cloud mitigation infrastructure for several SCA groups.	Classification of DSCAs used to exploit isolation violations was introduced	virtualization problems related to isolation of cloud computing infrastructures	they have outlined a method to reduce side-channel attacks
[19]	increases protection for existing federations and reduces the frequency and impact of TrustNss..	using the Goal-Question-Metric (GQM).	compare the security levels of CSPs and federations using a known Federated-SEC baseline	minimizing security losses and avoiding unstable federations
[37]	Best manage attacks on IoT device required ML techniques	AI and security can be mixed And cloud-based transport systems.	Internet features of Transportation Networks, Protection and Privacy Systems.	it has been more secure
[26]	Cloud storage data efficiently, ensuring optimum service levels.	Created an integer cloud flow optimization program and performed (GREY) for optimization.	enhance the QoS for cloud storage	uses fewer system resources, and reduces the average transmission delay
[38]	They want safe, fast, and affordable. With all this tremendous industry growth.	a new way to handle malicious users, by using Honeypot.	using the Honeypot strategy in Organizations	track alleged rogue members more comfortably. one can easily understand the victim's actions.
[39]	focused on risk recognition and review of the collaborative platform's entire life cycle.	dynamic and active security system.	collaborative manufacturing platform.	It offers new theoretical support for collaborative security technology research.
[40]	mitigating of cloud issues	Risk-driven Fault Injection (RDFI) techniques	RDFI applies chaos engineering principles to cloud security	a useful during testing of security requirements (integrity, confidentiality, and availability).
[41]	emphasized the importance of cloud service providers and governments as sharing their resources	Incorporating the international standard ISO 27002 and a number of good practice security controls	cloud services by local governments	provide critical insights for governments that are adopting cloud services
[42]	address issue of leaked data by hackers or cloud internal managers	blockchain-based access control framework with privacy protection called AuthPrivacyChain	implemented AuthPrivacyChain based on an enterprise operation system (EOS),	hacks and admins can be prevented, along with privacy being safeguarded
[29]	identification of fake and actual users.	Biometric based Security technique	performance of this proposed architecture is done in the .Net	predictive efficacy of the cloud architecture and provide 100% accuracy of fake and real user IDs
[43]	Solve the problems related to the effects of the inaccessibility of the data	an open standardized framework in each of the influential usage examples.	major cloud paradigm security threats	denial of service attacks
[44]	enhance the cloud security levels	a multilevel security scheme	Cloud space of individual users	faster and better while doing so when accessing a certain file
[45]	system that continuously scans the cloud for malicious and unauthorized activity	CSBAuditor	cloud infrastructure	It can find configuration errors in real time with an accuracy rate of 98% The performance requirements are also met.

VIII. CONCLUSION

Over the past decade, cloud-based market opportunities have expanded tremendously. Cloud technologies are now a vital part of corporate life, providing a momentous opportunity to drive business by allowing us to be agile with our capital, generating new collaborative opportunities. The cloud gives companies, organizations, and even nations many advantages. Despite several advantages, the cloud still faces many security challenges. That's why the cloud's greatest challenge is stability. Despite bringing many benefits, the cloud also faces several security challenges. That's why stability is the cloud's biggest problem. Customers and suppliers are mindful of security risks. This paper reviewed the cloud computing model in terms of different viewpoints including definitions, cloud architectures, methods, and challenges. Three service models (SaaS, PaaS and IaaS) and four deployment models (private, public, hybrid and community cloud) are identified, and the main objective of the current study is to present all possible security challenges in cloud computing and provide adequate solutions to these problems.

REFERENCES

[1] L. M. Abdulrahman, S. Zeebaree, S. F. Kak, M. Sadeeq, A. Adel, B. W. Salim, et al., "A state of art for smart gateways issues and modification," Asian Journal of Research in Computer Science, pp. 1-13, 2021.

[2] Z. Ageed, M. R. Mahmood, M. Sadeeq, M. B. Abdulrazzaq, and H. Dino, "Cloud computing resources impacts on heavy-load parallel processing approaches," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 22, pp. 30-41, 2020.

[3] C. A. Sennewald and C. Baillie, Effective security management: Butterworth-Heinemann, 2020.

[4] F. Abedi, S. R. Zeebaree, Z. S. Ageed, H. M. Ghanimi, A. Alkhayyat, M. A. Sadeeq, et al., "Severity Based Light-Weight Encryption Model for Secure Medical Information System."

[5] H. Malallah, S. Zeebaree, R. R. Zebari, M. Sadeeq, Z. S. Ageed, I. M. Ibrahim, et al., "A comprehensive study of kernel (issues and concepts) in different operating systems," Asian Journal of Research in Computer Science, vol. 8, pp. 16-31, 2021.

[6] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," Information Processing & Management, vol. 58, p. 102397, 2021.

[7] L. M. Haji, O. M. Ahmad, S. Zeebaree, H. I. Dino, R. R. Zebari, and H. M. Shukur, "Impact of cloud computing and internet of things on the future internet," Technology Reports of Kansai University, vol. 62, pp. 2179-2190, 2020.

[8] K. D. Ahmed and S. R. Zeebaree, "Resource allocation in fog computing: A review," International Journal of Science and Business, vol. 5, pp. 54-63, 2021.

[9] Z. S. Ageed, S. R. Zeebaree, M. M. Sadeeq, S. F. Kak, Z. N. Rashid, A. A. Salih, et al., "A survey of data mining implementation in smart city applications," Qubahan Academic Journal, vol. 1, pp. 91-99, 2021.

[10] S. S. Wagle, M. Guzek, P. Bouvry, and R. Bisdorff, "An evaluation model for selecting cloud services from commercially available cloud providers," in 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), 2015, pp. 107-114.

[11] R. W. Anwar, T. Abdullah, and F. Pastore, "Firewall Best Practices for Securing Smart Healthcare Environment: A Review," Applied Sciences, vol. 11, p. 9183, 2021.

[12] A. Sunyaev and S. Schneider, "Cloud services certification," Communications of the ACM, vol. 56, pp. 33-36, 2013.

[13] Z. S. Ageed, S. R. Zeebaree, M. M. Sadeeq, S. F. Kak, H. S. Yahia, M. R. Mahmood, et al., "Comprehensive survey of big data mining approaches in cloud systems," Qubahan Academic Journal, vol. 1, pp. 29-38, 2021.

[14] H. Al-Shqeerat, F. Al-Shrouf, M. R. Hassan, and H. Fajraoui, "Cloud computing security challenges in higher educational institutions-A survey," International Journal of Computer Applications, vol. 161, pp. 22-29, 2017.

[15] M. H. Ryu, J. Kim, and S. Kim, "Factors affecting application developers' loyalty to mobile platforms," Computers in Human Behavior, vol. 40, pp. 78-85, 2014.

[16] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio, "Security issues in cloud environments: a survey," International Journal of Information Security, vol. 13, pp. 113-170, 2014.

[17] S. H. Haji, S. Zeebaree, R. H. Saeed, S. Y. Ameen, H. M. Shukur, N. Omar, et al., "Comparison of software defined networking with traditional networking," Asian Journal of Research in Computer Science, pp. 1-18, 2021.

[18] Z. J. Hamad and S. R. Zeebaree, "Recourses utilization in a distributed system: A review," International Journal of Science and Business, vol. 5, pp. 42-53, 2021.

[19] T. Halabi and M. Bellaiche, "Towards security-based formation of cloud federations: A game theoretical approach," IEEE transactions on cloud computing, vol. 8, pp. 928-942, 2018.

[20] Z. S. Hammed, S. Y. Ameen, and S. R. Zeebaree, "Massive MIMO-OFDM performance enhancement on 5G," in 2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2021, pp. 1-6.

[21] R. J. Hassan, S. Zeebaree, S. Y. Ameen, S. F. Kak, M. Sadeeq, Z. S. Ageed, et al., "State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions," Asian Journal of Research in Computer Science, vol. 22, pp. 32-48, 2021.

[22] T. M. G. Sami, Z. S. Ageed, Z. N. Rashid, and Y. S. Jghef, "Distributed, Cloud, and Fog Computing Motivations on Improving Security and Privacy of Internet of Things," Mathematical Statistician and Engineering Applications, vol. 71, pp. 7630-7660, 2022.

[23] Y. S. Jghef and S. Zeebaree, "State of art survey for significant relations between cloud computing and distributed computing," International Journal of Science and Business, vol. 4, pp. 53-61, 2020.

[24] Y.-W. Huang, S.-K. Huang, T.-P. Lin, and C.-H. Tsai, "Web application security assessment by fault injection and behavior monitoring," in Proceedings of the 12th international conference on World Wide Web, 2003, pp. 148-159.

[25] B. T. Jijo, S. Zeebaree, R. R. Zebari, M. Sadeeq, A. B. Sallow, S. Mohsin, et al., "A comprehensive survey of 5G mm-wave technology design challenges," Asian Journal of Research in Computer Science, vol. 8, pp. 1-20, 2021.

[26] W. Ke, Y. Wang, and M. Ye, "GRSA: service-aware flow scheduling for cloud storage datacenter networks," China Communications, vol. 17, pp. 164-179, 2020.

[27] A. Kumar, P. S. Kumar, and T. Sairam, "Organization Assignment in Federated Cloud Environments based on Multi‐Target Optimization of Security," Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, pp. 139-147, 2019.

[28] N. T. Muhammed, S. R. Zeebaree, and Z. N. Rashid, "Distributed Cloud Computing and Mobile Cloud Computing: A Review," QALAAI ZANIST JOURNAL, vol. 7, pp. 1183-1201, 2022.

[29] A. Narang, D. Gupta, and A. Kaur, "Biometrics-based un-locker to enhance cloud security systems," International journal of cloud applications and computing (IJCAC), vol. 10, pp. 1-12, 2020.

[30] G. A. Qadir and S. R. Zeebaree, "Evaluation of QoS in distributed systems: A review," International Journal of Science and Business, vol. 5, pp. 89-101, 2021.

[31] H. S. Yahia, S. Zeebaree, M. Sadeeq, N. Salim, S. F. Kak, A. Adel, et al., "Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling," Asian Journal of Research in Computer Science, vol. 8, pp. 1-16, 2021.

[32] A. Dumka, M. Memoria, and A. Ashok, "Security and Challenges in Mobile Cloud Computing," Security Designs for the Cloud, Iot, and Social Networking, pp. 43-57, 2019.

[33] A. A. Abbasi, A. Abbasi, S. Shamshirband, A. T. Chronopoulos, V. Persico, and A. Pescapè, "Software-defined cloud computing: A systematic review on latest trends and developments," IEEE Access, vol. 7, pp. 93294-93314, 2019.

[34] E. Okai, X. Feng, and P. Sant, "Security and Forensics Challenges to The MK Smart Project," in 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2019, pp. 1666-1670.

[35] C. Lei, H. Dai, Z. Yu, and R. Li, "A service recommendation algorithm with the transfer learning based matrix factorization to improve cloud security," Information Sciences, vol. 513, pp. 98-111, 2020.

[36] M.-M. Bazm, M. Lacoste, M. Südholt, and J.-M. Menaud, "Isolation in cloud computing infrastructures: new security challenges," Annals of Telecommunications, vol. 74, pp. 197-209, 2019.

[37] B. Thuraisingham, "Cyber security and artificial intelligence for cloud-based internet of transportation systems," in 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2020, pp. 8-10.

[38] P. S. Negi, A. Garg, and R. Lal, "Intrusion detection and prevention using honeypot network for cloud security," in 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2020, pp. 129-132.

[39] K. Lu, Q. Han, G. Zhu, and B. Huang, "Research on the whole process security system framework of network collaborative manufacture," in 2020 Chinese Control And Decision Conference (CCDC), 2020, pp. 5530-5534.

[40] K. A. Torkura, M. I. Sukmana, F. Cheng, and C. Meinel, "Cloudstrike: Chaos engineering for security and resiliency in cloud infrastructure," IEEE Access, vol. 8, pp. 123044-123060, 2020.

[41] O. Ali, A. Shrestha, A. Chatfield, and P. Murray, "Assessing information security risks in the cloud: A case study of Australian local government authorities," Government Information Quarterly, vol. 37, p. 101419, 2020.

[42] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," IEEE Access, vol. 8, pp. 70604-70615, 2020.

[43] T. Alam, "Cloud Computing and its role in the Information Technology," IAIC Transactions on Sustainable Digital Innovation (ITSDI), vol. 1, pp. 108-115, 2020.

[44] S. M. Altowaijri, "An architecture to improve the security of cloud computing in the healthcare sector," in Smart Infrastructure and Applications, ed: Springer, 2020, pp. 249-266.

[45] K. A. Torkura, M. I. Sukmana, F. Cheng, and C. Meinel, "Continuous auditing and threat detection in multi-cloud infrastructure," Computers & Security, vol. 102, p. 102124, 2021.