Security Issues and Challenges of Cloud operating systems: A Systematic Review

Mohamed Buhary Fathima Sanjeetha

Department of Management and IT,
South Eastern University of Sri Lanka

sanjeetha.mit@seu.ac.lk

Abstract. This systematic review paper investigates a potential security concern in cloud operating systems in this study. The cloud computing operating system is an efficient and cost-effective solution for providing IT services to both individual users and enterprises. It offers scalability and reliability, ensuring that resources can be easily adjusted to meet changing demands. Additionally, it is a cost-efficient option, making it accessible to a wide range of users. Nevertheless, the outsourcing of crucial services to a third-party cloud provider introduces an additional element of risk. The challenges of data security and privacy, data and service availability, and compliance verification are exacerbated as a consequence with regulatory mandates. The problems with security that come with cloud computing have already been covered in this article. These problems were identified as the most significant ones in this category of systems and the most significant obstacles that can be found in the literature on cloud computing operating systems and their environments. In addition, researchers advised that a way be proposed that would enable users to pick certain security levels before making the decision to utilize cloud-based services. This is something that all users should be aware of before making their decision. Additionally, future researchers will be able to gain something from the methodical investigation that is suggested in this study.

Keywords: Cloud Operating Systems, Security Challenges, Security Issues, SPI Model, Standardization

1 Introduction

IoT, cloud computing, and big data are the most promising new generation of technologies since parallel computing, distributed computing, and grid computing. New information technologies are driving this new wave of progress, and these technologies are at the forefront of it. Innovative concepts such as virtualization, utility computing, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are what have ultimately led to the rise of cloud computing. When these cutting-edge ideas are combined and unified, we get cloud computing. Computing in the cloud is a flexible and scalable method. In this setup, everything including the underlying infrastructure, servers, data storage, applications, and processing power is virtualized and made available as a web-based service. Great compatibility, low cost, and high efficiency are just a few of the perks of cloud computing that have the ability to provide more economic value and benefits to consumers and enterprises [1].

© Faculty of Management and Commerce
South Eastern University of Sri Lanka (SEUSL)
University Park, Oluvil 32360. Sri Lanka

Received: 06th June 2024
Revised and Accepted: 14th Aug, 2024

Computing in the cloud is the emerging trend in the field of information technology (IT), which has emerged as a consensus among the majority of nations' governing bodies and commercial sectors all over the globe. From the point of view of apps, users are able to access cloud-based resources via the internet, choose on-demand services, and then pay only for the number of resources they use. In the meanwhile, cloud computing might offer a suitable environment and Services that possess the ability to accommodate evolving requirements via the utilization of diverse hardware and software components, as well as flexible distribution of resources. In essence, the cloud operating system has primary responsibility for performing two distinct duties.

Companies like Google, IBM, Microsoft, Oracle, SAP, and Amazon have all created their very own cloud operating systems [2]. For instance, Google has produced Chrome OS, which is their cloud operating system, as well as Android, which is their intelligent terminal operating system. Up until 2014, the open-source Android operating system had more than 80 percent of the market share for mobile phone operating systems [3]. Enterprise cloud solutions are mostly what the large software firms like SAP and Oracle offer their customers. For instance, Oracle Database Cloud Service offers cloud services for the database layer, while Oracle Java Cloud Service offers cloud services for the application layer. Both of these services are provided by Oracle. VMware and vSphere are examples of open cloud operating systems that are available to be bought from the market for use in application development [4]. This arrangement is not beneficial for the IT infrastructure security of other nations since the vast majority of cloud computing applications are based on cloud operating systems that are created and controlled by a small number of corporations in a few industrialized countries.

In this article, the author focuses mostly on discussing the problems and difficulties associated with using cloud operating systems for cloud applications. In the first part, an introduction is given to cloud computing and virtualization, as well as SaaS, PaaS and IaaS. An analysis of the architecture of cloud operating systems is presented in part II, together with information that is specific to cloud applications and cloud operating systems. The methodologies and the most important findings are discussed in third part. In part four, an independent analysis is performed on the primary substance of cloud operating system security concerns, and in fifth part, the cloud's standardization of security levels is presented. In the last portion, part six, conclusion and recommendations for the future are offered.

2 Related Work

The most current advancement in internet-based computing is referred to as "cloud computing," which is an extremely generic word. This section offers a concise introduction to cloud computing, followed by an examination of cloud OS. The purpose of this section is to provide readers with a foundational understanding of knowledge, so facilitating a more comprehensive comprehension of security problems as well as current security mechanisms that are present within cloud computing.

2.1 Cloud Computing

The scientific and business sectors are paying an increasing amount of attention to the concept of cloud computing as its significance continues to rise. According to one survey [6], cloud computing is now ranked #1 among the top 10 most essential technologies, and it is expected to continue to enjoy this position among businesses and other types of organizations over the next years. Cloud computing offers ubiquitous, easy, and The concept being described is the use of a centralized computer system that is accessible and adjustable on demand over a network. The efficient allocation and timely distribution of these resources may be achieved with little intervention or exertion from the administration of service providers. Cloud computing enables customers to use a readily available pool of computers as per their need. is a term used to describe a computer paradigm and a technique of data transmission. The primary goal of the service is to provide consumers a reliable, efficient, and straightforward method for storing and processing data via the internet. The whole of computer power that is now accessible is conceptualized as a collection of services and is made accessible via the use of the internet [7] [8]. The cloud offers several benefits such as improved cooperation, agility, scalability, availability, and adaptability to changes in demand. Additionally, it enhances the speed and efficiency of development work and presents the potential for cost savings via streamlined and efficient processing [4-7].

Although the use of cloud computing offers several potential advantages, it is important to acknowledge the presence of various complex issues that must be addressed. Following the issue of security, issues over compliance, privacy, and legal complexities emerge as significant obstacles to the adoption process. The issue of security across several layers, such as network, host, application, and data, and the potential migration of application security to cloud computing, remains unclear due to the relatively recent emergence of cloud computing as a computing paradigm [9]. The lack of understanding around cloud computing sometimes leads information executives to express security worries as their primary fear [10].

Several risk factors that give rise to security issues include off-site data storage, dependence on the "public" internet, limited control, numerous tenants, and the absence of integration between internal and external security measures. The cloud has several distinct characteristics that differentiate it from conventional technologies. The cloud's many distinguishing features stem from its massive scale and the wide variety, widespread distribution, and virtualization of its providers' underlying physical infrastructure. Identification, authentication, and permission-based security measures are insufficient for modern clouds [11]. In most cases, the security measures used in a cloud computing environment are not vastly dissimilar to those taken in any other kind of IT setting.

Nevertheless, the use of cloud computing in a commercial setting may potentially give rise to new hazards that are absent in conventional IT systems. The reason for this may be attributed to the utilization of various cloud service models, the implementation of certain operational models, and the incorporation of supporting technology. Unfortunately, many people have the misconception that putting security into these systems would make them more rigid [7]. The migration of mission-critical apps and sensitive data to environments hosted inside the public cloud is a major source of worry for businesses that are expanding outside the network that is under their control within their data center. In order to address these concerns, it is essential for cloud service providers to provide uninterrupted access for their customers to their existing security and privacy configurations for on-premises applications and services. Additionally, they should furnish evidence of their robust security measures, their ability to satisfy service level agreements (SLAs), and their readiness for audits [12].

2.2 Cloud Applications

SaaS is the most frequent kind of cloud applications. In this model, a corporation makes a piece of software accessible to customers via the internet. The users then pay the firm for access to the programme. Popular examples of software as a service include banking and document applications, as well as practically any other kind of programme one would anticipate seeing on a personal computer. There are also free varieties of the prominent example of SaaS is Google Apps, which encompasses Google Docs and offers users the capability to execute several operations often associated with desktop publishing, akin to Microsoft Windows Office. In contrast, Google Docs offers a more limited range of functions compared to conventional desktop publishing software. However, this feature facilitates the dynamic storage of materials, ensuring that every change is automatically saved. Consequently, it provides a guarantee that data will be retained even in the event of a loss of connection between the user and the cloud., the user will not lose any materials. In addition, users have the ability to concurrently modify and distribute documents while doing so over the web. This makes it simpler for people to work together, and it cuts down on how much time is spent by people on drafting different documents.

Building and administering the whole cloud computing infrastructure allows for the quick delivery of a wide range of improved application services thanks to a cloud operating system that is both comprehensive and standard. In general, the cloud operating system consists of three primary tasks:

- Centralize the management and maintenance of a massive quantity of computer infrastructure, such as servers and storage, by merging the physical resources of all linked data centers into a single virtual cloud server.
- Offer a uniform and common set of functions, services, and user interfaces for a variety of applications. Each user chooses and pays for the cloud-based application services that are appropriate for their needs.
- Manage in a dynamic manner the extensive computational duties, the deployment of applications, and the various resource migrations.

Since it is at the center of all resource management, the Cloud Operating System (OS) performs the function of the central nervous system for the whole cloud computing architecture. If one wants to be able to ensure the safety of the whole cloud infrastructure, it is important to do one's own research and development on the technology of cloud operating systems.

2.3 Cloud Operating Systems

Cloud Operating Systems have been built, building on the foundation laid by the creation of JeOSs. Major developments include Google's rollout of its Chrome operating system on a laptop as part of a test programme. The Google Chrome operating system is, in essence, a type of JeOS is an operating system that offers fundamental capabilities for accessing cloud-based services via the use of the Chrome web browser [15]. Given the potential for users to get hardware at much reduced prices compared to conventional PCs operating on non-cloud-based operating systems, it is anticipated that the usage of OS will become more commonplace within the marketplace. Additionally, as was discussed previously, the elimination of the need for organizations to buy operating systems or pay for labor to manage servers is another way that this configuration helps organizations save money.

In order to guarantee the safety of cloud computing and its implementation on a broad scale, a cloud operating system (cloud OS), which is an extensible extension of conventional stand-alone OS, has to be separately created. In comparison to conventional OS, cloud OS offers a comprehensive range of services that are compatible with the majority of forms of infrastructure, such as networks, hardware, software, terminals, and applications.

2.4 Virtualization, IAAS, SAAS and PAAS

Cloud computing relies heavily on virtualization as its underpinning technology [8]. Virtualization is a technique that, in its most basic form, enables a single computer or server to concurrently execute many sessions of an operating system on different virtual machines. This gives customers the ability to execute apps that were developed for many operating systems on a one computer, which eliminates the need for cloud OS.

In order to enable the concurrent operation of several operating systems on a single computer, it is necessary to construct a "virtual machine" that emulates the underlying hardware. Hypervisors, also known as virtual machines, refer to software applications that facilitate the communication between an operating system and the central processor unit (CPU) of a computer or server [13], as well as storing data and connecting to a network. IaaS is a kind of cloud computing that allows a client to run their own virtual machines. A user is able to perform practically everything that is possible with a real PC or server, including the installation of applications and the storage of data.

Because to virtualization, providers were able to significantly increase their capacities for server-side operations, and the usage of IaaS by customers became more cost-effective as a result. Customers were liberated from the financial burden of spending money for hardware and upkeep. Instead, the supplier is in a position to provide extremely powerful computers housed in a vast data warehouse. SaaS, is a subscription model used by service providers to distribute software. The concept of cloud computing was born then. Sometimes referred to as "software on demand," which describes the situation in which a customer may utilize software that is given by a company and pay for the use on a per-unit or per-measurement basis. The concept of cloud computing was conceived by inventive minds as a result of the development of this new technology. The concept of the cloud may be summed up in a single sentence: more calculations are carried out on the server side. However, as was noted before, this phrase is expansive and can refer to a wide variety of concepts and practices. Since servers play the key role in providing service, they are managed and optimized inside datacenters, allowing customers to experience a system that seems instantaneous, more competent, and dynamic.

3 Cloud Computing Architecture

Computing in the cloud may be broken down into two distinct parts: the user and the cloud itself. In the vast majority of use cases, the user connects to the cloud by way of the internet. It is also feasible for a company to establish its own private cloud, to which users may join by logging into the company's own intranet. Nevertheless, each of these situations are exactly the same with the exception of whether a private or public network or cloud is used [12]. The user is responsible for sending requests to the cloud, which is then responsible for providing the service in figure 1.

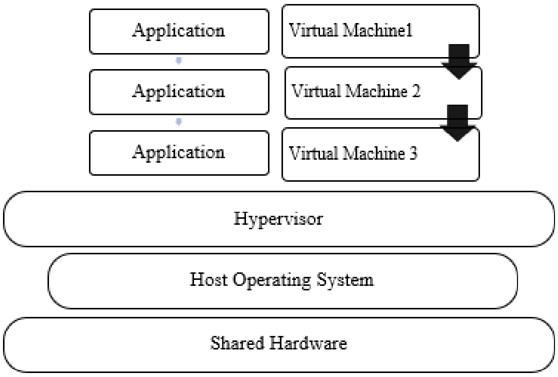

Fig. 1. Cloud OS architecture

A centralized server inside the cloud is in charge of the system's administration and, in many respects, serves in the same capacity as the cloud OS, one of its other names is "middleware," which refers to the server for a certain cloud [14].

4 Methods

4.1 Systematic Review of Security Issues

We have conducted a comprehensive review [13-15] of the existing research on cloud computing security in order to not only provide a summary of the existing issues and challenges pertaining to this topic, but also to identify and evaluate the current state of cloud computing security as well as the most significant security concerns associated with cloud computing.

4.2 Question formalization

The purpose of this question was to determine which Cloud Computing concerns are the most important, taking into account the problems, obstacles, dangers, prerequisites, and potential answers concerning cloud computing security. This question needed to be connected to the purpose of this effort, which was to determine and link the problems and difficulties associated with standardizing the various degrees of security. As a result, the following research question was the one that our investigation attempted to answer: Which aspects of cloud computing's security, in particular, stand out as the most significant obstacles to be overcome, and which aspects of cloud computing's operating systems need to be investigated in further detail? The following is a list of the linked ideas and phrases that make up this question and that were used in the process of carrying out the review: safe Cloud OS, Cloud security, the SPI model, problems with SaaS security, concerns with PaaS security, difficulties with IaaS security, issues with Cloud OS, threats to Cloud OS, suggestions for the cloud, and best practices in cloud computing.

4.3 Selection of sources

The inclusion of these sources has been limited by the following criteria: all selected research must be written in the English language, and all chosen resources must be available online without any cost. The selection of sources for this study was guided by the authors' previous research experience, which inspired the assessment criteria we used. This list has been compiled by considering resources such as ScienceDirect, the Google Scholar library, and the IEEE digital library. In subsequent iterations, further refinement of these findings will be conducted, including essential scholarly contributions that were not initially retrieved from the aforementioned archives. The present study will undergo revision to include additional constraints, namely the impact factor and citation counts, prominent journals, recognized authors, and more. Ultimately, it will provide a more accurate picture of the situation. After the sources were identified, it was required to provide a description of the procedure as well as the criteria for the selection and assessment of the studies. The determination of the study's inclusion and exclusion criteria was influenced, to some extent, by the research subject that was being asked. Therefore, the researchers decided that the studies needed to cover themes and subjects that considered the security of cloud computing, and that these studies needed to discuss the concerns, obstacles, standardization, and different degrees of security.

4.4 Review Execution

This research used a refined PRISMA methodology including four stages: identification, screening, eligibility, and inclusion. entries were found using systematic searches in ScienceDirect, Google Scholar, and the IEEE digital library, yielding 1,121 initial entries. Following the elimination of 21 duplicate entries, 1,100 records were reviewed, of which 800 were discarded due to irrelevance in title and abstract. Out of the 300 records requested for full-text retrieval, 260 were either inaccessible or did not satisfy the retrieval requirements. Forty reports were evaluated for eligibility, and twenty-five were discarded for failing to fulfil inclusion criteria. In conclusion, the final review included 15 research. The PRISMA flow diagram (Figure 2) visibly delineates the selection process and guarantees openness in the systematic review technique.

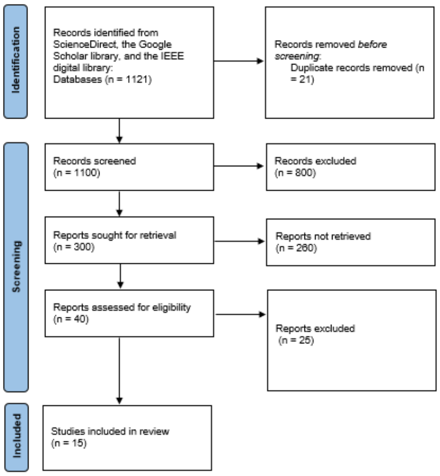
Identification
Records identified from ScienceDirect, the Google Scholar library, and the IEEE digital library: Databases (n = 1121)
Records removed *before screening*: Duplicate records removed (n = 21)
Screening
Records screened (n = 1100)
Records excluded (n = 800)
Reports sought for retrieval (n = 300)
Reports not retrieved (n = 260)
Reports assessed for eligibility (n = 40)
Reports excluded (n = 25)
Included
Studies included in review (n = 15)

Fig. 2. PRISMA flowchart

5 Results and Discussion

The findings of the systematic review are shown in Table 1, which provides an overview of the issues and ideas that were taken into consideration for each method.

The majority of the methodologies that have been presented identify, categories, evaluate, and list a number of concerns and obstacles that are associated with cloud computing, as is seen in Table 1. The studies conduct an analysis of the problems and difficulties, and often provide standardizations on Methods for Avoiding or Protecting Against Them. This establishes a direct relationship between problems and viable strategies for resolving them. Furthermore, it is worth noting that a significant number of the methodologies used not only address and emphasize existing challenges and obstacles but also delve into supplementary considerations pertaining to the security of Cloud computing. Additional considerations in such environments include data security, trust, and adherence to security requirements and solutions to address possible risks.

Table 1. Summary of the topics

Topics/ References	**[6]**	**[7]**	**[8]**	**[9]**	**[11]**	**[12]**	**[13]**	**[14]**	**[15]**	**[16]**	**[17]**	**[18]**	**[19]**	**[20]**	**[21]**	**[22]**
SaaS security issues	X			X	X	X	X		X	X						
PaaS security issues	X				X	X	X		X	X						
IaaS security issues	X			X	X	X			X	X						
Signed in with XML	X	X	X	X		X	X	X	X		X	X	X	X	X	
Web browser protection	X	X		X	X	X		X	X	X	X	X		X	X	
Flooding	X	X	X		X	X	X	X	X	X		X	X	X	X	
Sharing of reputation fate	X	X	X	X	X	X	X			X	X	X	X	X	X	
Side channels	X	X	X		X			X	X	X	X	X	X	X	X	
Lack of data control	X	X	X		X	X	X		X		X	X	X		X	
Internet reliance	X	X	X	X	X		X	X	X	X		X	X		X	X

6 Security Issues

As was said before, there are a great deal of safety considerations associated with the use of cloud computing. These safety worries include a wide range of potential threats, some of which are associated with more conventional forms of computing and some of which are unique to cloud computing. Additionally, there are security concerns that impact both the customers and the service providers. When people hear the term "computer security," the majority of them immediately think of assaults on the user's PC. It is essential, on the other hand, to keep in mind that anyone might use cloud computing in order to set up a virtual bot network.

6.1 SPI Model Issues

SaaS security issues

Email, conferencing software, and enterprise software like ERP, CRM, and SCM are some examples of the types of application services that may be obtained on demand with SaaS [11]. When compared to customers of the other two primary delivery models in the cloud, SaaS consumers have far less influence over the system's security. The use of software provided as a service could give rise to various security problems [6].

PaaS security issues

The use of PaaS allows companies to deploy cloud-based applications without incurring the expenses associated with procuring and managing the necessary hardware and software [16]. Similar to SaaS and IaaS, PaaS necessitates the use of a reliable and secure network infrastructure, as well as a trustworthy and secure web browser. PaaS application security comprises two tiers of software [11]. The first tier is responsible for protecting the PaaS platform, while the subsequent tier is responsible for safeguarding the client applications that operate on the PaaS. The PaaS provider assumes the duty for ensuring the security of the platform software stack, which encompasses the runtime engine governing the client applications. Similar to SaaS, there are apprehensions over the security of data in PaaS environments. PaaS encompasses additional web service components [9] [11-13], including mashups, with the conventional programming languages. A mashup refers to the process of combining distinct components or elements to create a unified entity. Hence, PaaS models also inherit the security vulnerabilities often associated with mashups, namely in relation to data and network security [17]. In addition to relying on the security provided by web-hosted development tools, users of PaaS also need to rely on the security measures given by external services.

IaaS security issues

IaaS makes available, in the form of virtualized systems that can be accessed over the internet, a pool of resources that may be used for computing, examples of technological components often used in modern computing systems include computers, hard drives, networks, and software [14]. Users have the right to execute whatever programme they want, and they have complete control over the resources that have been allotted to them [18]. When compared to the other models, users of IaaS have superior control over the cloud's level of security. This is the case so long as the virtual machine monitor does not have any vulnerabilities [19]. They are responsible for appropriately configuring security policies [17], since they own the software that is operating in their virtual machines and have control over it. Cloud providers, on the other hand, are in charge of the infrastructure that underpins the computing, The topics of interest in this discussion are connection and data storage. The mitigation of risks related to the establishment, distribution, and utilization of IaaS necessitates substantial efforts by service providers to enhance the security of their underlying infrastructure, monitoring, modification, and movement of their customers' data [20]. IaaS is related with a number of security vulnerabilities, some of which are listed below.

6.2 Signed in with XML

There are several methods available to secure the legitimacy of information sent using the Simple Object Access Protocol (SOAP), one of which involves the use of XML Signatures. XML signatures are often used to provide assurance to the receiver that the received XML data is genuine and has not been altered [21]. However, there exists a phenomenon known as a "wrapper attack," which occurs when an assailant introduces redundant XML code with additional code that compels the system to execute supplementary undesirable operations. According to what the technique's name suggests, the attacker essentially places the signature on top of the malicious code and then transmits it as if it were authentic.

Sharing information across different computer systems requires XML, which is necessary for cloud computing. Wrapper attacks are a possible means by which malicious difficulties might be caused; as a result, suppliers are required to think of inventive methods to stop wrapping assaults from being successful.

6.3 Web Browser Protection

In cloud-based OS, the web browser functions as the primary input/output device. Cloud-based browsers have many issues in terms of online safety. The Same Origin Policy (SOP) serves as a fundamental security measure implemented by web browsers. It mandates that servers maintain records of the requesting browser's location and only authorize access if the request originates from the same geographical region [7]. This notion serves as the fundamental basis for all aspects of browser security. Nevertheless, empirical evidence has shown that this kind of security is inadequate. Based on the findings of the study conducted by researchers [9], it has been identified that the primary issue lies in the browsers' incapability to use XML Signature or encryption. Addressing this concern in forthcoming iterations is seen as a crucial objective.

Nevertheless, the browser is forced to employ it’s important to note that Transport Layer Security (TLS), sometimes referred to as "Secure Socket Layer," does not possess the capability to encrypt or digitally sign XML data. The two components of the TLS protocol are the record layer. This is the main kind of protection that browsers provide for their users. Having a digital certificate is necessary for the server, and even then, not every website can be trusted to be safe. Phishing refers to a type of cyberattack and fraudulent activity in which an attacker, often posing as a trustworthy or legitimate entity, attempts to deceive individuals into revealing sensitive information, such as login credentials, personal information, or financial details. Phishing may be done in a number of different ways. TLS is rendered useless as a data protection mechanism as soon as the attacker has access to the data [14].

6.4 Flooding

In the context of computer networks, flooding can refer to a type of network attack or behavior where a large volume of data or traffic is sent to a network or a specific network node, with the intention of overwhelming it. For example, in a Distributed Denial of Service (DDoS) attack, attackers flood a target system with massive traffic, causing it to become slow or unresponsive. The term "Denial-of-Service" refers to a certain kind of assault that may occur. An infected computer is used as part of this form of assault, which is carried out by a hacker, to link all of the infected machines to a particular website. This floods unable to operate effectively [18]. When using conventional servers, you are restricted in your skills due to the constraints of the actual server. in the other hand, if the website is hosted in the cloud and the owner pays based on the amount of traffic the website receives, there seems to be a limitless supply of resources for the server. If a distributed denial of service attack were launched against a cloud OS.

6.5 Sharing of Reputation Fate

Sharing a single piece of hardware amongst several users has a number of unintended consequences, one of which is that the reputations of all of the people who use that piece of hardware might be harmed by the actions of the other users. There are some examples taken from real-world events in which people have suffered significantly as a result of reputation destiny sharing [19]. The criminal activity was being carried out on computer hardware located inside the facility. As a consequence of this, the operations of a great number of users who were not involved in the criminal activity were disrupted [21] while authority investigators looked for evidence related to the criminal activity. In point of fact, a number of the businesses that were subject to the seizure indicated that they had sustained large losses but were unable to take any steps to recoup what they had lost.

This form of security risk is caused by one user abusing the cloud service, and it has the potential to damage a number of different parties. Even while these security threats are serious, the fact of the matter is that datacenters are more equipped to cope with security than people are. The difficulty is that when a security weakness in a data center is discovered, a large number of victims will be impacted. This includes individuals who practice safe behaviors.

6.6 Side Channels

This functionality enables the flow of information across virtual machines residing on the same hardware infrastructure that accommodates several virtual machines. The simultaneous deployment of many virtual machines has the potential to initiate a resource-sharing attack, whereby the combined utilization of the hardware's resources is exploited. In the event that an adversary successfully establishes a neighboring connection with a target, they will possess many alternatives to monitor the communication exchanged between the two virtual computers. Instances of this particular security vulnerability have been documented, and a range of mitigation strategies are now accessible [15].

Although it is crucial to note that there is security concerns associated with all kinds of computing, even though there are security faults within the cloud itself, it was previously said that the cloud infrastructure has inherent issues that render it susceptible to security breaches. Data centers provide a level of security that beyond what most people are capable of achieving alone [16]. On the other hand, average users are not likely to do system maintenance or keep their devices current with the latest security patches. However, datacenters are able to install and put into effect virtually instantaneous security upgrades, and they may deploy extra protection.

6.7 Lack of Data Control

The most important factor that prevents consumers and businesses from adopting cloud computing and cloud OS. On conventional personal computers or servers that are controlled by an organization or an individual, there is control over the manner in which the data is kept, access is limited only to those with a legitimate need, and contingency measures are implemented. Cloud computing is the storage of data on a remote server, whereby the maintenance responsibilities are delegated to a third-party provider. Additionally, there must be a certain degree of trust established between the supplier and the user. [17] In order for the user to be able to save data that may be considered private, secret, or sensitive, the user must have sufficient confidence in the provider.

Even though we were unable to locate any concrete evidence that organizations illegally shared Users are generally anticipated to authorize the provider to utilize analytics or data stored in order to solicit advertising in return for complimentary services, particularly if the provider intends to disclose the user's information to third-party entities. This is the case even though we were unable to locate any concrete evidence that organizations illegally shared data with third-party organizations. Google's business strategy is predicated on the idea that it should provide its customers a free service while simultaneously exploiting the information acquired to the advantage of its advertising. It is quite probable that businesses and people would not want for the information contained in their data to be mined for use by advertisements. Users will be required to pay for services that guarantee more privacy and do not share their information with marketing companies if they want to avoid this requirement [18].

6.8 Internet Reliance

Our reliance on the internet is growing at an exponential rate as a result of the growing popularity of cloud computing and the proliferation of online apps [21]. This is particularly relevant in light of the fact that users are becoming more reliant on servers for the operation of the vast majority of the programmed they use as well as for the storage of data. For any kind of computer, users are completely reliant on the internet, and this is especially true for those who utilize Cloud operating systems like Google Chrome OS. The occurrence of a catastrophic catastrophe that resulted in the unavailability of internet access to a significant segment of the population or the whole global population would have a profound negative impact on production. If a water utility business, for example, were to transition its computer activities entirely to distant servers, and the firm and its consumers would be exposing themselves to potential risks [22].

7 Standardization of security levels

Following an examination of the content presented earlier, it became clear that there are a great many aspects that need attention in order to achieve the highest possible level of security in the cloud. Because of this, we have compiled a list of security considerations that every person who uses the cloud should be aware of and investigate before making a decision about whether or not to utilize the cloud. To begin, however, we will discuss the possibility of standardizing the process of providing security permissions to things throughout the cloud.

The term "cloud computing" refers to a model of data storage and processing that makes use of a network of remote servers and data centers to provide a virtually unlimited amount of processing capacity. As has been shown throughout this article, security is a big problem and one of the numerous obstacles that must be overcome inside cloud computing. Researcher recommended that should be conducted on standardizing, and it should be in the cloud level. All participating organizations should adhere to these standards. Depending on the security level that was given, certain security procedures would be enforced by the servers. Because of this standardization, users would be able to assign different degrees of security protection to various types of information. For instance, a company whose primary focus is research and development may put a high level of importance on the confidentiality of information pertaining to initiatives that have not yet been disclosed or presented to consumers in the market. In addition, this hypothetical organization may not consider data to be sensitive once it has been made public, and as a result, a less stringent security policy could be implemented.

International standards like ISO/IEC 27001 and NIST SP 800-53 provide critical recommendations for organising security levels in cloud systems. These frameworks assist organisations in aligning security procedures with internationally recognised standards, particularly in data categorisation, access control, and incident management.

In principle, the workload and the degrees of security might be concentrated on just those objects that need to be secured if it were allowed that certain items may be designated as requiring to be secure while others were allowed to be assigned as not needing protection [22]. In addition, service providers may charge a higher or lower fee depending on the level of safety required for the user's data that is being stored by the provider.

It's possible that giving users the freedom to designate their own security levels might lead to difficulties, as some of them could decide to lock down everything. Because of this, there is a possibility that extra security procedures would be taken with data that could not have been securely stored via any other method. This might potentially result in suboptimal resource allocation and perhaps provide outcomes that are less efficacious compared to existing protocols. Categorizing objects as either safe or not secure has the potential to enable hackers to concentrate their efforts on areas that need the greatest attention. If hackers had a technique to selectively target these packets, the volume of packets requiring scrutiny for confidential information would be significantly reduced.

8 Conclusion and Future Direction

8.1 Conclusions

Cloud computing is an emerging paradigm that offers several advantages for users, although it also introduces some apprehensions about security that might impede its widespread adoption. The emergence of cloud computing has bestowed several benefits onto its users. Organizations that possess enough readiness to address the challenges associated with cloud operating systems have a smoother transition to cloud-based infrastructure. The cloud computing operating system encompasses a wide range of technologies, hence inheriting the security vulnerabilities associated with each of these platforms. The examination of standard web applications, data hosting, and virtualization has been conducted; nevertheless, it is worth noting that some of the suggested resolutions are either impractical or have not yet been put into practice. We have discussed some significant security concerns associated with the designs of IaaS, PaaS, and SaaS cloud computing models. The concerns expressed exhibit variation contingent upon the specific design. This research conducted an examination of several security concerns pertaining to cloud OS. This study also explored an innovative concept for standardizing the standards of data security throughout the cloud, which would be something that all servers would adhere to. Following much debate, it was determined that this concept requires a great deal more effort and thinking before it can be evolved into something that will be beneficial in the future. Also covered were a number of important security concerns that all consumers and organizations should be aware of before making a decision about whether or not to use cloud computing.

8.2 Future Direction

where we believe it is crucial to have a solid understanding of the safety concerns. It was not enough to just list all of these security flaws; thus, we need to determine which weaknesses contribute to the successful execution of these attacks in order to make the system more resistant. In addition, several existing remedies were outlined in order to reduce the impact of these dangers. However, in addition to revamped versions of tried-and-true security solutions, brand-new security approaches that are compatible with cloud infrastructures are required. Because the cloud is a complicated architecture that is made up of a mix of diverse technologies, it is possible that traditional security techniques will not operate very well in cloud situations. In conclusion, while our systematic research did touch on the underlying reasons that might lead to the occurrence of difficulties in cloud operating systems, more and more in-depth examinations of the core causes are still need to be carried out.

References

[1] M'rhaoaurh I, Okar C, Namir A, Chafiq N. Challenges of cloud computing use: A systematic literature review. InMATEC Web of Conferences 2018 (Vol. 200, p. 00007). EDP Sciences.

[2] Alonso J, Orue-Echevarria L, Casola V, Torre AI, Huarte M, Osaba E, Lobo JL. Understanding the challenges and novel architectural models of multi-cloud native applications–a systematic literature review. Journal of Cloud Computing. 2023 Dec;12(1):1-34.

[3] Latha KS, Githiki HV, Morla ML, Vanama AS, Tripathi Y. A Systematic Literature Review on Security in Cloud Technology. In2023 Second International Conference on Electronics and Renewable Systems (ICEARS) 2023 Mar 2 (pp. 832-837). IEEE.

[4] Sanjeetha MB, Ali GA, Nawaz SS, Almawgani AH, Ali YA. Development of an alignment model for the implementation of devops in smes: an exploratory study. IEEE Access. 2023 Dec 18;11:144213-25.

[5] Zhao S, Miao J, Zhao J, Naghshbandi N. A comprehensive and systematic review of the banking systems based on pay-as-you-go payment fashion and cloud computing in the pandemic era. Information Systems and e-Business Management. 2023 Jan 17:1-29.

[6] An YZ, Zaaba ZF, Samsudin NF. Reviews on security issues and challenges in cloud computing. InIOP Conference Series: Materials Science and Engineering 2016 Nov (Vol. 160, No. 1, p. 012106). IOP Publishing.

[7] Roberts JC, Al-Hamdani W. Who can you trust in the cloud? A review of security issues within cloud computing. InProceedings of the 2011 Information Security Curriculum Development Conference 2011 Sep 30 (pp. 15-19).

[8] Sethi S, Sruti S. Cloud security issues and challenges. InResource Management and Efficiency in Cloud Computing Environments 2017 (pp. 89-104). IGI Global.

[9] Sen AK, Tiwari PK. Security issues and solutions in cloud computing. IOSR Journal of Computer Engineering. 2017 Mar;19(2):67-72.

[10] Dave D, Meruliya N, Gajjar TD, Ghoda GT, Parekh DH, Sridaran R. Cloud security issues and challenges. InBig Data Analytics: Proceedings of CSI 2015 2018 (pp. 499-514). Springer Singapore.

[11] Padhy RP, Patra MR, Satapathy SC. Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS). 2011 Dec;1(2):136-46.

[12] Nadeem MA. Cloud computing: security issues and challenges. Journal of Wireless Communications. 2016 Dec 15;1(1):10-5.

[13] Pandey NK, Kumar K, Saini G, Mishra AK. Security issues and challenges in cloud of things-based applications for industrial automation. Annals of Operations Research. 2023 Mar 21:1-20.

[14] Akbar H, Zubair M, Malik MS. The Security Issues and challenges in Cloud Computing. International Journal for Electronic Crime Investigation. 2023 Mar 3;7(1):13-32.

[15] Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N. Cloud security threats and solutions: A survey. Wireless Personal Communications. 2023 Jan;128(1):387-413.

[16] Agapito G, Cannataro M. An Overview on the Challenges and Limitations Using Cloud Computing in Healthcare Corporations. Big Data and Cognitive Computing. 2023 Apr 6;7(2):68.

[17] Agulleiro C, Perez M. Exploring the Use of Real-Time Operating Systems for Enhancing Security in Smart Devices. Journal homepage: www. ijrpr. com ISSN.;2582:7421.

[18] Pallathadka H, Sajja GS, Phasinam K, Ritonga M, Naved M, Bansal R, Quiñonez-Choquecota J. An investigation of various applications and related challenges in cloud computing. Materials Today: Proceedings. 2022 Jan 1;51:2245-8.

[19] El Kafhali S, El Mir I, Hanini M. Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering. 2022 Jan;29(1):223-46.

[20] Hassan W, Chou TS, Tamer O, Pickard J, Appiah-Kubi P, Pagliari L. Cloud computing survey on services, enhancements and challenges in the era of machine learning and data science. International Journal of Informatics and Communication Technology (IJ-ICT). 2020 Aug;9(2):117-39.

[21] Kumari P, Singh M. Different Challenges in Energy-Efficient Cloud Security: A Brief Review. Research Developments in Science and Technology Vol. 6. 2022 May 27:112-22.

[22] Sun P. Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications. 2020 Jun 15;160:102642.