International Journal of Current Science Research and Review

ISSN: 2581-8341

Volume 05 Issue 05 May 2022

DOI: 10.47191/ijcsrr/V5-i5-09, Impact Factor: 5.995

IJCSRR @ 2022

www.ijcsrr.org

Data Security and Privacy in Cloud Computing Platforms: A Comprehensive Review

Md. Kishor Morol[1], Shuvra Smaran Das[2], Sharfuddin Mahmood[3]

[1,2,3] Department of Computer Science, AIUB

ABSTRACT: Cloud computing is the on-demand usage of computer resources through the internet, allowing us to relocate application software and databases. Its purpose is to deliver IT services that enable clients to benefit from the pay-per-use model's substantial cost advantages and the ability to flexibly scale up or down without having to make significant investments in new hardware. On the other hand, the provider manages the data and services under this cloud architecture. Consequently, cloud clients have less control over their outsourced data and depend on cloud service providers to safeguard their data and infrastructure from both external and internal threats. In this study, we look at information security in cloud computing. It is the consideration of information on the cloud, considering security concerns. This article will go through data protection strategies utilized all around the globe to provide optimum data security by lowering risks and threats. Information accessibility is beneficial for various cloud applications, but it poses risks by exposing data to apps that already have security escape clauses. In addition, the presentation will outline information security highlights for Data in Transit and Data at Rest.

KEYWORDS: Cloud Computing, Data Security, Hardware Security, IaaS, PaaS, SaaS.

1. INTRODUCTION

Cloud computing is a novel service that comprises a mix of technologies and Internet-based support for distant applications with high quality of service (QoS). Cloud computing is a service that provides contemporary energy of computing in real-time scaling and virtualized assets as a service through the internet [1]. It handles how cloud computing can protect and develop trust in cloud user data. "A template for providing the appropriate and when needed access to the internet, to a collective pool of programmable grids, storage, servers, software, and amenities that can be rapidly emancipated, with little communication and supervision from the provider," according to the National Institute of Standards and Technology (NIST) [3]. Cloud computing is built on a benefit-level agreement between the service provider and clients and offers a shared pool of customizable IT resources on demand through a networked infrastructure that needs little management effort. It often takes the shape of web-based tools or programs that users can access and use as if they were software installed locally on their computer using a web browser. Cloud data adaptability is a significant risk for data security and privacy. Cloud computing relies heavily on data integrity, privacy, and protection. Different service providers use various regulations and processes depending on the nature, kind, and scale of data [6]. The cloud manages the servers, databases, software, social media, and eCommerce sites. Hybrid, Community, Private, and Public clouds are the four deployment types available.

Public Cloud*:* A public cloud is a kind of computing in which a service provider makes resources available to the general public through the Internet. Examples: Dropbox, SkyDrive, and Google drive.
Private Cloud*:* Private cloud is a computing model which is a cloud environment solely dedicated to a single customer. It is a more secure platform for employees exclusively dedicated to a single customer. It is a more secure platform for the employees and customers of an organization. For example, in any organization, customers or employees are assigned by them. Only they can access the data.
Hybrid Cloud: The term "hybrid cloud" refers to a mix of public and private clouds. The sensitive data is kept in the private cloud and maintained by the public cloud, but the hybrid cloud is controlled by a single aircraft. As a result, a hybrid cloud is more effective.
Community Cloud: Community shared infrastructure several organizations managed, operated, and hosted by third-party providers. For example, U.S.-based dedicated IBM SoftLayer cloud.

1.1 CLOUD SECURITY

There are different security issues for cloud computing because it comprises many advances including networks, databases, operating systems, virtualization, resource scheduling, transaction management and memory management. Since cloud computing and web administrations are based on a organize design, they are open to arrange sort assaults. One of these assaults is the dispersed dissent of benefit attacks.

- Service Provider Security Issues
- Identity and access management
- Securing Data in Transmission
- Infrastructure Security Issues
- Securing Data-Storage
- Network and Server
- Browser Security
- Authentication

The cloud model provided the three following major service categories:

1.1.1 INFRASTRUCTURE AS A SERVICE (IAAS)

'Infrastructure as a Service' is the abbreviation for IASS. It provided us with nothing more than computing architecture and infrastructure. Additionally, data storage, virtualization, servers, and networking are covered. The vendor administers these resources, whereas users have access to the data. [7] With IaaS, the user may install and execute any software where operating systems and apps are included. The user does not have authority over or responsibility for the underlying cloud infrastructure but does have control over the operating system, applications, and storage and some limited control over specific networking components. [8] IaaS cloud providers deliver these resources on-demand from their extensive equipment pools located in data centers. Customers may connect to a vast area network or a specialized virtual private network through the Internet. With IaaS, IT administrators merely buy the computing, storage, and infrastructure application resources required to run their particular environment, and the rest is virtualized. It enables the flexibility, stability, and scalability sought by many enterprises in the cloud while also eliminating the need for hardware. Additionally, it is a cost-effective IT solution for corporate expansion. Due to the elasticity of IaaS, large companies may utilize the public cloud to scale up or down as required. The instance resources (CPU, memory, and size) may be resized in seconds from minuscule to colossal without installing a single DIMM chip. The primary benefits of deploying IaaS are that it may help identify a business's storage requirements, and all agreements are always negotiated before installation. The majority of suppliers are in charge of their management. When someone uses this service, they are responsible for managing additional resources, such as applications, data, runtime, and middleware. This is mostly for system administrators.

1.1.2 PLATFORM AS A SERVICE (PAAS)

Platform as a Service (PaaS) is a cloud computing service that provides users with a secure environment for developing, running, and managing applications. It is responsible for providing the runtime environment for applications, development, and deployment tools. [10] Additionally, it offers the infrastructure necessary to handle the whole life cycle of developing and deploying web applications. It provides a platform with tools for concurrently testing, developing, and running programs. It enables an organization to focus on development. It gives managed security, operating system, server software, and backups. There are many platforms in cloud computing in this modern era [11]. The Google cloud platform, Microsoft Azure, Amazon web services, IBM Cloud, Digital Ocean, etc. In this Platform, we develop and deploy our application. There are four types of Platforms is a service (PaaS). These are application delivery-only environments, standalone development environments, open Platform as service, and add-on development facilities. Application delivery only environment means on-demand scaling. A standalone development environment means it works independently. It is not dependent on others. Open Platform as a service offers open-source software. [12] Platform as a service (PaaS) has so many benefits. These are lower administrative overhead, a lower total cost of ownership, scalable solutions, pay-as-peruse, and more current system software. Administrative overhead is those cost that is not involved in the development or production. The total cost of ownership is used to calculate the total cost of buying and operating technology. [13] The total cost of ownership is important for evaluating technology costs. Pay per use means how much storage we used. Only pay for this used storage. Platform as a service (PaaS) has many issues. These are a lack of portability between Platform is a service, event-based processor scheduling, and security engineering of Platform is a service (PaaS) application. Portability means transferring the data from one Platform to another platform [14].

1.1.3 SOFTWARE AS A SERVICE (SAAS)

Program as a benefit, there is a method of transmitting programs via the Internet as a service, also known as SaaS. Rather than introducing and maintaining software, we may easily access it over the Internet, freeing ourselves from complicated software and infrastructure. On-demand software or hosted software are other terms for SaaS apps. Software as a service (SaaS) means delivering software to consumers. Rather than acquiring and installing a program, SaaS users support it. This implies that users of SaaS applications do not need to download software, manage existing IT infrastructures, or deal with any aspect of software administration. Users may quickly enter the system and utilize a SaaS application through the Internet from any suitable device. SaaS providers supply the following services:

Business Services: A SaaS provider may help a new firm with several business services. ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), invoicing, and sales services are all included in the SaaS business services.

Document Management: SaaS document management is a software program for creating, managing, and tracking electronic documents provided by a third party (SaaS providers). Slack, Samepage, Box and Zoho Forms are other examples.

Social Networks: Because the general public uses social networking sites, social networking service providers employ SaaS for their convenience and to manage the general public's information.

Mail Services: Many e-mail providers employ SaaS services to handle the unexpected number of users and load on their e-mail services.

2. RELATED WORKS

Because cloud computing has several benefits over benefit computing and inevitability computing, it is becoming more popular. Different metrics, such as capacity, interface, and data sort synchronization, are compared [1]. Despite the notion that cloud computing is concerned with security, the system lacks a response plan for threats inside the information cloud [2]. Excellent database management The technique is presented in diagrammatic and ordered declines [3]. Reduces the size of the outline Unmistakable mappers in a cloud-based database management approach for enterprises. However, when mapping is done, a problem arises. Because optional essential parts are kept in a disorderly way, a client-centric key organization scheme encourages the client to save the critical component and enables the client to utilize the encryption key. Interlopers who have gotten the convenient gadget lost by any client may leak encryption secrets, which is a problem. [4] In cloud computing, data from cloud customers or clients is stored on the cloud advantage provider's premises, raising data security and insight worries and lowering the adoption of the cloud computing paradigm. We present the bound-together data encryption strategy in this work, ensuring information security and protection while reducing the computer system's execution cost. [5]. The study showed hardware that can generate symmetric keys using a combination of crucial seeding, combined symmetric key computation, and enhanced signature [4][6]. A previously undiscovered symmetric critical cryptography approach is used for the encryption and decryption of any record. They used a 65536-component self-assertive essential square structure, yet the software developers could still locate the actual critical network. A predetermined period will also be consumed for a sweeping measured record [6-7]. An unused asymmetric-key cryptography computation provides a strategy for encryption and unscrambling. It strengthens the system against Brute-duty assault in growth, but there are a few areas of worry in essential understandings and obstacles to the number of keys that must be maintained in-group [8]. Security and protection are the most significant concerns in cloud computing. Cloud computing has security concerns: systems, databases, working frameworks, virtualization, resource planning, exchange administration, stack adjustment, concurrency management, and memory administration. As a result, cloud computing raises security concerns for many frameworks and technologies [9].

Fuzzy Keyword Search over Encrypted Data in Cloud Computing: As of late outsourcing, unstable data needs typically be scrambled a few times to provide data assurance. This technique formalizes and comprehends the problem of achieving adequate fluffy watchword visibility over mixed cloud data while maintaining catchy security. When users' seeking inputs facilitate the specified watchwords or the closest possible matching records based on watchword similarity semantics, feathery watchword see considerably increases framework comfort by returning the coordinating papers. We use isolated to assess catch expressions similarity and develop a progressive technique for generating comfy catch sets in our course of action, which significantly minimizes capacity and representation overheads.

Cloud Data Protection for Masses: This study presents a modern cloud computing paradigm that emphasizes information confirmation as a benefit. DPaaS is a set of security primitives made public by a cloud platform that implements data security and protection and provides proof of protection to data owners, even when they are near potentially hacked or destructive apps. Data assurance is achieved by using three primitives: access control, key management, and logging. There's also an inspector who keeps track of all the transactions inside the framework. At the end of the process, the reviewer produces an audit report based on all the talks.

Graphical User Authentication: An Approach Based on Time Interims. In recent years, many graphical-based confirmation mechanisms have been presented. Although content-based passwords are the most often used for authentication, they are very vulnerable to various attacks. Graphical approaches are emerging as a viable alternative to traditional confirmation tactics. We provide a visual way of verification in this study that uses graphic arrangements in addition to a new display of the time gap between successive clicks [10]. The client must remember the aids and the time interval between the subsequent clicks. As a result, the benefits of following graphics techniques are combined with the extra security provided by the use of time interim. Compared to other recent graphical verification techniques, the suggested plot has a substantially larger hidden word space [11]. The narrative is dynamic, safe, and very user-friendly.

2.1 IAAS, PAAS, AND SAAS CLOUD MODELS

2.1.1 INFRASTRUCTURE AS A SERVICE (IAAS)

Foundation as a Service (IAAS) is one of the three critical components in cloud computing. Foundation as a Benefit may be a sort of cloud service that gives clients a moment computing infrastructure that can be provisioned and overseen over the internet.[18] Infrastructure as a Benefit is fundamentally called the backbone of the cloud computing framework. It's giving the virtualized hardware stage or the Framework utilized in computing. When Foundation as a Benefit is used, it offers virtual machines and servers. And it provides storage space, bandwidth, network connections, and load balancers [30]. In an IaaS service model, a service or cloud provider hosts infrastructure components traditionally present in the data center [18]. Scaling of bandwidth storage and memory are generally included. The vendors compete on the performance, offering their prices for dynamic services. This IaaS can be purchased with either a contract or a pay-as-you-go basis. There are many examples of IaaS vendors and products. IaaS products are offered by the three largest cloud service providers—Amazon web service, Google, and Microsoft. In IaaS, Virtualization is utilized for integrating and breaking down assets in a respectable way to meet the ask for contracting aids from the cloud consumers. According to the creator, with the assistance of virtual machines, the benefits supplier of cloud supplies administrations to all users and capacity for rectifying the trade adeptness [17].

IaaS Advantages: IaaS can be obtained with either a contract or a pay-as-you-go premise. One self-evident advantage of IaaS is that never got to purchase equipment, introduce, or coordinate it. These services are given by the cloud, which saves businesses worth an hour. That's why no requirement has to purchase hardware, install, or coordinate it. It's simpler, speedier, and more cost-efficient. The comfort of Framework as a Benefit is worth viability, pay-on-demand for utilities, versatility, location independence, excess, and the security of information, which is imperative [19].

IaaS Risk: IaaS model sometimes has a particular shortcoming. The security of any service run in the cloud relies on the protection of the cloud infrastructure. Against a compromised hypervisor, it is not possible to defend or protect a virtual machine. Breaches concerning the infrastructure are a primary excessive security concern beyond those facing traditional servers. Sometimes, IaaS is more expensive than other cloud stages as you need to take the whole hardware infrastructure on rent. Also, Organizations ought to provide an adequate sum of preparation to their IT group to create them recognizable with the administration of the entire infrastructure [22].

2.1.2 PLATFORM AS A SERVICE (PAAS)

PaaS (Platform as a Service) is providing a platform and environment for developers to build applications and administrations [23]. PaaS is the movement of offices necessary to support the whole lifecycle of creating and passing on applications and organizations over a cloud system. It may be a collection of programming languages and program and thing methods disobedient in this manner. The user or customer does not manipulate or control the radical cloud system's servers, organization, operating systems, or capacity, but they do have control over the enlarged apps and maybe the course of action setup. Application development, design, testing, encouraging, arrangement, group collaborations, capacity, web service integration, security, adaptability, state organization, and versioning are provided by PaaS providers [24]. Platform as a Service (PaaS) allows users or customers to extend over the cloud infrastructure and create apps using the provider's programming languages and tools [25]. In this model, the cloud service providers give an application development platform for the programmers. They also provide a set of APIs for the programmers to develop and start their customized applications. It is not necessary to install development tools on their local devices [26]. Platform as a Service (PaaS) provides prebuilt application materials such as Application Programmable Interface (API). Developers and programmers generally use it for building upper-level applications. The developers generate and deploy application services for the consumers. It is unnecessary to operate the OS and Databases manually [27].
The clients don't handle the crucial cloud framework counting arrange, capacity, working frameworks, and servers but have overseen the deployed applications. Case: Android like Google Play Store, Facebook.com, application administrations, and online gaming [28]. PaaS could be a cloud benefit provider's facilitated foundation. Users usually get to PaaS offerings web browser. It can be delivered through private, open, or crossover clouds. With a private cloud, PaaS is provided as a computer program or an appliance within a client's firewall, by and large in its on-premises data center. With an open cloud in PaaS, the clients maintain software arrangement, whereas the supplier conveys all the major IT apparatuses to the visitor of the applications, counting systems, storage systems, databases, servers, and working frameworks. With a hybrid cloud, PaaS offers a blend of the private and open types of cloud service. PaaS gives fundamental administrations such as Java advancement or application facilitating for an organization's whole IT infrastructure for computer program advancement. A few PaaS include application plan, testing, refinement and sending, database integration, improvement group collaboration, web benefit integration, and data security. As with other cloud computing administrations, the client's installment for PaaS is on a per-use premise, with a few cloud suppliers charging a monthly expense forgetting to the organize.

PaaS advantages: The top focal point of PaaS is that endeavors can satisfy the condition in which to build and expand new applications without spending time and money on construction, Make, and maintenance. This will conduct to speedier advance and conveyance of applications, a massive plus for businesses looking to attain a combatant edge or that necessity to induce result to advertise rapidly. PaaS also lets them test the utilization of new dialects, databases, operating systems, and other improvement innovations quickly because they don't need to develop the supporting foundation for them.

PaaS Risk: PaaS could be a cloud-based benefit; it comes with numerous intuitive dangers that other cloud offerings have, such as information security dangers. PaaS is based on the motivation to use common property such as systems and servers, so the security dangers incorporate putting unsafe information into this circumstance and having their data stolen due to Unlawful get or attacks by programmers or other awful individuals. With PaaS, ventures are indebted to benefit suppliers building appropriate get to controls and other security repast and approaches into their infrastructures and operations. Ventures are too tried and true for supplying their claim security securities for their applications [29].

2.1.3 SOFTWARE AS A SERVICE (SAAS)

Software as a service model is deployed to run behind the firewall in a Local area network (LAN) or personal computer (PC) or laptop, and this is a" pay-as-you-go" model. In the SaaS model, the service provider provides applications related to software applications and all the components required for its execution.
Using a thin client interface like a web browser makes these applications accessible from different client devices. Cloud infrastructure includes networks, servers, operating systems (Microsoft Windows, macOS, and Linux), storage or individual application capabilities, etc. The end-user does not have to manage or control this cloud infrastructure [12]. There are many end customers who are frequent users of SaaS. For example, SaaS's products and services are Google ecosystems like Gmail, Google Drive, and Google docs [16]. A computer program is facilitated on a farther server which is available through a web browser

[13][15]. This application is managed from a central location, and application users don't need to worry about hardware or software (update, patch, etc.). SaaS administrations incorporate mail and office efficiency applications, client relations administration (CRM), undertaking assets arranging (ERP), etc. [13-14]. SaaS plays a crucial role in security, and it provides user authentication and password verification.

SaaS Advantages: SaaS decreases the time went through on establishment and setup. Moreover, it can diminish the issues. On the other hand, the entire support costs are reduced as well. SAAS supplier possesses the condition, and it is partitioning among all customers [20]. A SaaS application requirement is a browser and an online association. SaaS is generally get-at-able on a broad run of gadgets. Compared with other traditional commerce program installations from any place in the world, SaaS is more available than others. Another thing is security, and SaaS gives the protection of the program.

SaaS Risk: SaaS demonstrates, in some cases, has a specific deficiency. The SaaS demonstration is based on web conveyance; if the internet service falls flat, the client will be dispossessed get to their software or information. Another thing is to get to administration, and the privacy of naive data may be a significant judgment around cloud and facilitated administrations [21].

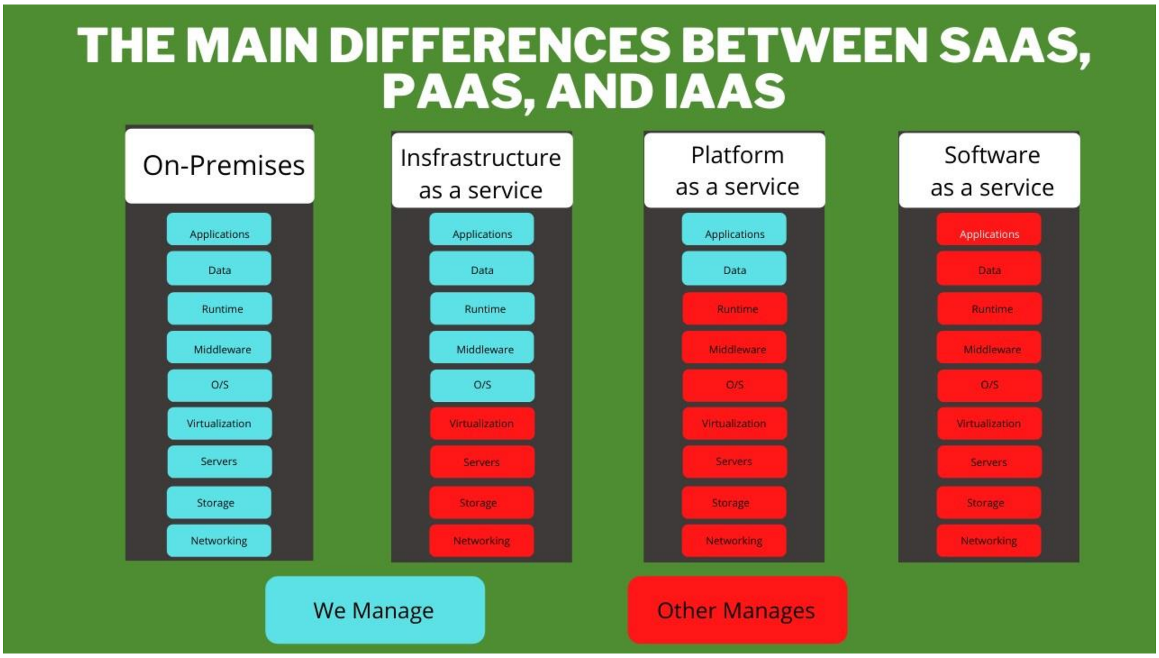

Fig-2.1: Difference between SaaS, PaaS, IaaS.

3. EXISTING METHODS

SaaS could be a program arrangement demonstrated by a third-party supplier that builds applications on a cloud framework and makes them accessible to clients through the web. SaaS is the most common structure of cloud computing. The SaaS provider oversees everything from equipment soundness to app functioning. Clients are not dependable for anything in this model; they, as it was, utilized programs to total their errands. In this case, the client program involvement is entirely subordinate to the supplier. Using a program as a benefit looks suitable for most businesses, but some downsides have to be considered. Here are some of the drawbacks of SaaS transformation - Instead of relying on local computers or remote servers, cloud computing distributes processing over many distributed devices. The data center's functioning is more or less identical to that of the Internet. Businesses may use this method to transfer resources. These resources are capable of allocating the appropriate applications. On-demand, most endeavors may gain access to PCs and capacity frameworks. Cloud computing has many high points, including total size, virtualization, consistently high quality, adaptability, high flexibility, on-demand administrations, prospective dangers, and so on [36]. These properties of cloud computing favor significantly more severe security concerns than traditional security concerns. The vast majority of widely used SaaS stages result from actual businesses with a focus on security.

3.1 DATA SECURITY ISSUES

Data security is almost exclusively considered judgment, privacy [39], and comfort. These three estimates are both correlated and limiting. The term "information insight" refers to the fact that data in the cloud cannot be balanced without the users' permission. The security of the users' data is implied by secrecy. And since this knowledge is irrevocable, it is unimaginable to share it with others. Clients with an availability license may access and use data from cloud companies without any restrictions.

3.2 THE USERS' PRIVACY ISSUES

The cloud advantage vendors assure the customers' data security underneath the cloud computing environment. Clients also have the right to know which suppliers profit from the cloud and whose users' data is protected. Users' data information is shattered or not smashed when they do not use this benefit supplier's cloud service. Once the cloud benefit providers have the consumers' personal information, the provider fails to safeguard the data adequately. Others may be able to steal this information. Clients are entirely unprotected.

3.3 VIRTUALIZATION SECURITY ISSUES

Plans to interact with each other between servers via virtualization have evolved as cloud computing livelihoods moved away. When shared vulnerabilities occur between physical and virtual machines inside the communication channel, this may cause many problems. The German laws are ineffective. Cloud computing applications, information streams, information administrations, and client information come in various flavors in various locations and even nations. In addition, the information security and legal issues of government control are fraught with controversy. At the same time, many customers' information assets are not copyrighted, and cloud administrations are stored in other nations. These concerns cannot be held liable for a few linked customers due to various regulations in various countries.

3.4 LOSS OF CONTROL

The dealer manages everything, making you subordinate to the vendor's capabilities. After you put your data in a SaaS framework, you ensure that somebody who doesn't work for you can—and will—access your information. The as-it-where questions are who, when, and why. The basic expression to seek in terms of benefits document is the "principle of slightest privilege," which suggests that, as it were, those representatives who must have got information do have to get to it. It sounds basic, but it's beautiful uncommon among SaaS new companies, who regularly oversee information on the honor framework. Which SaaS supplier workers have gotten to my information? Beneath what circumstances are the provider's representatives permitted to see my data.
How much of my information is recorded for the look? Is my information ever shared with a third party without my unequivocal authorization? On the off chance that my information is shared, how is it anonymized? If your SaaS is free but upheld by publicizing, it implies the app supplier is either checking you're utilizing the app to better target advertisements at you, observing you use the app to offer that utilization information to other promoters, or both. A few of these focusing on may include more than fair how you utilize the app, but what information you store in it. Your SaaS terms of benefit ought to be expressed around what information and exercises are followed, what viewpoints of the tracked information are shared, whom that information is shared with, and, overall, how the followed information is anonymized so your data isn't given out in an identifiable way [36].

3.5 LIMITED CUSTOMIZATION

Diverse Free Program Merchants (ISV) see customization in several ways. A few feel it is critical and go the additional mile, whereas others make their SaaS item intensely configurable. It is up to the item directors to require a choice as to what is configurable. Arrangement versus customization is an old wrangle, and the reply is continuously situational. [37] Select the SaaS applications that offer the closest fit to your commerce prerequisites. It requires having a great understanding of your necessities and a well-established choice system to prioritize them. Decide which necessities are fundamental to your commerce and which ones are essentially pleasant to have. The previous ought to direct your determination, and the last-mentioned ought to be maintained a strategic distance from through and through. Adjust your forms to the arrangement, not the other way around. Rather than customizing SaaS applications until your clients are fulfilled, your clients ought to be willing to receive the most excellent hones built into the arrangement. Thousands of companies utilize numerous SaaS applications, so the address you must inquire about is if your company is that diverse from what innumerable others have embraced as best hones. The primary approach requires you to prioritize a few trade necessities sufficient to base your choice on them. The moment approach sees most other prerequisites as adaptable adequate to be adjusted to anything the chosen arrangement offers. Changing these two approaches requires profound trade understanding and dynamic collaboration between all the partners. Everybody needs to move absent from the conventional thinking that commerce prerequisites may be satisfied by building customizations. [38]

3.6 CONFIDENTIALITY

Cloud administrations have become a growingly prevalent arrangement to supply diverse administrations to clients. One of the SaaS administrations is a database as a benefit (DBaaS), in which the service supplier gives various assets such as software and hardware and arranges for the clients to be able to manage and regulate the database. In any case, the mistrustful service supplier controls the information and the execution of database questions. This deficiency of belief opens contemporary security issues and serves as the most inspiration for our work. This study appears an outline of different cryptographic algorithms which is based on specific plans within the outsourced database security and inquiry authentication [38].

3.7 LIMITED RANGE OF APPLICATIONS

The cloud benefit supplier has the application and makes it accessible to clients by utilizing the web. Presently, SaaS is becoming more well-known, but it still has numerous applications that do not offer a facilitated platform. [37] We may discover it necessary to still have specific applications on location, mainly if our company depends on different program arrangements. SaaS offerings are still constrained control over program parameters, deployment, testing strategy, overhauls, etc. Overhauls got to be available to all clients at once. When working with an outside SaaS service supplier to have numerous apps, able to see, there might be an integration issue with the existing in-house software. [36] The in-house APIs and information structures might not be coordinated legitimately with the outside program. As a result, we ought to continuously perform compatibility checks with all SaaS applications for superior comes about.

3.8 CONNECTIVITY REQUIREMENT

SaaS may be a way of conveying program applications to the end-user over the web since the SaaS program is web-hosted, so we cannot utilize these applications without an online connection. If the Web benefit goes down or in case portable laborers are in a dead Web zone, we won't have got to the software or data [39]. A customer is given an appropriate component, and they have complete operational authority over the part. A cloud cube display shows the degree of security closeness.

4. CONCLUSION

Data security has long been a significant problem in information technology. Because data is kept in various places, even worldwide, it becomes riskier in the cloud computing environment. The most common worries users have regarding cloud technology are data security and privacy protection. There have been various views on how to utilize cloud computing, but data security and privacy protection are becoming more critical as cloud computing technologies become more widely used in government, industry, and business. Data security and privacy are hardware and software concerns in cloud architecture [31]. Cloud computing is a relatively new technology that has piqued the attention of both the corporate and academic communities. It provides internet-based services, letting customers use numerous apps' online services rather than purchasing or installing them on their computers [32]. The National Institute of Standards and Technology (NIST) defines cloud computing as a model for providing useable, on-demand network access to a shared pool of programmable computer resources [33]. Cloud computing has several benefits, including cost savings, fast implementation, and increased accessibility. By offering numerous methods mentioned in this article, several researchers have contributed to the decrease of data security challenges in this arena. This study reviews the literature on cloud computing data security and presents the results. There are, however, a host of practical concerns to be addressed. Data confidentiality is one of them. Data security should be a concern for users who wish to utilize cloud computing. This technology needs appropriate security ideas and practices to handle user concerns. The majority of cloud service customers, according to [34], are concerned that their data may be utilized for other reasons or transferred to other cloud service providers.

The user data needs to be protected and separated into several categories [35]:

i. Information gathered from computer devices; use data
ii. Confidential information, such as health or bank account information.
iii. Personally identifiable information (PII) is data that may be used to identify a person.
iv. Unique device IDs; data can be traced back to a specific device, such as IP addresses.

Cloud computing can be considered a new computing paradigm that provides low-cost on-demand services. The three most well-known and commonly utilized service models in the cloud paradigm are a software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) (IaaS). A cloud service provider distributes software and associated data that customers may access via web browsers under SaaS. PaaS is a service paradigm in which a business provides clients with a collection of software applications that enable them to do specific tasks. In IaaS, the cloud service provider supplies consumers with virtual computers and storage to allow them to expand their company capabilities. Cloud computing is a promising and rapidly evolving technology for future IT applications. Data security and privacy issues are significant impediments to cloud computing's fast growth. Reduced data storage and processing costs are essential for every company, and data and information analysis is one of the most critical roles in any company's decision-making process.

Consequently, no organization will move its data or information to the cloud unless cloud service providers and users have established confidence. Researchers have presented many data protection strategies and achieved the most significant degree of data security in the cloud. However, many gaps still need to be addressed for these tactics to be more successful. More work is required in this subject to make cloud computing acceptable to cloud service consumers. To create confidence between cloud service providers and customers, this article looked at a variety of data security and privacy solutions for data protection in cloud computing environments, emphasizing data storage and usage in the cloud. Even though our review looked into the matter, further study is required to back up the conclusions. Another long-term aim is to explore numerous security issues in the cloud computing environment and develop a security model based on encryption technology. Other security challenges in the cloud computing environment and the creation of a security model for data concealment in cloud computing using encryption methods will be studied in the future.

REFERENCES

1. W.K.Chan, Lijun Mei, T.HTse : “A Tale of Clouds- Paradigm Comparisons and Some Thoughts on Research Issues”, IEEE Asia-Pacific Services Computing Confer- ence pg: 464-469 2008.
2. Siani Pearson, Yun Shen and Miranda Mowbray.: “A Privacy Manager for Cloud Computing”, HP Labs, Long Down Avenue, Stoke Gifford, Bristol BS34 8QZ, UK.
3. Dean J. Ghemawat S.: “Map Reduce: Simplified data processing on large clusters” in Communications of the ACM, Vol. 51, No. 1 2008.
4. ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India, Mr. Krunal Patel M.Tech CSE-SCSE Vel- lore Institute of Technology Vellore India, Prof. Sendhil Kumar K.S Assistant Professor(Sr)- SCSE Vellore In- stitute of Technology Vellore India, Mr. Navneet Singh, Mr.Kushang Parikh M.Tech CSE-SCSE Vellore Institute of Technology Vellore India, Dr. Jaisankar N. Professor SCSE Vellore Institute of Technology Vellore India.: “Data Security and Privacy using Data Partition and Centric key management in Cloud”.
5. Dharmendra S. Raghuwanshi Cloud Security Group Centre for development of advanced computing, Chennai, India E-mail: dharmendrar@cdac.in, M.R.Rajagopalan Cloud Computing Group Centre for development of advanced computing, Chennai, India E-mail: mrambi53@gmail.com.: “MS2: Practical Data Privacy and Security Framework for Data at Rest in Cloud”.
6. Wu Suyan, Li wenbo and Hu Xiangyi.: “Study of Digital Signature with Encryption Based on Combined Symmetric Key”, 2009 IEEE.
7. Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta and Asoke Nath.:“A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmet- ric key algorithm”, 2011 IEEE.
8. ThongponTeerakanok and SinchaiKamolphiwong.: “Accelerating Asymmetric-Key Cryptography using Parallel-key Cryptographic Algorithm (PCA)”, 2009 IEEE.

9. Sunumol Cherian, Kavitha Murukezhan Department of computer Science, Vedavyasa Institute of Technology, Calicut ** Head of computer science De- partment, Vedavyasa Institute of Technology.: “Providing Data Protection as a Service in Cloud Computing”, International Journal of Scientific and Research Publi- cations, Volume 3, Issue 6, June 2013 1 ISSN 2250- 3153.
10. Aejaz Ahmad Dar,School of Engineering and Technology, Islamic University of Science and Technology, Awantipora, Jammu and Kashmir, India: “Cloud Computing-Positive Impacts and Challenges in Business Perspective”.
11. https://scholarworks.wmich.edu/cgi/viewcontent.cgi? article=1932context=masters theses
12. Mohammad Sarosh Umar1, Mohammad Qasim Rafiq2 and Juned Ahmad Ansari3 Department of Computer Engineeing Aligarh Muslim University Aligarh, India.: “Graphical User Authentication: A Time Interval Based Approach”.
13. Z. Gilani, A. Salam, and S. Ul Haq.: “Deploying and managing a cloud infrastructure: real world skills for the ComTIA cloud+ certification and beyond,” Wiley, Jan. 2015.
14. S. Subashini and V. Kavitha.: “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34(1), Jan.2011, pp. 1–11.
15. L. Wei et al.: “Security and privacy for storage and computation in cloud computing,” Inf. Sci. (Ny).,vol. 258, pp. 371386, Feb. 2014.
16. https://www.researchgate.net/publication/341979640 Cloud Computing Security Challenges
17. F. Howell and R. Mcnab. SimJava: A discrete event simulation library for java. In Proceedings of the first International Conference on Web-Based Modeling and Simulation, 1998.
18. R. Buyya, C. S. Yeo, and S. Venugopal. Marketoriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities. In Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, 2008
19. https://wheelhouse.solutions/what-are-the-advantages- of-infrastructure-as-a-service/
20. https://www.ibm.com/cloud/blog/top-5-advantages-of- software-as-a-service
21. https://www.nibusinessinfo.co.uk/content/advantages-and-disadvantages-software-servicesaas
22. https://www.rswebsols.com/tutorials/softwaretutorials/saas-paas-iaas-advantagesdisadvantagescomparison
23. https://www.guru99.com/cloud-computing-for-beginners.html
24. M. Carroll, A. van der Merwe and P. Kotzé, "Secure cloud computing: Benefits, risks and controls," 2011 Information Security for South Africa, 2011, pp. 1-9, doi: 10.1109/ISSA.2011.6027519.
25. https://www.sciencedirect.com/science/article/pii/S0167739X10002554
26. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.640.1140rep=rep1type=pdf
27. Lawrence, Dr. L. Arockiam & Donald, A. Cecil & Oli, S.. (2013). Mobile Cloud Security Issues and Challenges: A Perspective. International Journal of Engineering and Innovative Technology. 3. 401-406.
28. M. Arfan, "Mobile cloud computing security using cryptographic hash function algorithm," 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), 2016, pp. 1-5, doi: 10.1109/ICITACEE.2016.7892480.
29. https://www.infoworld.com/article/3223434/what-is-paas-software-development-in-thecloud.html
30. Sun, Yunchuan & Zhang 张均胜, Junsheng & Xiong, Yongping & Zhu, Guangyu. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks. 2014. 1-9. 10.1155/2014/190903.
31. https://research.ijcaonline.org/volume94/number5/pxc3895625.pdf
32. NIST SP 800-145, “A NIST definition of cloud computing”, [online] 2012, http://csrc.nist.gov/publications/drafts/800-45/Draft- SP-800-145 cloud-definition.pdf(Accessed: 23 December 2013)
33. Elahi, T., Pearson,S.(2007). Privacy Assurance:Bridging the Gap Between Preference and Practice.In C.Labrinoudakis, G. Pernul A. Tjoa (Eds.),Trust, Privacy and Security in Digital Business(Vol. 4657, pp. 65-74): Spriner Berlin Heidelberg.
34. Siani Pearson,: “Taking Account of Privacy when De-signing Cloud Computing Services,” CLOUD’09, May 23, 2009, Vancouver, Canada, pp. 44-52.
35. 2018 2nd IEEE Advanced Information Management Communicates, Electronic and Automation Control Conference(IMCEC 2018): “The Research on SaaS Model Based on Cloud Computing”.

36. Liu Yingjie, Wang Lunyan, Hu Fangyuan, Yuan Lu. Security Access Control in SaaS Mode Based on Improved RBAC Model [J] .Modern Computer, 2017 (15): 81-84.
37. Huang Y. Pure design and implementation of RBAC system based on SaaS model [D]. Northeast Normal University, 2013.
38. Huang Xiuli. Interpreting Cloud Cube Model [J]. Com- puter Technology and Development, 2012,22 (03): 245-248.
39. Modak, G., Das, S. S., Miraj, M. A. I., & Morol, M. K. (2022, March). A Deep Learning Framework to Reconstruct Face under Mask. In 2022 7th International Conference on Data Science and Machine Learning Applications (CDMA) (pp. 200-205). IEEE.