Computational and Analytical Approach for Cloud Computing Security with User Data Management

Dr. P. Phanindra Kumar Reddy Department of Artificial Intelligence and Data Science, Annamacharya Institute of Technology and Sciences(Autonomous), Rajampet, Andhra Pradesh, India-516126.

P. Anusha, A. Geetha Chowdary, M. Chandrasekhar, K. Banu Prasad, S. Anusha Kumari, Department of Artificial Intelligence and Data Science, Annamacharya Institute Of Technology And Sciences (Autonomous), Rajampet,, Andhra Pradesh, India – 516126.

ABSTRACT:

The entire organization wants to implement the same security settings they already use with their internal data/resources. It is mandatory to understand and find the data protection challenges before outsourcing data security in cloud computing. In the current study, we discuss the impact of security in cloud computing, including all the associated challenges.

KEYWORDS:

Cloud Computing, SaaS, PaaS, IaaS, Data Security

INTRODUCTION:

When implementing cloud technology [1], data security is one of the biggest concerns. Almost all organizations (which implement cloud technology) still fear for the security of their data in the cloud environment. The entire organization wants to create the same security settings they already use with their internal data/resources. It is mandatory to understand and find the data protection challenges before outsourcing data security in cloud computing.

Cloud computing brings many different data security concerns and challenges. When you use cloud computing to store the data, you have to choose or find a third-party provider and you need the internet to access the data. Therefore, we can say that data visibility and control is limited when using cloud computing. The use of cloud-based technology also raises the question of how to properly secure data.

CLOUD COMPUTING

The concept of Cloud Computing is based on online access to data or services. This can be achieved through the use of the Internet. In this concept, different ICT devices are connected to each other through different technological concepts. It is a set of components that can be used to meet the requirements of computer hardware and software on-demand services.

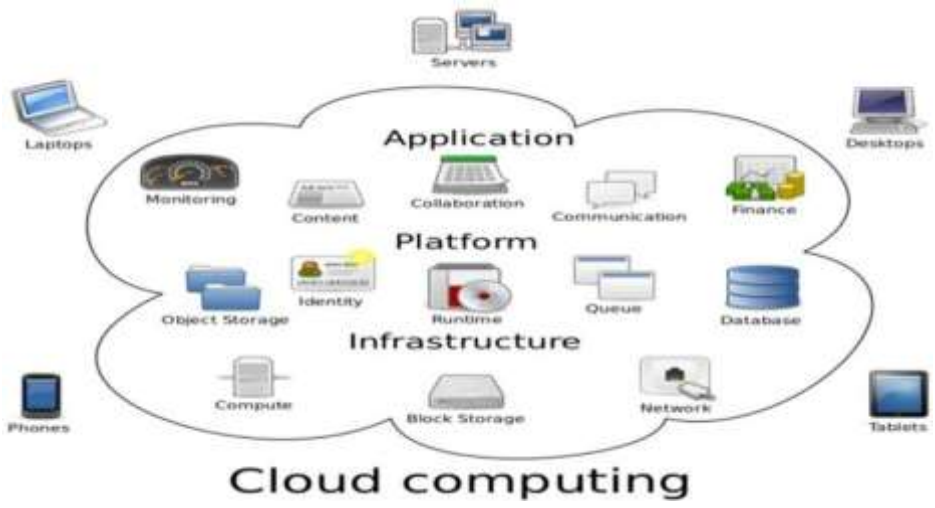


Figure 1[2]: Cloud Computing Model

The whole cloud computing architecture is divided into the following elements:

A. Cloud Computing deployment level

According to the standards defined by NIST [3], there are four cloud deployment models, but before discussing the model further, we need to define "what is a deployment model", this model specifies how cloud services are offered or made available to users. Cloud deployment models are categorized as follows.

B. Public Cloud

When public level services are used or required, a model is called a public cloud. This model is based on the concept of sharing and use or on the concept of pay as you go. Users have no control over the cloud location or infrastructure under this scheme. The cost of ownership is very low compared to other cloud models available.

C. Private Cloud

When the use of services is limited to a limited number of users, a model is called a private cloud. As the name suggests, the private cloud is designed when an infrastructure is limited to an organization. This scheme is very useful when we need a high level of data security.

D. Hybrid Cloud

This is a set of common features for both private and public cloud. This type of deployment is done when we have a private-public relationship between the user and a provider.

E. Community Cloud

This type of model is used at the organizational level. It is used by a particular community, such as a specific government department, bank, etc. This type of model is used to provide specific services to the user through a community.

F. Service Model of Cloud Computing

As we have already mentioned in connection with the deployment model (i.e. used for the deployment process), another classification of cloud computing is done under the "service model [4]" of the cloud. In this concept, we learned about the features and it also helps to categorize the users who work under cloud computing.

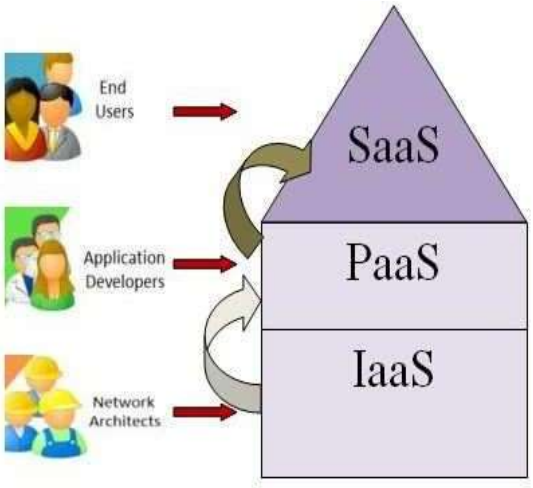


Figure 2: Service Delivery Model of Cloud

SaaS (Software as a Service)

SaaS is the first layer of cloud computing. It is also known as the interaction layer [5] of cloud computing (i.e. users can interact with the cloud through this layer). This layer offers all cloud applications on a shared basis. In general, the Internet can be used to connect SaaS to other cloud layers.

I. SECURITY CHALLENGES IN CLOUD COMPUTING

In the current scenario, data security [7] is seen as a shared responsibility in cloud computing. In accordance with the cloud service provider model, data security in the cloud is divided into two parts: the provider is responsible for the security of the cloud, while the data security issue (entered by the user) is borne by the user himself.

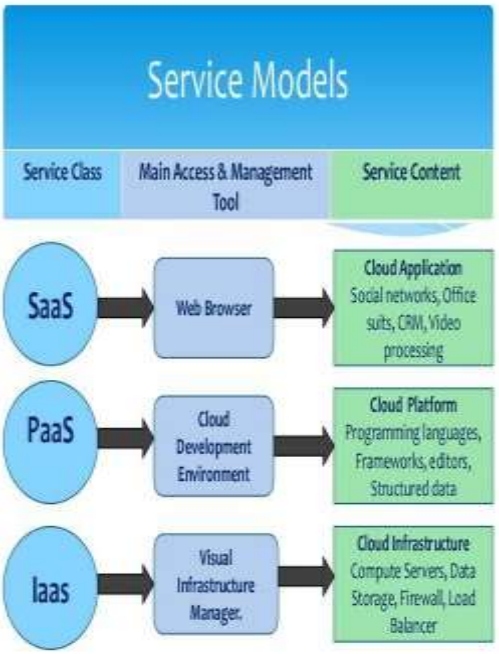


Figure 3 [6]: Service Offered Under Cloud

Data security is one of the main concerns when considering the risk associated with using or deploying cloud computing. Some of the problems associated with implementing cloud computing include lack of data visibility, poor data auditing, and many more. The next part of this research paper showed the risks or security issues in cloud computing services.

As indicated above, the entire cloud architecture is divided into SaaS, IaaS and PaaS. That's why we've discussed low-level security issues related to this, so that people get a clear understanding of security in the cloud computing model.

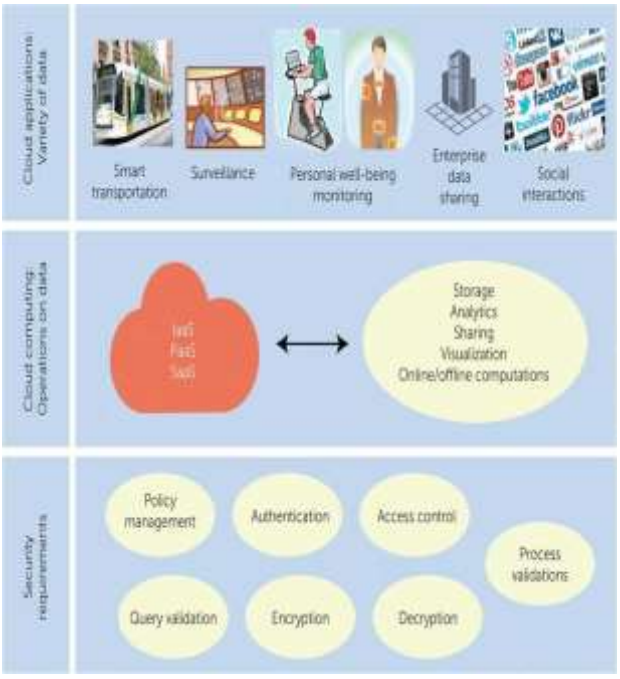


Figure 3[8]: Security Requirements of a Cloud

SECURITY ISSUES IN SAAS (SOFTWARE AS ASERVICE) LAYER

The security issues associated with the SaaS layer are almost data-centric [9]. Since it is the responsibility of the user or organizations (who would like to keep their data in the cloud) to do the authentication, such as who can access the data, what kind of security settings have been applied by the provider, etc. during or before storing the data in the cloud

Some common security vulnerabilities associated with the SaaS layer are:

- There is no visibility of user data in cloud applications
- Security vulnerability resulting from one or more malware attacks.
- Uncontrolled access to sensitive data
- No adequate monitoring of data during data transfer. Lack of IT staff skills to manage cloud security.
- Lack of previous assumptions about cloud security.
- Lack of an appropriate framework for cloud regulatory compliance.

Therefore, when considering the above concerns, it is important to consider the role of the SaaS provider in the cloud computing model. In view of the above points, it has been determined that in order to protect our organizations or corporate data, we must regularly review the security programs of our cloud service providers.

I. SECURITY ISSUES IN PAAS (PLATFORM AS ASERVICE) LAYER

The PaaS layer enables the deployment of cloud-enabled applications. In this layer we have a collection of necessary or required software for application development. Compared to the SaaS and IaaS layers, the PaaS layer relies on the security of a network and web browser used to access applications. According to the analysis of several PaaS layer [10] we find that the security of the PaaS layer is divided into two parts, namely the security of the platform itself and the security of the applications deployed on the platform. The PaaS layer provider is responsible for securing any software that is present or required while the application is running. Some of the major concerns associated with this layer are listed below:

- Security reliance on web-hosted developer tools and various third-party vendors.
- Rapid changes in PaaS applications.
- Storing data on different platforms may have a security vulnerability.

Vulnerabilities with developer tools provided by PaaS vendors.

Finally, it can be said that for securing data at the PaaS level, we need the support of external service providers.

II. SECURITY ISSUES IN IAAS LAYER

As we mentioned above about the issues and challenges of data security in the SaaS layer. Building on this, we now discuss the challenges we face when protecting data at the IaaS layer [11]. Some of the major concerns of the IaaS layer are listed below:

- No appropriate workload distribution.
- No proper control of access to sensitive data.
- Malware data theft problem.
- No suitable skills for employees who work with cloud applications.

While considering the aforementioned threats in the IaaS layer, we should also consider the recent development of malware (e.g. XcodeGhost, etc.) [12] That takes over various computer resources. This type of malicious code leads to the reuse of computing resources against the infrastructure of other organizations and vendors.

Therefore, when designing or developing the infrastructure of the cloud environment, it is very important to assess the capacity of our existing hardware. We also need to consider a number of things, such as who can

enter the information into our cloud-enabled system, needing a tracking system to identify changes or behavioral changes in our system, creating an effective security mechanism for our orchestration tools such as salt, puppet and retaliation etc.

III. TECHNIQUES OF DATA SECURITY IN CLOUD COMPUTING

Some common techniques that can be used by the provider or the user to secure our data in the cloud are as follows [13]:

- ***Firewalls***

Firewalls are central to the security of cloud-based systems.

It is used to protect our data by securing the network from intruders. It uses a function called ACL, i.e. "Access Checklist" for limited use of apps in a cloud environment.

- ***VPN's (Virtual Private Network)***

This connects our cloud or private network to other public networks to securely exchange data. Various mobile phones or tablets can also connect to our cloud system via this network. Finally, we can say that the VPN allows our private network to connect to external networks over the Internet in a safe mode.

- ***Encryption***

It is a process of encoding messages in such a way that only the authorized person has access to the message. It always denies access to an understandable content for Unauthorized user. Therefore, such a technique can be used in a cloud model so that we can secure our data from unauthorized access.

- ***Masking***

Is a message encryption process. You can use the

Message before it is sent in a network; this makes content safe and accessible.

In addition to the above, other measures [14, 15] can be taken to secure our data in cloud computing, including data storage regulations. Most countries have their own data regulations, such as storing data in their country; this allows the development of a secure data storage center. So one should always check if the country has enforced such legal laws.

IV. COMPARATIVE ANALYSIS OF CLOUD COMPUTING AND TRADITIONAL SYSTEM

Traditional System	Cloud Computing System
1) It needs purchase, installation and maintenance equipment at our own locations.	1) Access services on demand, so very economical.
2) Need more IT staff for maintenance.	2) Less IT staff is needed.
3) Need to design or develop our own infrastructure to secure content in the traditional system.	3) Cloud security can be outsourced to a recognized agency [16].
4) Making a contingency plan is not easy.	4) A disaster plan can be made easily.
5) Its not easy to use multiple encryption techniques to secure content.	5) It's easy to use multiple encryption techniques at different layers of cloud computing.
6) Only limited options are available to protect content.	6) AI-based techniques can be used to secure content.

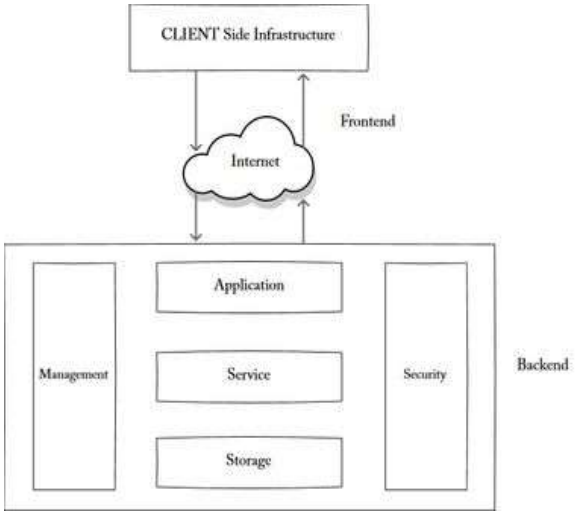
V. BENEFITS OF USING A SECURE CLOUD SYSTEM

In the above part of the article, we explored the methods by which we can secure the data [17, 14]. This helps our business model in the following ways.

- Protect our important business data from threats.
- It acts as a guard against threats to homeland security.
- And, most importantly, it prevents data loss

CLOUD COMPUTING ARCHITECTURE: OVERVIEW

Both the cloud and the user can be included under cloud computing. The majority of the time, the user is online and linked to the cloud. Additionally, a private cloud that users access to through an intranet is a possibility for a corporation. A private or public network or cloud is used in both instances, but other than that, they are identical [18]. The cloud fulfils the user's demands for services after receiving their requests.



CLOUD COMPUTING ENTITIES

The two largest groups in the commercial cloud market are cloud providers and consumers. Service brokers and resellers, however, are the two more recent additions to the cloud service level structure. Here is how they are discussed:

Cloud Providers: Includes firms that offer either the infrastructure (hosted data centres) or the media (Internet connections) that allow users to access cloud services. Also includes telecommunications providers and big business process outsourcing companies. Systems integrators are another kind of service providers. They construct and maintain the data centers that house private clouds and give customers, service brokers, and resellers with a variety of services (such as SaaS, PaaS, IaaS, and others) [19].

Cloud Service Brokers: includes industry influencers who aid in assisting customers in making decisions about cloud computing solutions, as well as technology consultants, business professional service companies, registered brokers and agents, and others. Brokers of services, who do not own or manage the entire Cloud infrastructure, focus on negotiating the partnerships between clients and suppliers. The user's Cloud environment is created by them by layering additional services on top of the infrastructure of a Cloud provider.

Cloud Resellers: When cloud providers spread their company across continents, resellers may play a significant role in the market for cloud services. As "resellers" for their cloud-based products in a certain area, cloud providers may opt for regional IT consultation companies or local distributors of their already-existing goods. Users of the cloud: End users fall under the umbrella of cloud consumers. But when they are clients of another cloud provider, broker, or reseller, cloud service brokers and resellers might also fall under this category.

RESEARCH CHALLENGES IN CLOUD COMPUTING

The issues of enabling applications and development platforms to benefit from cloud computing are addressed in cloud computing research, as well as the obstacles of meeting the requirements of the next generation of private, public, and hybrid cloud computing infrastructures. The study of cloud computing is still in its infancy. While many current problems remain unresolved, new difficulties continue to arise as a result of business applications. Below are a few of the difficult research problems in cloud computing [20, 21].

- Service Level Agreements (SLA's)
- Cloud Data Management & Security
- Data Encryption
- Migration of virtual Machines
- Interoperability
- Access Controls
- Energy Management
- Multi-tenancy
- Server Consolidation
- Reliability & Availability of Service
- Common Cloud Standards
- Platform Management

Service Level Agreements (SLA's): A lower level application may be minimized or shut down in the cloud depending on the priority system; service level agreements govern how the cloud is managed and permit several instances of one application to be duplicated over numerous servers if necessary. The evaluation of SLAs provided by cloud vendors is a significant difficulty for clients. The majority of suppliers only give their clients the barest of guarantees when they develop SLAs, which serve as a protective barrier against legal action. As a result, before entering into a contract with a provider, clients must consider a number of crucial factors, such as data protection, outages, and pricing [22]. If SLAs are specified to handle the necessary issues at the appropriate time, the needs of the customers will be more accurately reflected in the SLAs.

Cloud Data Management: Unstructured or semi-structured cloud data, which is often append-only with infrequent changes, can be exceedingly vast (for example, for text-based or scientific applications). In the field of cloud computing, cloud data management is a crucial research area. In order to ensure complete data security, service providers must rely on the infrastructure provider since they often do not have access to the physical security system of data centres. Even in the case of a virtual private cloud, the service provider is only able to remotely specify the security configuration without knowing whether it has been fully applied. In this instance, the infrastructure provider must fulfil requirements for auditability and secrecy. In order to access and transfer data securely, confidentiality is required, as is auditability, which verifies whether or not applications' security settings have been altered. While auditability can be accomplished via remote attestation methods, confidentiality is often achieved using cryptographic protocols. Directly employing remote attestation, however, is insufficient in a virtualized environment like the clouds since VMs might move about in a dynamic manner. At each architectural layer of the cloud in this situation, trust mechanisms must be developed. For the distributed processing of data-intensive activities, software frameworks like MapReduce and its many implementations, such as Hadoop, are created; these frameworks often work with Internet-scale file systems like GFS and HDFS. These file systems differ from conventional distributed file systems in terms of their application programming interface, access pattern, and storage architecture. They specifically do not implement the required POSIX interface, which creates compatibility problems with older file systems and programmes. This issue has been the subject of numerous research projects [23].

Data Encryption: A crucial tool for data security is encryption. Become familiar with data encryption both in

transit and at rest. Keep in mind that security can range from simple (easily managed, inexpensive, and, to be honest, not very secure) to very secure (very complex, expensive to manage, and quite limiting in terms of access). There are numerous options and selections for both you and the vendor of your cloud computing system to think about. For instance, does SSL encryption for access to the Web services APIs that you use to reach the cloud, either programmatically or with clients written to those APIs? This is typically thought of as a standard. The object is decrypted and stored once it has reached the cloud. Exists a way to encrypt it before.

Migration of Virtual Machines: Applications don't care about the hardware they run on; they can run on multiple machines at once or on a single machine utilising virtualization. By allowing for virtual machine migration to equalise load among the data center's servers, virtualization can offer substantial advantages in the cloud computing industry. Virtual machine migration also makes it possible for data centres to provide services that are both reliable and quick to respond. Process migration approaches have given way to virtual machine migration. Recently, VMs can be moved "live" with only tens of milliseconds to a second of downtime, thanks to the implementation of this feature by Xen and VMWare. Avoiding hotspots is a big advantage of VM migration, but it's not easy to do. The ability to quickly adapt to rapid workload fluctuations is currently lacking in workload hotspot detection and migration. Additionally, the in-memory state transfer should be efficient and consistent, taking into account both the physical servers' and apps' resource needs [24].

Interoperability: This is the capacity of two or more systems to collaborate and communicate information while also making use of that information. Numerous open public cloud networks are set up as closed systems and are not intended to communicate with one another. Organizations find it challenging to join their IT systems in the cloud and experience productivity and cost benefits since these networks are not integrated. Industry standards must be created to assist cloud service providers in designing platforms that can communicate with one another and support data portability in order to address this issue. Businesses require a single tool set that can interact with their current software and various cloud providers to automatically deploy services, manage VM instances, and integrate with both enterprise- and cloud-based applications. The requirement for cloud interoperability is present in this situation. The solution to this issue is being worked on. For instance, an industry association called the Open Grid Forum is developing a cloud platform management API called the Open Cloud Computing Interface. Cloud computing hasn't gotten any easier yet, thus this work is still difficult.

Access Controls: It is more crucial than ever to manage identification and authentication. And there aren't many differences at all. How strictly does the service provider enforce the need for frequent password changes and strong passwords? Which recovery procedure is used for account name and password? By what method are updated passwords sent to users? The ability to audit access and logs are two things to consider. If you use strong passwords that are regularly changed along with standard IT security procedures, you will be able to protect that element of access. This is not all that unlike from how you secure your internal systems and data.

Energy Resource Management: An attractive financial incentive for data center operators and a crucial step toward greater environmental sustainability is a large reduction in a cloud data center's energy consumption without compromising SLA. A 53% share of data centers' overall operational costs have been projected to go toward power and cooling. The objective is to meet environmental standards and government laws in addition to reducing energy costs in data centers. There has been a lot of focus lately on designing data centers that are energy efficient. One can tackle this issue in a number of different ways. For instance, energy-efficient hardware architecture that enables reducing CPU speeds and turning off selected hardware components has become ubiquitous. Other methods to cut down on power consumption besides turning off underutilised workstations include energy-conscious job scheduling and server consolidation. Energy-efficient network infrastructures and protocols are also being studied in recent research. Finding a proper balance between energy savings and application performance is a major problem for all of the aforementioned strategies. In this regard, a small number of academics have just lately begun to look into coordinated solutions for performance and power control in a dynamic cloud context. Companies can keep tabs on the trends of energy usage from various sources with the aid of the Global Energy Management Center (GEMC). Numerous methods that aid in energy optimization allow for further analysis of these patterns' usage, cost, and carbon impact [25].

Multi-tenancy: Internet users have access to a variety of cloud apps, from little Internet-based widgets to huge business software applications, all of which have different security needs depending on the kind of data being held on the infrastructure of the software provider. For a variety of reasons, the most crucial of which is cost, these application requests demand multi-tenancy. Response times and performance for other customers may be impacted by several users accessing the same hardware, application servers, and databases. Resources are

shared at every infrastructure tier, and there are legitimate security and performance concerns when it comes to application-layer multi-tenancy. The number of connections to an HTTP server has been reached, so the service must wait until it can use an available connection or, in the worst case, drops the service request [39]. Other examples include multiple service requests accessing resources concurrently, which lengthen wait times but not necessarily CPU time.

Server Consolidation: The server consolidation process is now being extended into the cloud, where it will boost resource utilization and reduce the amount of power and cooling needed. In a cloud computing context, consolidating servers is an efficient strategy for increasing resource usage while reducing energy consumption. VMs that are spread over several underutilized servers are frequently consolidated into one server using live VM migration technology, allowing the remaining servers to be switched to an energy-saving mode. In many cases, the vector bin packing problem, an NP-hard optimization problem, is used to represent the issue of efficiently consolidating computers in a data center. For this issue, a number of heuristics have been presented. Recently, it has also been thought about how VM dependencies, such the need for communication. Application performance shouldn't be negatively impacted by server consolidation actions. It is well known that individual VMs' resource usage—also referred to as their "footprint"—can change over time. When a VM alters its footprint on the server, the maximum amount of server consolidation may cause resource congestion for shared server resources including bandwidth, memory cache, and disc I/O. As a result, it can be crucial to monitor changes in VM footprints and use that data to consolidate servers in a useful way. Finally, when resource congestions do arise, the system needs to respond swiftly.

Reliability & Availability of Service: When a cloud provider offers software as a service that is available on demand, the problem of reliability enters the picture. In order for users to access the program under all network situations, it must have a reliability quality factor (such as during slow network connections). Due to the unpredictability of on-demand software, a few incidents have been identified. One illustration is Apple's MobileMe cloud service, which synchronizes and stores data across many devices. When many users were unable to read mail and properly synchronize data, it got off to a humiliating start**.** In order to circumvent these issues, service providers are relying on technologies like Google Gears, Adobe AIR, and Curl, some of which even enable cloud-based applications to function without a network connection. These solutions create a connection between the cloud and the user's personal computer by granting web apps access to the desktop's processing and storage resources. Reliability is still difficult to attain for an IT solution based on cloud computing due to the use of software like 3D gaming applications and video conferencing systems. [26].

Common Cloud Standards: Three key aspects, namely operations, personnel, and technology, would be covered by security-based certification for cloud computing. Prior to being certified by recognized authorities like ISO2, organisations like Jericho Forum1 are likely to be the driving force behind technical standards (International Standard Organization). For security professionals, formal accreditation is already available through the Institute for Information Security Professionals3 (IISP). There are various practical options for the operational components, like as modifying ISO 27001 and utilising it as the default measurement standard within the SAS 704 framework. One of the primary issues at the moment is that there are numerous disparate operations moving in the direction of Cloud accreditation, but there is no central organisation to coordinate such activities. Another significant challenge would be the establishment of a single accreditation authority to certify Cloud services [27].

Platform Management: There are difficulties in providing middleware capabilities for creating, deploying, integrating, and maintaining applications in multi-tenant, elastic, and scalable settings. One of the most crucial aspects of cloud platforms is that they give developers a variety of platforms to use when creating apps for the cloud, using cloud services, or doing both. The terms "on-demand platform" and "platform as a service" are two that are now used to describe this type of platform (PaaS). The potential for this novel approach to application support is enormous. A lot of what an on-premises application—one that will function inside an organization—needs already exists, so its development team may focus on other tasks. These days, everyone is talking about cloud computing, which is envisioned as the next generation of IT enterprise design. A significant shift towards the cloud might be anticipated in the upcoming years given how the cloud has been dominating the IT sector. For businesses looking for a competitive edge in today's environment, cloud computing provides substantial advantages. As more companies enter this market, prices are falling even further due to the competition. More firms will continue to embrace cloud computing due to appealing cost, the capacity to free up workers for other tasks, and the capacity to pay for services as needed. . Cloud service providers and cloud developers anticipate

that mobile cloud computing will become one of their largest markets. Despite the fact that cloud computing is a relatively recent development that is expected to alter how we use the Internet, there are many things to be wary of. Rapid technological breakthroughs are resulting in the emergence of numerous new technologies, all of which have the potential to improve human life. The security dangers and difficulties created by using these technologies must, however, be understood with great care. The same is true for cloud computing. The level of security offered by cloud service providers must be disclosed to customers. This research endeavor offers an overview of cloud computing, its components, including several cloud computing models, cloud computing entities, and cloud computing architecture. The difficulties in research that are now encountered in cloud computing were also highlighted. Future IT solutions that are safe, virtual, and financially feasible could be promoted in large part because to cloud computing. This study endeavor will help to better understand the design problems of cloud computing and pave the path for additional research in this field because cloud computing technology is still in its early stages of development.

PRIVACY CHALLENGES IN CLOUD ENVIRONMENTS

Resources are shared over the Internet, rather than on local servers, in cloud computing, a contemporary method of computing. This means that rather of using local computer hard discs to store and retrieve data, it is done via specialized Internet-based software. The term "cloud computing" refers to Internet-based computing in which various servers, storage, and applications are utilized to deliver data and reports anywhere, at any time, without having their own system. In terms of security and privacy, this section provides a synopsis of the major cloud computing challenges.

A. *Loss of control*

A major issue with cloud computing is loss of control. After uploading their data to the cloud, consumers are afraid about losing control over it. The public has access to cloud computing anywhere. Furthermore, the cloud service provider is the owner of the networks, software, hardware, and physical [28] that house the user data. Without taking into account the information being kept, every cloud user relies on the usual procedures and technical requirements. Given that cloud services function on a multi-tenancy basis, this makes cloud users concerned about their data being lost or even compromised. [28].

B. *Lack of Transparency*

Different aspects of cloud computing lack transparency, which undermines the reliability of the data that is stored. The methodology, processes, controls, and activities affecting the cloud environment are not likely to be disclosed by cloud providers [29]. A significant problem with this technology is people's inclination to communicate and leak encrypted information, such as trade secrets. The sorts of information that should be published as well as those that should remain restricted are specified by security principles [29]. One of the biggest security issues that takes longer than expected is the accessibility of stored data. Most frequently, a cloud user is ignorant of the complicated method required to access archived data, which indicates a lack of openness. To reach an agreement regarding the security of the stored data, the cloud provider is compelled to negotiate with the user. Typically, mistrust between the two parties lengthens the degrees of interaction [29].

C. *Multi-tenancy*

A cloud service or application that uses multi-tenancy architecture allows it to serve several customers from a single instance. Tenant refers to each of these customers [29]. Tenants may be allowed to alter the programmers' graphical user interface (GUI) and some portions of their business rules, but they are not allowed to alter the apps' fundamental components or source code. Remote access and virtualization technologies are used to implement multi-tenancy [29].

D. *Virtualization*

Refers to a practice whereby many applications within an environment are permitted to share massive mainframes. In order to improve security, cut costs, and increase availability and dependability, virtualization has been used at all levels of cloud computing [30]. As a result of their vulnerability to hacker exploitation, hypervisors are vulnerable to attacks. Virtual machine (VM) hijacking is a scenario where the hypervisor is deceived into having its memory overwritten, leading to complete exploitation. The attack known as "VM

hopping" enables access to the hypervisors, other VMs, and the main computer by compromising the VMs'

projections and separations. Another issue is VM Escape, in which a hacker interacts directly with the hypervisor after executing specific programmes that help get into the operating system [30]. When an attacker physically moves a VM across hosts, this is known as VM mobility.

E. *Management*

Numerous variables affect how a multi-tenant architecture and cloud platform are managed. The SLA and the kind of cloud deployment model are the primary variables. The service provider will be in charge of managing the key components of the application if the deployment strategy is public cloud [28]. The consumers' capacity to change things may be constrained. The business can engage inside staff to manage the application, however, if the cloud deployment option is a private cloud.

SOLUTIONS OF PRIVACY IN CLOUD ENVIRONMENTS

A. *Encryption Solution*

More than the architecture of the firm, cloud-based organizations must safeguard its data [31]. Using encryption techniques that are appropriate for the level of sensitivity of the data being kept in the cloud, cloud data encryption lessens the susceptibility of cloud data. Unauthorized users cannot access some types of data from the cloud because of cloud data encryption. Classified material from reputable sources is accessible to third parties [32]. Interfaces that send secured data in real-time to third-party users are a privilege. Some cloud information is protected from access by encryption, which stops unauthorized users. Reliable sources that have further simplified information management now allow third-party users access to secret material. User interfaces are made available to third-party users as a privilege.

B. *Access Control Solution*

For user authentication in cloud computing, access control systems offer security [32]. Access control systems assist in supplying data for the service provider that has been confirmed to be of a particular clearance level [33]. The elimination of data theft is made possible via access control. Data can only be transferred to and provided by authorized individuals. This makes it easier for businesses and organizations to control who has access to sensitive information [33]. Regular hacking attempts can be made against access control systems. The distinction between which service providers pose a danger is simple [34]. Significant losses could result from the loss of classified material, which could have disastrous consequences. Additionally, users cannot combine systems with pre-existing applications using cloud computing access control technologies [35]. To maximize the many advantages of cloud computing, users must consult professionals.

C. *Third Party Audit*

Data integrity can be protected and ensured through third party audit (TPA) [36]. In a cloud environment where users must sign off on any changes or additions to existing information, TPA is capable of monitoring data and information [33]. To protect the integrity of data, TPA uses encryption technologies that are supported by hardware [36]. The integrity of cloud data can be harmed by internal hacker changes to TPA software and hardware, which can modify information that has been stored.

CONCLUSION

In this article, we have described the various security vulnerabilities related to cloud computing. We also discussed that cloud computing is a new concept or the beginning of a new era that has good benefits for its subscribers. But during a study [37, 38], we learned that data security is a major concern in cloud computing, which can slow down the implementation process. After discussing the problems or challenges of the cloud based system, it is easy for an organization to monitor the implementation of the cloud system in their respective organization. Finally, we discussed the security issues at the level of each cloud computing service (SaaS, PaaS, and IaaS). The article ended by discussing solutions such as encryption, masking, VPN and firewall in cloud-enabled systems.

REFERENCES

[1] Pranathi, k, & Yellari, M. S. S. L. (2016). Data Security on Cloud Computing, International Journal of Latest Trends in Engineering and Technology (IJLTET), 7(2), 150–153

[2] https://upload.wikimedia.org/wikipedia/commons/thumb/b/b5/ Cloud_computing.svg/1200px-

Cloud_computing.svg.png

[3] Albugmi, A., & Alassafi , M. (2016). Data Security in CloudComputing. IEEE, 55–59.

[4] Shuijing, H. (2014). Data Security: the Challenges of CloudComputing. IEEE, 203–206. Doi: 10.1109

[5] Chang, V. (2016). Towards Achieving Data Security with the Cloud Computing Adoption Framework. IEEE TRANSACTIONSON SERVICES COMPUTING, 9(1), 138–151

[6] https://www.devteam.space/wp-content/ uploads /2017/07/Cloud-Models.jpg

[7] Parikh, S., & Dave, D. (2019). Security and Privacy Issues inCloud,Fog and Edge Computing. ELSEVIER, 734–739

[8] https://csdl-images.computer. org/mags/cd/2015/02 /figures/mcd20150200301.gif

[9] Ramchandra, G., & Iftikhar, M. (2017). A Comprehensive Surveyon Security in Cloud Computing. Elesvier, 465–472

[10] Savu, L. (2011). Cloud Computing. IEEE

[11] Chan,D.(2012).Data Security and Privacy Protection Issues in Cloud Computing .IEEE, 647-651.doi:10.1109 /ICCSEE.2012.193

[12] Mahalle,A.,&Yong,J.(2018).Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure.IEEE, 407-413

[13] Barhami,M. (2015).A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing.IEEE, 189-196.doi:DOI 10.1109/MobileCloud.2015.36

[14] Leloglu, E.(2013).A Review of Cloud Deployment Models for E-Learning Systems. IEEE

[15] Abbasi, A.A.et al.(2019). Software-Defined Cloud Computing:A Systematic Review on Latest Trends and Developments.Software-Defined Cloud Computing: A Systematic Review on Latest Trends and Developments, IEEE,7(1), 93294-93314.

[16] Alsenani Y. (2016).Pro Trust: A Probabilistic Trust Framework for Volunteer Cloud Computing. IEEE,4(1),1-

[17] H. Farooq, "A Review on Cloud Computing Security Using Authentication Techniques, "International Journal of Advanced Research in Computer Sciences, vol. 8,no. 2,2017.

[18] Ertaul, L. and Singhal, S. 2009. Security Challenges in Cloud Computing. California State University, East Bay. Academic paper.http://www.mcs.csueastbay.edu/~lertaul/Cloud%20Security%20CamREADY.pdf.

[19] Pring et al., —Forecast: Sizing the cloud; understanding the opportunities in cloud services,‖ Gartner Inc., Tech. Rep. G00166525, March 2009.

[20] Rabi Prasad Padhy, ManasRajanPatra and Suresh Chandra Satapathy, —Cloud Computing: Security Issues & Research Challenges‖, IJCSITS, Vol. 1-No.2, December 2011, pp. 136-146.

[21] V. Krishna Reddy, B. ThirumalRao, Dr. L.S.S. Reddy, P.SaiKiran —Research Issues in Cloud Computing — Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.

[22] Harold C. Lin, ShivnathBabu, Jeffrey S. Chase, Sujay S. Parekh, —Automated Control in Cloud Computing: Opportunities and Challenges‖, Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.

[23] X. Zhang, N. Wuwong, H. Li, and X. J. Zhang, —Information Security Risk Management Framework for the Cloud Computing Environments‖, In Proceedings of 10th IEEE International Conference on Computer and Information Technology, pp. 1328- 1334, 2010.

[24] Cong Wang, Qian Wang, KuiRen, and Wenjing Lou, —Ensuring Data Storage Security in Cloud Computing,‖ 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4.

[25] Hanqian Wu, Yi Ding, Winer, C., Li Yao, —Network Security for Virtual Machines in Cloud Computing,‖ 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010. ISBN: 978-1-4244-8567-3.

[26] V. Krishna Reddy, B. ThirumalRao, Dr. L.S.S. Reddy, P.SaiKiran —Research Issues in Cloud Computing — Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.

[27] Harold C. Lin, ShivnathBabu, Jeffrey S. Chase, Sujay S. Parekh, —Automated Control in Cloud Computing: Opportunities and Challenges‖, Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.

[28] S. Hosseinzadeh, S. Hyrynsalmi, M. Conti, and V. Leppnen, "Security and privacy in cloud computing via obfuscation and diversification: A survey," in 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), Nov 2015, pp. 529–535.

[29] A. Kumbhar, F. Koohifar,. Gven, and B. Mueller, "A survey on legacy and emerging technologies for public safety communications,"IEEE Communications Surveys Tutorials, vol. 19, no. 1, pp. 97–124, Firstquarter 2017.

[30] Y. Liu, Y. L. Sun, J. Ryoo, S. Rizvi, and A. V. Vasilakos, "A survey of security and privacy challenges in cloud computing: solutions and future directions," Journal of Computing Science and Engineering, vol. 9, no. 3, pp. 119–133, 2