A Comprehensive Overview of Privacy and Data Security for Cloud Storage

Dr. Nikhat Akhtar, Bedine Kerim, Dr. Yusuf Perwej, Anurag Tiwari, Dr. Sheeba Praveen

▶ **To cite this version:**

Dr. Nikhat Akhtar, Bedine Kerim, Dr. Yusuf Perwej, Anurag Tiwari, Dr. Sheeba Praveen. A Comprehensive Overview of Privacy and Data Security for Cloud Storage. International Journal of Scientific Research in Science Engineering and Technology, 2021, 10.32628/IJSRSET21852 . hal-03350900

HAL Id: hal-03350900
https://hal.science/hal-03350900

Submitted on 21 Sep 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET21852

A Comprehensive Overview of Privacy and Data Security for Cloud Storage

Dr. Nikhat Akhtar*[1], Dr. Bedine Kerim[2], Dr. Yusuf Perwej[3], Dr. Anurag Tiwari[4], Dr. Sheeba Praveen[5]

[1*]Assistant Professor, Department of Computer Science & Engineering, Babu Banarasi Das Northern India Institute of Technology (BBDNIIT), Lucknow, Uttar Pradesh, India

[2]Assistant Professor, Department of Computer Science, Faculty of Computer Science & IT, Al Baha Universit, Baha, KSA

[3]Associate Professor, Department of Computer Science & Engineering, India

[4]Associate Professor, Department of Information Technology, Babu Banarasi Das National Institute of Technology and Management (BBDNITM), Lucknow, Uttar Pradesh, India

[5]Assistant Professor, Department of Computer Science & Engineering, Integral University, Lucknow, Uttar Pradesh, India

Article Info
Volume 8, Issue 5
Page Number: 113-152

Publication Issue:
September-October-2021

Article History
Accepted: 08 Sep 2021
Published: 18 Sep 2021

ABSTRACT

People used to carry their documents about on CDs only a few years ago. Many people have recently turned to memory sticks. Cloud computing, in this case, refers to the capacity to access and edit data stored on remote servers from any Internet-connected platform. Cloud computing is a self-service Internet infrastructure that allows people to access computing resources at any location worldwide. The world has altered as a result of cloud computing. Cloud computing can be thought of as a new computing typology that can provide on-demand services at a low cost. By increasing the capacity and flexibility of data storage and providing scalable compute and processing power that fits the dynamic data requirements, cloud computing has aided the advancement of IT to higher heights. In the field of information technology, privacy and data security have long been a serious concern. It becomes more severe in the cloud computing environment because data is stored in multiple locations, often across the globe. Users' primary challenges regarding the cloud technology revolve around data security and privacy. We conduct a thorough assessment of the literature on data security and privacy issues, data encryption technologies, and related countermeasures in cloud storage systems in this study. Ubiquitous network connectivity, location-independent resource pooling, quick resource flexibility, usage-based pricing, and risk transference are all features of cloud computing.

Keywords: Cloud Computing, Data Security, Artificial Intelligence as a Service (AIaaS), Cloud Storage, Data Access Control, Data Privacy.

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

I. INTRODUCTION

Today scenario, big data [1] is now rapidly developing in all research and engineering areas, including physical, Medical Internet of Things (MIoT) [2], biological, and biomedical sciences, due to the rapid expansion of networking, data storage, and data collection capacity. The rate of data production has grown significantly in recent years. Many organizations are looking for cost-effective ways to store and analyses large amounts of data generated by a variety of sources, including high-throughput equipment, sensors, and connected devices. Big data [3] technologies can take advantage of cloud computing [4] to deliver major benefits, such as the capability to build, connect, configure, and reconfigure virtualized resources on demand with automated tools. Cloud computing is a new paradigm that is altering how institutions, businesses, organizations, and individuals see and use various software systems [5]. Organizations that use cloud-based solutions don't have to host their software or manage their own servers [6]. The cloud computing is made up of hardware and software resources that are made available as managed external services over the internet.

Advanced software applications and high-end server computer networks are used to provide these services. With the rapid expansion of computer, storage, and communication technology, the cloud computing [7] is a new computing model that may give users with programmable and shared resources. Cloud computing [8] providers link a huge number of nodes and network devices [9] to create one or more big data centers. Then they offer infrastructure, platform, storage, and software services, all of which are centered on data centers. The most well-known technology in the world is cloud computing. It offers a variety of services to its customers, and cloud storage is one of the most important aspects of cloud computing [10]. To store data in the cloud network, we can use cloud storage. As a result, the cloud will require sufficient storage space as well as sufficient speed to load data simultaneously. The cloud era is arrived! It's a game-changing invention that combines public, private, and business process outsourcing capabilities. Scalability, elasticity, and flexibility are all advantages of cloud-based services. User groups and cloud service providers alike are concerned about data security and privacy [11] in cloud computing. In the context of cloud computing, sensitive information covers data from a wide range of various fields and specialties [12]. As a result of the recent growth of new cloud technologies, privacy and data protection requirements have evolved to safeguard individuals against monitoring and database exposure. The study on data security and privacy in cloud computing systems is summarized in this publication.

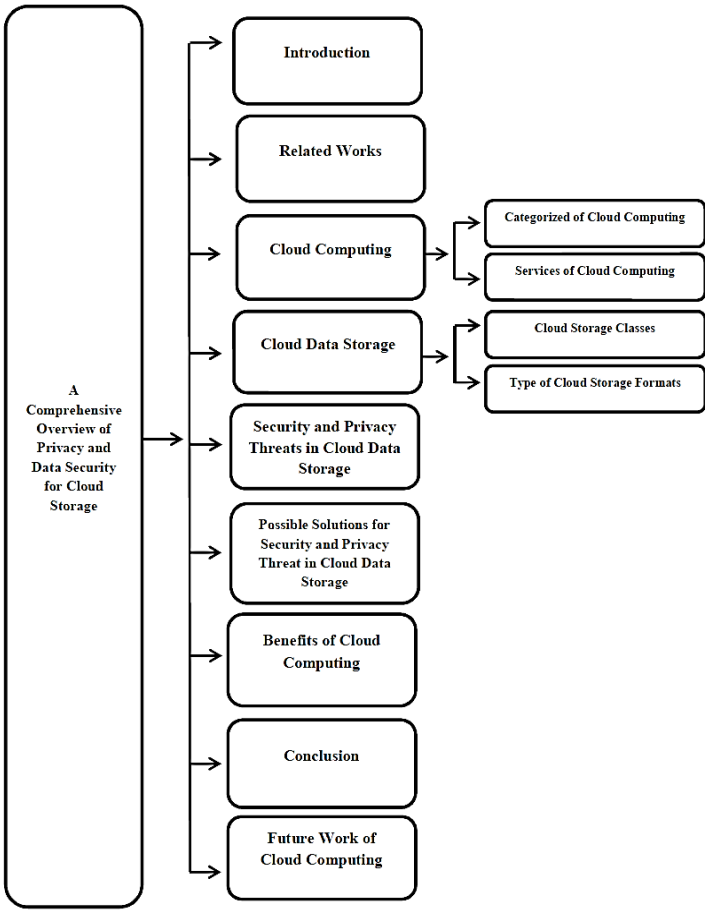

Figure 1 The Organization of Research Paper Framework

The remaining sections of this work are organized as follows. The related works is presented in section II. We describe the cloud computing in section III cloud data storage in section IV. In section V, we present the security and privacy threats in cloud data storage. We are widely discussing the possible solutions for security and privacy threat in cloud data storage in section VI. We present benefits of cloud computing in sections VII. We conclude this paper in section VIII. In section IX, we present future work of cloud computing. This paper gives an organizational framework in figure 1 to clearly depict the general structure.

II. RELATED WORKS

Any hosted service offered over the internet is referred to as cloud computing. Servers, databases, software, analytics, and other computing tasks that may be operated over the cloud are frequently included in these services [13]. The act of operating workloads within clouds is known as cloud computing. IT settings in which scalable resources are abstracted, pooled, and shared across networks.

In recent years, cloud computing privacy and security issues have been a popular topic [14]. Data privacy, data protection, data availability, data location, and secure transmission are the most pressing concerns in cloud data security. Threats, data loss, service disruption, outside malicious assaults, and multi-tenancy difficulties are among the security challenges in the cloud [15]. Users of this technology outsource their data to a cloud provider's server located outside of their premises [16]. Memory, processor, bandwidth, and storage are also visible and accessible via the Internet by a client. By focusing on privacy protection, data segregation, and cloud security, Chen et al. [17] investigated privacy and data security challenges in cloud computing. Data security issues are primarily at SPI (SaaS, PaaS, and IaaS) level and the major challenge in cloud computing is data sharing.

This paradigm shift that comes with cloud computing usage is increasingly causing security and privacy concerns about aspects of cloud computing such multi-tenancy, trust, loss of control, and accountability [18]. Before consumers and businesses use cloud computing, users' security concerns must be addressed in order for the cloud environment to be trusted. The trustworthy environment is the basic prerequisite to win confidence of users to adopt such a technology. The assessment of cloud computing hazards was examined by Latif et al. [19]. In other research, cloud infrastructures are combined with unique services aimed at specific businesses. To put it another way, the cloud is designed to provide specific services to clients, such as cloud computing for manufacturing or cloud computing for health care [20].

Shynu et al. [21] explored several ways of secret communication, such as the secret channel, side channel attack, and fuzzy technology, addressed secret communication technology in relation to application situations, and demonstrated its benefits and drawbacks. Lo'ai et al. [22] presented a mobile cloud computing concept that may be applied to a wide range of applications. The proposed architecture can be used to store and analyse data collected by various sensors and IoT devices. In restricted circumstances, the obtained data will be transferred to the mobile [23] cloud model for analysis and making the best decision possible. Johanna et al. [24] looked into a variety of covert communication technologies, including hidden channels, bypass, and fuzzy technology. These approaches, on the other hand, are a type of non-mainstream technology and application, with a very limited application scope. Cloud storage is similar to cloud computing in terms of accessible interfaces, scalability, and measurement resources because it is based on virtualization

infrastructure. It consists of four layers [25], cloud storage supplies data access services including data storage, data computation, authentication, and access control. Due to the characteristics of cloud storage, data security and privacy issues are inevitably generated in this process.

Furthermore, the cloud provides the required administration and control capabilities to support (regulatory) governance [26] rules while also meeting the needs of multinational corporations [27]. Zhang et al. [28] provided a technical review of four SE systems, including searchable symmetric encryption (SSE), public key encryption with keyword search (PEK), attribute-based encryption with keyword search (ABK), and proxy re-encryption (PRES). Several SE technologies, including searchable symmetric encryption (SSE), public key encryption keyword search (PEKS), attribute-based encryption keyword search (ABKS), and proxy re-encryption keyword search, were summarised by Zhang et al [29]. (PRES).

They just provided a technical description of the searchable encryption paradigm, with no relevant algorithms or performance comparison studies. Yusuf Perwej et al. [30] in this paper highlight the main Hadoop security, technological viewpoint and analysis that may affect big data. Moreover, big data [31] can be advantageous as a base for the development of the future technologies that will transform the world as we see it, like the cloud computing, Internet of Things (IoT) [32], or on-demand services, and Blockchain [33]. Edemacu et al. [34] examined and analysed the security, revocation ability, and efficiency of various attribute-based cooperative electronic health encryption methods. The privacy protection technology mentioned in this study, on the other hand, is relatively simple. Yusuf Perwej and colleagues take a quick look at the technical components of IoT security. Because when only two instruments were combined in the field of medical care, security was a major concern [35]. Tara et. al [36] investigated several security service methods based on Blockchain, such as authentication, confidentiality, access control list, resource sources and integrity assurance, and discussed the challenges of security services.

A Blockchain [37] controller, cloud server, and authentication server (AS) are used to establish a cloud-based software defined network (SDN). To obtain the secret key, researchers recommend that all users register with the AS [38]. Nikhat Akhtar at. al. [39] presents a comprehensive literature review of recent contributions focused on the Medical Internet of Things (MIoT). Medical Internet of Things-based healthcare services are expected to improve the user's quality of life, lower prices using clouds. In this publication, Jeffrey and colleagues [40] investigate the effectiveness of deep learning algorithms based on Recurrent Neural Networks (RNNs) [41] for identifying malware in cloud Virtual Machines (VMs). We concentrate on two key RNN architectures: LSTMs (Long Short-Term Memory RNNs) [42] and Bidirectional RNNs (Bidirectional RNNs) (BIDIs). Based on run-time fine-grained processes system metrics like as CPU, memory, and disk use, these models learn the behavior of malware over time. Bader et al. [43] conduct a thorough literature review to assess existing research on cloud computing security, dangers, and problems. This systematic literature review examined the research studies published between 2010 and 2020 within the popular digital libraries.

III. Cloud Computing

This section delves deeper into cloud computing. The Internet of Things (IoT) [44], or the interconnection of people, devices, and "things," is growing as the number of information detecting devices connected to the Internet grows. The cloud service provider platform [45] generates and hosts an unprecedented volume of data. Many applications and services will be hosted in the cloud due to the cloud's high performance, scalability, and reliability. The word

"cloud," often known as "cloud computing," refers to any type of remote data storage solution [46] shown in figure 2. To be clear, your data is saved on remote servers and may be accessed via the Internet, rather than on your hard discs or local memories. You can rent rather than buy your IT using cloud computing. Companies prefer to access their compute capacity over the internet [47], or the cloud, and pay for it as they use it, rather than investing extensively in databases, software, and hardware. Servers, storage, databases, networking, software, analytics, and business intelligence are now among the cloud services available. Cloud computing enables businesses to develop, innovate, and support business IT solutions with the speed, scalability, and flexibility that they require. There has been a substantial growth in cloud computing usage over the last several years as firms increasingly [48] appreciate the cost savings, easy scalability, and work flexibility afforded by cloud. The global market for cloud-based services is expected to grow to $436 billion by 2024, up from $326 billion in 2020, with over 64 percent of businesses [49] adopting the cloud in some way. Cloud computing saves businesses money on both hardware and software upkeep. By ensuring that our data is always available, an internet cloud architecture improves organization productivity and efficiency.

Figure 2 The Cloud Computing

3.1 Categorized of Cloud Computing

Several kinds of cloud computing models have emerged as the cloud has evolved. Public cloud, edge cloud, private cloud, multi cloud, hybrid cloud, distributed cloud, and community cloud are the different types of cloud computing deployments. Each form necessitates a different level of client control and offers varying levels of protection and privacy [50].

3.1.1 Public Cloud

In a public cloud, the cloud provider's whole computing infrastructure is housed on its premises, while the customer receives services via the internet. Customers don't have to worry about maintaining their own IT, and they can easily add more users or computer power as needed. Multiple tenants share the cloud provider's IT infrastructure in this scenario. Typically, the public cloud is highly [51] segregated to prevent cloud service overlap among different enterprises and to ensure each business's privacy and security. The public cloud's scalability is one of its

most appealing features. Furthermore, most public clouds operate on a pay-as-you-go basis, meaning that users only pay for the cloud services that they use.

3.1.2 Edge Cloud

To lower processing costs and provide more low-latency experiences for consumers, edge clouds decentralize computing power to clients and devices at the network edge. Edge cloud [52] will be a one-of-a-kind ecosystem of open and interconnected data centers, with data center operators and carrier alliances allowing it to reach critical mass Depending on the QoE objectives and resource requirements for a given application, the edge cloud can be located in any number of network locations. The location of the Edge cloud will vary depending on the perspective of an end-user, network operator, or application provider.

3.1.3 Private Cloud

A private cloud is a cloud that is only used by one company. It could be hosted on the organization's premises or in the data center of the cloud provider [53]. The maximum level of protection and control is provided by a private cloud. This private cloud is exclusively available to customers of a single firm or group of companies, and the [51] organization has the freedom to build the private cloud to meet its specific needs. Administrative control, privacy, and security are all advantages of private clouds for business owners. Private clouds are often surrounded by high-security firewalls, with only approved users permitted access. For businesses that deal with sensitive information or that have strict regulatory requirements, using a private cloud enables them to easily make any configuration modifications that are relevant to their line of business.

3.1.4 Multi Cloud

Enterprises are attempting to de-risk themselves by putting various workloads in different clouds, hence a multi cloud strategy is the preferred model nowadays. The usage of multiple cloud computing and storage [54] devices in a single architecture distinguishes hybrid cloud from multi cloud. Some organizations also prefer multiple clouds, as each cloud may offer a different technology capability. Businesses may personalize and compartmentalize their cloud network with multi cloud.

3.1.5 Hybrid Cloud

Hybrid clouds, as the name implies, are a mix of public and private clouds meant to work together seamlessly, transferring services and applications from one to the other. Hybrid cloud customers typically host business-critical apps on their own servers for increased protection and control, while storing secondary applications at the cloud [55] provider's location. With hybrid clouds, business owners can simply scale up their network infrastructure by leveraging the public cloud while keeping their data privacy, security, and access control in the private cloud. The hybrid cloud model is also preferable for hosting workloads that must meet compliance or data security standards.

3.1.6 Distributed Cloud

Distributed cloud is a public cloud computing service that allows you to run public cloud infrastructure in multiple locations, including on premises, in the data centers of other cloud providers, and in third-party data centers or co-location centers, all while managing everything from a single control plane. According to a current trend, Gartner defines distributed cloud as the distribution of public cloud services to different physical locations, but the original public cloud provider is responsible for the

services' operation, governance, updates, and evolution [56]. Distributed cloud speeds up worldwide service communication while also allowing for more responsive communications for any given region. Distributed cloud computing provides repeatability and dependability, as well as geo-replication, which helps to save costs while also providing instantaneous fail-overs via remote replicas that may be reset in the event of a failure. Distributed cloud allows breaking complex problems and data into smaller pieces and has multiple computers which can be worked upon in parallel.

3.1.7 Community Cloud

A community cloud allows a group of multiple organizations to access systems and services in order to communicate information between the organization and a specific community. The goal of this concept is to allow numerous customers to collaborate on community-owned projects and apps when a centralized cloud infrastructure is required. In other words, Community Cloud is a distributed infrastructure that integrates the services given by many types of cloud solutions to answer the specific concerns of business sectors. With hybrid clouds, business owners can simply scale up their network infrastructure by leveraging the public cloud while keeping their data privacy, security, and access control in the private cloud. The hybrid cloud model is also preferable for hosting workloads that must meet compliance or data security standards. Because of the exclusive user group, organizations do not have to be concerned about the security problems associated with public cloud. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them. The community cloud is scalable and versatile since it is generally compatible with all users and may be modified to suit their needs.

3.2 Services of Cloud Computing

Cloud services are now available to satisfy almost any IT requirement. It's more about finding the proper solution to suit your business and personal needs than there is a one-size-fits-all strategy to cloud. Each service model represents a different component of the cloud stack with its own set of responsibilities for you and the service provider [58].

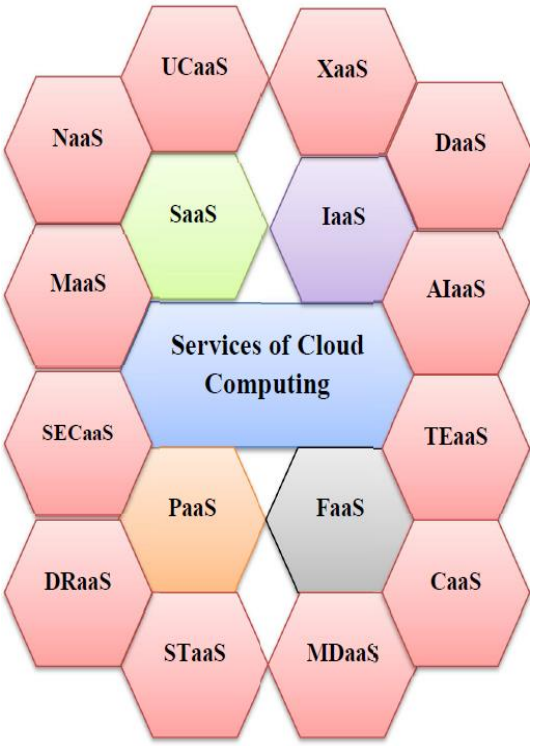

Figure 3 Types of Cloud Computing Service Models

Infrastructure, platforms, and software that are hosted by third-party providers and made available to consumers via the internet are known as cloud services. Although there's great variety among cloud services, all such services have certain basic features and benefits in common, and all can be categorized into a few basic cloud service types shown in figure 3.

3.2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is the service paradigm that your cloud technology deployment is built on. You can get on-demand access to essential IT

resources like computers, networking, and storage through an IaaS provider [59]. IaaS gives you access to a scalable, state-of-the-art hardware resource that can be scaled to match your company's processing and storage requirements. We're using this infrastructure to provide your company's applications, software, and platforms while relieving you of the burden of administering and supporting them.

3.2.2 Everything as a Service (XaaS)

The X in Xaas serves as a variable in the same way as it does in mathematics. As a result, this word might mean "Anything as a Service" or "Everything as a Service." The name XaaS stands for "everything as a Service," and it refers to a wide range of products, tools, and technology that are becoming increasingly popular as a service offering [60]. XaaS is frequently chosen by businesses because the as-a-service approach can reduce costs and simplify IT implementations. With every additional cloud service, an organization can shed pieces of its in-house IT infrastructure, leading to fewer servers, hard drives, network switches, software deployments and more. The primary financial advantage of employing the XaaS model is that it saves money. The Internet of Things (IoT) [61] is another cornerstone of many businesses that need to function online, and XaaS is a major contributing factor to how well this works for you, too.

3.2.3 Unified Communications as a Service (UCaaS)

In light of recent developments, unified communications as a service (UCaaS) has gotten a lot of attention. Unified communications as a service (UCaaS) is a cloud-based solution paradigm for all of a company's communication needs. This will typically combine tools like email, video conferencing, instant messaging and more into a fully-mobile suite that can be accessed from any device. UCaaS (Unified Communications as a Service) is a technology that uses cloud-based services to streamline enterprise communications. Through a partnership with a united communications organization, UCaaS provides collaboration features such as instant messaging, video conferencing, file sharing, and more. Businesses can save a significant amount of money by using UCaaS.

3.2.4 Software as a Service (SaaS)

SaaS (Software as a Service) is a cloud service paradigm that gives you access to a fully functional software product that is run and managed by the service provider. The majority of SaaS solutions are end-user applications. The customer uses the internet to access those applications. Rather than purchasing and maintaining their own computing infrastructure, [62] SaaS customers opt for a pay-as-you-go subscription to the service. SaaS is the best choice for many businesses since it allows them to get up and running quickly with the most cutting-edge technology available. A web-based customer relationship management (CRM) solution is a frequent SaaS example. We are store and manage all your contacts via CRM [63] without having to upgrade the software to the latest version or maintaining the server and operation system the software is running on.

3.2.5 Storage as a service (STaaS)

Storage as a Service (STaaS) allows businesses to consume storage as needed. Instead of purchasing and maintaining storage infrastructure, this service allows businesses to add, delete, or adjust storage requirements as needed, and only pay for the storage that is used. Enterprises, small and medium organisations, home offices, and individuals can use the cloud for multimedia storage, data repositories, data backup and recovery, and disaster recovery with STaaS. There are other higher-tier managed services that build on STaaS, such as database as a service,

which allows you to write data into tables hosted by CSP resources.

3.2.6 Platform as a Service (PaaS)

Platform as a Service (PaaS) is a cloud service model in which you use a service provider to access a combination of hardware and software tools. The most prevalent usage of PaaS is for application development. Customers can use the PaaS to get the developer tools they need to build and manage mobile and web applications without having to invest in [64] or maintain the underlying infrastructure. The infrastructure and middleware components are hosted by the provider, and the consumer uses a web browser to access them. PaaS solutions must have ready-to-use programming components that enable developers to include new features into their apps, such as artificial intelligence (AI) [65], chatbots, Blockchain [66], and the Internet of Things (IoT) [67]. The right PaaS offering also should include solutions for analysts, end users, and professional IT administrators, including big data analytics [68], content management, database management, systems management, and security.

3.2.7 Security as a Service (SECaaS)

The Security as a Service (SECaaS) is a service given by a managed security services provider that allows businesses to free up security resources by having the service provider take full responsibility for security. Because it enables secure access to apps and services regardless of where they are hosted or when users connect, security as a service has become a key business enabler in the increasingly cloud and mobile world. SECaaS solutions can be scaled up or down as required and are provided on demand where and when you need them. That means you won't have to worry about deployment or updates because everything is handled by your SECaaS provider and accessible via a web-based dashboard. Data loss prevention, antivirus management, spam filtering, network security, identity management, and other services may be included.

3.2.8 Functions as a Service (FaaS)

Before we can comprehend Functions as a Service, we must first comprehend the most commonly used technical word for FaaS server less computing. Server less computing [69] is a cloud computing approach in which developers are relieved of low-level infrastructure decisions and server maintenance. The allocation of resources is handled by the cloud service provider, so the application architect does not have to worry about it. FaaS is a new cloud computing service that is transforming many industries. It's a server-less computing idea that allows software developers to create apps and distribute particular "functions," pieces of business logic, or actions without the need for a server. It increases the efficiency as developers need not to consider server operations because they are hosted externally. Examples of FaaS include Google Cloud Function, Microsoft Azure Functions, Webtask.io, Iron.io, Open Whisk, and AWS Lambda.

3.2.9 Test environment as a Service (TEaaS)

The test environment as a service paradigm, which is an on-demand test environment, allows businesses to test their software or apps using only a web browser. Clients save money on the deployment of test infrastructure for testing, as well as the tools needed for testing and maintenance. Clients benefit from TEaaS since it reduces the costs of physical infrastructure, testing tools, IT support staff maintenance, testing resources, and so on. Concerns concerning cyber security in a cloud-based test environment, on the other hand, are a major impediment to the worldwide test environment as a service market's growth.

3.2.10 Communication as a Service (CaaS)

The "Communications" is represented by the C in CaaS. This means we'll use a single vendor to handle all of your communication needs. This cover, among other things, phone over IP, instant messaging, collaboration, and video conferencing. The supplier is in charge of all hardware and software administration in this situation. They usually charge on an on-demand basis so you'll always only pay for what you need. This means that this model is flexible and will grow as your need for communication grows.

3.2.11 Artificial Intelligence as a Service (AIaaS)

Artificial intelligence as a service (AIaaS) is a third-party AI outsourcing service. AIaaS refers to AI platforms that allow businesses to implement and grow AI approaches for a fraction of the expense of a full-fledged AI department [70]. The term "service" in AIaaS refers not only to the cloud-based software delivery model, but also to the extent to which the vendor is involved in the process. The nine yards of AI [71] are delivered as a unified platform by IT companies delivering AIaaS, from problem conceptualization to keeping the model on track and expanding to new use cases, through constructing the model, deploying the solution in production, and sustaining it in real-world settings. AI cloud offerings including Amazon Machine Learning, Microsoft Cognitive Services and Google Cloud Machine Learning [72] can help organizations what might be possible with their data. AIaaS solutions also provide more scalability, flexibility, and also use.

3.2.12 Desktop as a Service (DaaS)

Desktop as a Service (DaaS) is a sort of offering that provides virtual desktops to end customers. It is extremely popular in the remote working environment. Virtual desktops promise robust security, as all information is stored on the server, and not on individual machines or laptops. The service provider is responsible for all data management, backup, and storage [73]. DaaS runs across a range of operating systems and device kinds, which promotes the trend of employees bringing their own devices to work and relieves the cloud service provider of the responsibility of supporting the desktop on all of those devices. Desktop as a Service (DaaS) has a number of distinct advantages over the traditional desktop paradigm. Deploying or decommissioning active end users with DaaS is much faster and less expensive.

3.2.13 Network-as-a-Service (NaaS)

Network-as-a-Service enables us to gain direct and secure access to network infrastructure. Custom routing protocols can be deployed using NaaS. To provide network services to customers, NaaS employs virtualized network infrastructure. The network resources must be maintained and managed by the NaaS provider. Having a provider work for a customer reduces the customer's workload. Furthermore, NaaS provides network as a service. NaaS is also based on pay-per-use model.

3.2.14 Disaster Recovery as a Service (DRaaS)

Disaster recovery as a service, or DRaaS, is the replication of physical or virtual servers hosted by a third party to offer failover in the case of a man-made or natural disaster. DRaaS can be especially useful to organizations that lack the necessary expertise to provision, configure, and test an effective disaster recovery plan. The goal of DRaaS is to achieve a quick recovery point [74]. This means that the data will be restored as closely as feasible to its current "now" state. Typical recuperation time goals are 4 hours or less, and equipment that are geographically located in a different place will be brought up. Third parties bear complete responsibility for disaster recovery under the managed DRaaS paradigm. Choosing this

option requires organizations to work closely with DRaaS providers to keep all infrastructure, application, and service changes up to date. If you don't have the expertise and time to manage your own disaster recovery, this is the best option.

3.2.15 Monitoring as a Service (MaaS)

Monitoring as a Service (MaaS) is a security service that protects a company's IT assets 24 hours a day, seven days a week. It is critical in protecting an organization's or government's clientele from cyber threats. It is a framework that facilitates the deployment of monitoring functionalities for various other services and applications within the cloud. MaaS is an outsourced monitoring service with a flexible and consumption-based [75] subscription model. However, in order to monitor effectively and efficiently, the business needs have up-to-date equipment, professionals with extensive technical capabilities, and scalable security processes, all of which come at a significant cost. Online state monitoring is the most typical MaaS application, networks, systems, which continuously monitors particular states of apps, instances, or any other element that can be deployed in the cloud.

3.2.16 Model as a Service (MDaaS)

A Model as a Service (MDaaS) is a service that allows you to run simulation models. The MDaaS is primarily concerned with the application of a model to data. The model can be pre-deployed, has a well-known service endpoint, and extra data services may be available. This is a regular occurrence in operational models used in a production setting. Before execution, this model can be dynamically deployed from the client. Such behavior is required for the development of model services for research purposes. Both approaches cater to a distinct workflow, as well as the requirements for availability and security. Web services are used as the client's communication interface in MDaaS. Data is exchanged as structured text, such as XML or JSON (JavaScript Object Notation) in a specified syntax. However, data may also be passed to the service in the model's native format.

IV. Cloud Data Storage

Cloud storage is a cloud computing approach in which data is stored on the Internet and managed and operated by a cloud computing provider. It's on-demand, with just-in-time capacity and costs, and it saves you money by not having to buy and manage your own data storage infrastructure. Cloud computing integrates the concepts of [76] grid computing, distribution, and utility computing, among others, to create a vast pool of shared virtual resources by connecting a large number of computers, storage, and software resources. Cloud data storage is a type of data storage that involves sending data over the Internet and storing it on remote systems that may span several servers and locations. Cloud storage can be offered by a service provider, installed on-premises in a company's own data center, or a hybrid of the two. Large data centers are maintained by cloud service providers in numerous locations across the world. Depending on the extent of the cloud provider's operation, the server with which you connect sends your data [78] to a pool of computers situated in one or more data centers. Using a cloud service provider's infrastructure to securely store your data, apps, and workloads is known as cloud storage. Users that want to adopt cloud computing are concerned about data security and privacy. This technology needs proper security principles and mechanisms to eliminate users concerns.

4.1 Cloud Storage Classes

The concept of cloud storage is similar to that of data storage. Information is saved in logical pools in cloud storage, whereas physical storage necessitates a large number of computers and, in certain cases, many

locations. Unmanaged cloud storage and managed cloud storage are the two primary categories in which cloud storage may be found. The storage [79] is preconfigured for the customer in unmanaged cloud storage. The consumer is unable to format, install his own file system, or change the properties of his hard drive. Managed cloud storage provides on-demand internet storage capacity. The managed cloud storage system appears to the user to be a raw disk that the user can partition and format.

4.2 Type of Cloud Storage Formats

Cloud storage employs a logical memory paradigm, which enables providers to store your data on several servers in various regions while being completely transparent to you. People may now upload all personal data stored on their mobile phones to their cloud storage accounts with a single click using specialized software available for various OS versions. Dropbox and Google Drive are two examples of popular cloud storage options. The three most common forms of cloud storage formats are block storage, object storage, and file storage.

4.2.1 Block Storage

Block storage, which is commonly used in SANs, is also widely used in cloud storage settings. Data is grouped into big volumes called "blocks" in this storage model. Each block corresponds to a different hard drive. Cloud storage providers use blocks to split large amounts of data among multiple storage nodes. Block storage is quick, efficient, and delivers the low latency that database and high-performance workloads require [80]. Block storage, when used in the cloud, grows effortlessly to meet the development of your company's databases and applications. If your website collects a lot of visitor data that has to be saved, block storage can be a good option. The primary disadvantages of block storage are its lack of metadata, which limits organizational flexibility, and its higher price and complexity.

4.2.2 Object Storage

Object storage is distinct from file and block storage in that data is managed as objects. The data in a file, its accompanying metadata, and an identifier are all included in each object. Objects save data in the format in which it is received and allow metadata to be customised in ways that make the data easier to access and analyse. An object storage protocol uses the RESTful API to store a file and its associated metadata as a single object and assign it an ID number. The user gives the ID to the system to retrieve content, and the content is assembled with full information, authentication, and security. Objects are stored in repositories that provide almost infinite scalability, rather than being structured in [81] files or folder hierarchies. Object storage helps you to optimise storage resources in a cost-effective manner because there is no filing hierarchy and the metadata is customisable. The object storage protocol is used by all backup apps, which is one of the reasons why online backup to a cloud service was the first successful cloud storage application. The main disadvantage of object storage is that data cannot be modified segment by segment. Only the whole object can be changed, which has an impact on performance. We need to restore the object, add a new row, and write the entire object back into the object storage system. As a result, this type of storage is unsuitable for applications with frequent data changes.

4.2.3 File Storage

The file storage method preserves data in a hierarchical file and folder structure that is familiar to most of us. It is often used with network attached storage and personal computer storage discs (NAS). Regardless of whether the data is stored in the storage

system or on the client, the hierarchy makes it easier and more natural to search and retrieve files when needed [82]. Development platforms, home folders, and repositories for video, audio, and other data all need file storage. The primary disadvantages of file storage, if we plan for your data to grow, there is a certain point at which the hierarchy and permissions will become complex enough to slow the system significantly.

V. Security and Privacy Threats in Cloud Data Storage

Today, the cloud makes software, platforms, infrastructure, and storage more flexible and economical for businesses of all sizes. In this part, we'll discuss the security and privacy risks associated with cloud data storage. Security and privacy are broad topics in cloud computing. In comparison to traditional systems, the cloud has novel security requirements [83]. Because the consumer no longer owns the infrastructure, traditional security architecture is broken. When data is kept on a remote server, users lose physical control over it [84], and they delegate that control to an untrustworthy cloud provider or party. Because cloud computing is made up of numerous technologies, such as databases, operating systems, different networks, transaction management, [85] virtualization, it poses a number of security risks. As a result, security concerns about these systems and applications apply to the cloud computing as well. Privacy is a complex topic that has different interpretations depending on contexts, cultures and communities, and it has been recognized as a fundamental human right by the United Nations [86]. Other difficult challenges in cloud computing security include the formulation of a legal definition for cybercrime, the issue of jurisdiction (who is liable for what information and where are they held responsible for it), and the regulation of data transfers to third nations. Access control, user authentication, and data encryption [87] are all standard security features offered by most cloud storage providers. This means that there are significant security and privacy problems that must be considered by all parties involved in the cloud computing arena while employing cloud computing. Cloud computing has a number of problems. The following are the issues that need to be addressed.

5.1 Handle Access for Remote Work

One of the most appealing features of cloud applications is that they can be accessed from any device with an internet connection. However, more apps mean more URLs and passwords to maintain and support, and the rise of mobile devices adds yet another access point to handle. IT departments must facilitate access across multiple devices and platforms without compromising security.

5.2 Privacy of Cloud Data

The data on the cloud is distributed all over the world. The user has no knowledge of the location of data and has no control over the physical access mechanisms to that data. Many countries, cultures, and jurisdictions have vastly different ideas about privacy. When an investigation happens, there is also the issue of whose jurisdiction the data belongs under. There are several databases and applications in a distributed system. Governments [26] should have at least a rudimentary policy in place to deal with such circumstances.

5.3 Administrative Entrance

Administrative access in cloud computing is done over the internet, which raises the danger. It is very important to control administrative access to data and monitor the access to maintain protocols.

5.4 Access Control

Data security must be given extra attention when data is outsourced to the cloud, which is untrustworthy since it is in a domain where security is not regulated by the data owner. When more than one entity wants to exchange data, a method must be in place to limit who has access to that data. The literature [88] has discussed a variety of strategies. Those techniques were proposed to keep data content confidential and keep unauthorized entity from accessing and disclosing the data by using access control while permitting many authorized entities to share those data.

5.5 Data Breaches

A data breach happens when an unauthorized person or group of persons accesses protected, secure, sensitive, or confidential data. Users and organizations in a cloud environment all have access to the same data. Any breach of this [89] cloud environment would open the door to all users' and businesses' data. The attacker's primary aim is usually not the user, although the user is ultimately affected. Because of multi-tenancy, customers using different applications on virtual machines could share the same database and any corruption event that happens to it is going to affect others sharing the same database [90].

5.6 Cloud Data Control and Loss of Transparency

Consumers are ignorant of the data loss that is out of their control due to the cloud service provider's storage of data. The user's access to confidential data stored in the cloud could be compromised [91]. The user has no idea where, how, or when the data is handled due to a lack of transparency. To fix this issue, the user must understand what happens to the data. Cloud service providers are technically able to do data mining as well as data abstraction need techniques to analyse user data. As a result, customers can store and analyze data on the cloud with the help of a cloud service provider. The lack of transparency might also result in the loss of a significant amount of data.

5.7 Service Hijacking

Phishing, fraud, and software exploitation flaws are the most common ways to steal an account's credentials and passwords, and they still work. Credentials and passwords can be reused, which increases the impact of such assaults. All the transactions achieve network traffic between user and cloud service provider. When an attacker acquires access to a user's credentials, he can listen in on the user's transactions and personal information [92].

5.8 Denial of Service

Because of the crucial services they provide, certain businesses require their systems to be available at all times. The cloud services provider makes resources available to a large number of clients. If an attacker uses all available resources, others cannot use those resources, which leads to denial of service and could slow accessing those resources. Customers that use cloud services and are victimized by the botnet could also seek to disrupt the availability of other providers.

5.9 Transmission of Data

Data is transmitted from one location to another in a cloud system. Although encryption is used to protect data during transmission, most data is not encrypted during processing, and it must be unencrypted in order to be processed for any purpose. An attacker can find a place between communication paths. The attacker can change the communication.

5.10 Lack of Trust and Dependence on Cloud Provider

The availability of cloud services is a key issue. Due to a shortage of funds, the cloud service provider has ceased to provide services, and users may experience difficulties accessing their data. Some widely used cloud service provider, for instance Google Drive does not provide any contract between the user and cloud service provider.

5.11 APIs and Storage Gateways

To help them migrate their data to the cloud, several businesses employ cloud storage APIs or storage gateways. Between the [93] user and the storage provider, these products serve as a go-between. They may make it easier for your employees to access and manage data in your cloud, but an insecure API or gateway could endanger your data. If you want or need to utilize a storage API or gateway, ensure sure it has a good reputation for security.

5.12 Sharing of Data

The utilisation of data is rising as a result of data sharing. The data owners can grant one party access to the data, and that party can then share the data with others. This sharing can lead to major issues, such as data leaks to an unauthorized people. Therefore, during the data sharing especially when shared with a third party, the data owners need to consider whether the third party continues to maintain the original protection measures and usage restriction.

5.13 Destruction of Data

When data is no longer needed, it is expected to be totally deleted. The data destroyed may still persist and be restored due to the physical features of the storage medium. This could lead to the disclosure of sensitive information.

5.14 Keeping Application Integrations Up to Date

Enterprise cloud apps of today are built on cutting-edge, internet-optimized architectures. Vendors can design their services and accompanying interfaces using the contemporary web technologies that underpin these apps. Unfortunately for the IT professionals, that also means that every new vendor may require a new approach when it comes to integration, particularly concerning user authentication and management.

5.15 Data Location

Cloud providers have a slew of data centres strewn over the globe. Users of cloud computing need to know where their data is stored, hence data location is a problem. Depending on the jurisdiction, some countries compel corporations to retain their data in their country. Also, there are regulations in some countries where the company can store their data. Also, the data location matters when the user data is stored in a location that is prone to wars and disasters.

5.16 Latency

Traffic congestion can cause delays in data transmission to and from the cloud, especially when using shared public internet connections. Companies, on the other hand, can reduce latency by increasing connection bandwidth.

5.17 Distributed Denial of Service (DDoS) Attacks

DDoS attacks aren't new, but they can be particularly debilitating when directed against our company's public cloud. DDoS attacks have a significant impact on the availability and security of key infrastructure in the cloud [94]. This form of assault can be crippling, causing systems to slow down or shut down. DDoS attacks also consume significant amounts

of processing power a bill that the cloud customer (you) will have to pay.

5.18 Multi Tenancy

The term “multi-tenancy” refers to the sharing of physical equipment and virtualized resources among numerous users. An attacker could be on the same physical machine as the target if this arrangement is used. Multi-tenancy characteristics are used by cloud providers to create infrastructures that can easily scale to meet customers' needs; nevertheless, because resources are shared, it may be easier for an attacker to obtain access to the target's data.

5.19 Virtual Machine Rollback

Rolling back a virtual computer to its earlier state is a process. This procedure has additional security risks because it gives the user more flexibility. For example, a virtual machine could be rolled back to a previous vulnerable state that has not been repaired [95] or to an out-dated security policy or old configuration. In another example, a user could be deactivated in a previous state but still have access when the virtual machine's owner rolls back.

5.20 Denial of Service (DoS) Attacks

Denials of service assaults are an old approach in the internet world, but they still pose a concern. Before operations are clogged by hundreds of thousands or millions of automated requests for service, they must be discovered and screened out. However, attackers have devised increasingly sophisticated and dispersed methods of carrying out the attack, making it more difficult to distinguish between malicious actors and legitimate users in a modern-day botnet attack. For cloud customers, "experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock: there's no way to get to your destination, and nothing you can do about it except sit and wait," according to the report [96]. When a denial of service assault is launched against a client's cloud service, the service may be harmed rather than shut down, in which case the customer will be billed by his cloud service for any resources utilized during the attack. Cloud computing, on the other hand, has increased their popularity [97]. These assaults consume a lot of computing power and slow down cloud availability. The worst part is that there's nothing you can do but sit and wait once it happens.

5.21 Regulatory Compliance

Certain industries, such as healthcare and finance, have to comply with strict data privacy and archival regulations, which may prevent companies from using cloud storage for certain types of files, such as medical and investment records. Choose a cloud storage provider that enables compliance with any industry rules that affect your business if at all possible.

5.22 Loss of Control

Another potential security breach that can occur when customers' data, apps, and resources are housed on the cloud provider's premises is loss of control. As the users do not have explicit control over their data, this makes it possible for cloud providers to perform data mining over the users’ data, which can lead to security issues. Furthermore, because cloud providers store data in multiple data centers, customers cannot be certain that their data is truly deleted when they remove it. This could lead to data being misused that hasn't been removed. In these types of situations where the consumers lose control over their data, they see the cloud provider as a black-box where they cannot directly monitor the resources transparently.

5.23 Cryptojacking

Cryptojacking is a sort of cyber-attack in which a hacker uses a target's processing capacity to mine crypto money on his or her own behalf. Individual customers, large institutions, and even industrial control systems can all be targets of cryptojacking. Cryptojacking virus slows down infected machines since the mining process takes precedence over other legitimate tasks [98]. Cryptojacking has become a serious global problem, with cybercriminals gaining unauthorized entry to computer systems to make money with minimal risk and effort. Hackers are inventing new techniques to steal computer resources and mine for crypto currency, which is known as cryptojacking.

5.24 Accidental Exposure of Credentials

In their phishing attempts, phishers frequently leverage cloud apps and environments as a pretext. Employees have become accustomed to receiving emails with links that may ask them to confirm their account credentials before gaining access to a particular document or website, thanks to the growing use of cloud-based email (G-Suite, Microsoft 365, etc.) and document sharing services (Google Drive, Dropbox, OneDrive). This makes it easy for cybercriminals to learn an employee's credentials for cloud services. As a result, 46 percent of firms are concerned about unintentional exposure of cloud credentials, which could endanger the privacy and security of their cloud-based data and other resources.

5.25 Trust Chain in Clouds

By ensuring on cloud providers, trust plays a key function in recruiting more customers. Cloud users rely on cloud providers to employ trust mechanisms as an alternative to offering them visible control over their data and cloud resources due to a loss of control. As a result, cloud providers genuine trust in their clients by ensuring them that their operations are certified to meet organizational safeguards and standards.

5.26 Cross Virtual Machine (VM) Side-Channel Attacks

The attacker must be in a different virtual computer on the same physical hardware as the victim to carry out this attack. The attacker and the victim are both using the same CPU and cache in this attack. When the attacker switches the virtual machine execution of the victim, the attacker can learn about the victim's behaviour. An example of a virtual machine side-channel attack and how an attacker can deduce information about a victim can be found here. The timing side channel attack is one kind of virtual machine side channel attacks. This attack is based on calculating how long certain computations take. This attack has the potential to leak sensitive information, such as the identity of the person performing the calculation or information from the cloud provider itself. Due to privacy concerns, the owner of the virtual machine can check other [99] virtual machines, making this attack difficult to detect.

5.27 Misconfigured Cloud Storage

For cybercriminals, cloud storage is a valuable supply of stolen data. Despite the high stakes, businesses continue to make the error of misconfiguring cloud storage, which has resulted in significant losses for many businesses. According to a report by Symantec, nearly 70 million records were stolen or leaked in 2018 due to misconfigured cloud storage buckets. The survey also noted the advent of a number of technologies that allow attackers to discover and target misconfigured cloud storage. Cloud storage misconfiguration can quickly escalate into a major cloud security breach for an organization and its customers.

5.28 Snooping

Without security precautions in place, files in the cloud are among the most vulnerable to being hacked. The fact that they are saved and transmitted across the internet adds to the danger. Snooping in network security compromises the privacy of a variety of data that should be kept private on a computer network.

5.29 Lack of Backup Services

One of the most common concerns about storage systems is that they lack automatic backup capabilities. They expect you to back up the data you put in the cloud instead. This problem does not affect all storage providers; in fact, some will automatically backup your data for you. Those that do not provide backups, on the other hand, do not provide a safety net in the event of a sudden data loss.

5.30 Weak Authentication and Identity Management

Data breaches in businesses are caused by a lack of adequate authentication and identity management. Businesses sometimes struggle with identity management because they try to assign access to each user based on their job function [100]. Enterprise cyber-security might be endangered by poor identity management. For example, cyber-criminals gained access to 80 million records containing personal and medical information as a result of the Anthem Inc. data breach. Anthem had neglected to implement multi-factor authentications hence this vulnerability was the result of stolen user credentials.

5.31 Trojan Horse

A Trojan horse is a programme that appears to be useful but is actually destructive to the host PC. A dangerous payload is concealed in some areas of this sort of malware that can exploit or damage the host system. Trojan horses can also be spyware because of their malicious actions such as the unauthorized collection of a user's data.

5.32 Data Breaches

A data breach occurs when sensitive, protected, or confidential information is copied, communicated, viewed, stolen, or exploited by someone who is not allowed to do so. As a result of the huge data held in the clouds, cloud providers are an attractive target for hackers. The severity of the attack is determined by the confidentiality of the information that will be disclosed. If the disclosed material is personal, such as health information, trade secrets, or intellectual property of a person or an organisation, the damage will be serious [101]. This will result in significant harm.

5.33 Synchronization Mechanisms Issues

In cloud storage SaaS deployments, synchronisation methods are widespread. When files are modified on a local device [102], such technologies allow updates to be propagated to all other devices that are interested in those files. Tokens are commonly used to implement these procedures, which have been found to introduce new vulnerabilities that can lead to data exfiltration. An example of attack exploiting such [103] vulnerability is the Man in the Cloud (MitC) attack. Because of its propagation properties, this type of attack can be carried out on both an IoT device and a Cloud platform, allowing it to be used against other IoT [104] devices that use the same implementation.

5.34 Abuse of Cloud Services

One of the most significant advantages of cloud computing is that it gives even tiny businesses access to massive amounts of processing power. Purchasing and maintaining tens of thousands of servers would be prohibitively expensive for most businesses, but

renting time on tens of thousands of servers from a cloud computing provider is far cheaper. Not everyone, however, wants to put this power to good use. An attacker could take a year to crack an encryption key using his own constrained gear, but he could crack it in minutes utilising a network of cloud computers.

5.35 Shared Technology Vulnerabilities

Cloud computing enables the sharing of infrastructure, platform, and software to provide services. Different components such as CPUs and GPUs, on the other hand, may not be able to meet cloud security criteria such as absolute isolation. Furthermore, certain apps may be created without the use of trusted computing standards [106], resulting in shared technology dangers that can be exploited in a variety of ways. Attackers have utilised shared technological weaknesses to launch cloud attacks in recent years. One such attack is gaining access to the hypervisor to run malicious code, get unauthorized access to the cloud resources, virtual machines, and custom subscriber data.

VI. Possible Solutions for Security and Privacy Threat in Cloud Data Storage

Many new technologies are rapidly emerging, each with technological improvements and the promise to make people's lives easier. Although cloud computing provides numerous benefits, there are still many [106] security and privacy issues. As a result, it is critical to understand the security and privacy risks associated with using these technologies. Data security [107] and privacy concerns are the biggest roadblocks to cloud computing are rapid growth. It's reasonable to be concerned about the security of your data when it's stored in the cloud infrastructure. After all, your documents, images, and videos are saved on servers that you do not control. You might be wondering if these servers are vulnerable to cyber criminals [108]. The security and privacy of cloud storage is a critical problem, especially if your company handles sensitive data such as corporate data, credit card information, and medical records, among other things. However, if you wish to store information virtually, we must consider the added risk that your information may be accessible to other potentially people who you do not wish to have access. Subscribers to the cloud want reassurance that their data is protected from cyber threats using the most up-to-date ways [109]. Layered security and privacy solutions for the cloud subscriber will be required, including endpoint protection, content and email filtering, and threat analysis, as well as best practices such as regular updates and patches. We require clear access and authentication policies, as well as privacy policies. In this section, a number of techniques have been proposed by in this paper for data protection and to attain highest level of data security and privacy in the cloud storage [110].

6.1 Consistent Security Updates

How frequently do you ignore the prompts to upgrade your operating system, browser, or email client? In the area of computer security, that's a no-no. Such upgrades frequently include capabilities to defend your devices from the most recent viruses and malware. When you save your data on the cloud, however, the companies in charge of the servers should keep their security procedures up to date. We won't have to worry about forgetting to run an update. Your cloud service provider's security measures will be updated on a regular basis.

6.2 Encryption Mechanisms

These mechanisms are responsible for implementing the encryption technique that is used to conceal or obfuscate data. The majority use on key-based algorithms, which employ either a shared key or a public & private key combination. Tokenization, on the other hand, is a method of replacing anonymous

data tokens with specified token fields. This approach is widely used in business applications such as CRM and other business apps. Data can now be encrypted in the database and only decrypted when utilised with an approved application and allowed user credentials, according to most database software. Another option is to utilise encryption appliances, which encrypt data as it leaves a private network and decode it when accessed by a trusted user. The encryption we use must be compatible with the capabilities of the application we're using and the cloud service provider we're utilising. Different mechanisms may have a considerable impact on the user experience, so the impact on end-user performance must also be addressed.

6.3 Formal Change Control Process

The cloud is fast and secure for time-sensitive data if enterprises have a formal control process modification. If the organisation does not have a proper change process control in place during routine upgrades, the servers will fall down and no one will be able to access the data. And if the data is time sensitive than this cloud which do not have formal change process control, they are not safe for tie sensitive data. Organizations that execute changes and setup in a specially appointed way will probably encounter huge downtime in their condition. Lack of foresight and a lack of progress management are the primary causes of system outages. If the data you're sending to the cloud is time-sensitive, we'll need to work with a vendor who follows a structured change management process, avoiding the inherent risk of unplanned modifications.

6.4 Attribute Based Encryption

For the first time, Sahai et al. presented fuzzy identity-based encryption [111], which is the origin of attribute-based encryption (ABE). In contrast to identity-based encryption, attribute-based encryption replaces identity with a set of attributes, and only users whose attribute set fits the access policy can access the encrypted material. The ABE algorithm is divided into four sections. The setup phase, also known as the system initialization phase, is where relevant security parameters are entered and associated public parameters (PK) and master keys (MK) are generated. The data owner provides their own attributes to the system in the second phase of the KeyGen step, namely the key generation stage, to acquire the private key associated with the attributes. The data owner encrypts the data using his or her public key, obtains the cypher text (CT), and delivers it to the receiver or to the public cloud in the third part encryption phase. In the last part decryption phase, decryption users get cipher text, decryption with their own private key SK. In data sharing applications, attribute-based encryption promises to give fine-grained access control over encrypted files, allowing the data owner to select who can access the protected data.

6.5 Access Control in Cloud Computing

In cloud computing, access control is a critical security method for ensuring data security. It ensures that only authorised users have access to the cloud-based data they've requested. In cloud computing, there are a variety of security techniques that allow for adequate access management. On separate network and cloud tiers, intrusion detection systems, firewalls, and responsibility separation could be deployed. Only restricted content is allowed to enter over the cloud network due to the firewall. Typically, a firewall is configured according to the user's established security policies.

6.6 Homomorphic Encryption

Encryption is commonly used to protect data secrecy. Rivest et al. [112] devised a type of encryption system called homomorphic encryption. It assures that the

results of the cypher text algebraic operation are compatible with the clear operation following encryption results, and it also eliminates the necessity to decrypt the data throughout the procedure. The application of this technology has the potential to solve the problem of data and data operations secrecy in the cloud. Gentry et. al. firstly proposed the fully homomorphic encryption method [113], which can do any operation that can be performed in clear text without decrypting. It's a significant step forward in homomorphic encryption technology. In figure 4 shown, the easier for us to understand how homomorphic encryption works in cloud. The data owner protects the data and sends it to the cloud server using homomorphic encryption. With the associated private keys, authorised users can decrypt the cypher text. User 2 just needs to send the functions corresponding to the operations to the cloud server if he wants to do certain specific operations on cypher text. The servers get operand and perform the operation without decrypt the cipher text and return the encrypted result to user second. Homomorphic encryption effectively protects the security of outsourced data.

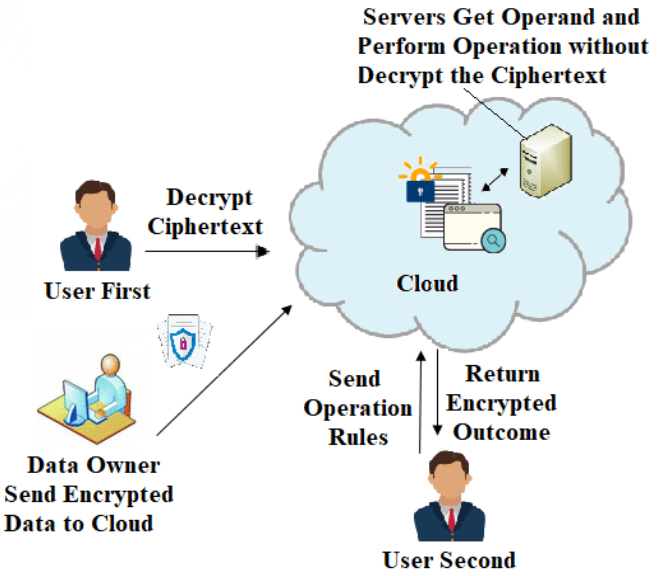

Figure 4 Homomorphic Encryption

6.7 Secure Data Destruction

When data must be destroyed, it must be done safely. The hazards of data leaking are present if data destruction is not safeguarded. When data is not securely destroyed, anyone can retrieve it. If you store classified and sensitive data on the cloud and the vendor fails to properly destroy data from defunct equipment, the data is put at risk unnecessarily. A data deletion service's purpose is to fully obliterate sensitive or critical data. Third-party or proprietary software is used to make it possible. After the process, it is expected that data can no longer be recovered and used for any unauthorised or fraudulent purposes.

6.8 Multi-Authority Attribute Based Encryption (MA-ABE)

The figure 5 shows how many attributes are managed by distinct authorities. Each attribute creates an encrypted private key to prevent the authority centre from stealing it [114]. To ensure proper decryption, each policy authority has a master key. The total keys of the attribute authority are equivalent to the system's master key [115].

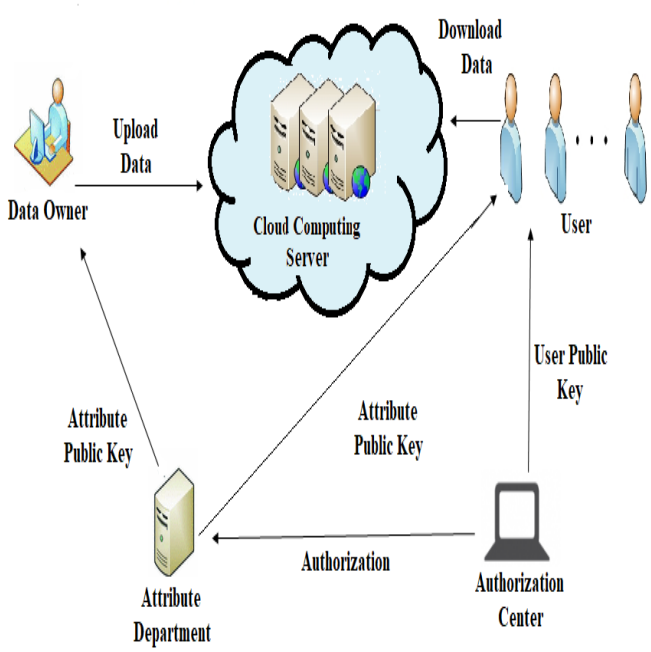

Figure 5 Multi-Authority Attribute Based Encryption

Different colluding users can recover the master key, putting the system's security at risk. As a result, the contradiction between the system's correctness and security is a tough problem in ABE research. Because the central authority (CA) guarantees the operation of decryption, the research of multi-authority is divided into two categories first ABE with CA and second ABE without CA. In the standard model, Liu et al. [116] built a new multi-privilege cypher text strategy ABE scheme for cloud storage data access control system, which was shown to be self-adaptive and secure, and supported monotonous access strategy.

6.9 Encrypted Search and Database

For the privacy and security of sensitive data in an untrusted cloud environment, an in-memory database encryption solution is proposed [117]. In order to gain access to the data, a synchronizer exists between the owner and the client. To decode the encrypted shared data, it receives from the owner, the client would need a key from the synchronizer. The synchronizer is used to keep track of the associated shared data as well as the keys. For cloud databases, Huang et al. [118] presented an asymmetric encryption technique. Commutative encryption is employed on data several times in the proposed process, and the order of public/private keys used for encryption/decryption is irrelevant.

6.10 AI Tools and Auto Patching

Artificial intelligence, or AI, is also being used by cloud providers to help protect your data. This is critical, yet finding skilled security personnel to supervise data is difficult. Cloud providers, on the other hand, can use artificial intelligence to handle at least the initial level of security assessments. Built-in algorithms are used by these tools to look for and identify potential security flaws.

6.11 Encryption of Backups

Data backups in the cloud must be encrypted; otherwise, data encryption is worthless if the backups are not encrypted. If these backups are not safeguarded with adequate encryptions, any hacker can gain access to them. Data is not secure if backups are not encrypted. A reinforcement that hasn't been tested is a useless reinforcement. In the generation condition, a decoded reinforcement overcomes the security measures. Data should be protected throughout its entire existence.

6.12 Built-in firewalls

Firewalls are used by cloud providers to protect your files as well. This technology works in the same way as a wall, keeping your data safe. Firewalls, which can be either hardware or software-based, apply rules to all network traffic. These rules are intended to filter out potentially harmful traffic and keep your data safe behind the firewall. This makes it more difficult for hackers to slip malware or viruses past the security measures used by your cloud service provider.

6.13 Hierarchical Attribute Set Based Encryption (HASBE)

Each user or data owner is maintained by a domain authority, which combines the properties of attribute set based encryption (ASBE) and hierarchical identity-based encryption (HIBE). The system can have five types of participants: the first is the data owner, the second is the user, the third is the domain authority, the fourth is the parent and trusted authority, and the fifth is the cloud service provider. To build the hierarchy of system users, the scheme employs the delegation algorithm. Rachel et. al. [119] proposed a hierarchical encryption based on attribute set, which extended the user hierarchy to ASBE. This system inherited flexibility and fine-grained access control in enabling composite attributes, as well as

scalability of hierarchical structure. Wan et al. [120] proposed the HASBE system, which expanded attribute set encryption based on a user hierarchical structure's cypher text strategy while inheriting ASBE's fine-grained access control. Data owners and service providers are rarely in the same trusted domain in cloud computing. Further, [121] proposed a secure and efficient cloud computing data collaboration scheme based on hierarchical attribute encryption. This approach provided partial decryption structure and produced partial signatures by outsourcing signature calculation when users decrypted cypher text. A hierarchical attribute-set-based encryption was proposed by Gokuldev et al. [122]. This system inherited not just the scalability of a hierarchical structure, but also the flexibility and fine-grained access control that ASBE composite attributes require.

6.14 Redundancy (ultra-backed-up data)

What if there's a hardware breakdown or a power outage? Will you be able to access your data in the event of a natural disaster or a large-scale outage at your cloud provider. Because the majority of the world's largest cloud providers use redundancy. This means that they copy your data several times and store them on many different data centers. You can access your files from a backup server if one machine breaks down.

6.15 Hybrid Technique

For data secrecy and integrity, a hybrid solution [123] is presented, which combines key sharing and authentication techniques. Using strong key sharing and authentication mechanisms, the user's connection to the cloud service provider can be made more secure. RSA public key algorithm can be used for secure distribution of the keys between the user and cloud service providers. A three-layered data security method is offered [124]. The first tier ensures the cloud user's authenticity through one-factor or two-factor authentications, the second layer encrypts the user's data for security and privacy, and the third layer ensures quick data recovery through a fast decryption procedure.

6.16 Written Security Policies Plan

The security of the data will be guaranteed if the cloud service provider has a written security plan of policies. If the cloud service provider does not have a written security plan of policies, the cloud is not safe and the security of the data cannot be guaranteed because they do not have a written plan of security policies. This indicates that they are working on a data security programme. Organizations that have not formalized their security strategies cannot be trusted with your touchy corporate/ client information. Strategies shape the system and establishment and without security is just an idea in retrospect

6.17 Ranked Keyword Search

Ranked keyword search refers to the system's feedback returns sorted by relevant parameters such keyword frequency, which improves the system's applicability and meets the real-world need for privacy protection in cloud computing. To safeguard privacy, Sun et al. [125] suggested a multi-keyword search technique based on similarity ranking. Based on cosine similarity, this approach developed a search index based on word frequency, and the vector space model can gain improved search result precision. A cypher text keyword ranking search technique was proposed by Cao et al. [126]. They use "coordinate matching" and "inner product similarity" to quantify the similarity, according to safe inner product computation. Wang et al. [127] suggested a ranked search symmetric encryption (RSSE) system with little information leakage. This technique also created a novel encryption primitive that employed one-to-

many mappings to safeguard privacy and verify search results in order to search the encrypted file set. A multi keyword ranked search technique was developed to capture the correlation between data documents and search queries by creating a coordinate matching mechanism [128]. In addition, the scheme used the inner product similarity to quantitatively evaluate the related similarity measure.

6.18 Proper Usage of Administrative Privileges

Administrative powers should be limited in cloud computing organisations, and administrative accounts should only be used when absolutely necessary. All administrator accounts should be inventoried using automated techniques, and each user with administrative access on laptops, desktops, and servers should be authorised by a senior executive. All administrator passwords should be complicated, containing a combination of digits, letters, and special characters, and should not contain dictionary words [129]. Before introducing any new devices in the networked systems, all default passwords for operating systems, applications, firewalls, routers, wireless access points, and other systems should be changed. Passwords for service accounts should be changed on a regular basis and should be long and difficult to guess. Passwords should be encrypted or hashed before being stored. Hashed passwords should follow the guidance supplied in NIST SP 800-132 or similar guidance. Administrator must use unique and different passwords for their administrative and non-administrative accounts. This objective can be accomplished by enforcing policies and increasing user knowledge.

6.19 Data Concealment

Data hiding could potentially be utilised in the cloud to maintain data secrecy. Delettre et al. [130] proposed a database security concealing concept. Data concealing techniques combine genuine data with visual false data to distort the volume of the real data. Authorized users, on the other hand, can quickly distinguish between bogus and authentic data. Data concealing techniques boost the overall volume of genuine data while improving the security of personal information. The goal of data hiding is to protect sensitive information from harmful users and attackers. Watermarking [131] can be used as a key to unlock the real data. Only the authorized users have key of watermarking, so the authentication of users is the key to ensure the true data to be accessible for right users.

6.20 Key Management Strategy

This refers to the way you manage your encryption keys. There are already a number of cloud services that provide key management solutions, many of which are part of a broader cloud service suite. The drawback with these options is that you're still giving someone else power over your data. An approach that keeps the keys under your organization's control, either through a key management solution or an encryption appliance, may provide better risk mitigation, especially in jurisdictions that have strict data localization laws.

6.21 Multi-Tenant

The core of cloud computing is virtualization technology, which paved the way for multi-tenant cloud computing. Multi-tenant software is frequently installed on the same physical host, which might cause problems for other users, such as channel attacks. Because the virtual machine can be dynamically transferred based on performance and requirements, and access permissions can be changed, ensuring privacy protection is critical. Landuyt et al. [132] suggested a multi-tenant and flexible access control strategy that ensured strong data isolation for businesses in cloud stores. It can turn an employee into an unauthorised user with no access to others

and ensure that cloud data is properly isolated Ngo et al. [133] developed a new multi-tenant access control approach based on the safety obligation separation principle. CSP may manage the security issues of cloud tenants such as addition, deletion, and management under this approach. Gonzales et. al. [134] proposed a service-oriented multi-tenant access control model that can meet the requirements of the users and automatic generate related roles in the cloud environment.

6.22 Strategies for Secure Transition to the Cloud

Protecting what matters is the most important aspect of data security. Solutions that allow businesses to reliably migrate to the cloud while retaining most of their existing infrastructure and investments provide considerable benefits. By securing data inside the operating environment while setting security policies and keeping control through a centralized management interface, vormetric data security addresses the enterprise cloud security conundrum. Vormetric collaborates with cloud providers and businesses to protect data, regardless of whether it's [135] stored in physical, virtual, or cloud environments. Organizations can establish access policies and achieve complete control of data in private, public, or hybrid cloud environments. Only vormetric provides a complete platform for protecting both local data within the internal environment and cloud-based data within infrastructure or hosted application sites when moving to the cloud [136]. The combination of structured and unstructured data protection, as well as fine-grained user and process access controls that guard against unauthorized access to protected data. Because it is installed atop the file system and logical storage volume levels, the vormetric data security transparently secures data without needing application or database redesign or recoding,[137]and is transparent to users, applications, and cloud storage. In IaaS environments such as Amazon EC2, IBM Smart Cloud, Savvis, Rackspace, etc., enterprises can spin up instances to encrypt structured and unstructured data without rearchitecting or recoding applications.

6.23 Third-Party Security Testing

Outside security organizations should be hired by the cloud provider to test their servers and software on a regular basis to ensure that they are safe from hackers, cybercriminals, and the newest malware and viruses. This outside testing boosts the odds that your cloud provider will have the defenses needed to keep your files away from hackers.

6.24 Reliability of Hard-Drive

In the cloud environment, hard drives are now the most used storage medium. The core of cloud storage is the reliability of hard discs. Pinheiro et al. investigated the error rate of hard drives using historical hard-drive data [138]. They discovered that hard-drive error rates are not significantly related to temperature or frequency of usage, and that hard-drive error rates have strong clustering characteristics.

6.25 Encrypt Your Data

To begin, ensure sure your files are sent to a cloud service provider that encrypts data. We aim to make it as difficult for hackers to access your information as possible. The storing your images and files with a provider that relies on encryption will give hackers pause. They have an easier time stealing data that hasn't been scrambled.

6.26 Service Abuse

Attackers can utilise the cloud service to obtain extra data or ruin the interests of other users by abusing it. Other users may misuse user information. In cloud storage, de-duplication technology is extensively employed, which means that the same data is

frequently kept once but shared by several users [139]. This reduces storage space and lowers cloud service provider costs, but attackers who know the hash code of the stored files can access the data. The sensitive data could then be leaked on the cloud. So, proof of ownership approach has been proposed to check the authentication of cloud users. Idziorek et. al. proposed this question and researched on the detection and identification of fraud resource consumption [140].

6.27 Perform Data Backups

Ensure that you only engage with cloud service providers who back up your data. We don't want all of your data to be stored on a single server. If that server goes offline, you won't be able to access your data. Even if you save your most sensitive data in the cloud, you should consider backing it up on your own external hard drives. This will provide you with an extra layer of protection should something happen with your cloud provider.

6.28 Access to Data

Enterprise data must only be accessed and viewed by administrators, not by users. This access will improve the security of data stored in the cloud. Although many cloud apps are designed to facilitate client collaboration, free programming trials and join opportunities make cloud administrations accessible to unscrupulous clients. DoS attacks, email spam, computerised click extortion, and pilfered content are only a few of the actual assault types that can ride in on a download or sign in.

6.29 Enable Two Factor Authentication

When you log onto a website using two-factor authentication, you must submit two pieces of information. Let's pretend we're logging into your bank's website. We begin by providing your login and password, as is customary. We next wait for your bank to issue you a code by email or phone. To gain access to your accounts, we are entering this code into the system. Hackers will have a harder time gaining access to your emails, personal information, or financial information if you take this extra step.

6.30 Deploy Multi-Factor Authentication (MFA)

The conventional username and password combinations are frequently insufficient to secure user accounts from hackers, and stolen credentials are one of the most common ways for hackers to get access to your online business data and apps. They can log into all of the cloud-based programs and services that you use every day to run your organization once they have your user credentials [141]. Multi factor authentication (MFA) protects all of your cloud users, ensuring that only authorized workers can log in to your cloud apps and access critical data in your on- or off-premise environment. MFA is one of the simplest yet most effective security measures for preventing hackers from gaining access to your cloud applications. In fact, most security experts will warn you that failing to deploy MFA as part of your infrastructure as a service (IAAS) design is now regarded careless.

VII. Benefits of Cloud Computing

To put it another way, cloud computing is computing that is fully based on the internet. People no longer need to download software from a server or a physical computer to run programs or apps; instead, cloud computing services enable them to access those applications via the internet [142]. Cloud computing is a type of computing in which software and services are supplied virtually across a private or public network. The cloud's fundamental goal is to provide cost-effective, adaptable resources to improve user experience. The practice of installing remote servers accessed via the internet to store, manage, and process healthcare-related data is known as cloud computing

in healthcare [143]. The advantages of cloud computing are numerous and remarkable. Here are just few of the many cloud computing advantages discussed.

7.1 Time-Saving, On-Demand Services

Self-service delivery is a characteristic of cloud computing for various workloads and requirements. Its allure stems from the fact that any service can be accessed on demand. This means you can gain new capabilities right away without investing in new hardware or software.

7.2 Sustainability

Given the current situation of the environment, it is no longer sufficient for businesses to place a recycling bin in the break room and claim that they are helping the environment. True sustainability necessitates solutions that address waste at all levels of a company. Cloud hosting is more environmentally friendly and leaves a smaller carbon footprint [144]. Cloud infrastructures help the environment by powering virtual services rather than actual items and hardware, minimizing paper waste, increasing energy efficiency, and lowering commuting emissions. Based on the expansion of cloud computing and other virtual data alternatives, a Pike research report anticipated that data center energy consumption will decline by 31% from 2010 to 2020.

7.3 Flexible Costs

The cloud flips the script on traditional capital expenditure investment, with the vast bulk of cloud spending being operational. Since a third-party vendor will take care of maintenance, a company doesn't have to fund a support team to fix problem servers. The initial expenses of infrastructure requirements, such as the purchase of local servers, are significantly reduced.

7.4 Flexibility

Clients benefit from a great deal of flexibility provided by the cloud computing. The cloud makes service testing and deployment a breeze. Customers can pick and choose which services they want and how much they want to pay for them. By providing a variety of services, cloud services can better meet changing business demands. If any application provided by the cloud is not getting our job done, we have the flexibility to switch to another cloud.

7.5 Easy Data Backup and Restore

Data backup and restore has become a critical requirement for businesses as the number of cyber-attacks and security breaches has increased. Cloud computing solutions can help you store vital data offsite, duplicate it, and restore it when needed. Traditional data backup and restore alternatives are available, but they are inefficient and difficult to scale. Cloud-based data backup allows you to save a large amount of data in the cloud and expand your storage space without the need for additional hardware. Most of the cloud backup service providers ensure that data is encrypted during upload and download. They also meet data security and compliance requirements.

7.6 Improved Mobility

Apps and data may be accessed from anywhere at any time thanks to the cloud. All of this is attributable to the rising number of mobile devices such as smartphones and tablets. The "anywhere, anytime" benefit also certainly applies to business. Employees gain flexibility, becoming more efficient with workflows and customer service.

7.7 Disaster Recovery

Unexpected events, natural disasters, and operational hiccups are an unavoidable reality for which

everyone must prepare. When such unforeseeable events hit, however, any organisation might suffer significant losses. While physical infrastructure failure can be remedied, the loss of data has a long-term impact on an organization's structure and stability [145]. On the other side, storing data in the cloud protects all of your vital information from damage, even in the face of the most terrifying tragedies. With cloud services, you can count on quick data recovery in an emergency, be it a natural disaster like a flood or human-made trouble such as a fire or even something as simple as power outages.

7.8 Easily Manageable

Cloud computing enables IT maintenance and management to be simplified and improved through SLA-backed agreements, central resource administration, and managed infrastructure. We get to enjoy a basic user interface without any requirement for installation and we are assured guaranteed and timely management, maintenance, and delivery of the IT services.

7.9 Increased Collaboration

Cloud computing is primarily designed to enhance work operations, which includes data exchange between co-workers and business partners. Organizations demand more apps for file sharing and streamlined workflows. Remote workers can instantly connect and communicate with fellow employees and important clients.

7.10 Carbon Footprint

Cloud computing is assisting businesses in reducing their carbon impact. Organizations only use the resources they require, avoiding any unnecessary over-provisioning.

7.11 Loss Prevention

All of your valuable data is inextricably linked to the office computers if your company does not invest in a cloud-computing solution. This may not appear to be a concern, but if your local hardware fails, you could lose your data forever. Computers can fail for a variety of causes, ranging from viral infections [146] to age-related hardware degeneration to simple user error. They can also be misplaced or stolen, despite the best of intentions. If we don't use the cloud, you risk losing all of the data you've saved locally. With a cloud-based server, however, all of the data you've uploaded to the cloud is safe and accessible from any computer with an internet connection, even if your primary computer isn't working.

7.12 Economies of Scale

Cloud computing saves money by taking advantage of economies of scale. According to a study by Booz Allen Hamilton, cloud computing could cut costs by 50 to 72 percent for a deployment of 1000 servers. Customers who use the cloud can save money by taking advantage of vendor economies of scale and reducing their investments in on-premises infrastructure.

7.13 Multimedia Cloud Computing

Users can now quickly access multimedia information through the internet at any time thanks to the invention of cloud computing. After subscribing, the user can easily store multimedia [147] content of any sort and size in the cloud. Because the calculation time for processing media data is longer in complicated hardware, the cloud can not only store but also process media material such as audio, video, and image. After processing, processed data can be simply retrieved from the cloud via a client without the need for complex hardware installation.

7.14 Operational

Technology will never be perfect, but some of it is simpler than others. This includes cloud computing infrastructure, which is often hosted on separate servers by a third-party vendor. So, when problems do arise, it's the vendor's job to promptly fix the problem instead of having on-site IT staffs spend time and resources file claims or updating servers.

7.15 Quality Control

Few things are as damaging to a company's growth as poor quality and inconsistent reporting. All documents are stored in one place and in the same format in a cloud-based system. We can preserve data consistency, avoid human error, and have a clear record of any edits or updates if everyone has access to the same information. Managing information in silos, on the other hand, can result in employees saving different versions of documents by accident, resulting in confusion and diluted data.

7.16 Multi-Sharing

Cloud computing allows several users to share architecture and other applications. Multiple users and apps can operate more efficiently and save money by using common infrastructure when using the cloud in a distributed and shared way [148].

7.17 Automatic Updates

Users that use the cloud don't have to worry about keeping their software up to date. Instead of involving IT teams and forcing them to do a manual upgrade, cloud-based applications automatically refresh and update themselves.

7.18 improved communication

Having access to instant messaging, conference, and video conferencing options through cloud computing promotes staff communication and cooperation. They can collaborate on papers and projects together, resulting in greater cohesion and teamwork. This is made possible by data centralization and real-time cloud server updates.

7.19 Real-Time Insights

Millions of data points exist in your business data that can be used to improve it. It can be difficult [149] to assess how your firm is doing and what route to take next if your data is concealed in silos of data, on local workstations, or in diverse forms. Moving your business systems to the cloud allows you to get better visibility over your business performance, in real-time, so that you can make informed decisions.

7.20 Processing Speed

The practically infinite computational power accessible in the cloud allows you to reap the benefits of faster processing. Complex workloads that would normally take hours to accomplish on-premises are now completed in minutes. Websites will load faster, and video will render more quickly [150]. The possibilities are endless. When it comes to data crunching, processing speed is equally important. Using the cloud's near-limitless compute resources for services like big data and machine learning allows you to gain deep insights from your data much more quickly than traditional analytics.

VIII. Conclusion

Cloud computing is a novel means of delivering resources to users "as a service" over the internet. Cloud computing consumers no longer own the infrastructure that is completely controlled by these service providers, unlike traditional approaches that are based on hardware ownership where data is stored. You may sync your cloud storage service with your smartphone, tablet, or other mobile devices for

convenient access while on the road once you've signed up for it and uploaded your files. Cloud computing is a computing model that enables on-demand network access to a pool of configurable computing resources, such as networks, services, storage, and applications, that can be quickly supplied and released with minimal administration effort or service provider contact. Cloud computing is a new concept that allows users to access scalable and virtualized resources, such as bandwidth, software, and hardware, on demand. Although it has gained a lot of attention in recent years, the issue of privacy and data security is one of the key roadblocks to cloud computing's progress. In this article, we looked at numerous significant security risks for cloud computing environments from various angles, as well as the solutions that all users and companies should be aware of when selecting whether or not to use the cloud. This work contributes to the discovery of a solution for the security and privacy issues in cloud data storage that have been identified in other techniques, as well as the development of a novel solution or approach to secure the cloud.

IX. Future Work of Cloud Computing

Because of the flexibility of cloud computing, users will access and share their software applications online and access information via remote server networks rather than relying on primary tools and information hosted on their personal computers in the future. Cloud computing privacy and data security issues are constantly one of the key study topics for researchers and developers to find appropriate solutions. From the standpoint of this paper, we recommend that you discover the best and most appropriate privacy and data security solutions for the cloud services you use. Compliance, physical security, cloud migration, transparency, password security, data ownership, detrimental competition, and hostile insiders are all prospective concerns in cloud security that can be addressed with guidelines.

X. REFERENCES

[1]. Yusuf Perwej, “An Experiential Study of the Big Data,” for published in the International Transaction of Electrical and Computer Engineers System (ITECES), USA, Vol. 4, No. 1, page 14-25, March 2017, DOI:10.12691/iteces-4-1-3.

[2]. L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M.L. Stefanizzi, et al., "An iot-aware architecture for smart healthcare systems", IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515-526, 2015

[3]. Nikhat Akhtar, Firoj Parwej, Yusuf Perwej, “A Perusal of Big Data Classification and Hadoop Technology”, International Transaction of Electrical and Computer Engineers System (ITECES), USA, Volume 4, No. 1, Pages 26-38, 2017, DOI: 10.12691/iteces-4-1-4

[4]. Y. Zhang, "Research on the security mechanism of cloud computing service model," Autom. Control Comput. Sci., vol. 50, no. 2, pp. 98-106, Mar. 2016

[5]. P. G. Shynu and K. J. Singh, "A comprehensive survey and analysis on access control schemes in cloud environment," Inf. Technol., vol. 16, no. 1, pp. 19-38, 2016

[6]. R. K. Aluvalu and L. Muddana, "A survey on access control models in cloud computing," in Proc. 49th Annu. Conv. Comput. Soc. India (CSI), vol. 1, pp. 653-664, 2015

[7]. J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Comput. Secur., vol. 72, pp. 1_2, Jan. 2018

[8]. Z. Xiao andY.Xiao, “Security and privacy in cloud computing,” IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013

[9]. Yusuf Perwej, M. K. Omer, O. E. Sheta, Hani Ali M. Harb, M. S. Adrees, "The Future of Internet of Things (IoT) and Its Empowering Technology", International Journal of Engineering Science and Computing (IJESC), Vol. 9, Iss., No.3, Pages 20192– 20203, 2019

[10]. D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzingsecurity, privacy and trust issues in cloud computing environments," in Proceedings of the International Conference on Advanced in Control Engineering and Information Science (CEIS'11), pp. 2852–2856, chn, August 2011

[11]. M. Y. A. Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: a survey," Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013

[12]. J. Yang and Z. Chen, "Cloud computing research and security issues," in Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on. IEEE, pp. 1–3, 2010

[13]. E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in High Performance Cloud Auditing and Applications. Springer, pp. 3–33, 2014

[14]. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Information Sciences, vol. 258, pp. 371–386, 2014

[15]. A. Behl, "Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation", Proceedings of the World Congress on Information and Communication Technologies (WICT '11), pp. 217–222, IEEE, 2011

[16]. Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in Proceedings of the 8th International Conference on Network and Service Management. International Federation for Information Processing, pp. 37–45, 2012

[17]. D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), vol. 1, pp. 647–651,Hangzhou, China, March 2012

[18]. S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for Cloud Computing, Computer Communications and Networks, pp. 3–42, Springer London, 2013

[19]. R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: a systematic literature review," in Future Information Technology, pp. 285–295, Springer, Berlin, Germany, 2014

[20]. Jemal, H., Kechaou, Z., Ayed, M.B., Alimi, A.M., "Mobile cloud computing in healthcare system.", Computational Collective Intelligence. Springer International Publishing, Cham, pp. 408–417, 2015

[21]. P. G. Shynu and K. J. Singh, "A comprehensive survey and analysis on access control schemes in cloud environment," Inf. Technol., vol. 16, no. 1, pp. 19-38, 2016.

[22]. Lo'ai, A.T., Bakhader, W., Mehmood, R., Song, H., 2016. Cloudlet-based mobile cloud computing for healthcare applications. In: 2016 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 1–6.

[23]. Yusuf Perwej, S. A. Hannan, Firoj Parwej, Nikhat Akhtar ,"A Posteriori Perusal of Mobile Computing", International Journal of Computer Applications Technology and Research, ATS (Association of Technology and Science), Vol. 3, Issue 9, pp. 569 - 578, 2014, DOI: 10.7753/IJCATR0309.1008

[24]. Johanna Ullrich, Tanja Zseby. Network-Based Secret Communication in Clouds: A Survey.

IEEE communications surveys & tutorials, vol. 19, no. 2, second quarter 2017

[25]. D. Zhe,W. Qinghong, S. Naizheng, and Z.Yuhan, "Study on data security policy based on cloud storage," in Proc. IEEE IEEE 3rd Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput., (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS), China, pp. 145-149, 2017

[26]. Al-Mushayt O, Haq K and Yusuf P., "Electronic-Government in Saudi Arabia; a Positive Revolution in the Peninsula", International Transactions in Applied Sciences, India, 1(1), 87-98, 2009

[27]. Oussous, Ahmed, Benjelloun, Fatima-Zahra, Lahcen, Ayoub Ait, Belfkih, Samir, "Big data technologies: a survey", J. King Saud Univ.-Comput. Inf. Sci. 30 (4), 431– 448, 2018

[28]. R. Zhang, R. Xue, and L. Liu, "Searchable encryption for healthcare clouds: A survey," IEEE Trans. Service Comput., vol. 11, no. 6, pp. 978_996, Nov./Dec. 2018.

[29]. Zhang Jie. Fu, Xinle. Wu. Toward Efficient Multi-keyword Fuzzy Search over Encrypted Out sourced Data with Accuracy Improvement. IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2706-2716, Dec. 2016

[30]. Yusuf Perwej, " The Hadoop Security in Big Data: A Technological Viewpoint and Analysis ", International Journal of Scientific Research in Computer Science and Engineering, E-ISSN: 2320-7639, Volume 7, Issue 3, Pages 1- 14, 2019, DOI: 10.26438/ijsrcse/v7i3.1014

[31]. Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "A Close-Up View About Spark in Big Data Jurisdiction", International Journal of Engineering Research and Application, Vol. 8, Issue 1, PP. 26-41, 2018 DOI: 10.9790/9622-0801022641

[32]. Nikhat Akhtar, Yusuf Perwej, "The Internet of Nano Things (IoNT) Existing State and Future Prospects", GSC Advanced Research and Reviews, Volume 5, Issue 2, Pages 131-150, 2020, DOI: 10.30574/gscarr.2020.5.2.0110

[33]. Yusuf Perwej, "A Pervasive Review of Blockchain Technology and Its Potential Applications", Open Science Journal of Electrical and Electronic Engineering (OSJEEE), New York, USA, Volume 5, No. 4, Pages 30 - 43, 2018

[34]. K. Edemacu, H. K. Park, B. Jang, and J. W. Kim, "Privacy provision in collaborative Ehealth with attribute-based encryption: Survey, challenges and future directions", IEEE Access, vol. 7, pp. 89614-89636, 2019

[35]. Yusuf Perwej, Firoj Parwej, Mumdouh Mirghani Mohamed Hassan, Nikhat Akhtar, "The Internet-of-Things (IoT) Security: A Technological Perspective and Review", International Journal of Scientific Research in Computer Science Engineering and Information Technology (IJSRCSEIT), Volume 5, Issue 1, Pages 462-482, February 2019, DOI: 10.32628/CSEIT195193

[36]. Tara Salman, Maede Zolanvari. Security Services Using Blockchains: A State-of-the-Art Survey. IEEE communications surveys & tutorials, vol. 21, no. 1, 2019

[37]. Yusuf Perwej, Nikhat Akhtar, Firoj Parwej, "A Technological Perspective of Blockchain Security", International Journal of Recent Scientific Research (IJRSR), ISSN: 0976-3031, Volume 9, Issue 11, (A), Pages 29472 – 29493, 2018, DOI: 10.24327/ijrsr.2018.0911.2869

[38]. J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," J. Inf. Secur. Appl., vol. 57, Mar. 2021, Art. no. 102686

[39]. Nikhat Akhtar, Saima Rahman, Halima Sadia, Yusuf Perwej, "A Holistic Analysis of Medical

Internet of Things (MIoT)", Journal of Information and Computational Science (JOICS), ISSN: 1548 - 7741, Volume 11, Issue 4, Pages 209 - 222, 2021, DOI:10.12733/JICS.2021/V11I3.535569.31023

[40]. Jeffrey C. Kimmell at.al.,"Recurrent Neural Networks Based Online Behavioural Malware Detection Techniques for Cloud Infrastructure",IEEE, PP. 68066 – 68080, Vol. 9, 2021

[41]. Yusuf Perwej, "Recurrent Neural Network Method in Arabic Words Recognition System", International Journal of Computer Science and Telecommunications, Sysbase Solution (Ltd), UK, London, Vol. 3, Issue 11, Pages 43-48, 2012

[42]. Yusuf Perwej, "The Bidirectional Long-Short-Term Memory Neural Network based Word Retrieval for Arabic Documents" Transactions on Machine Learning and Artificial Intelligence (TMLAI), Society for Science and Education, Manchester, United Kingdom (UK), Vol. 03, No.01, Pages 16 – 27, 2015, DOI : 10.14738/tmlai.31.863

[43]. Bader Alouffi at. al.," A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies",IEEE, VOLUME 9, 2021

[44]. Yusuf Perwej, Kashiful Haq, Firoj Parwej, M. M. Mohamed Hassan, "The Internet of Things (IoT) and its Application Domains", International Journal of Computer Applications (IJCA) , USA , Volume 182, No.49, Pages 36- 49, 2019, DOI: 10.5120/ijca2019918763

[45]. Y.-Y. Teing, A. Dehghantanha, K.-K.-R. Choo, and L. T. Yang, "Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent sync as a case study," Comput. Electr. Eng., vol. 58, pp. 350_363, Feb. 2017

[46]. Ferrer, A.J., Marques, J.M., Jorba, J.,. Towards the decentralized cloud. ACM Comput. Surv. 51 (6), 1–36, 2019

[47]. Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "An Empirical Analysis of Web of Things (WoT)", International Journal of Advanced Research in Computer Science, Vol. 10, No. 3, PP. 32-40, 2019, DOI: 10.26483/ijarcs.v10i3.6434

[48]. Kameswara Rao Poranki, Yusuf Perwej, Nikhat Akhtar,"Integration of SCM and ERP for Competitive Advantage", TIJ's Research Journal of Science & IT Management RJSITM, International Journal Research Journal of Science & IT Management of Singapore, ISSN:2251-1563, Singapore, Volume 04, Number 05, Pages 17-24, 2015

[49]. Kameswara Rao Poranki, Asif Perwej,"The buying Attitudes of Consumers of Cosmetic Products in Saudi Arabia", TIJ's Research Journal of Social Science & Management RJSSM, International Journal Research Journal of Social Science & Management of Singapore, Volume: 04, Number: 08, December 2014 Page 138-145, 2014

[50]. J. W. Rittinghouse and J. F. Ransome, Cloud computing: implementation management and security, CRC press, 2016

[51]. Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, 2014

[52]. N. Abbas, A. Zhang, Y. Taherkordi and T. Skeie, "Mobile edge computing: A survey", IEEE Int. Things J., vol. 5, no. 1, pp. 450-465, Feb. 2018

[53]. Cristian Chilipirea at.al.," A Comparison of Private Cloud Systems", 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA),IEEE, Switzerland, 2016

[54]. J. Chase and D. Niyato, "Joint optimization of resource provisioning in cloud computing", IEEE Transactions on Services Computing, vol. 10, pp. 396-409, 2017

[55]. Kyriakos Kritikos at. al.," Towards the Modelling of Hybrid Cloud Applications", IEEE 12th International Conference on Cloud Computing (CLOUD), IEEE, Italy, 2019

[56]. X. L. Xingong and X. Lv, "Distributed Cloud Storage and Parallel Topology Processing of Power Network", Third International Conference on Trustworthy Systems and Their Applications pages 18-22 Wuhan China, Sept. 2016

[57]. M. K. Skadsem, R. Karlsen, G. Blair and K. Mitchell, "Community Cloud – Cloud Computing for the Community", Proceedings of the 1st International Conference on Cloud Computing and Services Science, pp. 418-423, 2011

[58]. Mohamed M. M., "Current Services in Cloud Computing: A Survey", International Journal of Computer Science Engineering and Information Technology, vol. 3, no. 5, 2013

[59]. M. Bist, M. Wariya and A. Agarwal, "Comparing delta open stack and xen cloud platforms: A survey on open source iaas", Advance Computing Conference (IACC) 2013 IEEE 3rd International, pp. 96-100, 2013

[60]. Yucong Duan at. al.," Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends ", IEEE 8th International Con. on Cloud Computing, IEEE, USA, 2015

[61]. Yusuf Perwej, M. A. AbouGhaly, Bedine Kerim, Hani Ali Mahmoud Harb. "An Extended Review on Internet of Things (IoT) and its Promising Applications", Communications on Applied Electronics (CAE), New York, USA, Volume 9, Number 26, Pages 8– 22, 2019, DOI: 10.5120/cae2019652812

[62]. Gabriella Laatikainen and Arto Ojala, "saas architecture andx pricing models", IEEE international conf. on services computing, pp. 597-604, 2014

[63]. Asif Perwej, "Effective Management of Customer Relationship Management (CRM) In Banking Industry". YOJNA The Management Journal of KITE Group, Vol. No. 2 & 3, No. 1, 2010

[64]. T. F. M. Pasquier, J. Singh and J. Bacon, "Information flow control for strong protection with flexible sharing in paas", Cloud Engineering (IC2E) 2015 IEEE International Conference on, pp. 279-282, 2015

[65]. Yusuf Perwej, "An Evaluation of Deep Learning Miniature Concerning in Soft Computing", the International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 4, Issue 2, Pages 10 - 16, 2015, DOI: 10.17148/IJARCCE.2015.4203

[66]. Asif Perwej, Kashiful Haq, Yusuf Perwej, " Blockchain and its Influence on Market", International Journal of Computer Science Trends and Technology (IJCST), Volume 7, Issue 5, Pages 82- 91, Sep – Oct 2019, DOI: 10.33144/23478578/IJCST-V7I5P10

[67]. Nikhat Akhtar, Yusuf Perwej, " The Internet of Nano Things (IoNT) Existing State and Future Prospects" , GSC Advanced Research and Reviews, Volume 5, Issue 2, Pages 131-150, 2020, DOI: 10.30574/gscarr.2020.5.2.0110

[68]. Yusuf Perwej, Md. Husamuddin, Fokrul Alom Mazarbhuiya,"An Extensive Investigate the MapReduce Technology", International Journal of Computer Sciences and Engineering (IJCSE), Volume-5, Issue-10, Page No. 218-225, 2017, DOI: 10.26438/ijcse/v5i10.218225

[69]. T. Lynn et al., "A Preliminary Review of Enterprise Serverless Cloud Computing

(Function-as-a-Service) Platforms", Proc. CloudCom, 2017

[70]. Lins, S., Pandl, K.D., T., H. et al. "Artificial Intelligence as a Service", Bus Inf Syst Eng 63, PP. 441–456, 2021

[71]. Yusuf Perwej , Firoj Parwej, "A Neuroplasticity (Brain Plasticity) Approach to Use in Artificial Neural Network", International Journal of Scientific & Engineering Research (IJSER), France , ISSN 2229 – 5518, Volume 3, Issue 6, Pages 1- 9, 2012, DOI: 10.13140/2.1.1693.2808

[72]. Nikhat Akhtar, Dr. Yusuf Perwej, Firoj Parwej, Jai Pratap Dixit, "A Review of Solving Real Domain Problems in Engineering for Computational Intelligence Using Soft Computing" Proceedings of the 11th INDIACom; INDIACom-2017; IEEE Conference, 4th International Conference on "Computing for Sustainable Global Development", ISSN 0973-7529; ISBN 978-93-80544-24-3, Pages 706–711, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), Delhi, 2017

[73]. S. Kibe, T. Koyama and M. Uehara, "The Evaluations of Desktop as a Service in an Educational Cloud", 15th International Conference on Network-Based Information Systems, 2015

[74]. T. Wood, E. Cecchet, K. K. Ramakrishnan, P. Shenoy, J. Van der Merwe and A. Venkataramani, "Disaster recovery as a cloud service: Economic benefits & deployment challenges", 2nd USENIX Work. on Hot Topics in Cloud Computing, 2010

[75]. Shicong Meng at.al., "Enhanced Monitoring-as-a-Service for Effective Cloud Management", IEEE Transactions on Computers, Volume: 62, Issue 9, PP. 1705 – 1720, 2013

[76]. C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Cloud Computing Date of Publication, vol. 5, no. 2, April-June 2012

[77]. Y. Cao, C. Chen, F. Guo, D. Jiang, Y. Lin, B. Ooi, et al., ES2: A Cloud Data Storage System for Supporting Both OLTP and OLAP, PP 34-46, 2018

[78]. Wassim Itani Ayman Kayssi Ali Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures", Eighth IEEE International Conference on Dependable, 2009

[79]. H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon. RACS: A Case for Cloud Storage Diversity. In Proceedings of the 1st ACM symposium on Cloud computing (SoCC 2010), Indianapolis, IN, June 10-11 2010

[80]. M. Wajahat, A. Yele, T. Estro, A. Gandhi and E. Zadok, "Distribution fitting and performance modeling for storage traces", Proc. of IEEE Mascots, pp. 138-151, 2019

[81]. Chang Guo, Ying Li and Zhonghai Wu, "SLA-DO: A SLA-based Data Distribution Strategy on Multiple Cloud Storage Systems", IEEE 22nd Int. Conference on Parallel and Distributed Systems (ICPADS), pp. 602-609, 2016

[82]. N. Cao, C. Wang, M. Li, K. Ren and W. Lou, "Privacy preserving Multi keyword Ranked Search over Encrypted Cloud Data", 30thIEEE Conference on Computer Communications, pp. 829-837, 2011

[83]. Xiaotong Sun, "Critical Security Issues in Cloud Computing: A Survey", 4th IEEE International Conference on Big Data Security on Cloud, 2018

[84]. C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," Network, IEEE, vol. 24, no. 4, pp. 19–24, 2010

[85]. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Information Sciences, vol. 258, pp. 371–386, 2014

[86]. United Nations, "The Universal Declaration of Human Rights." http://www.un.org/en/documents/udhr/index.shtml, 1948. Retrieved August 2021

[87]. D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz, and A. Scherrer, "Fighting cybercrime and protecting privacy in the cloud." European Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs, 2012

[88]. Wei Nie, Xiangfei Xiao, Zhaohui Wu, Yuanhui Wu, Fang Shen and Xionglan Luo, "The Research of Information Security for The Education Cloud Platform Based on AppScan Technology", 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), 2018

[89]. Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in Proceedings of the 8th International Conference on Network and Service Management. International Federation for Information Processing, pp. 37–45, 2012

[90]. A. M. Farooqi at.al.,"The notorious nine: top cloud computing security challenges in 2017", International Journal of Advanced Research in Computer Science, Vol. 8, No. 5, PP. 2804 – 2808, 2017

[91]. Hongwei Li, Yuanshun Dai1, Ling Tian, "Identity based authentication for cloud computing", Springer-Verlag Berlin Heidelberg, pp 157- 166, 2009

[92]. Priya anand, jungwoo ryoo, hyoungshick kim "addressing security challenges in cloud computing a pattern-based approach", first international conference on software security and assurance, 2016, doi 10.1109/icssa.2015.1113

[93]. Z. Zhang, C. Wu and D. W. L. Cheung, "A survey on cloud interoperability: taxonomies standards and practice", SIGMETRICS Perform. Eval. Rev., vol. 40, pp. 13-22, 2013

[94]. S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046-2069

[95]. K. Hashizume, D. G. Rosado, E. Fern´andez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, vol. 4, no. 1, pp. 1–13, 2013

[96]. Kiattikul Treseangrat, Samad Salehi Kolahi and Bahman Sarrafpour, "Analysis of UDP DDoS cyber Flood Attack and Defence Mechanism on Windows Serevr 2012 and Linux Ubuntu 13", IEEE, 2015

[97]. Istvan Kiss, Piroska Haller and Adela Beres, "Denial of Service attack Detection in case of Tennessee Eastman challenge process" in 8th INTER-ENG 2014, Romania, vol. 19, pp. 835-841, 2015

[98]. G. Rydstedt, E. Bursztein, D. Boneh and C. Jackson, "Busting frame busting: a study of clickjacking vulnerabilities at popular sites", IEEE SSP, vol. 2, 2010

[99]. H. Hlavacs, T. Treutner, J.-P. Gelas, L. Lefevre, and A.-C. Orgerie, "Energy consumption side-channel attack at virtual machines in a cloud," in Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on. IEEE, pp. 605–612, 2011

[100]. B. C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks", IEEE Communicaion, vol. 32, no. 9, pp. 33-38, 1994

[101]. Garbarino S, Holland J,"Quantitative and Qualitative Methods in Impact Evaluation and Measuring Results", GSDRC Emerging Issues Research Service, pp: 1-59, 2009

[102]. Nakouri, I.; Hamdi, M.; Kim, T.H. A new biometric-based security framework for cloud storage. In Proceedings of the 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30, pp. 390–395, 2017

[103]. Liang, X.,Shetty, S.; Zhang, L. Kamhoua, C., Kwiat, K. Man in the Cloud (MITC) Defender: SGX-Based User Credential Protection for Synchronization Applications in Cloud Computing Platform. In Proceedings of the IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, CA, USA, 25–30, pp. 302–309, 2017

[104]. Yusuf Perwej, Md. Husamuddin, Majzoob K.Omer, Bedine Kerim, "A Comprehend the Apache Flink in Big Data Environments" , IOSR Journal of Computer Engineering (IOSR-JCE), Volume 20, Issue 1, Ver. IV, Pages 48-58, 2018, DOI: 10.9790/0661-2001044858

[105]. L. A. Gordon, M. P. Loeb and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis", Journal of Accounting and Public Policy, vol. 22, no. 6, pp. 461-485, 2003

[106]. Balogh, Z., Turčáni, M."Modeling of data security in cloud computing", In IEEE Annual Systems Conference, pp. 1–6. IEEE, 2016

[107]. Meng, D." Data security in cloud computing", In IEEE International Conference on Computer Science & Education, pp. 810–813. IEEE, 2013

[108]. An, Y.Z., Zaaba, Z.F., Samsudin, N.F."Reviews on security issues and challenges in cloud computing", In IOP Conference Series: Materials Science and Engineering, vol. 160, p. 012106. IOP Publishing, 2016

[109]. H. Takabi, J.B.D. Joshi and G. Ahn, "Security and privacy challenges in cloud computing environments", IEEE security privacy magazine, vol. 8, pp. 24-31, 2010

[110]. lbugmi, A.A., Alassafi, M.O., Walters, R., Wills, G." Data security in cloud computing", In IEEE Fifth International Conference on Future Generation Communication Technologies, pp. 55–59, IEEE, 2016

[111]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, pp. 457- 473, 2005

[112]. R. L. Rivest, L. Adleman, andM. L.Dertouzos, "On data banks and privacy homomorphisms," Foundations of Secure Computation, vol. 4, no. 11, pp. 169–180, 1978

[113]. C. Gentry, A fully homomorphic encryption scheme Ph.D. thesis], Stanford University, 2009

[114]. Y. Rouselakis and B. Waters, "Ef_cient statically-secure large-universe multi-authority attribute-based encryption," in Proc. Int. Conf. Financial Cryptogr. Data Secur., pp. 315-332, 2015

[115]. Q. Li, J. Ma, R. Li, X. Liu, J. Xiong, and D. Chen, "Secure, efficient and revocable multi-authority access control system in cloud storage," Comput. Secur., vol. 59, pp. 45_59, 2016

[116]. X. Liu, Y. Xia, S. Jiang, F. Xia, and Y. Wang, "Hierarchical attributebased access control with authentication for outsourced data in cloud computing," in Proc. 12th IEEE Int. Conf. Trust Secur. Privacy Comput. Commun., pp. 477-484, 2013

[117]. F. Pagano and D. Pagano, "Using in-memory encrypted databases on the cloud," in Proceedings of the 1st IEEE International Workshop on Securing Services on the Cloud (IWSSC '11), pp. 30–37, 2011

[118]. K.Huang and R. Tso, “A commutative encryption scheme based on ElGamal encryption,” in Proceedings of the 3rd International Conference on Information Security and Intelligent Control (ISIC'12), pp. 156–159, IEEE, 2012

[119]. D. H. Rachel and S. Prathiba, "An enhanced Hasbe for cloud computing environment," Int. J. Comput. Sci. Mobile Comput., vol. 2, no. 4, pp. 396_401, 2013

[120]. Z.Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743_754, Apr. 2012

[121]. Q. Huang, Y. Yang, and M. Shen, "Secure and ef_cient data collaboration with hierarchical attribute-based encryption in cloud computing," Future Gener. Comput. Syst., vol. 72, pp. 239_249, Jul. 2017

[122]. S. Gokuldev and S. Leelavathi, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control by separate encryption/ decryption in cloud computing," Int. J. Eng. Sci. Innov. Technol.,vol. 2, no. 3, pp. 1_7, 2013

[123]. A. Rao, “Centralized database security in cloud,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, pp. 544–549, 2012

[124]. E. M.Mohamed, H. S. Abdelkader, and S. El-Etriby, “Enhanced data security model for cloud computing,” in Proceedings of the 8th International Conference on Informatics and Systems (INFOS '12), pp. CC-12–CC-17, IEEE, 2012

[125]. W. Sun, B.Wang, N. Cao, M. Li,W. Lou, Y. T. Hou, and H. Li, "Privacy preserving multi-keyword text search in the cloud supporting similarity based ranking," in Proc. 8th ACM SIGSAC Symp. Inf. Comput. Comm. Secur., pp. 71_82, 2013

[126]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM, Apr., pp. 829_837, 2011

[127]. C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and ef_cient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467_1479, Aug. 2012

[128]. N. Cao, C.Wang, M. Li, K. Ren, andW. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222_233, Nov. 2013

[129]. M. Fujimoto at.al.,” Detecting Abuse of Domain Administrator Privilege Using Windows Event Log”, IEEE Conference on Application, Information and Network Security (AINS),IEEE, Malaysia, 2019

[130]. C. Delettre, K. Boudaoud, and M. Riveill, “Cloud computing, security and data concealment,” in Proceedings of the 16th IEEE Symposium on Computers and Comm. (ISCC '11), pp. 424–431, Kerkyra, Greece, July 2011

[131]. Yusuf Perwej, Asif Perwej, Firoj Parwej, “An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection”, International Journal of Multimedia & Its Applications (IJMA), Academy & Industry Research Collaboration Center (AIRCC) , USA , Volume 4, No.2, Pages 21- 38, 2012, DOI: 10.5121/ijma.2012.4202

[132]. A. Ra_que, D. V. Landuyt, B. Lagaisse, and W. Joosen, "Policy-driven data management middleware for multi-cloud storage in multi-tenant SaaS," in Proc. IEEE Int. Symp. Big Data Comput. (BDC), pp. 78_84, Dec. 2015

[133]. C. Ngo, Y. Demchenko, and C. de Laat, "Multi-tenant attribute-based access control

for cloud infrastructure services," J. Inf. Secur. Appl., vol. 27, pp. 65_84, Apr. 2016

[134]. D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-trust_A security assessment model for infrastructure as a service (IaaS) clouds," IEEE Trans. Cloud Comput., vol. 5, no. 3, pp. 523_536, Jul./Sep. 2017

[135]. J. Zhou et al., "Security and privacy for cloud-based IoT: Challenges", IEEE Communications Magazine, vol. 55, no. 1, pp. 26-33, 2017

[136]. C. Stergiou et al., "Secure integration of IoT and cloud computing", Future Generation Computer Systems, vol. 78, pp. 964-975, 2018

[137]. S. Kianoush et al., "A cloud-IoT platform for passive radio sensing: Challenges and application case studies", IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3624-3636, 2018

[138]. E. Pinheiro, W.-D.Weber, and L. A. Barroso, “Failure trends in a large disk drive population,” in Proceedings of the 5th USENIX conference on File and Storage Technologies (FAST '07), vol. 7, pp. 17–23, 2007

[139]. C. Cachin and M. Schunter, “A cloud you can trust,” IEEE Spectrum, vol. 48, no. 12, pp. 28–51, 2011

[140]. J. Idziorek, M. Tannian, and D. Jacobson, “Attribution of Fraudulent Resource Consumption in the cloud,” in Proceedings of the IEEE 5th International Conference on Cloud Computing (CLOUD '12), pp. 99–106, June 2012

[141]. D. Wang, D. He, P. Wang and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment", IEEE Trans. Dependable Secur. Comput., vol. 12, no. 4, pp. 428-442, 2015

[142]. T. Galibus, V. V. Krasnoproshin, R. Albuquerque and E. Freitas, Elements of Cloud Storage Security: Concepts Designs and Optimized Practices, Berlin:Springer, 2016

[143]. S. M. Riazul, Islam, Daehan Kwak, M.D. Humaun Kabir and Mahmud Hossain, "The Internet of Things for Health Care: A Comprehensive Survey", IEEE, vol. 3, pp. 678-708, 2015

[144]. T. S. Az-Zahra, "The Advantages from Cloud Computing Application Towards SMME (UMKM)", Journal Online Informatika, vol. 4, pp. 28-32, 2019

[145]. C. T. S. Xue and F. T. W. Xin, "Benefits and challenges of the adoption of cloud computing in business", International Journal on Cloud Computing: Services and Architecture, vol. 6, pp. 01-15, 2016

[146]. Y. Al-Dhuraibi, F. Paraiso, N. Djarallah and P. Merle, "Elasticity in cloud computing: state of the art and research challenges", IEEE Transactions on Services Computing, vol. 11, pp. 430-447, 2017

[147]. Yusuf Perwej, Faiyaz Ahamad, Mohammad Zunnun Khan, Nikhat Akhtar, “An Empirical Study on the Current State of Internet of Multimedia Things (IoMT)”, International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), Volume 8, Issue 3, Pages 25 - 42, March 2021, DOI: 10.1617/vol8/iss3/pid85026

[148]. Sultan Aldossary, William Allen, “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions”, International Journal of Advanced Computer Science and Applications, Vol. 7, 2016

[149]. I. Nwobodo, "Cloud computing: models services utility advantages security issues and prototype", Wireless Communications Networking and Applications, pp. 1207-1222, 2016

[150]. P. A. Abdalla and A. Varol, "Advantages to Disadvantages of Cloud Computing for Small-

Sized Business", 7th International Symposium on Digital Forensics and Security (ISDFS), 2019

Cite this article as:

Dr. Nikhat Akhtar, Dr. Bedine Kerim, Dr. Yusuf Perwej, Dr. Anurag Tiwari, Dr. Sheeba Praveen, "A Comprehensive Overview of Privacy and Data Security for Cloud Storage", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 5, pp. 113-151, September-October 2021. Available at doi : https://doi.org/10.32628/IJSRSET21852
Journal URL : https://ijsrset.com/IJSRSET21852