International Journal of Communication Networks and Information Security

ISSN: 2073-607X, 2076-0930

Volume ***14*** *Issue* ***02 Year 2022*** *Page* ***33:52***

Analysis of Computer Network Security Storage System Based on Cloud Computing Environment

[1] Dr. Daxa Vekariya, [2]Dr MK Jayanthi Kannan, [3]Mr. Sachin Gupta,[4] P. Muthusamy, [5]Mrs. Rohini Mahajan, [6]Dr. Arvind Kumar Pandey

[1] Associate Professor, Department of Computer Science and Engineering, Parul Institute of Engineering and Technology, Parul University, Vadodara, Gujarat, India.

[2] Professor and HOD, Professor and HOD of Information Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed-To-Be University), Bangalore, India.

[3] Chancellor, Department of Management, Sanskriti University, Mathura, Uttar Pradesh, India.

[4]Professor, School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India.

[5]Assistant Professor, Department of Computer Science Engineering, Chandigarh Engineering College, Jhanjeri, India.

[6]Assistant Professor, Department of Computer Science, ARKA JAIN University, Jamshedpur, Jharkhand, India.

[1] daxa.vekariya18436@paruluniversity.ac.in, [2]k.jayanthi@jainuniversity.ac.in, [3]chancellor@sanskriti.edu.in, [4]p.muthusamy@galgotiasuniversity.edu.in, [5]rohini.j1129@cgc.ac.in, [6]arvind.p@arkajainuniversity.ac.in

Article History

Received: 14 Feb 2022
Revised: 30 May 2022
Accepted: 18 June 2022

Abstract

A fundamental component of cloud computers from a business perspective is that users are allowed to use any desire and pay with a product that desire. Its cloud services were accessible anytime and anywhere consumers needed them. As a result, consumers are free to purchase whatever IT services they want, and they don't have to worry about how easy things can be managed. The remote server is used in a new information storage computing architecture that is considered an Internet generation. Ensuring security, material at resource providers' sites is a challenge that must be addressed in cloud technology. Thus, rather than reliance on a single provider for knowledge storing, this research implies developing construction for protection of knowledge stockpiling with a variation of operations, in which knowledge is scrambled and divided into numerous cipher frames and distributed across a large number of provider places. This support was applied to provide greater security, scalability, or reliability that was suggested according to the new structure. This paper, presented an encoded model for the cloud environment to improve security. The proposed model comprises the parity metadata for the database management provision to the provider. In the developed encoder chunks parity is not stored within the single resources with the provision of the available information chunks. The constructed security architecture in the RAID layer increases the dependability of the data with the deployment of the RAID 10 deployment. The developed RAID-based encoder chunks exhibit improved efficiency for the higher uptime at a minimal cost.

 | ***Keywords: Storage, Cloud Computing; Network Security; Encryption method, Cloud storage system, IaaS, Data encryption.*** |

1. Introduction

Computer technologies have evolved tremendously and evolved progressively during the last century. For instance, the web has progressively expanded the velocity of its offerings by replacing ancient computer paradigms (Shankar, A., et al, 2021). Owing to its difficulty of both procedure and high expense, these ancient commercial proposals have increasingly been acknowledged as obsolete. Aside from that, the sheer number and variety of equipment and programming required to run them are unsettling (Chen, J., et al, 2018). By managing hardware and software transfers from consumers to skilled Service Suppliers, the newest era of clouds providers spanned the divide in computer technologies and abolished conventional systems limitations. Cloud storage is a current computer paradigm that proposes a new economic strategy for institutions to use in the lack of explicit capital. With clouds technology, all databases and software applications are turned into large data towers, making information delivery and administration ineffective (Ibrahim, I. M.et al, 2021). The traditional storing solution has fewer advantages and advantages than cloud storing, notably in terms of cost, flexibility, mobility, and applicability. Internet storage is defined as a service that manages and preserves information on the internet (Tian, Z., et al, 2019).

That application may be found on the web. The visitor has the authority to save and retrieve documents from any website that uses the network. If the submitted documents are held on an outside computer by the provider business, the user can receive data digitally. Clouds storing solutions may be made available for businesses to use quickly and simply, but they are likely to be pricey. Because data retrieval through internet stores is slower than physically-backed, customers' information must still be backed up if cloud storing solutions are used (Wang, X. V, et al, 2017). With clouds storing, breaking information into tiny pieces and storing these in several places keeps the information safe; as such result, if information portions in one information facility or a disc are damaged, the data may have restarted using the left chunks. Information privacy is limited in clouds computers since data is stored at open in-service provider facilities (Xu, B, et al, 2017). Clouds technology makes the advantages more appealing than ever, but it equally brings with it a slew of new safety concerns for consumers' information. The primary security issue is that the whereabouts of the users' information are not monitored (Qi, Q, et al, 2019). It is risky to rely on a single service provider as information storage in internet technology.

Contribution and organization of paper:

In this paper developed a security model for the cloud computing environment. The proposed model integrates the RAID for the security.

1. The proposed model comprises of the encoder model ton increases the data security in the cloud environment.
2. The proposed model comprises the parity metadata for the database management provision to the provider.
3. In the developed encoder chunks parity is not stored within the single resources with the provision of the available information chunks.
4. The constructed security architecture in the RAID layer increases the dependability of the data with the deployment of the RAID 10 deployment. The developed RAID-based encoder chunks exhibit improved efficiency for the higher uptime at a minimal cost.

This present paper is organized as follows: In section 2 the research background for cloud computing is presented. The materials and methods involved are presented in section 3 is explained followed by the proposed architecture in section 4. The cloud security problem statement is presented in section 5 followed by the description of the results. Finally, the overall conclusion with the proposed model is presented.

2. Research Background

The cloud technology is considered as one of the advanced systems in the data storage system, the network is accessed to store the data in cloud system it can be accessed from any place in the world and at any time using the internet, as this process is made in the network some security concerns need to be checked and so few articles were considered for research are as follows,

The researcher Ibrahim IM. (2021) stated that cloud computing provides huge resources it can be accessed only through the internet for using resources of cloud-like storage, application and other services that need to be managed and scheduled, the main idea of the scheduling is to minimize the time of loss, workload and so on, the author has given the idea of different task scheduling algorithms in cloud computing the comparative analysis is made with these scheduling algorithms.

Wang XV (2017) made research on the recent cloud services like cloud manufacturing and cloud robotics are reviewed, the block-based integrations were developed to integrate with various types of manufacturing methods. The mechanism and frameworks were evaluated using both the machines and robotic applications, it is found that it provides a flexible structure of integrated methodology and is ubiquitous for cloud systems of manufacturing.

Dong L (2017) designed a pre-alarm system based on real-time monitoring using the internet of things and cloud storage. As IoT is an evolving technology that uses various sensors, the cloud is used to predict the state of the phreatic line based on the real-time monitoring process. In this system, the numerical simulation models are established to consider the predicted equations. The main solving method for the key parameters and the pre-alarm process is presented through a case study. It is proved that the pre-alarm system is an efficient and real-time platform for tailings dam stability while using IoT and cloud storage systems.

Santamaria AF. (2019) considered an IoT surveillance system based on a decentralized architecture, in this research the author proposed the novel based method to create decentralized architecture for managing the patrolling drones and cameras using the lightweight protocols in the IoT domain, hence it provides high scalability, feasibility, and security.

Arunarani AR (2019) made a survey based on the task scheduling methods on cloud computing systems. In the cloud clients may use different visualized assets for each task, hence felt that the manual scheduling method will not suit and hence research were made on different task scheduling methods. In the proposed system the survey is taken for task scheduling methods with the metrics which is suitable for cloud environment, it studied various issues which are related to different scheduling process to overcome the limitations, in this paper the survey is made based on three perspectives like methods, applications and the parameters which are based on the measurements and the future issues related to cloud-based on scheduling were identified as the result of survey.

3. Materials and Methods

Every networking or equipment failure at the resource provider site causes information loss; however, information may be restored employing a dispersed integrity system and a Redundant Array of Inexpensive Disks (RAID) is a storing strategy that use multiple hard disks to store data and different method are used for storage are helps in achieving various levels of redundancies. (Dong, L., et al, 2017) Explored how you distribute information over many servers in a way that allows an adversary to disrupt just one connection. Within (Shankar, A., et al, 2021), the fundamentals of the RAID memory technique in clouds computer were covered namely mirroring combination, striping, parity technology, and duplexing, each level uses different algorithms to implement fault tolerance mechanisms. Since it is insufficient for ensuring personal secrecy with clouds computers, cryptography limits alone will not be able to meet the privacy requirements. The idea of disseminating knowledge across several clouds resource provider locations rather than a single main site was put out (Mezni, H., et al, 2018). Admissions level and user interaction level make up the cloud storage framework's architecture. The use of internet storage in conjunction with a personal server was considered.

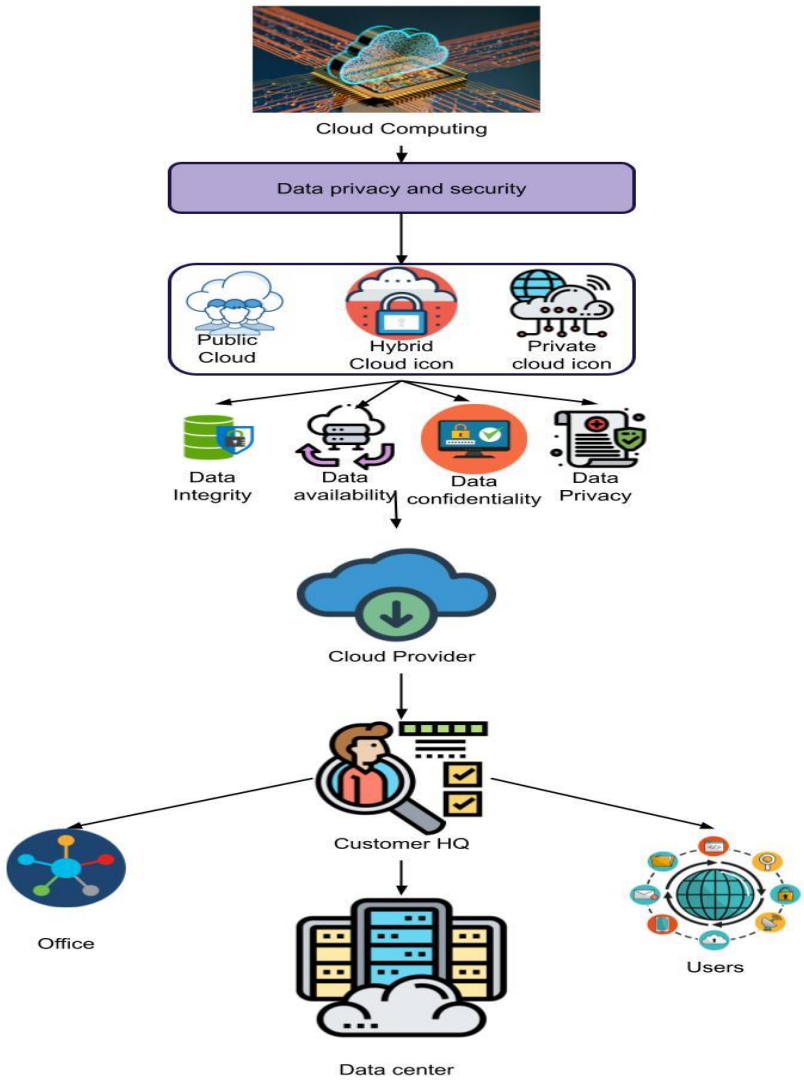


Figure 1 *cloud computing structure*

Figure 1 shows types of cloud computing, and different type of service provided by it. Security provided by cloud computing is because of nearby server or remote server.

(Lee, D., et al, 2018) Proposed internet storing to hide the complexity of equipment and programming from its administrators. The utility and feasibility of the Hadoop-based secret clouds storing system were investigated. Hadoop is the framework based on java that helps to manipulate data in the cloud, as cloud systems cannot manage a huge amount of data thus Hadoop can be used in the cloud to manage big data. Service Level Agreement (SLA) is introduced in (Mushtaq, M. F, et al, 2017) for a uniform baseline for service providers and consumers to ensure data security in cloud storing structures. The architecture to securely keep user data in public clouds or isolated clouds completed using cryptography (Peng, K, et al, 2018) is presented in (Liu, S., et al, 2019). The incorporation of the RAID in the redundant array applied over the independent disks comprises storing data in various places with the multiple hard disks. In case of the drive failure to secure data to improve redundancy and reliability. RAID is considered a standard level with the data striping in the block level between two or more independent disks and the performance of the parity disk evaluation. The evaluation demand for the storing parity data and redundancy. With the implementation and computation of the parity calculation, the datasets are retrieved in the disk when one or more array fails. With the appropriate mirroring, RAID is involved in the copy of data from one disk to another disk with the additional process in the available data from one place to another. The incorporation of the SLA agreement involved in contractual mechanism for holding the service providers for accountable and extraction of payment and penalties.

According to digital computer conceptions of environments of, the security issues in online storing were investigated. Its data load structure is shown in Figure 1, comprising the hosting computer as the client and the resource providers shown as SP1 to SPn.

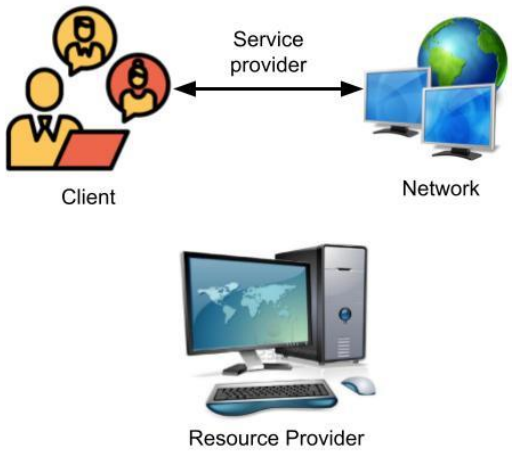


Figure 2: *Framework for Cloud storage*

The above Figure 2 states the cloud storage framework,

- The cloud data transmission process is intiated from the client side where client will sent the request by accessing the internet to the service provides whenever the client is in need of service.
- The request will be received by the service provider through network as there are many service providers the client can choose any of the providers to store huge amount of data which will be easy to retrieve when it is needed.
- In return a response will be sent to the client to use the resource provided by the particular service provider as the whole process takes place with internet the security plays a big constrains.

The clouds computer safety threats & issues, as well as proactive methods which a company may undertake to decrease potential risks and safeguard its assets. They've also gone through the advantages & disadvantages of clouds technology, as well as the areas where it may be used in informational security control. (Garikapati, P, et al, 2021). published a study in which they attempted to assess cybersecurity by first defining individual safety needs and then attempting to propose a feasible answer that removes these possible vulnerabilities. The study recommended the use of a Verified Third Party to ensure safety features in a virtual context (Zekri, M, et al, 2017), To assure the authenticity, authenticity, & secrecy of all related information & interactions, one suggested system uses encryption, especially Public Key Infrastructures working in conjunction with SSO and LDAP. SSO is a process wherein the authentication occurs by a user having the accessibility of multiple systems through a single login. LDAP is a process wherein the authentication of that protocol occurs by using an application that helps in receiving information from the server. This technology provides a horizontal degree of services and was accessible to all involved parties and creates a safety fabric that maintains critical confidence.

(Arunarani, A. R, et al, 2019), warranted the significance and encouragement of safety in heritage scheme migrations, and they conducted an assessment of various strategies to safety in sky migratory procedures intending to identify the necessities, worries, prerequisites, facets, possibilities, and advantages of safety in heritage scheme migrations. (Shaw, S., et al, 2021). offered a classification of safety concerns for Clouds Computer based on the SPI paradigm (SaaS, PaaS, and IaaS), highlighting the more common weaknesses in these platforms as well as the more common dangers reported in the research connected to Clouds Computation and its ecosystem. (Martín-Garín, A, et al, 2018) provided an overview on clouds computer fundamentals and also safety challenges that arise while using clouds computers and public architecture. (Yan, H., et al, 2018) Offered a theoretical examination on information safety difficulties and problems in clouds computers, as well as a discussion on numerous safety problems and problems.

(Latchoumi, T. P, et al, 2019) Provided an overview of many safety challenges like confidence, secrecy, validity, cryptography, key distribution, and asset pooling, as well as the attempts done to address these difficulties. (Jiang, D. et al, 2020), Suggested a regulatory organization structure intending to resolve safety and transparency problems by building relationships between services suppliers and generating information about potential risks depending on existing assaults on similar services suppliers. The Governance Board was in charge of Information Centre management, Policies regulate, regulatory regulate, customer knowledge, efficiency assessment, solutions design, and incentive for the many institutions engaged. The pattern matching in the IDS system need to provide the appropriate signature scheme for the attack and malware environment. With the implementation of the pattern-matching in the IDS performance of system is decreased with the additional overhead in CPU, power and memory.

3.1. Network Security

Concerning providing goods, like digital trade, systems are becoming increasingly complicated. As a consequence, systems are becoming increasingly vulnerable to a variety of complicated safety assaults. The activity which is designed to protect the data's usability and integrity in the network is stated as network security, the effective security system protects the data from various threats which take place in the network. As most of the process is now takes place using the internet the protection of data is considered as the main schema, it might get exploited if not secured properly. Existing safety scheme reactions had also attained one's boundaries in terms of sensing and guarding against numerous internet backbone threats but since existing threats are distributed, digitalized, and smart, and these processes were also silent throughout reaction to connectivity assaults even though users were also restricted to becoming regional; since there is neither automatic vehicle, network-wide reaction to discovered assaults. Several shortcomings of present technologies highlight the need for a fresh era of technologies that are better suited to a fluid context. Developed a dynamic networking technique for dealing with all those needs that has some intriguing aspects, it is the network that gets changed with respect to time. The safety of computing networks is crucial for today's computing technologies.

A variety more computer technologies are now being designed in an attempt to impose high degrees of security from harmful attacks. Because of the capacity to identify and block assaults by hostile network users, an Intrusion Detection System (IDS) is a network security method that is built for detecting vulnerability and lately has become a hot study issue. Regarding networking safety, a pattern-matched IDS was suggested. Routers may help meet the three basic objectives of networking safety: privacy, consistency, and resilience. Routers offer protection through implementing a safety rule to incoming frames, known as safety regulations. The applications raise the number of risks to database safety in firms and companies' day-to-day knowledge platforms concerning their everyday operations, putting them at greater risk of safety attacks. Established a complete networking protection strategy for an internet store that has experienced safety intrusions.

3.2 Cloud Computing

Cloud computing is a technology that uses the internet for storing and managing data on remote servers and then accessing data via the internet. ...

Clouds computers are a concept for providing on-demand internet connectivity to common pools of customizable computer assets (e.g., networking, computers, storage, programs, and functions) that may be quickly supplied and delivered with no administration labor or resource operator contact. The National Institute of Standards and Technology (NIST) in the United States has offered this description National Institute Standards & Technology. Based to Wikipedia, cloud technology is the provision of computation as a service instead of a commodity, in which common facilities, programs, and data are made available to machines and different gadgets across the web. Everything which includes offering housed resources via the Web is referred to as clouds technology. Windows innovation enables internet suppliers to transform one computer into multiple virtualized computers rather than using a monolithic systems design. Cloud computing is the evolving technology that uses the internet for storing data and managing data on remote servers.

Its open clouds enable customers to connect the clouds via browser applications, it can be accessed from anywhere and at any time of requirement. There are four different types of cloud storage systems they are private, public, hybrid, and community cloud storage. Customers must pay only for the time they employ the product, which is known as compensation or pay peruse. This may be likened to the power grid that we have in our houses; the same principle holds. A group's corporate information facility hosts a proprietary computing operation. The key benefit is that safety, management, or updates are simpler to handle, and you have more authority on installation and usage.

3.3 Cloud Storage Architecture

The public ends or rear ends of a cloud's computer platform can be separated. People were all linked to each other via a system, which is generally the computer. The cloud architecture is the process of connecting various technological components to build the cloud system, the resources of the cloud are pooled with virtualization and shared through the network. A user (user) gets a public side, while its rear end is the internet service. Both patient's machine and the interface needed to connect the clouds (Browser) are at the public side, while its rear completion contains clouds computers capabilities such as computation and information storing from numerous locations. The clouds computer systems design is depicted in Figure 3.

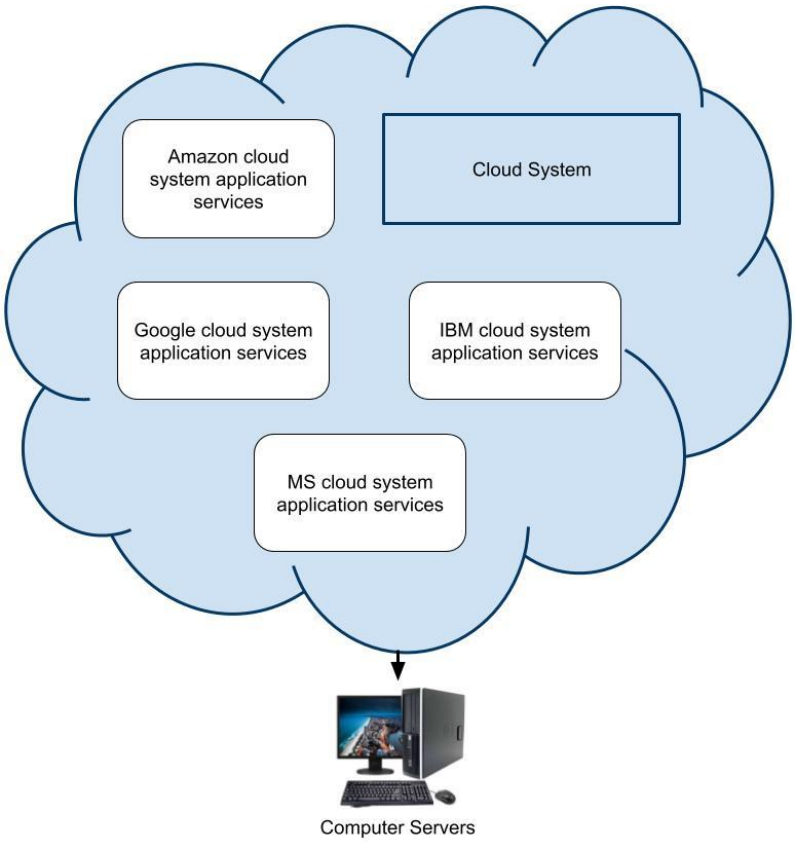


Figure 3: *Framework for cloud storage system*

The Framework of cloud storage system is shown in Figure 3, which is explained as follows,

Step 1: The computer system or client is in the need of cloud service to store, retrieve or transmit data from one point to the other.

Step 2: There are many service providers like AWS, Google cloud, IBM and MS cloud system thus the client can choose any of the service providers and if there is a need for cloud by the client the request will be sent to the cloud by them.

Step 3: Then in return the clients can access all process that are provided by them like data storage, processing, transmission and so on.

The developed model uses the IaaS cloud Service provider for the data security in the cloud network. Clouds computers is a web business model in which consumers employ the web to obtain a variety of products through a Cloud service provider (CSP). Whenever a client connects to a service and begins using its capabilities. However, internet computing seems unconcerned with the safety of the data transferred. These were several stages at which a privacy violation might occur, compromising the accuracy of data. Figures 4 and 5 below show different degrees of safety risks in a virtual system.

Figure 4: *Security in Cloud computing in different levels*

The above figure 5 determines the different levels in security of cloud computing system, it consist of 5 levels

Step 1: The first level is the network security as the entire process takes place in internet it begins with it.
Step 2: The next level is VM security refers to security solutions that are software-based and designed to work within a virtualized IT environment.
Step 3: Third level in cloud security is interface security system as the applications are created on this layer.
Step 4: The four level is Compliance in cloud is to complying to apply the rules and regulation for cloud system.
Step 5: The last state is privacy of cloud helps to reduce the risk of personal data during the process of storing, retrieving, collecting, sharing the data through cloud.

The structure of cloud security levels is stated in Figure 5 is explained as follows,

Step 1: In cloud security the network security is the first level of the process it contains authorized data sharing, Security protocols and information transmission.
Step 2: Next level is VM security level it contains VM management, Virtualization and the VM identifications.
Step 3: Security interface is the third level in cloud security it consists of Admin interface, Secure UI and Secure API.
Step 4: Fourth level in cloud system of security it consists of following process namely audit, service level agreement and the trust management.
Step 5: The final and fifth level of cloud security is privacy system it consists of data privacy, backup, and encryption techniques.

Given a user's perspective, internet computer faces serious safety dangers; in fact, one may argue that security is the single significant downside of internet computer. The pooling of assets was arguably among the most serious safety concerns with the cloud's computer concept. If personal or critical data was kept in a personal cloud, there is a far higher possibility that anyone may read it than most people think. Customers should only share their information or employ the internet company's technology if they are confident in these.

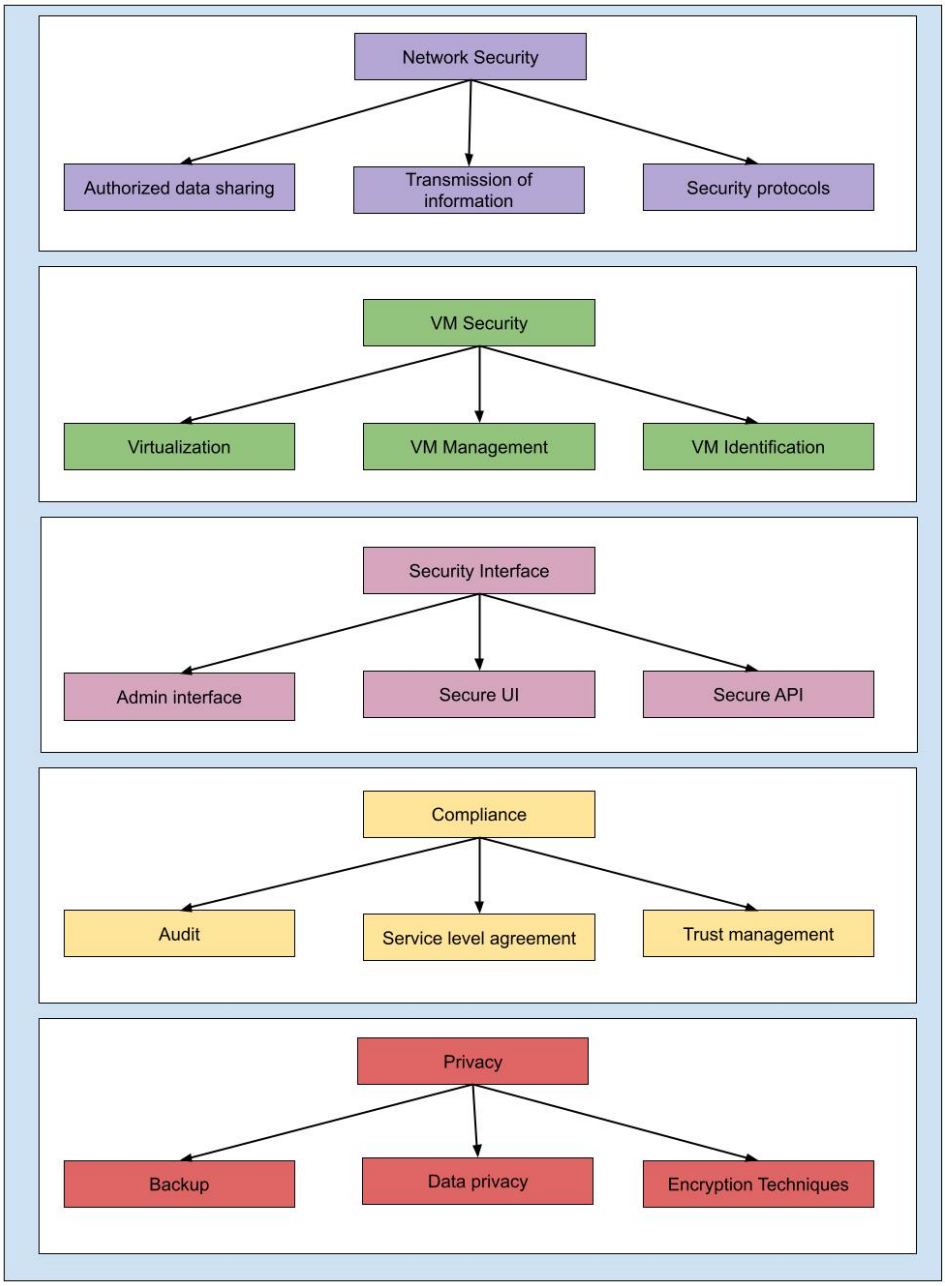
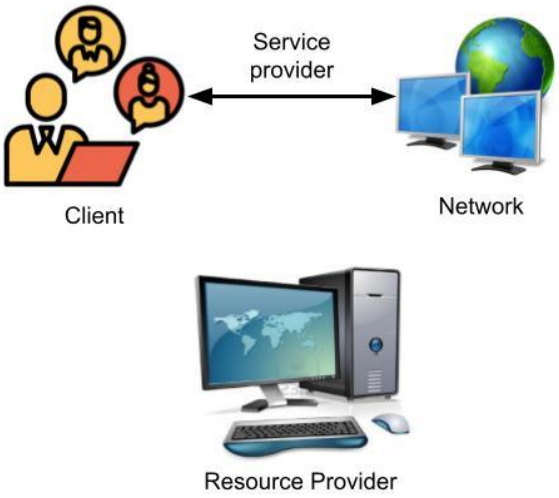


Figure 5: *Cloud security levels*

4. Proposed Architecture

These encoded chunks of communication, as well as the parity metadata connected to the dispersed knowledge, are stored on the knowledge database of the provider. That knowledge parity is not stored on a single resource provider's computer but is scattered across all available services providers to allow for a well actually of information using the available information chunks. Every information server on the services company's facilities would employ RAID layer architecture to improve the data dependability. Depending upon the effectiveness at many RAID levels, RAID 10 is a recommended RAID grade for deployment. The disk stripping is used for the process of data not chunks and hence it is separated across multiple disks. Although its syndicate all best advantages both striped & reflection, RAID 10 generates huge rows that good efficiency for many purposes & higher uptimes. RAID 10 has been theatrically gaining in adoption as hard drives get cheap shown in Figure 5.



A1	A2	B1	B2	P1	P2	G1	G2	C1	C2	D1	D2
E1	E2	R1	R2	F1	F2	S1	S2	H1	H2	R1	R2
T1	T2	T1	T2	J1	J2	U1	U2	K1	K2	L1	L2

Figure 6: *Proposed 6 service provider system*

Figure 6 shows the proposed 6 Service Provider system is determined as follows,

Step 1: The process begins at the client side if the client requires cloud storage, then the request will be sent from the client to the service provider.
Step 2: There are many services provided the client need to select any of the services provided to utilize the cloud service, they are stated as SP1, SP2, SP6.
Step 3: Each service provider contains 3 set of disks like (A1, A2), (E1, E2) and (T1, T2) for SP1 similarly all other providers will contain similar storage disk.

Site processes for business providers, as well as storing and servers' processes regarding information storage, choose Raid level 10. Suppose if (Z) represents all initial information that the customer wishes to save on the internet. The cipher block (Z) is then broken into variation cipher pieces and decrypted to (Z') The dispersed equality approach is employed in this case. Because RAID 10 will be used, the data and fairness chunks were prohibited and displayed individually. SP1's data block A is split into two blocks, A1 and A2, and a mirrored duplicate is also placed. Similarly, the data and equal bans on the websites of further services providers are banned and mirrored. In the RAID 10 packaging scheme shown in Figure 6, an even number of discs is needed.

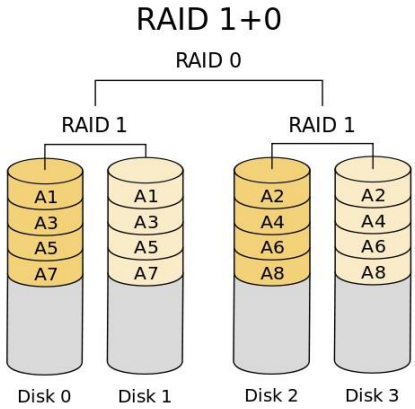


Figure 7: *Storage system with 4 SP with RAID*

Figure 7 determines the storage system with 4 SP with RAID is as follows,

Step 1: The RAID 0 packaging scheme contains the even number of discs that is RAID 0 is divided into two packages for storage purposes.
Step 2: The divided two packages of RAID 0 is again split into even numbers hence it has four packages of RAID 1.
Step 3: The separated RAID 1 package can be again divided and formed eight set of even packages to store data, with 120 GB storage space, it will be helpful in storing large amount of data.

Every disc array has a replica disc array, which is a reflected version of the original. To apply RAID 10, an estimate of 4 floppies is sought. Since double-disc keeps a mirroring duplicate all striping information, it can tolerate single disc failures. It is difficult to retrieve information with RAID 10 in event of a triple-disc loss. As a result, a balance system was included in our suggested design. The RAID 10 storing strategy is seen in Figure 8. Suppose the client information is shared across six services suppliers (SP1, SP2, SP3, SP4, SP5, and SP6). Tetrahedral stores the integrity knowledge (P) of storage blocks (A) recorded in SP1 with (B) recorded on SP2, whereas SP6 stores the integrity material (Q) for data blocks (C) recorded in SP4 and (D) written in SP5. The encryption of data takes place using the Advanced Encryption System [AES] method is a block cipher algorithm in which the data are divided into 128-bit chunks, the data will be converted using key ciphers after the process of encryption the data be joint together to form a ciphertext. The process of encryption plays a vital role in the security of data, in this proposed system the encrypted data will be scattered using the RAID method to provide well security for the cloud system. If any material in reference frames (A) from SP1 or (C) in SP4 is destroyed, material frames (A) or (C) can be rebuilt using other raw frames as illustrated in figure 8.

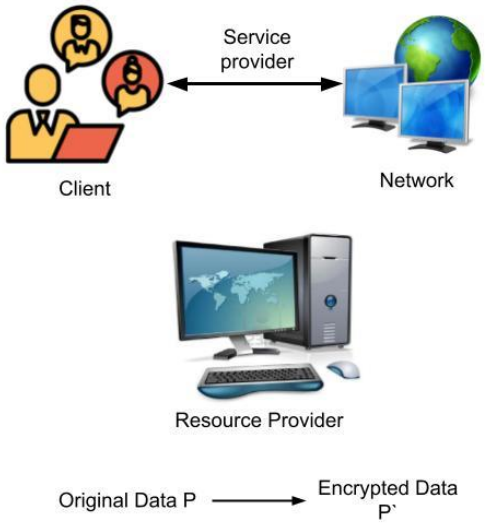


Figure 8: *6 SP's and their parity scheme*

Figure 8 shows the 6 Service Providers and their scheme is stated below,
Step 1: The process begins at the client side if the client requires cloud storage, then the request will be sent from the client to the service provider.
Step 2: There are many services provided the client need to select any of the services provided to utilize the cloud service, they are stated from A - F.
Step 3: The original data is encrypted for the security purpose while accessing the cloud for storage the encrypted data will be stored in the cloud.
As a result, whenever a dual disc fails, its information may be successfully reconstructed using this integrity approach. The system is used to resolve equipment faults and information losses due to

networking difficulties at any services company's location. As a result, the suggested architect's dependability is guaranteed. Even if the system provider is genuine, a large number of malicious users will inevitably cause a safety issue. As a result, essential information such as health or economic information is exposed in an unprotected danger since cloud services company workers have direct contact with the stored information. The danger of a singular source of failures is generated by any singular services company's administration of computer capabilities as a service, and the breakdown can be generated through a variety of factors such as equipment, programming, or networking malfunction. Sometimes providers' trusted data is corrupted or lost, which has an impact on properly retrieving material.

The effectiveness of internet store will be improved by:

- Guaranteeing the safety of data saved in the internet store, & addressing the privacy problem by encryption the underlying information and then dynamically spreading the pieces among many services suppliers.
- Using numerous internet store sources can achieve the principle of accessibility, where in no unique complete duplicate of the information remains in one place and only a fraction of sources is required to rebuild the information.
- The symmetry system achieves the principle of dependability by allowing the program to accurately receive information even if any of the suppliers mistake or lose the provided information.

5. Problem Statement

One of the most important factors for assessing the susceptibility of a clouds computer system is the distribution methodology. According to the American Institute of Standardization and Technologies, there are three service methods (NIST). The three distribution methods are IaaS, PaaS, and SaaS. The IaaS service layer is billed on a per-use basis. Its clouds services company's specialized capabilities are pooled with customers for a price. The infrastructural needs are not linked to the users in this paradigm. Developers may simply shape their applications around the technology that is provided. Nevertheless, on that layer, it takes both the cloud's services supplier and the customer liable for the cloud's safety, creating this layer a divided danger paradigm.

Platform as a service (PaaS) refers to a concept in which a public services company offers both a programming environment and an operational system. It is a pay-per-use approach, similar to IaaS. It is one of the cloud computing models it is provided by third parties but the software and hardware tools can be accessed through the internet, thus the PaaS provider host the software and hardware applications into the cloud infrastructure. The PaaS is often employed by individuals who lack the necessary equipment.

Infrastructure as a service (IaaS) in terms of how risk is distributed among the services supplier and the customer. An internet services supplier becomes primarily responsible regarding safety under this arrangement. This method of computing provides the following services namely compute, store, and utilize the resources of the network only when it is required.

The ultimate distribution paradigm recommended by NIST and adopted by the market is SaaS. These internet services suppliers supply entire end-to-end capabilities in this architecture. It is usually an internet application or a system technology. It is mostly employed by customers who lack the time or skills to construct and manage complete cloud infrastructure. In this instance, the customer is just required for ensuring client privacy; the supplier of the service is liable for the remainder. SaaS allows the user to use cloud-based applications through the internet, it provides the solution based on software that is based on pay as you use from the service providers.

To make the clouds computer systems work efficiently, various safety concerns that exist in each of the levels must be handled meticulously. This clouds computer concept could only be embraced & exploited in its fullest capacity if these safety issues are addressed. To aid address that, a unique strategy for coping against safety concerns has been presented for each of the service types separately as much as the public cloud overall.

6. Description for Security

The following is the suggested safety architecture for maintaining the safety and validity of different clouds computer platforms. Below Service Level Safety: As a firm entering the clouds computer market, impose a stringent first licensing and certification procedure. The industry's history must be confirmed by searching the UDDI (Universal Description Discovery and integration) online register. x Keep an eye on the official watchlist: Allowing registries or untrustworthy services into the clouds from the start is a bad idea. The National Purchasing Regulation Agency, or PPRA, maintains a list of illegal bidders. Keep an eye on credit card theft and unwanted transactions or customers. Upon entering your card's address, an OTP will be issued to the associated cell phone amount. A clear specification of the Service Level Agreement (SLA) is required. At EACH tier, a POP-UP notice should be issued to a user in case event of a safety breach. Credentials for entry should be highly secured. Mechanisms for credentials exchange must be properly established. The API connections between IaaS and PaaS must be properly stated. Networking safety criteria such as data protection, consistency of data, privacy protection, reliability, and foreign denunciation must be met by the IaaS Safety Level. To validate the person attempting to obtain information on the IaaS level, robust identification and permission mechanisms should be employed. To avoid connection swapping assaults, any changes towards a clouds storage company's URL should be communicated to all internet users. At periodic intervals, perform vulnerabilities scans and setup audits for the IaaS layer. Recovery and preservation techniques must be implemented regularly. PaaS Safety Coat: Use a two-stage authentication method to get access to PaaS applications. To prevent individuals or companies from exchanging account information. Improper behavior is detected by close monitoring. For a component of the SLA, identify people resources needs. The API connecting PaaS and SaaS must be described correctly. Comprehensive data safety and governance policies, as well as adherence monitoring, must be transparent. A layer of security for SaaS: Appropriate encrypting mechanisms are required to guarantee data secrecy. The user's mechanisms are designed or impersonating must be avoided. Information separation must be done with extreme caution. x All API requirements must be documented precisely. x Real-time POP-UP notice in the event of a safety incident. The following is a diagrammatic depiction of our prototype:

The security model of the cloud exhibits significant performance in the SaaS layer with the user privacy and data corporate upon the cloud subscription. As the SaaS layer comprises of a huge amount of sensitive data those needs to be protected with sensitive information with an appropriate privacy scheme. With the use of PaaS layer responsible communication between the service provider and customer is developed. The PaaS layer in the network is responsible for the maintenance of the user access, record maintenance and records in the physical infrastructure. IaaS layer provides the heavy information maintenance to manage the cloud environment those need to be accessible easily. Figure 9 states the cloud computing security model the security of each model is checked, the step-by-step explanation of the system is as follows,

Step 1: As the protection of each layer is important, the analysis is made for each layer of cloud-like IaaS, PaaS, and SaaS.
Step 2: At first the IaaS is checked for the security constraints of data by employing robust identification and permission mechanisms in the layer.
Step 3: Next after determining the data protection in the IaaS layer the process moves to PaaS to verify the security of this system, two-stage authentication mechanism is used.
Step 4: The security of SaaS is analyzed using an encryption mechanism the security of data is determined in this layer.

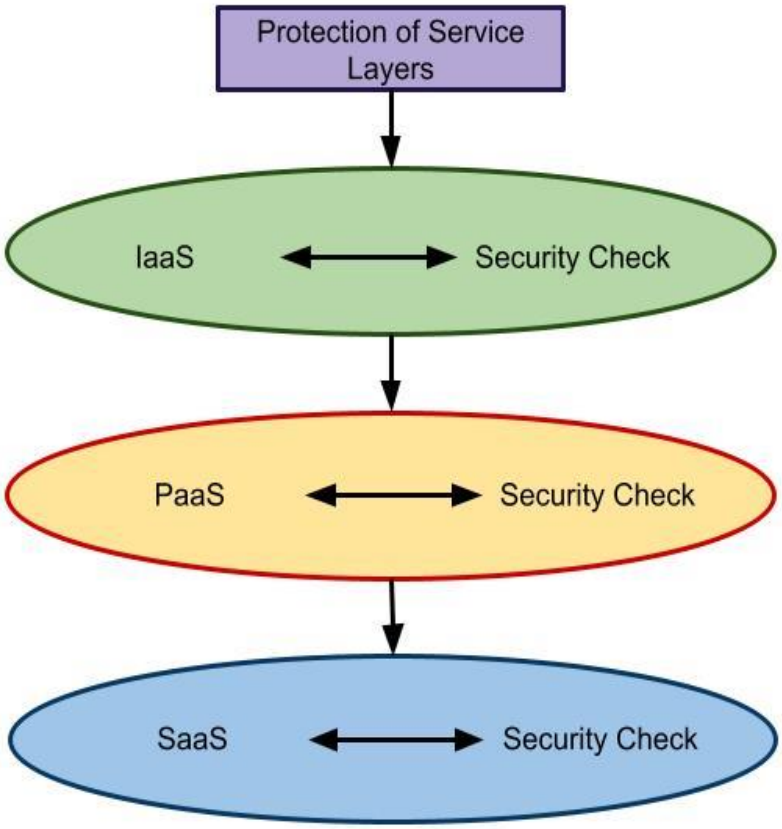


Figure 9: Cloud Computing Security Model

Table 1. *network security*

Factor Authentication	**Device Protections**	**User Security**
20	5	120
25.56	16.9	40.79133
30	27.5	8.695652
35.67	31.2	13.36922
40.67	38.3	6.002279
45.815	41.5	9.883754
50.96	47.6	6.818182

Table 1 shows, network security, in this table representation based on factor authentication, device protections and user security.

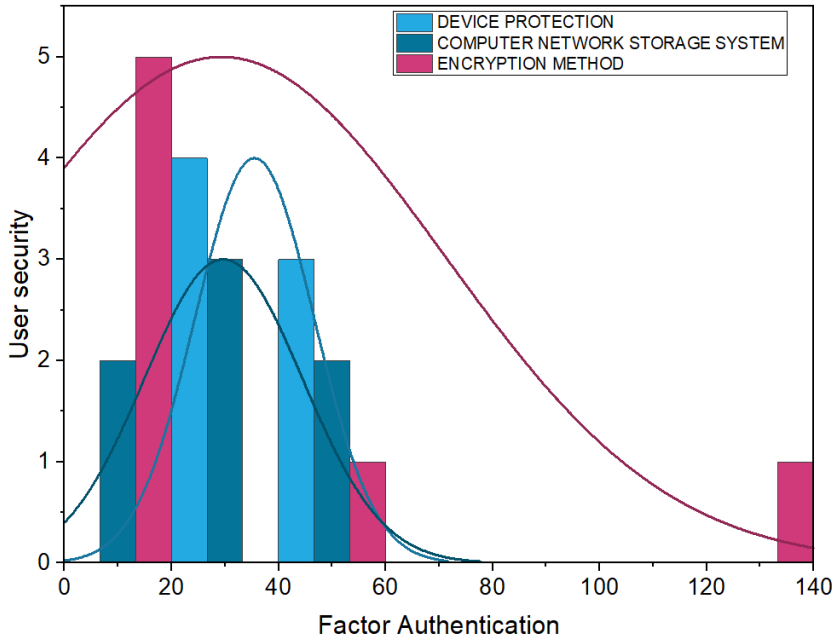


Figure 10. *network security*

Figure 10 shows, network security, in this graphical representation based on factor authentication, device protections and user security.

Table 2. *encryption method*

Data size	**Time**
12.5	0.5
20.3	1
28.1	1.5
35.9	2
43.7	2.5
51.5	3
59.3	3.5

Table 2 shows, encryption method, in this table representation based on data size and time.

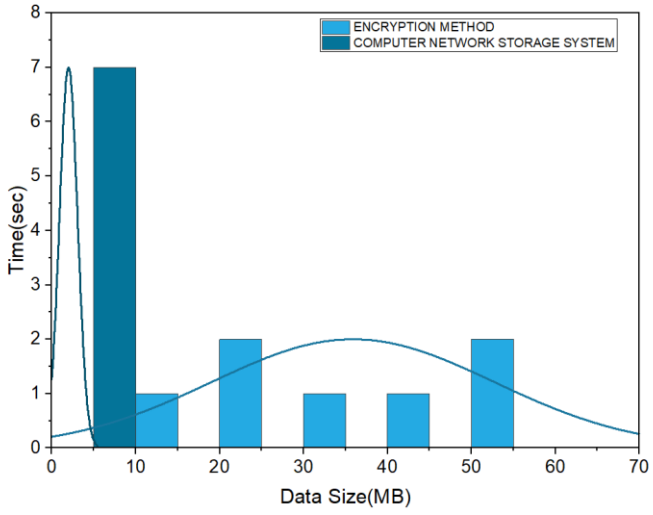


Figure 11. *encryption method*

Figure 11 shows, encryption method in this graphical representation based on data size and time.

Table 3*. cloud storage system*

File size	Time	Impression
3.67	0.5	25.6
15.78	1	32.8
27.89	1.5	40
40	2	47.2
52.11	2.5	54.4
64.22	3	61.6
76.33	3.5	68.8

Table 3 shows, cloud storage system, in this table representation based on file size, time and impression.

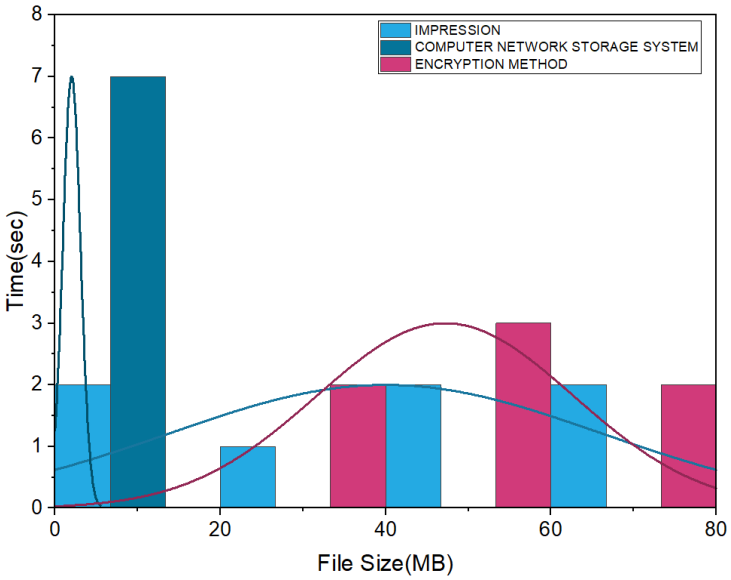


Figure 12. *cloud storage system*

Figure 12 shows, cloud storage system, in this graphical representation based on file size, time and impression.

Table 4. *traditional storing solution*

Drive	Dropbox
3.61	3.04
3.86	2.67
2.5	3.36
99.2	34.3
2.94	1.64
1.56	1.12
0.91	6.9

Table 4 shows, traditional storing solution, in this table representation based on, drive and dropbox.

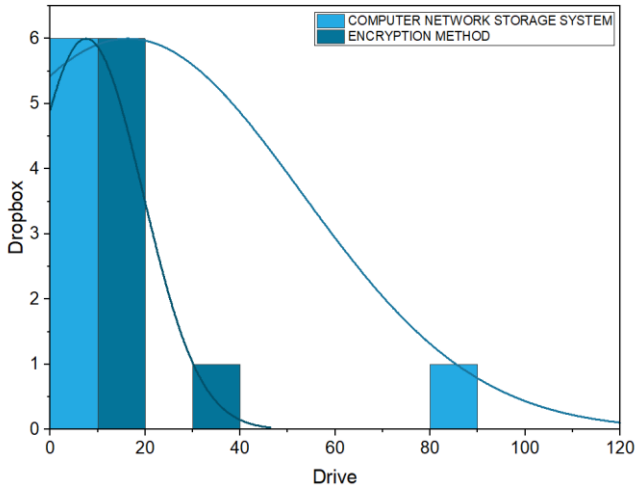


Figure 13. *traditional storing solution*

Figure 13 shows, traditional storing solution in this graphical representation based on, drive and drobox.

Table 5. *task scheduling methods*

Processor	Speed up
12.5	25.6
20.3	32.8
28.1	40
35.9	47.2
43.7	54.4
51.5	61.6
59.3	68.8

Table 5 shows, task scheduling methods, in this table representation based on processor and speed up.

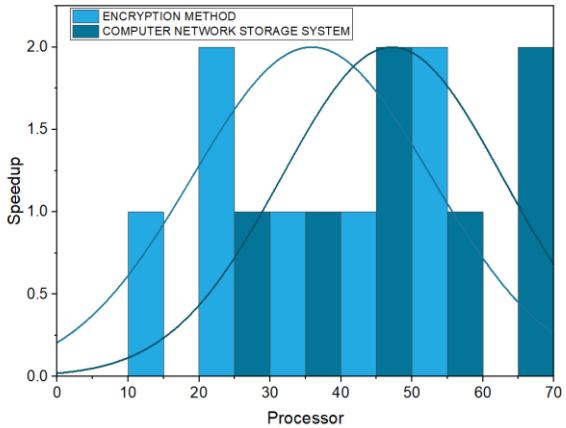


Figure 14. *task scheduling methods*

Figure 14 shows, task scheduling methods in this graphical representation based on processor and speed up.

7. Discussions and Conclusion

The suggested method encodes material and separates it into cipher pieces. The encryption pieces are then distributed throughout the available services company's websites. The decryption procedure would be carried out using this Advanced Encryption Standard (AES). AES is a cryptographic method that may be used to safeguard digital data. This technique was symmetrical in that it may apply both encrypting and decoding operations to user data. The encrypting system transforms client data to an unreadable version known as cipher-text, which may then be decrypted back into normal. This technique may be used with three different main ranges: (AES-256), (AES-192), or (AES-256) (AES-128). In addition to being employed as safety, the AES method may also be employed as exorbitant performance. Despite all of this, all software and hardware apps remain quicker.

Rather than keeping the entire material at one particular phone company site, then the safety of the data may be assured by dispersing their operator's data across available services suppliers. Assume that consumer data (F) will be obtained from external resources. With a shared file arrangement, all of the information is kept on a single services provider. As a result, data will not be secure under this arrangement. According to the safety viewpoint, initial data (F) will be encoded to (F') and then split down into cipher components (A, B, C, and D) in the suggested design. Assume there are 4 public cloud providers to choose from SP1, SP2, SP3, and SP4. This encoded data was distributed across services providers, with the cipher component (A) being saved in SP1, (B) being stored on SP2, (C) being stored on SP3, and (D) being saved on SP4. The memory in the suggested design is RAID 10. Parts (A, B, C, and D) are stripes and duplicated as a result (A: A1, A2, B: B1, B2, C: C1, C2, D: D1, D2).

It's vital to remember that data saved on a particular services supplier's system can be restored. Moreover, clouds services companies may work collectively to retrieve and restructure the information held by their clients. Both the decryption and transmission procedures are carried out in this suggested design, with the understanding that data reconstruction is difficult, even if a couple of service providers (A and B) or (C and D) plot against one other, making the suggested design secure. Information retrieval will be possible if the information saved on any storing media is duplicated, and is dependent on the speed of retrieval. The collected information influences the networking train's capacity. As a result, elevated internet links are used to access the data.

Within that subject or clouds computer safety, here exist several real issues to be resolved. Consumers would stand in quandary about how or never are they using this cloud's computers paradigm with networking apps unless and until a strong answer was developed. As a result, our study has developed a safety paradigm that gives a resolution at both the macroeconomic and microscopic levels. It is a type of comprehensive safety solution which operates just on various distribution tiers as much as the entire network. As a result, it could offer a complete safety solution to address cloud services challenges. The following step is to put the concept that was developed and described in the previous article into reality.

Conflict of interest

There is no conflict of interest among the authors**.**

References

[1] Arunarani, A. R., Manjula, D., & Sugumaran, V. (2019). Task scheduling techniques in cloud computing: A literature survey. Future Generation Computer Systems, 91, 407-415.

[2] Bui, D. M., Yoon, Y., Huh, E. N., Jun, S., & Lee, S. (2017). Energy efficiency for cloud computing system based on predictive optimization. Journal of Parallel and Distributed Computing, 102, 103-114.

[3] Chen, J., Li, K., Rong, H., Bilal, K., Yang, N., & Li, K. (2018). A disease diagnosis and treatment recommendation system based on big data mining and cloud computing. Information Sciences, 435, 124-149.

[4] Dong, L., Shu, W., Sun, D., Li, X., & Zhang, L. (2017). Pre-alarm system based on real-time monitoring and numerical simulation using internet of things and cloud computing for tailings dam in mines. IEEE Access, 5, 21080-21089.

[5] Ezhilarasi, T. P., Dilip, G., Latchoumi, T. P., & Balamurugan, K. (2020). UIP—A Smart Web Application to Manage Network Environments. In Proceedings of the Third International Conference on Computational Intelligence and Informatics (pp. 97-108). Springer, Singapore.

[6] Garikapati, P., Balamurugan, K., Latchoumi, T. P., & Malkapuram, R. (2021). A Cluster-Profile Comparative Study on Machining AlSi 7/63% of SiC Hybrid Composite Using Agglomerative Hierarchical Clustering and K-Means. Silicon, 13, 961-972.

[7] Ibrahim, I. M. (2021). Task scheduling algorithms in cloud computing: A review. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(4), 1041-1053.

[8] Jiang, D. (2020). The construction of smart city information system based on the Internet of Things and cloud computing. Computer Communications, 150, 158-166.

[9] Latchoumi, T. P., Balamurugan, K., Dinesh, K., & Ezhilarasi, T. P. (2019). Particle swarm optimization approach for waterjet cavitation peening. Measurement, 141, 184-189.

[10] Lee, D., Park, N., Kim, G., & Jin, S. (2018). De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment. Peer-to-Peer Networking and Applications, 11(6), 1299-1308.

[11] Goar, V. . (2022). 6LoWPAN in Wireless Sensor Network with IoT in 5G Technology for Network Secure Routing and Energy Efficiency. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 15–25.

[12] Liu, S., Guo, L., Webb, H., Ya, X., & Chang, X. (2019). Internet of Things monitoring system of modern eco-agriculture based on cloud computing. IEEE Access, 7, 37050-37058.

[13] Martín-Garín, A., Millán-García, J. A., Baïri, A., Millán-Medel, J., & Sala-Lizarraga, J. M. (2018). Environmental monitoring system based on an Open Source Platform and the Internet of Things for a building energy retrofit. Automation in Construction, 87, 201-214.

[14] Mezni, H., & Abdeljaoued, T. (2018). A cloud services recommendation system based on Fuzzy Formal Concept Analysis. Data & Knowledge Engineering, 116, 100-123.

[15] Tume-Bruce, B. A. A. ., Delgado, A. ., & Huamaní, E. L. . (2022). Implementation of a Web System for the Improvement in Sales and in the Application of Digital Marketing in the Company Selcom. International Journal on Recent and Innovation Trends in Computing and Communication, 10(5), 48–59.

[16] Khatri, K. ., & Sharma, A. . (2022). Energy Harvesting based Mobile Cloud Network in Latency and QoS Improvement using 5G Systems by Energy Routing Optimization. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 26–39.

[17] Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud computing environment and security challenges: A review. International Journal of Advanced Computer Science and Applications, 8(10), 183-195.

[18] Joy, P., Thanka, R., & Edwin, B. (2022). Smart Self-Pollination for Future Agricultural-A Computational Structure for Micro Air Vehicles with Man-Made and Artificial Intelligence. International Journal of Intelligent Systems and Applications in Engineering, 10(2), 170–174.

[19] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. Computer Communications, 151, 539-547.

[20] Chawla, A. (2022). Phishing website analysis and detection using Machine Learning. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 10–16.

[21] Ananthakrishnan, B., Padmaja, V. ., Nayagi, S. ., & M, V. . (2022). Deep Neural Network based Anomaly Detection for Real Time Video Surveillance. International Journal on Recent and Innovation Trends in Computing and Communication, 10(4), 54–64.

[22] Peng, K., Leung, V., Zheng, L., Wang, S., Huang, C., & Lin, T. (2018). Intrusion detection system based on decision tree over big data in fog environment. Wireless Communications and Mobile Computing, 2018.

[23] Pereira, R. I., Dupont, I. M., Carvalho, P. C., & Jucá, S. C. (2018). IoT embedded linux system based on Raspberry Pi applied to real-time cloud monitoring of a decentralized photovoltaic plant. Measurement, 114, 286-297.

[24] Qi, Q., & Tao, F. (2019). A smart manufacturing service system based on edge computing, fog computing, and cloud computing. IEEE Access, 7, 86769-86777.

[25] Paliwal, R. ., & Khan, I. . (2022). Design and Analysis of Soft Computing Based Improved Routing Protocol in WSN for Energy Efficiency and Lifetime Enhancement. International Journal on Recent and Innovation Trends in Computing and Communication, 10(3), 12–24.

[26] Salhaoui, M., Guerrero-González, A., Arioua, M., Ortiz, F. J., El Oualkadi, A., & Torregrosa, C. L. (2019). Smart industrial iot monitoring and control system based on UAV and cloud computing applied to a concrete plant. Sensors, 19(15), 3316.

[27] Santamaria, A. F., Raimondo, P., Tropea, M., De Rango, F., & Aiello, C. (2019). An IoT surveillance system based on a decentralised architecture. Sensors, 19(6), 1469.

[28] Shankar, A., Pandiaraja, P., Sumathi, K., Stephan, T., & Sharma, P. (2021). Privacy preserving E-voting cloud system based on ID based encryption. Peer-to-Peer Networking and Applications, 14(4), 2399-2409.

[29] Shankar, A., Pandiaraja, P., Sumathi, K., Stephan, T., & Sharma, P. (2021). Privacy preserving E-voting cloud system based on ID based encryption. Peer-to-Peer Networking and Applications, 14(4), 2399-2409.

[30] Shaw, S., Rowland, Z., & Machova, V. (2021). Internet of Things smart devices, sustainable industrial big data, and artificial intelligence-based decision-making algorithms in cyber-physical system-based manufacturing. Economics, Management and Financial Markets, 16(2), 106-116.

[31] Tian, Z., Shi, W., Wang, Y., Zhu, C., Du, X., Su, S., ... & Guizani, N. (2019). Real-time lateral movement detection based on evidence reasoning network for edge computing environment. IEEE Transactions on Industrial Informatics, 15(7), 4285-4294.

[32] Wang, X. V., Wang, L., Mohammed, A., & Givehchi, M. (2017). Ubiquitous manufacturing system based on Cloud: A robotics application. Robotics and Computer-Integrated Manufacturing, 45, 116-125.

[33] Xu, B., Xu, L., Cai, H., Jiang, L., Luo, Y., & Gu, Y. (2017). The design of an m-Health monitoring system based on a cloud computing platform. Enterprise Information Systems, 11(1), 17-36.

[34] Xu, K., Zhang, W., & Yan, Z. (2018). A privacy-preserving mobile application recommender system based on trust evaluation. Journal of computational science, 26, 87-107.

[35] Yan, H., Li, X., Wang, Y., & Jia, C. (2018). Centralized duplicate removal video storage system with privacy preservation in iot. Sensors, 18(6), 1814.

[36] Zekri, M., El Kafhali, S., Aboutabit, N., & Saadi, Y. (2017, October). DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd international conference of cloud computing technologies and applications (CloudTech) (pp. 1-7). IEEE.