e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 10, October 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

Examining Cloud Computing Data Confidentiality Techniques to Achieve Higher Security in Cloud Storage

Pankit Arora[1*], Sachin Bharadwaj[2]

Manager, Allowance & Loss Forecasting, National Money Mart Company, Canada[1]

Assistant Manager (IT Audits), MetLife GOSC, India[2]

ABSTRACT: Cloud computing is an emerging economical approach that allows businesses to move beyond creating their own IT teams towards outsourcing their applications, systems, including infrastructure requirements. Cloud technology was already emerged as a framework in addition to the fifth infrastructure services, after water, energy, fuel, and telecommunications. Moreover, the IT sector is undergoing a fundamental transition. Earlier, businesses would maintain existing operations by purchasing IT equipment, but then they are implementing technology on top of that architecture. Cloud computing is a paradigm wherein IT technology is rented as well as utilized as needed by the organization. This paper describes a comprehensive investigation of data confidentiality approaches in cloud technology, their limitations as well as various strategies for overcoming them.

KEYWORDS: Cloud computing, Data confidentiality, Threats, SaaS, PaaS, IaaS

I. INTRODUCTION

According to Forrester, cloud technology would be standardized IT capabilities including applications, technology, and architecture that would be supplied through Internet technologies in a cost-based, self-service model. The above would exclude the infrastructure component of the cloud computing concept. It indicates that it cannot distinguish between PaaS as well as IaaS. Moreover, this is unclear exactly what people imply as a self-service method.

Cloud computing is defined by the 451 Community as a communication approach that incorporates a particular organizing principle for IT delivery, network equipment, a structural framework, and an economic system - essentially, a synthesis of distributed systems, connectivity, virtual servers, hosting, and software as a service (SaaS). The above definition establishes a crucial difference between Distributed systems and virtualization and many other Internet programming approaches. This difference is highly important since it offers insights into Grid computing's effect on Cloud technology.

Cloud technology emerged as the gradual development of Distributed systems, however, it was argued if it provides something innovative or is simply a repackaging of existing concepts. Cloud technology shares the same ambition as Distributed systems: to lower processing costs, boost dependability, and improve flexibility by changing computer systems to become something users purchase from a third party and afterward charge per usage. Another of the primary distinctions between commercial cloud computing models and distributed systems is the fact that the cloud is visible to customers and developers, while the grid is task-oriented. In cloud technology, anybody may go digitally and have access to massive computing capabilities while just paying for the services they require. The emphasis in distributed systems is on projects. Customers or a network may enroll in Grid projects to contribute or manage resources based on their needs. All around the globe, there has been a movement to build a Grid economy utilizing Grids. The Infrastructure will provide applications like resource trade, negotiations, and distribution.

Several Grids employ a batch model for resource planning, in which users submit group tasks. These group tasks are added to a stack. The tasks are done in accordance with both the customer's specifications, for instance, the work will perform on 100 CPUs for one hour. The Cloud computing batch paradigm differs in that tasks are done simultaneously and customers share information. This raises privacy protection and remote access privacy concerns, including information leaking to unauthorized individuals.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

Virtualization is used in cloud technology to create abstractions and encapsulate them. By building a network of computing, memory, and networking devices, virtualization gives the appearance that multiple users' workloads are operating at one time. Grids allow all contributing companies to retain complete power above their capabilities (through not virtualizing these), hence they rely very little on virtualization than Cloud technology. Because an organization has total power over its assets in Distributed systems, the safety requirements created to meet the objectives of Distributed systems vary from those used in Cloud technology. The data controller loses track in Cloud technology since no precise control is accessible whenever information is hosted on the Cloud platform. This shift raises security problems regarding compliance with regulations, termination of access privileges, the confidentiality of information, remote access, and other issues [1-5].

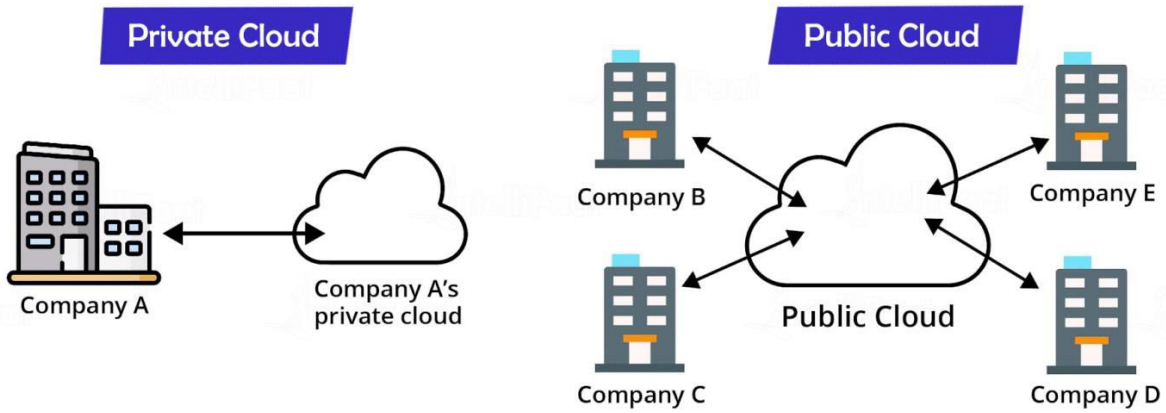

Figure 1. General data storage infrastructure in the cloud

In several aspects, cloud computing differs from distributed systems. The two types of technology have fundamentally different organizational models. Cloud technology is available on a cost basis, while Grid computing is available as a program. Furthermore, Cloud technology distribution methods (SaaS, PaaS, IaaS) vary unlike Grid computing deployment models that are centered on computing power. The above distinctions see an influence on Cloud computing environments and also address the dangers to Cloud technology in further depth.

The general data storage structure is depicted in Figure 1. After discussing cloud computing Technology and the way it varies from Distributed systems, one has to understand Cloud technology from a technological standpoint. The cloud includes five important properties that distinguish it from previous forms of computation. On-Demand Self-Service allows customers to access cloud-based services that do not necessitate human involvement among customers and cloud service providers (CSP). Broad network connection and high-bandwidth transmission media are required for connecting to web services.

Accessibility to a huge pool of computational resources is made possible through high-bandwidth internet connectivity. A multi-tenant approach is used to share computational services to satisfy several customers, with distinct hardware and virtual resources being allocated as well as reallocated based on the user's need. Nevertheless, such capabilities may be practically situated anyplace within the regions of the world and allocated as control factors as required. Flexibility allows additional units to be introduced or removed from the system in the same way as computer systems can, including very minor changes to both software and hardware.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

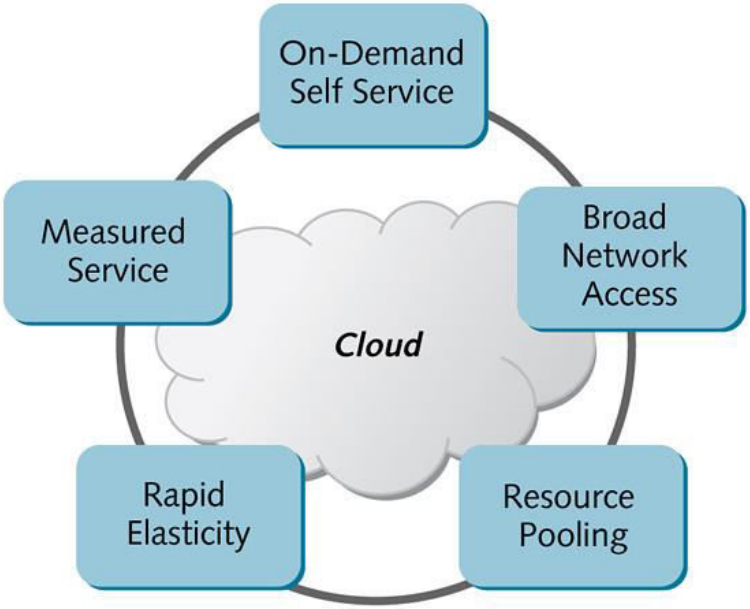

Figure 2. Cloud Technology Features

As per customer requirements, cloud infrastructure may grow either horizontally or vertically. Measurable Performance, customers are periodically invoiced depending on how they use cloud systems. Cloud platforms regulate and optimize energy use autonomously by exploiting meter capabilities at a certain degree of abstraction suited to the specific type of activity [6-8]. Figure 2 depicts the cloud computing capabilities with these levels. According to the Cloud Security Alliance, a cloud is divided into seven layers such as (1) The Facility, (2) The Network, (3) The Hardware, (4) The Operating System, (5) The Middleware, (6) The Application, and (7) The User levels. These levels may be managed by CSPs or data consumers [9].

(A) The Facility Layer

Physical safety is guaranteed by the facility layers. Protecting but also managing direct access to computer equipment must be given top importance. Security management supervision must include confined camera systems and mobile security personnel, a burglar alarm, administrative monitoring, authorization, legal agreements, security clearances, and guest accessibility. Furthermore, operational safety must be sufficient to protect the cloud infrastructure from whatever variety of physical threats.

(B) The Network Layer

The operator provides consumers with network connectivity to acquire client information stored in the cloud via the World wide web. As a result, intrusion prevention technologies must gather data on networking security alerts. The provider has the responsibility for maintaining, monitoring, as well as auditing routing statistics. In addition, the user must demand such assessments for confirmation.

(C) The Hardware Layer

Because consumer uses virtual servers for accessibility, the provider must ensure that its infrastructure is tamper-proof. The operator must have proper procedures in place that analyze underlying topologies of the connections, storage capacity, transit rates, CPU demands, hard disks, and other factors.

(D) The Operating System Layer

Protecting the server OS is indeed a critical aspect to think about in a cloud domain. The information of the customers will be affected if it was handled by different individuals. The supplier must implement an operating system that detects gaps in security strategy and design as well as stop potential intrusions.

(E) The Middleware Layer

Gateway includes virtualized monitoring tools, data type translation, safety functionality execution, as well as user access administration. The gateway acts as a go-between for the operating system and the apps. It is responsible for

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

monitoring and securing interactions between various networks. As a result, the service vendor must verify that such a gateway accepts or transmits exclusively digital signals while protecting it from unauthorized tampering.

(F) The Applications Layer

The software is offered to the public like a utility by the providers. As a result, potentially destructive individuals may have the code available to them. As a result, secure programming and secured application development must be taken into account. Users must choose apps where the original data or functionality could be thoroughly inspected for any problems by independent third parties. In addition, internet programs must be appropriately monitored for discovering infractions. The provider must implement better security restrictions inside the application level on a large scale.

(G) The User Layer

There are two categories of cloud services such as internet software service consumers and also members of organizations. The first utilizes data in the cloud in an unbalanced area, whereas the latter gathers information with security practices. Accessibility characteristics, on the other hand, could be checked for hostile activities. Google Apps, for instance, analyzes authentication behavior including the date as well as IP address, making this data visible to the same users, and warning them of abnormal conduct.

This concept might be expanded to provide IT administrators with fragments of similar warnings concerning the credentials over which the respective organization is accountable. Furthermore, the client may have access to sensitive information in open places. Due to various negligence, authorized individuals may destroy several access controls with a few taps, and web applications contain several flaws that may be exploited. As a result, client instruction is the most effective method for preventing these issues inside a cloud architecture.

II. DATA MANAGEMENT IN THE CLOUD

Information management is an essential feature in businesses. Businesses would like to take advantage of such cloud architecture, outsourcing the information to cloud-based data providers, as well as obtaining the files over the network [10-13]. Database as a Service (DaaS) is the term referring to this information management concept (Figure 3).

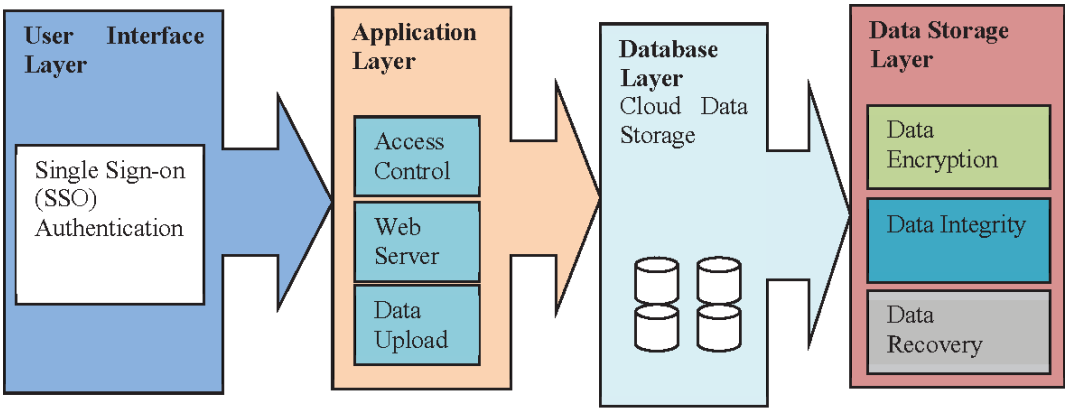

Figure 3. Cloud Database as a Service (DaaS)

One of the largest and most prominent implementations of such SaaS methodology is DaaS. The DaaS concept provides numerous advantages for businesses, including lower information administrative expenses and also more consistent hosting. Inside this DaaS paradigm, organizations save information over the internet inside a repository which is controlled mostly by Providers' Data Base Administrators (DBA). DBA required absolute authority over databases in order to fulfill DBA obligations including backup files, system restoration, as well as data restoration mostly in the instance of a crash, in addition to accomplishing computer performance and optimization. Such a condition generates two forms of assaults upon the cloud environment: cyberattacks by CSPs and cyberattacks from other internet customers. While the DaaS approach seems appealing, it is neither viable since such DBA could analyze the evidence and pass enterprise information to opponents.

2.1. Outsourced Data Confidentiality

Information that is transferred to clouds is also not retained on a particular cloud-based storage server. This is duplicated by other internet computer servers situated all over the world. Cloud servers were overseen and managed by

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

a variety of CSP professionals. Information from whatever data center could be exploited. The main consideration with cloud computing is protecting information secrecy. The guarantee ensuring confidential material will never be revealed to unauthorized people, procedures, and technologies are characterized as privacy. As a result, this should ensure that such customers' private information, wherein the consumers would not like CSPs can acquire, is still not exposed to CSPs in cloud-based computing systems such as programs, interfaces, CPUs, as well as actual storage.

It should be highlighted as consumers' sensitive information is just revealed to a CSP when all three of such following criteria are met at the very same time: The CSPs recognize where their customers' sensitive information is situated in cloud-based systems. The CSPs always had the power to view and acquire the consumers' private information in the cloud computing environments. In order to acquire customer information, these three criteria listed previously must be met. CSPs have to be conscious of the location of information stored in cloud services and also have access to that information. Table 1 enumerates the assessment of several data confidentiality approaches.

Table 1. The comparison of several data confidentiality strategies

Algorithms	Performance	Advantage	Disadvantage
Public auditing scheme, Dynamic hash table	A new 2-dimensional data format was utilized for verifying the data for dynamic auditing	Reduced computation costs and communication overheads	Need to be exploited further for performing multiple audit tasks parallelly
Entropy-based methods, Bell-Lapadula model	Deploying workflow applications on federated cloud	Highly secure and lesser expensive	Computational overhead
Cluster content caching	Improved data availability by integrating centralized cloud with client-centric storage features	High availability and reduced costs	-

III. ANALYSIS OF THE LITERATURE

Several researchers have presented various strategies for dealing with security considerations. It is needed to look somewhere at comprehensive literature activities undertaken by cybersecurity scholars in this field [14-21].

A threat intelligence system was developed in 2017 to predict potential threats within cloud-based systems. Potential methodologies as well as procedures for malware detection and internal threats have also been studied. MUSA EU is offered as just a security framework that monitors applications installed across multi-cloud environments inside cloud infrastructure systems. Variations in web server contracts were identified by the suggested technique to safeguard its heterogeneity framework from any threats. These outcomes are promising.

As in the publication concerning smart cryptographic algorithms for safe networked big data storage in cloud applications, the research highlighted issues of privacy and security in cloud applications encountered by public entities and important corporate enterprises. The above studies concentrated on using ingenious encryption to safeguard information provided by cloud owners. The file systems are separated as well as maintained in several sites in a decentralized system. Information theft is far less likely as a result. An additional approach to determining whether the information splitting is necessary had also been offered, as it requires additional process time. Security-Aware Efficient Distributed Storage is the model's name (SA-EDS). Numerous techniques have been considered when developing the framework. The strategy has produced positive performance concerning the information storing safety and performance inside the clouds. The computational complexity is better when compared to other conventional technologies.

The researchers presented a cloud service model that demonstrated the need for any organization and government agency to data loss prevention hosted in the cloud environment and ensure accuracy. To counteract DDoS attacks, the researcher presented an effective technique for collecting information using cryptographic technologies. The method used was a sophisticated computation, making it impossible for intruders to forecast how to break into the cloud

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

environment. For information protection, two approaches were suggested decryption and encryption techniques. Several technological innovations, such as Big Data as well as the Internet of Things, are encountering security risks that can be handled by the suggested technique.

The researchers suggested secured big data storing, verification, and auditing (SecSVA) in a cloud context. This technique contains an attribute-based duplication architecture in cloud-based storage, information identity management, and authorization dependent on the Kerberos procedure, as well as a Hash tree-based technique in transferring information over onto clouds so as to avoid unprotected Application Programming Interfaces (APIs). According to the critique's assessment, the suggested model could also provide reliable audits with authenticity in any cloud domain.

Research provides a methodology for data dissemination and storage safety in a multi-cloud context. The researcher created a working model to prevent serious problems resulting from internal or external intruders obtaining essential patient medical as well as private data, as well as to protect security and privacy, integrity, and integrity. To prevent purposeful or accidental security vulnerabilities in the cloud, a unique solution labeled block-based vulnerability management employing the Galois field is used to secure system information in a multi-cloud context. Amazon Simple Storage Service (S3) and Dropbox were used to represent many clouds. The findings indicated vulnerability management effectiveness as well as an effective way of encrypting and decrypting against intruders.

Studies found a client-server management software for providing secure applications in the cloud, which ensures the security and integrity of the information located in the cloud databases from cyberattacks. Various investigations have been conducted to check security and privacy utilizing web-based applications in an authentic multi-cloud context. The responsiveness, commencement, and completion period of the user's query for downloading and uploading information from either the cloud are all measured to determine effectiveness. It has demonstrated effective outcomes for the recommended strategy of avoiding the unprotected API concern.

Several academics focused on developing algorithms for safely storing massive amounts of information inside a multi-cloud data center. The section outlines a system for preventing cyberattacks, and manipulation assaults, including distributed denial of service. There are several ways such as information transfer, segmentation, categorization, encrypting, and decoding. The retrieving and merge procedure. A dual cryptosystem, a mix of the Feistal method and the AES algorithm, is constructed during encrypting, and the identical methodology is employed for decoding, although in inverse, to keep large amounts of information inside the clouds. Utilizing numerical simulations in an actual cloud infrastructure, the findings demonstrated good security and reliability.

In addition, research suggested a security-imposed prototype for healthcare that employs a Privacy Rating (PR) focused methodology to continue providing personal information with a data protection authentication mechanism in order to ensure data security, increased anonymity, and information protection, as well as accessibility in cloud storage via permissions management methods. In this methodology, the PR for both data and the end user is assessed in order to allow accessibility to every customer's information. To avoid an integrated framework during the permission-issuing procedure, this research used stochastic computer analysis. The findings revealed that such security assessment criteria are the regulatory authority for every other accessibility measure and are particularly suitable to information security.

The privacy implications in information sharing are handled as well as analyzed by applying evaluation methodologies as well as security procedures, both of which are resolved. Various approaches have been used to overcome confidence issues in cloud applications. An intra-cloud and inter-cloud standard of internet compatibility was already identified in order to highlight potential defiance that exists via cloud contact. A difficulty exists when cloud-based services are dispersed across the environment using various systems. The study focuses/attends on a survey conducted concerning cloud connectivity, confidentiality, and cybersecurity, trustworthiness is dependent on norms, and recommendations were examined. The basic objective of this research is to develop compatibility between various cloud providers for successful communication through maximizing cloud-based applications' QoS. This study presents the most recent replication by supplementing the TAM (Technology Acceptance Model) including three external frameworks: reliability, professional advancement, and computer self-efficacy. Among the most significant contributions of this research is indeed the incorporation of the most recent design, JO (Job Opportunity), for the first time in an equipment selection investigation. Information representing 101 IT professionals has been reviewed and analyzed using multiple linear regression (MLR) and neural network (NN) modeling. NN approaches have been shown to surpass the MLR approach based mostly on True positive rates from outcomes of such algorithms.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

Big information centers produce carbon dioxide that contributes to climate change. Therefore, in a bid to address the two challenges, researchers presented a structure that addresses combined safety and energy efficiency. The dual IDPS identifies, records, prevents, as well as alerts the part of the implementation depending on fingerprint and fault detection. The categorization of VMs upon that principle of security procedures allows for easier administration as well as allows IDPS to interact with them more effectively. The study contains a detailed assessment of current cybersecurity systems. Focusing on the constraints of the current structure, a conceptual platform for granting safety in network systems that rely on Intrusion Detection and Prevention System (IDPS) was already presented, as well as its issues that occurred were also established.

The analysis provided a review of cybersecurity problems in terms of privacy issues as well as associated mitigation. The contributions aim to analyze as well as categorize the significant security challenges and potential remedies which are accessible inside this research. They carry out a parameterized comparison of the risks encountered via the software platform. Furthermore, they align multiple preventative and vulnerability scanning systems used to handle security vulnerabilities. The reliable cloud technology approaches for managing information security among cloud services are investigated. Because the encryption process is evolving, they also include the upcoming advent of security management difficulties and possible responses.

Cloud technology has the potential to save businesses money, however, it also poses massive security risks. Companies considering cloud services technology as an opportunity to save costs and increase revenues must thoroughly investigate the potential risks of cloud applications. The capability to control risk greater efficiently out of a centralized location is a benefit of cloud applications in data risk mitigation. Though cloud technology is viewed as a recent miracle that is likely to revolutionize the way humans use the World wide web, there are numerous factors to consider.

Numerous emerging innovations were rapidly developing, all with technological advancements as well as the chance to make people's lives better. The article thoroughly explores as well as tackles cloud technology security problems. The research also examines cloud services flaws, privacy concerns that cloud technology confronts, as well as the secure goal that has to be met. On the one hand, cloud computing's authentication mechanisms require a heightened level of security; on either hand, cloud technology is inherently susceptible to security threats. As a result, they must be highly safe and resilient to fulfill the demanding expectations of the clients.

IV. CLOUD DELIVERY MODELS

CSPs provide solutions under three basic delivery methods, dependent mostly on the abstract level supplied as well as the company's service offering: Infrastructure as a Service, Platform as a Service, and Software as a Service. Figure 4 depicts the tiered organization of both the internet cloud through infrastructure facilities to programs, as well as principles and instances of global market implementations. The framework demonstrates an extent of abstraction and it could be considered like a protocol stack in which higher-level activities can indeed be created using lower-level operations. Such delivery strategies are described as follows.

(A) Infrastructure as a Service (IaaS)

Inside this IaaS delivery model, the CSP supplies improved IT architecture (space, computing power, storage, etc.) to execute programs and operating systems (OS), often using virtual machines such as VMware. IaaS cannot be confused as renting a host for a certain time frame for particular as well as permanent capabilities. There are various benefits of using IaaS versus conventional servers: It grows and modifies infrastructures with memories, data, processors, as well as other computational resources to meet capabilities needs nearly in real-time. At any moment, customers acquire and subscribe to the quantity of necessary infrastructure.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

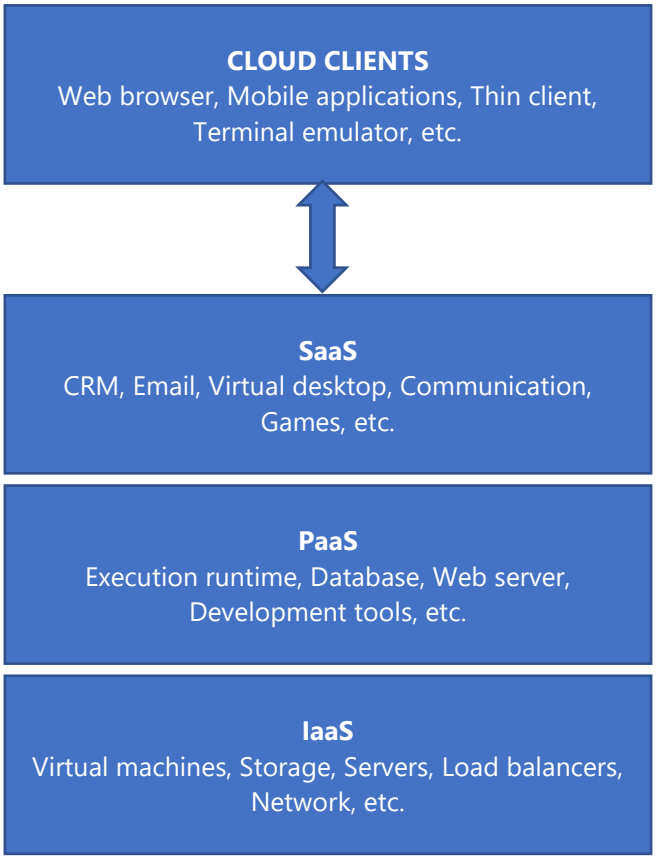

Figure 4. Cloud stack's layered structure

(B) Platform as a Service (PaaS)

In the PaaS (Figure 5) delivery method, distributed systems give programmers web development studio solutions, out of which products and services may be produced, maintained, and ultimately supplied to clients via the insurer's platforms.

PaaS often builds internet programs using specific APIs (Application Programming Interfaces), developer implementations, and protocols. Such solutions were created to provide applications as well as user interaction analytics, interaction with other internet services and applications, adaptability, dependability, privacy, pricing methods, and multi-tenancy while requiring no extensive programming. PaaS providers include Microsoft Azure, Google App Engine, and Force.com.

- The PaaS deployment paradigm provides various benefits: Given its inexpensive price, it enables a quick spread of computer programs.
- It permits individual programmers as well as small businesses can build internet programs without any of the expense and difficulty of purchasing or configuring infrastructure.
- Solutions that enable software developers can regulate, restrict usage, ban duplicating or redistribution, as well as enable configuration management of a product.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

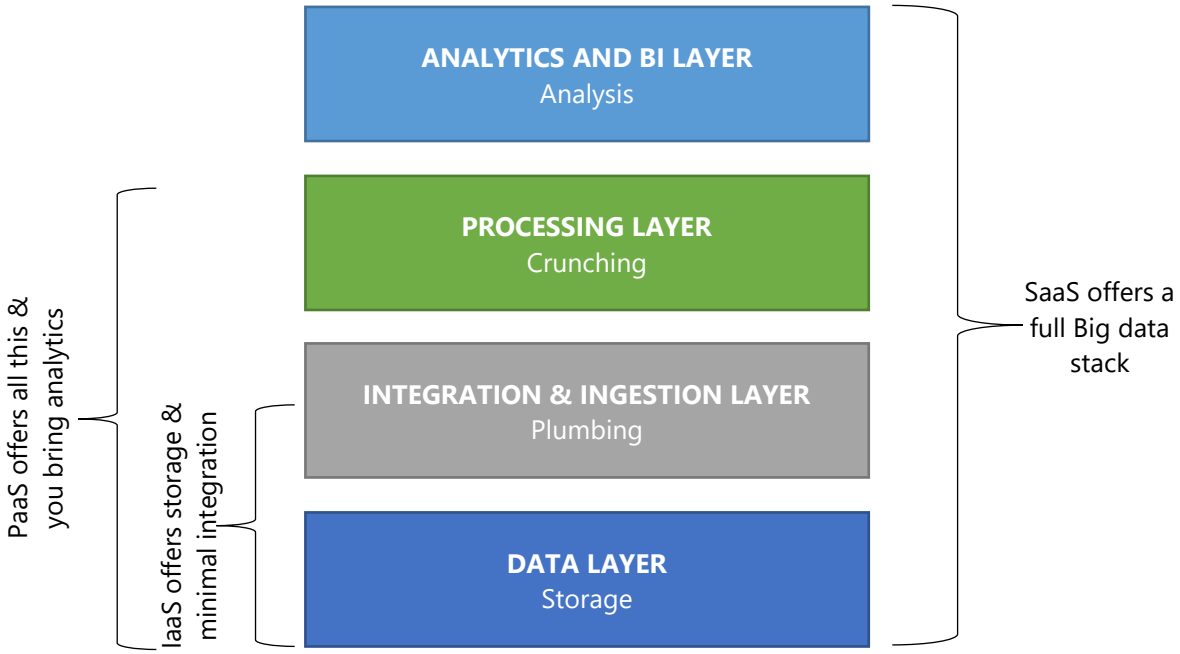

Figure 5. Operations of IaaS, PaaS, and SaaS

(C) SaaS (Software as a Service)

Clients have typically purchased digital products or installed these on their personal devices. Inside the SaaS distribution system, customers lease applications by subscriptions or charge-basis (often complimentary for a brief duration or below certain terms like enabling advertising) as well as receive the program over the Network (for instance, using a search engine) through some kind of authorization method. Cloud Vendors, in particular, deliver solutions from certain business operations and procedures in the manner of applications or solutions using existing infrastructure or platforms. The SaaS delivery paradigm offers various benefits:

1. Enables enterprises to outsource software deployment or administration toward a CSP, lowering license, staff, as well as infrastructural expenses.
2. Enables technology companies can regulate, restrict usage, ban duplicating as well as redistribution, or enable configuration management of the product.
3. The provider assists with SaaS application development. They could indeed, nevertheless, be altered.
4. Despite single-tenant design apps, SaaS hardware back-end capacity is distributed across several clients (although conceptually distinct to each), optimizing data exchange.

The following are the most frequent forms of Cloud offered mostly by companies; however, there are additional types of cloud that branch from the preceding three, that we will not discuss in depth throughout this study. Figure 6 depicts the extent of control over various aspects of the architecture to highlight the variations between the three service approaches. Whenever the architecture is located directly inside the company, the organization maintains entire authority over it all.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

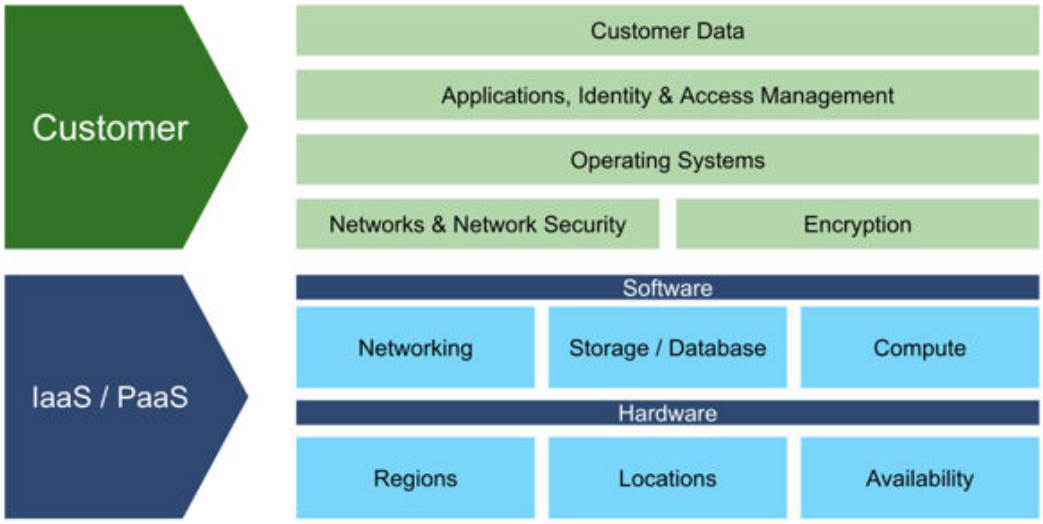

Figure 6. Areas of control between the users and service providers

While using leased infrastructures, the controller uses an underlying OS, that might run Virtual Machines and programs, however, the cloud service owns the actual servers. Users may handle the software that runs within a Virtual Environment and not the Virtual Machine management or even the real system while using IaaS. Users administer software and services through the service company's infrastructure while using PaaS. Furthermore, SaaS consumers have little influence over the programs that are utilized.

V. VULNERABILITIES AND COUNTERMEASURES

1. Defending Against DDoS Attacks

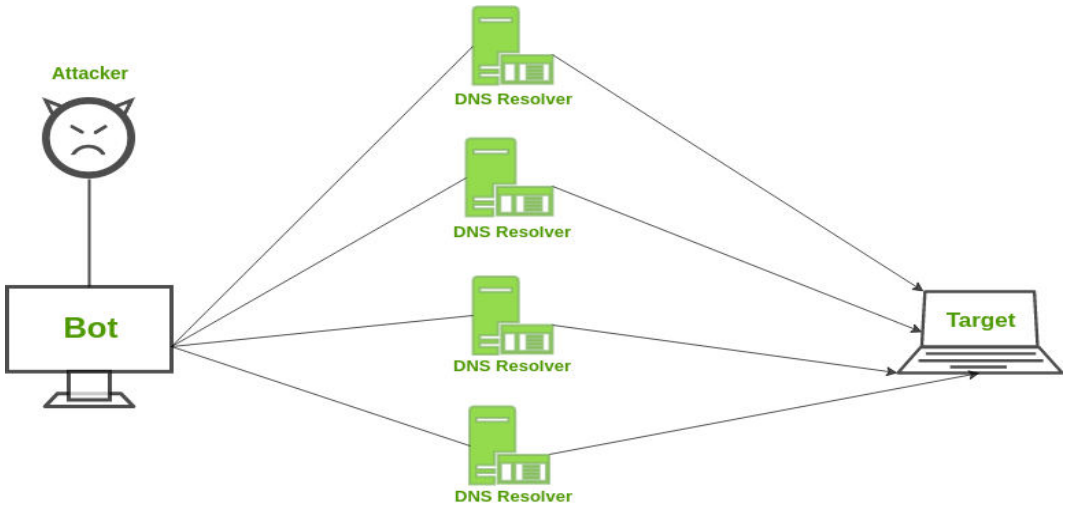

Figure 7. DDoS Attack Illustration

One of the most widely used methods for protecting from denial of service attacks is an intrusion detection system (IDS). Every computer is integrated with its own IDS throughout this strategy. These various intrusion detection technologies use the principle of exchanging data among computers.

Whenever a single cloud infrastructure is attacked, this collaborative IDS alerts the entire infrastructure, allowing everything to rapidly defend premium features. Figure 7 illustrates a denial of service attack.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

2. Defending Against SQL Injection Attacks

Customers may employ various filtration algorithms to clean customer data and safeguard themselves against attacks involving SQL injection. A middleware design that automatically detects or isolates user credentials with suspicious SQL control sequences is used to fight SQL injection threats. Attacks using SQL injection are shown in Figure 8.

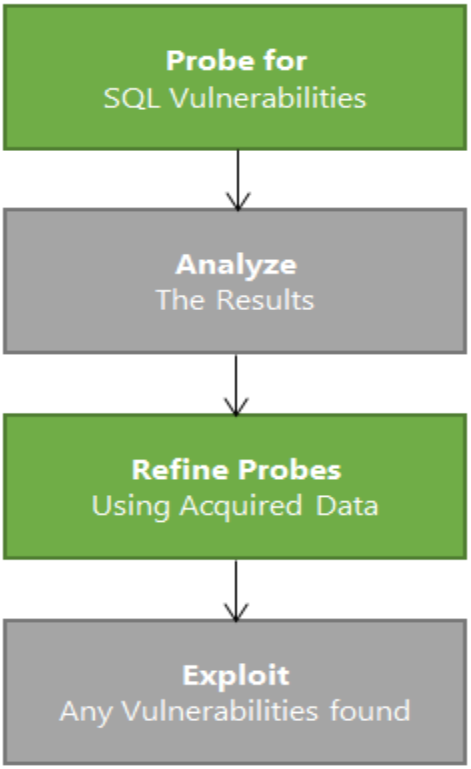

Figure 8. SQL Injection Attack Illustration

3. XSS (Cross-Site Scripting) threats

To avoid XSS assaults, many approaches such as proactive access restrictions, employing a range of information leakage protection technologies, and web application vulnerability identification techniques are used. As seen in Figure 9, such solutions use a variety of approaches to discover or repair security vulnerabilities.

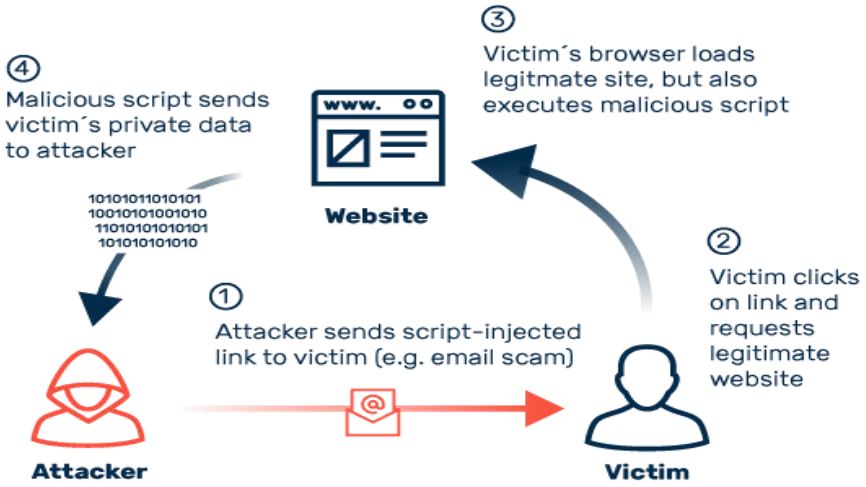

Figure 9. Cross-Site Scripting (XSS) attacks

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

4. Defending Against Sniffer Attacks

Accessibility to network content is restricted because then attackers cannot insert a single packet, cryptography methods are used to safeguard sensitive details, the gateway's MAC address is completely added to the ARP cache, IPV6 is utilized in place of IPV4 and SSH is utilized in place of Telnet, Secure copy (SCP) is utilized in place of FTP, and SSL is employed to email interconnection. As shown in Figure 10, a sniffer detection structure based on ARP and RTT may be used to identify a sniffer framework operating across a network.

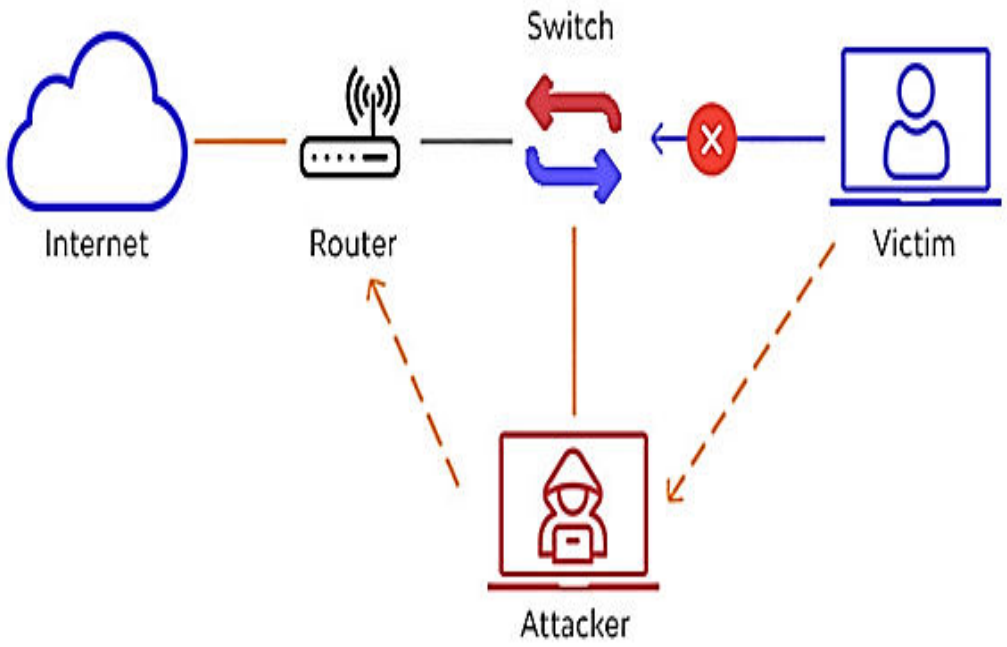

Figure 10. Sniffing and man-in-the-middle attacks

5. Dealing with Unsecure Application Programming Interfaces

To guard against such an issue, examine the overall security mechanism of cloud infrastructure connections. An additional strategy is to make sure that robust identification and accessibility restrictions are established using robust encryption software, while somehow understanding the requirements connected also with APIs.

6. Dealing with Data Loss/Leakage

To combat the problem, strict API password protection must be implemented. Some other useful techniques would be to secure and preserve the integrity of information in transmission, as well as to analyze information security between the architecture and implementation levels. Additional important actions to be taken include implementing robust cryptographic techniques, data management, and destroying policies, as well as explicitly requiring companies to delete permanent data before releasing it to the pools. The management might even explicitly stipulate backups as well as recovery options for providers.

7. Addressing Common Technology Vulnerabilities

To protect against such a vulnerability, use safeguards for implementation. Monitoring the infrastructure against unauthorized modifications seems to be another helpful approach, while already establishing robust identification and network management for administrator privileges as well as other processes. Enforcing service-level agreements regarding patches as well as risk management is another essential factor to consider. Perform security testing and installation checks on some kind of regular basis.

8. Data Transmission Security

While moving information from customers toward the cloud, an encoded private communication route such as SSL/TLS is required. This avoids other threats, such as MITM assaults, in which information may be taken through an adversary eavesdropping on the conversation.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

9. Google Hacking Defense

To prevent such vulnerabilities, software privacy must be reviewed in each of the major cloud service provider concepts: IaaS, PaaS, and SaaS. Mostly in the case of an IaaS deployment model, cloud vendors are often unconcerned only with the company's as well as the user's administration security requirements. Whenever developing the applications, consider the above aspects in mind.

10. Defending Against Domain Name System (DNS) Attacks

Using DNS attempts to build security, such as DNSSEC, minimizes the effect of DNS assaults; nonetheless, there seem to be times whenever these preventive controls are insufficient, including when the connection among a broadcaster and a recipient is diverted via harmful materials.

VI. CONCLUSION

This paper suggests that, since the major offender is the client, cloud platform clients must be educated and updated on various assaults. Also, an intruder may employ a variety of online destructive attack channels to mislead a target towards accessing infected websites, following which the attacker gets to the user's browser. Moreover, someone might also watch online behavior as well as access the same information that the individual is accessing, as well as acquire the identity of the user to connect to the cloud storage service. Hence, security awareness is a frequently overlooked privacy issue. This study discusses the critical examination of data confidentiality approaches in cloud computing for achieving increased security for cloud-based systems.

REFERENCES

[1] Abraham Ekow Dadzie, Literature Review On Data Security In Cloud Computing, 2019, DOI: 10.13140/RG.2.2.14044.23684.
[2] Du M, Wang Q, He M, Weng J (2018) Privacy-preserving indexing and query processing for secure dynamic cloud storage. IEEE Trans Inf Forensics Secur 13(9):2320–2332.
[3] Gagangeet Singh Aujla; Rajat Chaudhary; Neeraj Kumar; Ashok Kumar Das; Joel J. P. C. Rodrigues (2018) SecSVA: Secure Storage, Verification, and Auditing of Big Data in the Cloud Environment Page(s): 78 – 85 https://ieeexplore.ieee.org/document/82557.
[4] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, A Comprehensive Survey on Security in Cloud Computing, Elsevier, Volume 110, 2017, Pages 465-472.
[5] Jouini M, Rabai LBA (2019) A security framework for secure cloud computing environments. In: Cloud security: concepts, methodologies, tools, and applications. IGI Global, pp. 249–263.
[6] Komal Singh Gill; Sharad Saxena; Anju Sharma, Taxonomy of Security Attacks on Cloud Environment: A Case Study on Telemedicine, IEEE,2019 DOI: 10.1109/AICAI45948.2019.
[7] Latha, K., Sheela, T. Block based data security and data distribution on multi cloud environment. J Ambient Intell Human Comput (2019). https://doi.org/10.1007/s12652-019-01395-y.
[8] Li Yibin. Ke Kegai, Intelligent cryptography approach for secure distributed big data storage in cloud computing Volume 387, May 2017, Pages 103-115 https://doi.org/10.1016/j.ins.2016.09.005.
[9] Murtadha Arif Bin Sahbudin, Riccardo Di Pietro, Marco Scarpa, A Web Client Secure Storage Approach in Multi-Cloud Environment, IEEE, 2019, DOI: 10.1109/CCCS.2019.8888062.
[10] Nareshvurukonda B. Thirumala Rao, A Study on Data Storage Security Issues in Cloud Computing, Elsevier, Volume 92, 2016, Pages 128-135, https://doi.org/10.1016/j.procs.2016.07.335.
[11] Nishit Mishra, Tarun Kumar Sharma, Varun Sharma, Vrince Vimal, Secure Framework for Data Security in Cloud Computing, Springer, 2017, pp 61-71.
[12] Prince, P.B., Lovesum, S.P.J. Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System. SN COMPUT. SCI. 1, 239 (2020). https://doi.org/10.1007/s42979-020-00246-4.
[13] S. Senthilkumar, R. Nithya, P. Vaishali, R. Valli, G. Vanitha, & L. Ramachanndran, "Autonomous navigation robot", International Research Journal of Engineering and Technology, vol. 4, no. 2, 2017.
[14] S. Xu, G. Yang, Y. Mu, A new revocable and re-delegable proxy signature and its application.
[15] Shalu Malla Sushil Kumar Saroj, A New Security Framework for Cloud Data, Elsevier, Volume 143, 2018, Pages 765-775, https://doi.org/10.1016/j.procs.2018.10.397.
[16] Shen, J., Deng, X. & Xu, Z. Multi-security-level cloud storage system based on improved proxy re-encryption. J Wireless Com Network 2019, 277 (2019). https://doi.org/10.1186/s13638-019-1614-y.
[17] Sonali Chandel, Geng Yang, d Sumit Chakravarty RSA-CP-IDABE: A Secure Framework for Multi-User and Multi-Owner Cloud Environment, Information 2020, 11(8), 382.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 10, October 2023 |

| DOI:10.15680/IJMRSET.2023.0610016 |

[18] Sushil Kumar Saroj, Sanjeev Kumar Chauhan, Aravendra Kumar Sharma and Sundaram Vats. (2015) "Threshold Cryptography Based Data Security in Cloud Computing." IEEE International Conference on Computational Intelligence & Communication Technology: 202-207.
[19] A. Renuka Devi, S. Senthilkumar, L. Ramachandran, "Circularly Polarized Dualband Switched-Beam Antenna Array for GNSS" International Journal of Advanced Engineering Research and Science, vol. 2, no. 1, pp. 6-9; 2015.
[20] S. Senthilkumar, L. Ramachandran, R. S. Aarthi, "Pick and place of Robotic Vehicle by using an Arm based Solar tracking system", International Journal of Advanced Engineering Research and Science, vol. 1, no. 7, pp. 39-43, 2014.
[21] Yasmina Bensitel; Rahal Romadi, Secured Data Storage In Cloud Using Homomorphic Encryption, IEEE, 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), DOI: 10.1109/CloudTech.2016.7847680.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com